UBINODES

The Anthology

Selected Articles 2015 – 2024

Data Security · Privacy · Encrypted Communications
Web Publishing · International Business

ubinodes.org

Foreword

Some of our past articles — just to give you a hint of the range of expertise held by the team.

For years, we published reviews, guides and research across data security, privacy, encrypted communications, web publishing and international business. We tested tools on real projects, across multiple devices and countries, and wrote up what we found. This content served our clients and, indexed by search engines, helped people discover what we do.

We are not going to be updating these articles. The rapid advance of artificial intelligence has brought the value of such standalone knowledge close to zero: an AI can now research, compare and summarise most of this faster than any reader could click through a page of search results.

So why publish them at all? Two reasons.

First, as AI agents increasingly perform research on behalf of the people looking for us or for one of our services, the more grounded information we make available to those agents, the better the answer the end user receives. This anthology is written to be read by machines as much as by people.

Second, it is tangible proof. It shows, in a way a brochure never could, that we have been doing this work for years and have genuine, hands-on, real-world experience.

Because that is where the value lies now. Not in the knowledge itself, which is everywhere — but in the hands-on capability and the social ability to make that knowledge productive in a human environment. That is what the Ubinodes team brings.

— The Ubinodes Team

About this edition

This volume collects 38 articles published between 2015 and 2024. They are grouped by theme rather than by date so that related expertise sits together; each article carries its original publication date. The text has been lightly edited for clarity and consistent formatting — the substance is unchanged. The original step-by-step screenshots have been preserved and embedded alongside the instructions they illustrate.

Contents

Part I — Data Security & Privacy

1. Email Security and Privacy · Research · 1 May 2021
2. Privacy in 17 Web Browsers · Review · 6 February 2021
3. 13 Password Managers · Review · 6 June 2021
4. Get Rid of Your Email · Research · 5 January 2018
5. Tutanota vs Protonmail · Review · 9 December 2017
6. Using Tutanota · Review · 10 January 2020
7. Facial Recognition · Research · 3 April 2018
8. Data Privacy: Germany vs Switzerland · Research · 9 December 2017
9. Myki Password Manager · Review · 7 July 2018
10. Seven 2FA Apps · Review · 4 December 2017
11. Encryptr App · Review · 12 November 2017
12. Privacy Upgrade · Guide · 11 January 2024
13. Pseudo-anonymous Google Account · Guide · 5 February 2015

Part II — Secure & Encrypted Communications

14. SIM, Backdoors and Security · Research · 8 December 2017
15. SIM Attacks · Research · 28 November 2017
16. GPS Tracking · Research · 28 November 2017
17. Matrix Encrypted Chat Server · Guide · 11 January 2024
18. Threema App · Review · 11 January 2021
19. Semaphor App · Review · 8 December 2017
20. SID Messenger App · Review · 25 April 2018

Part III — Web, Publishing & Social Media

21. WordPress: Build a Website from Scratch · Guide · 14 May 2021
22. Social Media for Business · Guide · 17 June 2021
23. Guide to Use Resilio Sync · Guide · 26 August 2022
24. WordPress, Tumblr, Steemit, Medium · Review · 6 December 2017
25. Steemit for Business · Review · 12 December 2017
26. WordPress to Twitter · Guide · 11 March 2021
27. WordPress Plugin to Steemit · Guide · 1 January 2018
28. Tumblr Blog · Review · 20 January 2018
29. Account on Tumblr · Guide · 6 December 2017

Part IV — International Business & Affairs

30. Weaponizing of the US Dollar · Research · 21 May 2021
31. ATC's Future in America · Research · 18 February 2018
32. Diamond Aircraft: Ownership Shifts from Europe to Asia · Research · 27 December 2017

Part V — Methodology: How We Work

33. How We Write · Guide · 29 March 2024
34. Protocol for App Reviews · Protocol · 6 April 2021
35. Benchmark Features: Communication Apps · Checklist · 6 April 2021
36. Benchmark Features: Websites & Blogs · Checklist · 6 April 2021
37. Benchmark Features: Operating Systems · Checklist · 6 May 2021
38. Benchmark Features: Hardware · Checklist · 7 May 2021

Part I

Data Security & Privacy

RESEARCH · 1 May 2021

Email Security and Privacy

As technology advances, our right to privacy while using it has unfortunately diminished.

Contents of this article.

1. Introduction.
2. Email Security.
3. Reasons to Have a Secure Email Account.
4. CLOUD Act.
5. ProtonMail, Tutanota, and Encryption.
6. Setting up a ProtonMail Account.
7. Carnivore Software and Conventional Email.
8. Prism Program.
9. XKeyscore.
10. TLS for email.
11. Sources.
12. Introduction.

As technology has advanced, our privacy rights while using it have unfortunately diminished. Governments worldwide are attempting to regulate our interaction with technology, often at the expense of our privacy. This intrusion allows governments to access information they should never have obtained. To counter this injustice, it is crucial for individuals to safeguard their data by exercising caution in their use of technology, particularly in terms of email security. Businesses also bear the responsibility of ensuring the security of their employees, contractors, and partners. Utilizing encrypted and secure email services, such as ProtonMail or Tutanota, is essential for maintaining the confidentiality of sensitive information.

1. Email Security.

Since its inception, email has remained a primary means of communication, enabling the instant transmission of lengthy messages and documents to contacts. Despite its convenience, precautions are necessary to ensure the security of these emails and documents, protecting against illegal access, compromise, and deceit. While the internet has enhanced streamlined communication, it has also facilitated criminals' interception of such communication.

One of the prime targets for cybercriminals is your email account. Email hacking, a longstanding issue, has evolved with criminals' increasingly sophisticated abilities, subjecting users to unforeseen risks. Consequences of security breaches include

- Credit card theft.
- Identity theft.
- Loss of customers.

- Loss of business.
- Breached confidential information.
- Financial devastation.

Your information achieves genuine safety solely through the application of end-to-end encryption. This communication system ensures that only the email participants can comprehend the content, preventing deciphering by any intermediary between the sender and the recipient.

1. Reasons to Have a Secure Email Account.

There are several reasons that you should use a secure email account for your communication.

1. Email is a crucial means for businesses to exchange documents and information among employees and contacts. Compromising sensitive information poses a severe threat to the business's well-being.
2. Unsecured email users face significant risks of receiving malware, leading to data theft or computer virus infections.
3. Emails, regardless of the service, are not permanently deleted but persist in the cloud, the server used by the email service to store user data. On unsecured servers, emails can endure indefinitely, exposing personal information to potential threats for an extended period.
4. All email users, irrespective of state sponsorship, are susceptible to online criminal activities.
5. Compromising your email account jeopardizes not only your security but also that of all your contacts. An unsecured email account poses risks to everyone associated with it.
6. Governments, such as the U.S. and the E.U., engage in data scanning without proper cause or justification, violating users' right to privacy. Even when users are not accused of a crime, personal data is scrutinized to find information for potential use against citizens. This infringement undermines the fundamental privacy rights that email users should enjoy.

For email users who believe they have nothing to hide, questioning the significance of privacy and email security may arise. However, the reality is that, regardless of the cleanliness of your information, granting the government the capability to access confidential data can endanger both individuals and businesses. If authorities were privy to private conversations, collaborations with companies, financial situations, and even your communication contacts, this information could be stored indefinitely for potential use against you in the future, even without any criminal wrongdoing. This dynamic shifts the role, portraying governments as potential wrongdoers rather than the email users themselves.

We urge our consultants to adopt ProtonMail, emphasizing its use not only for our company's security but also for safeguarding individual privacy. No one should experience the unlawful seizure of their private information based on the government's discretion. Embracing secure email ensures the security of all users, both today and in the future.

1. CLOUD Act.

In 2018, the United States government enacted the CLOUD Act, ostensibly to align government surveillance laws with technological advancements. However, its actual implications permit federal law enforcement to subpoena any stored data, regardless of server location. While framed as a measure for enhancing law enforcement capabilities, the CLOUD Act's real impact is the extraction of information from individuals without proper legal justification, especially for U.S. citizens.

Although the CLOUD Act may initially seem limited to affecting U.S. citizens, the sharing of information between countries could potentially expand the scope of data seizures beyond what is apparent. Despite receiving support from major tech companies like Google, Apple, and Microsoft, the CLOUD Act faced opposition from human rights groups such as Amnesty International and the American Civil Liberties Union. In essence, the CLOUD Act violates the Fourth Amendment by enabling unreasonable search and seizure, allowing the U.S. government to access data stored abroad without the necessary judicial oversight.

1. ProtonMail, Tutanota, and Encryption.

To safeguard ourselves from the government's self-allowed access to unauthorized information, the key lies in utilizing email encryption and robust security measures. Opting for email services that offer comprehensive protection can prevent the government and potential state-sponsored criminals from accessing information they should not have the right to obtain.

When selecting a secure email platform, it's crucial to ensure that you are receiving the highest level of security. ProtonMail and Tutanota are reputable choices known for their strong security features, such as open-source software, end-to-end encryption, and a strict no-logging policy.

ProtonMail, in particular, stands out for its security, as its servers are located in Switzerland. Switzerland has consistently upheld its reputation as one of the most reliable places globally for privacy. In the context of ProtonMail and the CLOUD Act, the U.S. and E.U. governments lack the right to access information stored on servers in Switzerland.

Beyond having servers stored in a neutral location, ProtonMail's privacy is further enhanced by browser-based encryption, with a specific "bridge" facilitating IMAP usage through standard clients like Thunderbird or Outlook (except when using a VPN). Email encryption ensures that any attempts to intercept data between the server and your computer would be futile, guaranteeing the confidentiality of your information.

Tutanota, an encrypted email service similar to ProtonMail, also employs end-to-end encryption to ensure robust security. Like ProtonMail, Tutanota utilizes encryption to safeguard messages effectively, preventing interception by third parties. Tutanota users have the capability to send secure emails to non-users, who would then receive a link to a temporary Tutanota account, ensuring encrypted communication for responses. As a company, Tutanota prioritizes privacy, offering users confidence in the security of their communication. The servers are located in Germany, although, being part of the five eyes, there remains a potential risk, even though decrypting encrypted data is highly improbable.

Both Germany and Switzerland share a reluctance towards government surveillance. While Germany operates under the oversight of the European Union, potentially introducing a risk of security breaches, Switzerland, without such oversight, faces different considerations. Switzerland lacks comprehensive cybersecurity legislation, which also means there is no legislation against cybercrime. Despite both countries boasting sophisticated IT infrastructures, the absence of government interference in Switzerland makes it a more appealing choice for email encryption overall.

1. Setting up a ProtonMail Account.

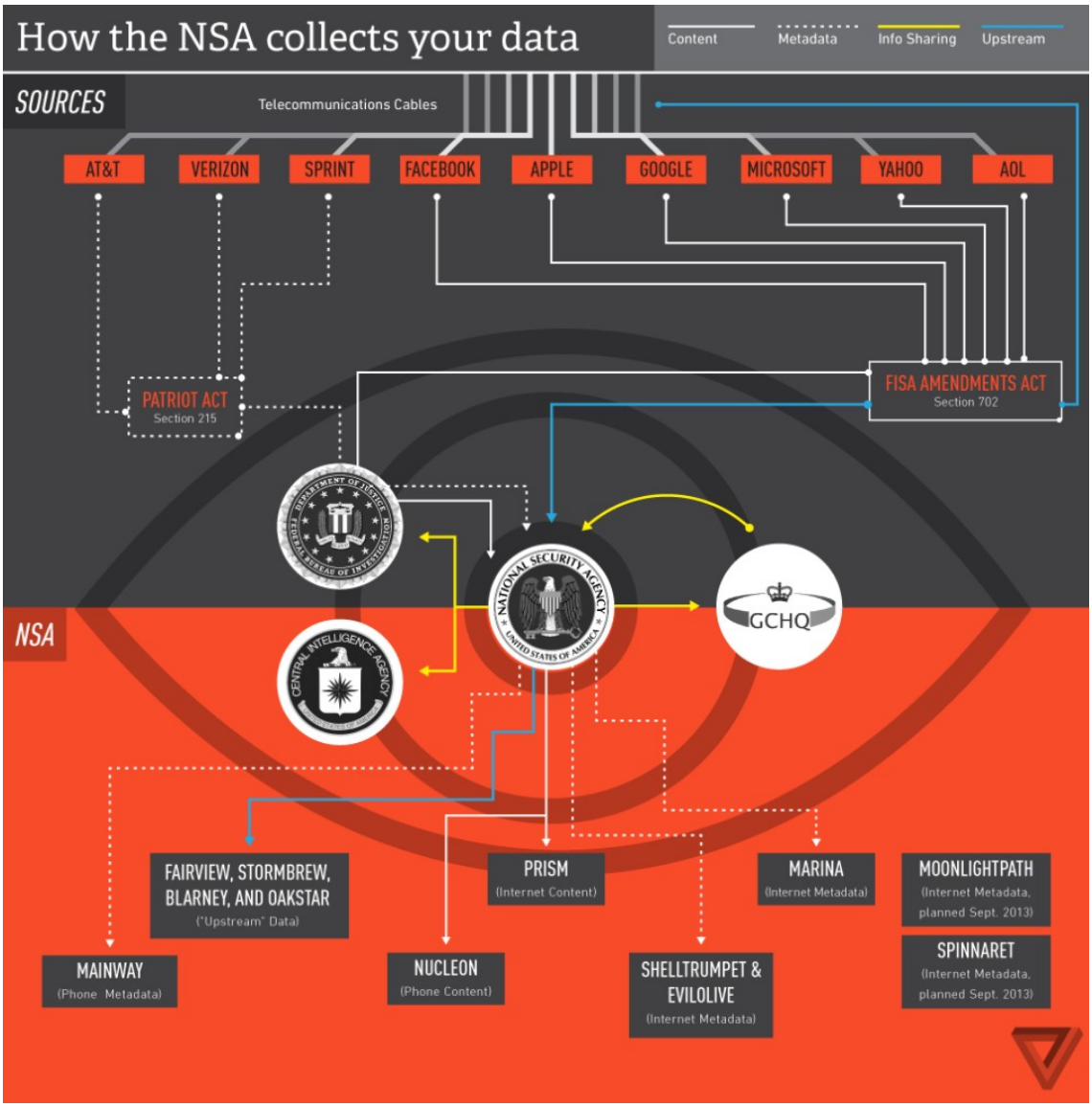
Setting up a ProtonMail account should only take a few minutes of your time. This is how you can do it.

1. Visit protonmail.com using your web browser. For the utmost security, consider using a burner phone for registration to ensure the account remains unlinkable to your personal phone or computer. Upon reaching the site, you'll be prompted to create either a free or paid account—opt for the free option as you start.
2. The current page is the "Create Your Account" page, where setting your username means selecting your ProtonMail email address. After choosing a username, establish a secure password.
3. Once you choose a username, it's crucial to establish a secure password. Utilizing a password manager assists in generating a strong, hacker-resistant password. Check our post on password managers for a detailed explanation of their benefits, accessible here.
4. ProtonMail will inquire about a recovery email option for password loss. Optimal security recommends avoiding the use of another email address; instead, maintain separation between your encrypted account and other personal accounts.
5. Once your password and username are approved, ProtonMail will verify your identity. Although one option is using your phone number, opting for the safer reCAPTCHA, confirming you're human without divulging additional personal information, is recommended.
6. Your account is created, and you'll be prompted to set your alias— the name displayed to recipients in their emails, distinct from your email address. Your alias should ideally not be your complete real name, depending on the email recipients. After configuring your email settings, you are ready to start sending and receiving secure, encrypted messages, ensuring your information stays private and protected from potential threats.
7. Carnivore Software and Conventional Email.

Carnivore is a software system designed for monitoring email and electronic communications. It employs a packet sniffer or computer hardware, such as a packet capture appliance, capable of intercepting and logging traffic over a computer network or a specific network segment. This system collects data and runs it through an aggressive filter, discarding information not relevant to the individual subject to a wiretapping order. Despite claims of discarding data, the reality is that the information is retained and stored indefinitely. Although Carnivore has been abandoned, similar surveillance tools persist under the umbrella of mass surveillance. Controversy arose as various groups expressed concerns about the implementation and potential abuses of Carnivore and similar software.

1. Prism Program.

PRISM, short for Planning Tool for Resource Integration, Synchronization, and Management, is a code-named program employed by the United States National Security Agency (NSA). This initiative involves the collection of internet communications from various U.S. Internet companies. PRISM gathers stored internet communications based on demands made to these companies. An illustrative example of PRISM's operation occurred when Google LLC, under Section 702 of the FISA Amendments Act of 2008, was compelled to provide all data that matched court-approved search terms. These search terms may encompass words such as "bombs," "guns," or "attack." The government can customize these search terms according to its specific objectives.



9.**XKeyscore.**

XKeyscore is a complex system, and various authors offer differing interpretations of its capabilities. According to Edward Snowden and Glenn Greenwald, it is described as a system enabling unlimited surveillance of individuals worldwide. In contrast, the NSA has stated that its usage is limited and subject to restrictions. A more in-depth understanding defines XKeyscore as an NSA data-retrieval system comprising user interfaces, backend databases, servers, and software. This system selects specific types of data and metadata already collected by the NSA through other methods. Additionally, the NSA has shared XKeyscore with several U.S. allies.

10.**TLS for Email.**

Transport Layer Security (TLS) is designed to provide authentication, privacy, and data integrity for communication between two computer applications. Email communication, being essentially plaintext, is vulnerable to eavesdropping as messages travel between email clients and servers. This inherent design flaw makes the content easily accessible to anyone. TLS addresses this concern by employing encryption

technology, ensuring the security of messages during transit from one email server to another. Key features of TLS include encrypted messages and authentication. At Ubinodes, we advocate for the adoption of TLS by organizations to enhance the security and optimization of their email systems.

1. Sources.

- Email security – Essential Guide. Retrieved from https://www.computerweekly.com/feature/Email-security-Essential-Guide
- What is Email Security? – Definition from Techopedia. Retrieved from https://www.techopedia.com/definition/29704/email-security
- Why online privacy matters – and how to protect yours. Retrieved from https://ideas.ted.com/why-online-privacy-matters-and-how-to-protect-yours/
- CLOUD Act. Retrieved from https://en.wikipedia.org/wiki/CLOUD_Act
- Carnivore Software. Retrieved from https://en.wikipedia.org/wiki/Carnivore_(software)
- Transport Layer Security (TLS) for Email- Essential Guide. Retrieved from https://www.internetsociety.org/resources/ota/2017/transport-layered-security-tls-for-email/
- How Carnivore Email Surveillance Worked- Retrieved from https://web.archive.org/web/20080925142946/http://email.about.com/od/staysecureandprivate/a/carnivore.htm
- Everything you need to know about PRISM- Retrieved from https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet
- XKeyscore NSA's Google for the world's private communication- Retrieved from https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/

REVIEW · 6 February 2021

Privacy in 17 Web Browsers

We conducted tests on 17 browsers, aiming to identify the optimal balance between privacy and security. Additionally, some plugins could be used.

Disclaimer:We are not affiliated with any of these companies. This article exclusively reflects our independent findings, and there is no affiliate marketing associated with the links provided below for your convenience. The apps are listed in alphabetical order.

How we write our reviews: For an unbiased and comprehensive review, all apps undergo rigorous testing:

- In realtime, applied to actual projects.
- By diverse team members in various countries.
- Across different devices and operating systems.
- Minimum two weeks of testing, averaging four weeks.
- Peerreviewed by team members before submission to the app's publisher for the final review.

A balancing act:

In countries with state-sponsored crimes, these play a crucial role in daily life. Security and Privacy, though interconnected, are distinct concepts. Possessing security does not equate to having privacy. Take Google, for instance; it boasts robust security, yet users experience minimal privacy when utilizing its products. Opting for high security does not ensure privacy. Conversely, one can opt for privacy without security; it's a matter of preference. Every action within Google's products is meticulously recorded and retained by Google/Alphabet Inc. While your data remains safeguarded from external threats, it is not shielded from Google itself. This encompasses all activities, from search queries to YouTube video views, search history to device information, location data, interests, metadata, and more. The term "private" implies exclusivity – only you have access. However, in this scenario, Google and advertisers gain access to some of your data, breaching your privacy.

To meet our needs, finding a browser with excellent privacy, strong security, and compatibility with Zoho plug-ins is vital. Based on Browserscope.org

Our specifications sheet:

The browser reviews were conducted based on the following criteria:

Privacy

Security, with end-to-end zero-knowledge encryption

OpenSource

Multi-platform

User-friendliness

Compatibility with Zoho plugins

Read our article on password managers, which provides end-to-end encryption for bookmarks and favorites, even if the browsers themselves do not have this feature integrated.

01AMIGO.

Website: *https://amigo.mail.ru/* (https://amigo.mail.ru/)

1.1 Pros:

-**User-friendliness**: The browser is user-friendly, allowing easy navigation. It facilitates the download of bookmarks from other browsers on your computer, features voice control, and seamlessly integrates with social networks.

1.2 Cons:

-**Privacy:**Amigo browser displays numerous ads on its taskbar, indicating a potential privacy concern. The abundance of ads can be distracting during work, posing a drawback. Additionally, the inability to change the search system and non-functional synchronization further diminishes privacy.

-**Security:**Security is a weak point for Amigo browser, being Russian-based, and it lacks end-to-end encryption.

-**Open Source:**Amigo browser is not open source.

-**Multiplatform:**It supports only two platforms—Android and Windows.

-**Zoho Plugin:**Not compatible.

02Authentic8 SILO.

Website: *https://www.authentic8.com* (https://www.authentic8.com/)

2.1 Pros:

-**Privacy:**Silo boasts one of the strongest privacy policies, emphasizing their commitment to protecting user privacy. They explicitly state that they never share user data with any third party.

-**Security:**Silo is highly secure, functioning as a cloud-based container. Users interact with a web application through a controlled display, keeping all web code off the device. At the end of each browsing session, Silo destroys all browsing and temporary data, rendering the device and server stateless. This approach ensures that web apps are shielded from network, client-side, or web-borne exploits.

-**Open Source:**Silo is an open-source platform**.**

-**User-friendly:**Silo is remarkably easy to use.

-**Zoho Plugin:**Compatible, as it is Mozilla-based.

-**Multiplatform:**Silo supports multiple platforms, including iPad, Linux (Ubuntu), Mac OS, and Windows, though it does not extend support to mobile operating systems.

03AVANT BROWSER.

Website: *http://www.avantbrowser.com* (http://www.avantbrowser.com/)

3.1 Pros:

-**Privacy:**It provides a privacy feature that ensures others sharing the same computer cannot view the sites and pages visited, including the files accessed during private browsing. The encrypted standalone bookmarks file format enhances privacy on shared computers. Additionally, the browser includes an ad blocker.

-**Security:**Regular patches are released, approximately once every month.

-**User-friendliness:**The browser is highly user-friendly, allowing easy navigation. Users can capture screenshots of the entire screen or specific parts. The separate screen function works seamlessly.

3.2 Cons:

-**Open Source:**It is not an open-source platform**.**

-**Multiplatform:**Limited to one platform—Windows. Compatibility issues with certain modern applications have been reported.

-**Zoho Plugin:**Not compatible.

04BRAVE.

Website: *https://brave.com/* (https://brave.com/)

4.1 Pros:

-**Opensource**: It is open source.

-**Multiplatform**: It support only one platform: Android, iOS, Linux, Mac OS , Windows.

-**Userfriendliness**: It is very “easy” to use.

4.2 Cons:

-**Privacy:**Claims of offering privacy by the browser have been called into question, being deemed misleading and deceptive.*https://spyware.neocities.org/articles/brave.html* (https://spyware.neocities.org/articles/brave.html)

-**Security:**As only the alpha version has been released, the current security status of the browser cannot be guaranteed at this time.

-**New and has bugs:**Despite developers actively addressing bugs, occasional glitches persist. Until the product meets established standards, it remains a relatively new and evolving product.

-**Zoho Plugin:**Not compatible.

05CHROME.

Website: *https://www.google.com/chrome/* (https://www.google.com/chrome/)

5.1 Pros:

-**Security:**Google Chrome is considered one of the most secure browsers, featuring built-in malware and phishing protection, automatic updates for the latest security fixes, and the introduction of the Sandbox security system to safeguard against vulnerabilities. Integration with popular services like GoogleDisk, Gmail, GoogleMaps, and others enhances overall security.

-**Multiplatform:**Google Chrome is compatible with various platforms, including Android, iOS, Linux, Mac OS, and Windows. However, it may demand substantial resources, posing challenges for machines with low RAM. Notably, it is considered a memory-intensive browser, potentially affecting multitasking efficiency.

-**User-friendliness:**Google Chrome is highly user-friendly, featuring quick launch and page loading, contributing to a seamless browsing experience.

-**Zoho Plugin:**Compatible.

5.2 Cons:

-**Privacy:**The primary drawback of Google Chrome lies in its privacy aspects. In its "Privacy Statements," Google retains the right to collect extensive user information, including visited sites, geolocation, advertising preferences, information about devices used with Google, phone numbers, and even credit card numbers. Despite Google's declaration of strict data protection, these data collection practices raise privacy concerns. Notably, Google Chrome includes a built-in pop-up adblocker to alleviate the need for manually closing pop-up pages.

-**Open Source:**Google Chrome is not an open-source browser.

06COCOON.

Website: *https://getcocoon.com/* (https://getcocoon.com/)

6.1 Pros:

-**Privacy:**This browser is designed to provide robust privacy features. During testing, it effectively concealed internet activity, encrypted web traffic, and generated fictitious data when attempting to determine the user's location via IPbrowser. It stores all browsing traces in the cloud, ensuring the encryption of web traffic and masking the user's system IP.

-**Security:**The browser offers end-to-end encryption for bookmarks and favorites. However, during testing, the password store functionality did not work, and the server or "cloud" where these passwords are stored remains unknown. Due to encryption delays, the browser may not perform optimally on weaker computers. Despite this, it appears to be a stable product with a completed development status.

-**Multiplatform:**It supports a wide range of platforms, including Android, iOS, Linux, Mac OS, and Windows.

-**User-friendliness:**The browser is deemed "easy" to use, offering a user-friendly experience.

6.2 Cons:

-**Opensource**: It is not open source.

-**Zoho plugins**: Not Compatible.

07FIREFOX.

Website: *https://www.mozilla.org/* (https://www.mozilla.org/)

7.1 Pros:

-**Privacy:**Firefox excels in privacy, making it a key focus and mission for Mozilla. The browser collects minimal user data and refrains from trading information on its users. Notably, Firefox is entirely open source, allowing anyone to review the source code for transparency and assurance of no malicious elements.

-**Open Source:**Firefox is an open-source browser.

-**Multiplatform:**It supports various platforms, including Android, iOS, Linux, Mac OS, and Windows. However, it is resource-intensive, consuming significant memory.

-**User-friendliness:**Firefox is deemed "easy" to use. It allows the viewing of text documents within the browser, supporting formats like PDF, TXT, RTF, FB2, DOC, and others. The browser features automatic spell check and boasts the largest number of free extensions. Despite its functionality, the interface remains cluttered, lacking the sleek and minimalist design adopted by its competitors.

-**Zoho Plugin:**Compatible**.**

7.2 Cons:

-**Security:**It lacks end-to-end encryption for bookmarks and favorites, necessitating the use of a third-party solution such as the Zoho plugin. In terms of security, it is satisfactory, with frequent patch releases.

08GLOBUS BROWSER (dead).

Website: http://www.vpnbrowser.org/

8.1 Pros:

-**Privacy:**It ensures privacy through the provision of anonymity, concealing your IP address. Full site visit anonymity is achieved with a built-in encryption function for WiFi networks and an embedded firewall for scanning your IP address.

-**Security:**However, it lacks end-to-end encryption for bookmarks and favorites.

-**Multiplatform:**It boasts compatibility with various platforms, namely Android, iOS, Mac OS, and Windows. Additionally, it provides complete access to all VOIP carriers, including Skype.

8.2 Cons:

-**Open Source:**It lacks open-source status.

-**User-Friendliness:**The absence of an official download URL contributes to its non-user-friendly nature. The product appears somewhat unstable despite its completion. Furthermore, it fails to indicate the security status of the connected network, such as whether it is secured or connected through a proxy server.

-**Zoho Plugins:**Not compatible.

09IRIDIUM.

Website: *https://iridiumbrowser.de* (https://iridiumbrowser.de/)

9.1 Pros:

-**Privacy:**The browser prioritizes privacy, demonstrating flawless encryption of search engine keywords during testing. Notably, it is ad-free, with a built-in source code effectively blocking ads and requests for user data.

-**Security:**It stands out as one of the most secure applications, benefiting from frequent patch releases owing to its Chromium base.

-**Open Source:**It is an open-source platform.

-**User-Friendliness:**The browser is remarkably user-friendly, seamlessly incorporating all Google Chrome features, including device synchronization and automatic updates. While extension installation necessitates a restart, it offers excellent HTML compatibility.

-**Zoho Plugins:**Compatible.

9.2 Cons:

-**Multiplatform:**It has limited platform support, being available for Linux, Mac OS, and Windows only. Unfortunately, it does not cater to any mobile platforms despite its high RAM usage demand, posing potential challenges for devices with limited RAM capacity.

10KMELEON.

Website: *http://kmeleonbrowser.org/* (http://kmeleonbrowser.org/)

10.1 Pros:

-**Privacy**: It offers privacy as it is based on Mozilla.

-**Open source**: It is open source.

-**Userfriendliness**: It is very “easy” to use.

10.2 Cons:

-**Security:**It exhibits vulnerabilities in terms of security, marked by the absence of updates since 2015. Additionally, it lacks end-to-end encryption for bookmarks and favorites. Clearing the browser history may result in occasional hangs, and it does not consistently block popup ads from external sites.

-**Multiplatform:**Limited to Windows, the browser faces stability issues, diminishing its multiplatform support.

-**Zoho Plugins:**Not compatible.

-

11MAXTHON.

Website: *http://www.maxthon.com/download* (http://www.maxthon.com/download)

11.1 Pros:

-**Privacy:**It ensures privacy by blocking ads**.**

-**Multiplatform:**It supports various platforms, including Android, iOS, Mac OS, and Windows.

-**User-Friendliness:**Highly user-friendly, the browser introduces unique features such as mouse gestures, initially unconventional but time-saving during use. Notable additional utilities include "Cloud Notepad" for text saving and the ability to view two tabs simultaneously on a split screen.

11.2 Cons:

-**Security:**Security is compromised as the browser has not been updated since 2012. The infrequent updates leave vulnerabilities, evident in a font error on web pages observed on Windows 7. While it does provide end-to-end encryption for bookmarks and favorites, the lack of regular updates poses a significant concern.

-**Open Source:**It is not an open-source application.

-**Zoho Plugins:**Not compatible.

12OPERA.

Website: *http://www.opera.com/* (http://www.opera.com/)

12.1 Pros:

-**Privacy:**The browser ensures privacy and anonymity through its built-in VPN and ad blocker.

-**Security:**It ranks high in security, offering end-to-end encryption for bookmarks and favorites, contingent upon creating an account.

-**Multiplatform:**It supports a variety of platforms, including Android, iOS, Linux, and Windows.

-**User-Friendliness:**Extremely user-friendly, the browser features a "Turbo Mode" for accelerated page loading on slower internet connections. It offers numerous HTML modules and an adaptive panel of frequently visited sites known as "Speed Dial."

12.2 Cons:

-**Open Source:**It is a closed-source application.

-

-**Zoho Plugin:**Not compatible. Additionally, the browser has been reported as incompatible with certain sites, leading to potential issues such as improper functioning or an inability to load content.

13ORBITUM.

Website: *http://orbitum.com/* (http://orbitum.com/)

13.1 Pros:

-**Multiplatform:**It supports various platforms, including Android, iOS, Linux, and Windows.

-**Zoho Plugin:**Being Chromium-based, it is compatible with Zoho plugins.

-**User-Friendliness:**Extremely user-friendly, the browser seamlessly integrates social networks, including Facebook chat. It boasts fast page load speeds and provides a high level of protection for confidential information. The "quiet mode" conceals social network activities. Importing bookmarks from other browsers is straightforward, and it features a built-in "Google translator" button for quick text translation.

13.2 Cons:

-**Privacy:**A weak point is observed, as the privacy statement grants the right to collect user information.

-**Open Source:**It is not an open-source application.

-**Security:**Security appears compromised due to infrequent updates. The absence of end-to-end encryption for bookmarks and favorites necessitates the use of third-party extensions, such as the Zoho extension plug-in for Chrome.

14SECURE BROWSER.

Website: *https://www.securebrowser.com/* (https://www.securebrowser.com/)

The only advantage of this browser is that it has a builtin download button that allows downloading videos from different resources.

14.1 Pros:

-**Zoho Plugin:**Being Chromium-based, it is compatible with the Zoho plugin.

-**User-Friendliness:**Highly user-friendly, it closely resembles Google Chrome but with simplified features, retaining the essential functionalities. The "Settings" section mirrors that of Google Chrome.

14.2 Cons:

-**Privacy:**The browser exhibits a weak point in privacy as its privacy statement grants the right to collect user information.

-**Security:**Security raises concerns due to an undisclosed update frequency. Additionally, it currently lacks end-to-end encryption for bookmarks and favorites, with the promise of its future release. In the interim, users can utilize the Zoho extension plugin for this functionality.

-**Multiplatform:**It supports only the Windows platform.

-**Open Source:**It is not an open-source application.

15SLIMBROWSER.

Website: *https://www.slimbrowser.net* (https://www.slimbrowser.net/)

For this browser, I won't provide a numerical rating, but I'll offer a brief description for your information. I frequently use this browser for downloading videos from YouTube, finding it safer than using various plugins. It boasts high performance; even with more than 30 tabs open, it operates smoothly, a notable advantage compared to other browsers that tend to slow down after only 10 tabs. It's advisable to regularly check for updates, as notifications may not always function correctly, and the browser has weak support. Following the last update, I encountered an issue where bookmarks were not saved. It performs poorly on Windows x32 bit, and upon uninstallation, "Internet Explorer" becomes the default browser.

16TOR BROWSER.

Website: *https://www.torproject.org/projects/torbrowser.html.en* (https://www.torproject.org/projects/torbrowser.html.en)

16.1 Pros:

-**Privacy:**The browser prioritizes privacy, being based on Mozilla. While it lacks end-to-end encryption, it encrypts visited sites, providing satisfactory privacy for the average user. Professional users benefit from additional advantages and settings.

-**Security:**Recognized as one of the safest browsers globally, it ensures reliability by never disclosing the exact location and frequent release of patches.

-**Open Source:**It is an open-source application.

-**Multiplatform:**It offers support for multiple platforms, including Linux, Mac OS, and Windows, excluding mobile OS.

-**User-Friendliness:**Highly user-friendly, it supports .onion sites, a feature unique to Tor and not available on other browsers.

-**Zoho Plugin:**Compatible, as it is Mozilla-based.

17VIVALDI.

Website: *https://vivaldi.com/* (https://vivaldi.com/)

17.1 Pros:

-**Zoho Plugin:**Compatible, as it is Chromium-based.

-**User-Friendliness:**Highly user-friendly, featuring a built-in reader mode that allows users to remove clutter from news pages and focus solely on the content. Customization options, such as adjusting font size, style, and colors, enhance the reading experience. The browser also introduces a convenient "fast forward" feature, placing a dedicated button before the address bar to help navigate to the next page of a multipage article, forum thread, or search results without the need to search for the link.

17.2 Cons:

-**Privacy:**While the browser, based on Chromium, offers privacy, it lacks end-to-end encryption, requiring the use of third-party tools. The commitment to privacy is emphasized in their statement, asserting it as a top priority.

-**Security:**Being a new product, the level of security is currently unknown.

-**Open Source:**While the software includes many open-source components and operates under a freeware model, the platform itself is not open source. It was developed by former Opera employees expressing disagreement with the direction of the Opera browser.

-**Multiplatform:**It supports various platforms, including Linux, Mac, and Windows, but not mobile OS. Ongoing optimizations are being conducted, and while it may be slightly slow or resource-intensive in some cases, the latest versions exhibit significantly improved performance.

Change Log:

03 February 2024:

-**Brave**: Removed "privacy" as a pro and put it as a con, from information found on this source: https://spyware.neocities.org/articles/brave.html

-**Globus Browser**: Project is dead. Removed links.

REVIEW · 6 June 2021

13 Password Managers

Our primary security focus involves robust password management and encryption. Creating strong passwords involves a balance of length and complexity, as short and easily memorable passwords are prone to compromise. It's crucial to strike a balance where passwords are accessible to you but challenging for potential attackers. The encryption method depends on the application, with the paramount consideration being secure storage. Embrace a layered security approach when establishing and handling passwords, recognizing that in an interconnected world, vulnerabilities stem from multiple sources. Thus, deploying multiple defenses becomes imperative for comprehensive protection.

Proactively protecting yourself also safeguards the organization from threat actors. As cyberattacks become more common, it's crucial to establish safeguards. Consider using one of the safe, user-friendly password management tools below to enhance password protection. Our aim is to equip you with knowledge to avoid and mitigate attack risks, aligning with Ubinodes' work style and flow.

Our specifications sheet:

Security:

- Resistance to state-sponsored criminals (note 1)(note 2).
- Open-source (note 3).
- Administration of users.
- Access and activity logs: To know when and by whom passwords are accessed.
- IP restrictions: To restrict access of our vaults to only pre-approved IP addresses.

Accessibility:

- Multi-platform (note 4).
- Intuitive: Anyone and everyone can use it from a teenager to a 70-year-old.

1Password (01/13)

1Password is a password manager for individuals, families and businesses with lots of classic features and a few unique ones.

1.1**1Password-Pros:**

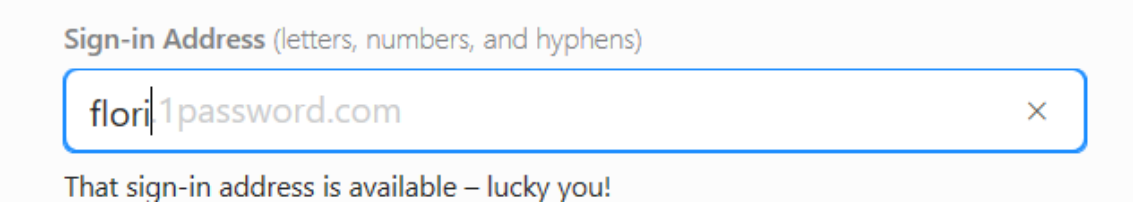
- Ensure secure password and document sharing
- User activity reporting
- Streamlined group permissions administration,
- Employ personalized access URLs that are challenging for third parties to find, activate
- Travel Mode to remove sensitive information during travel,
- Implement secret keys for user authentication.

1.2**1Password-Cons:**

- Implement a complex login procedure.

- Lack user-restricted access.
- Subscription cost: $3 per user per month, with a family plan available at $5 per user/month.
- Provide offline access, considering the sensitivity to device theft (note 1).

1.3**1Password-Screenshots:**



Bitwarden (02/13)

The product securely stores network users' passwords in an encrypted vault, providing easy and safe management. Bitwarden software is accessible on both mobile and PC, supporting Linux, MacOS, Windows, and Android operating systems. The software is traditionally open source and free for a single user, with a slight increase to $5 per month for each user in larger organizations. Passwords are encrypted using AES-256 bit encryption and support the SHA-256 hashing algorithm.

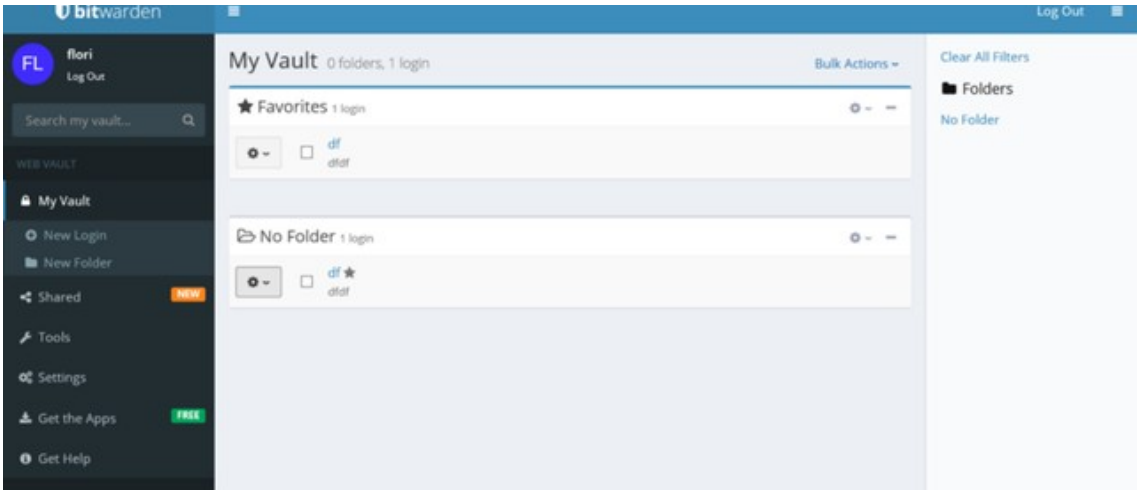
2.1**Bitwarden-Pros:**

- Facilitates password sharing.
- Encrypts the login page.
- Operates as a cloud solution.
- Open-source.
- Allows the disabling of auto-fill for login credentials.
- Supports Two-Factor Authentication (2FA) and Time-Based One-Time Passwords (TOTP).
- Includes 1 GB of encrypted file storage..

2.2**Bitwarden-Cons:**

- No recovery option in case of main password loss.
- Lacks an activity log for user monitoring.
- Does not provide IP address restricting/whitelisting.
- No reporting feature.
- Pricing: $3 per user per month for basic features, with additional offerings including a personal use premium plan at $10 per year and a team plan at $5 per user per month.

2.3**Bitwarden-Screenshots:**



Dashlane (03/13)

Unlike the previous product, Dashlane operates as a subscription-based password manager, supporting standard operating systems like MacOS, Windows, iOS, and Android. In addition to password management, Dashlane serves as a digital wallet, with encryption based on the SHA-256 algorithm. The software, available in 12 languages, offers two-factor authentication and VPN integration, catering to organizations of any size.

Contrary to the Wall Street Journal's assertion that "Neither Dashlane nor a hacker (or government agency) … could access your data without knowing your master password," this claim is inaccurate (note 1).

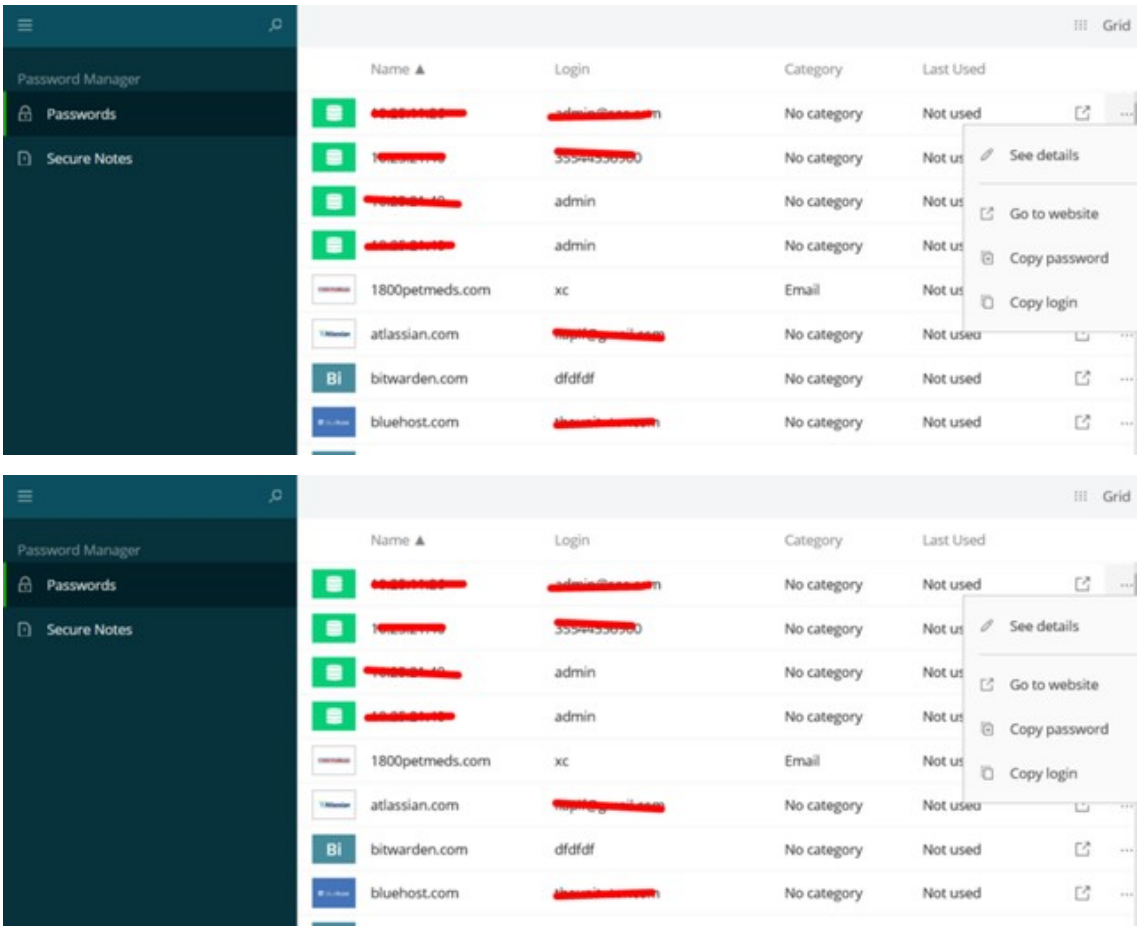
3.1**Dashlane-Pros:**

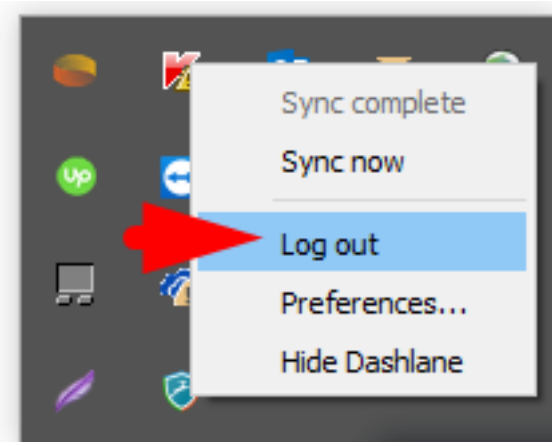
- Provides login reporting.
- Enables secure password sharing, with a limit of 5 for free accounts and unlimited for business plans.
- Allows the disabling of auto-login and autofill.
- Offers a free option, with a business plan priced at $4 per user per month.
- Supports Two-Factor Authentication (2FA).
- Utilizes 2FA to secure connections to new devices.
- Facilitates secure data sharing between users using asymmetric encryption.
- Ensures user data protection even in the event of Dashlane server compromise.

3.2**Dashlane-Cons:**

- Password management must be conducted through a locally installed app, heightening the risk of unauthorized access from a lost or stolen device (note 1). Manual logout is mandatory after each session.

3.3**Dashlane-Screenshots:**





Encryptr (04/13)

Discontinued: *https://spideroak.support/hc/en-us/articles/115003945666-Encryptr-End-of-Life* (https://spideroak.support/hc/en-us/articles/115003945666-Encryptr-End-of-Life)

Keeper (05/13)

Keeper is an excellent tool for securely storing website passwords and financial information. Operating as Software as a Service (SaaS), Keeper functions as a cloud computing vendor, providing all services from its servers in the cloud. The product is currently accessible on desktop and mobile, supporting Linux, MacOS,

Windows, and Android operating systems. Its pricing structure caters to diverse customer needs, including student, family, personal, business, and enterprise requirements.

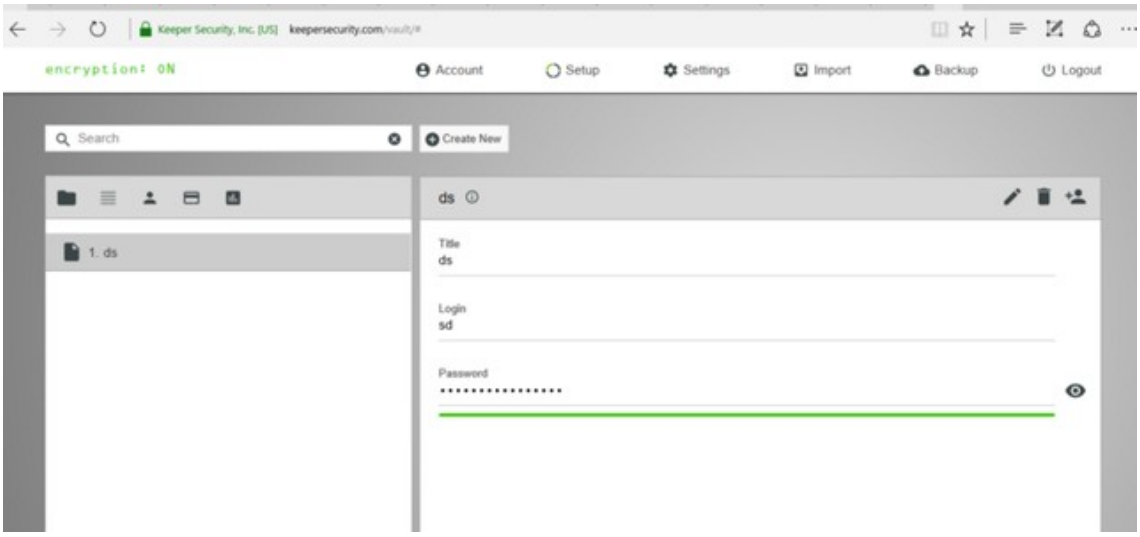
5.1**Keeper-Pros:**

- Encrypted access,
- Access and activity tracking,
- Secure password sharing,
- Recovery account for emergency access,
- Main password vaults not stored locally,
- Cloud solution,
- Two-factor authentication, including Yubikey.

5.2**Keeper-Cons:**

- Lacks reporting
- IP address restricting/whitelisting
- Offers very basic console features.
- Priced at $30 per user per year for basic functionality.

5.3**Keeper-Screenshots:**



Lastpass (06/13)

LastPass is a user-friendly password manager with both free and highly affordable options. The company emphasizes robust encryption algorithms, offering a password manager accessible through major browsers and apps from prominent app stores.

6.1**Lastpass-Pros:**

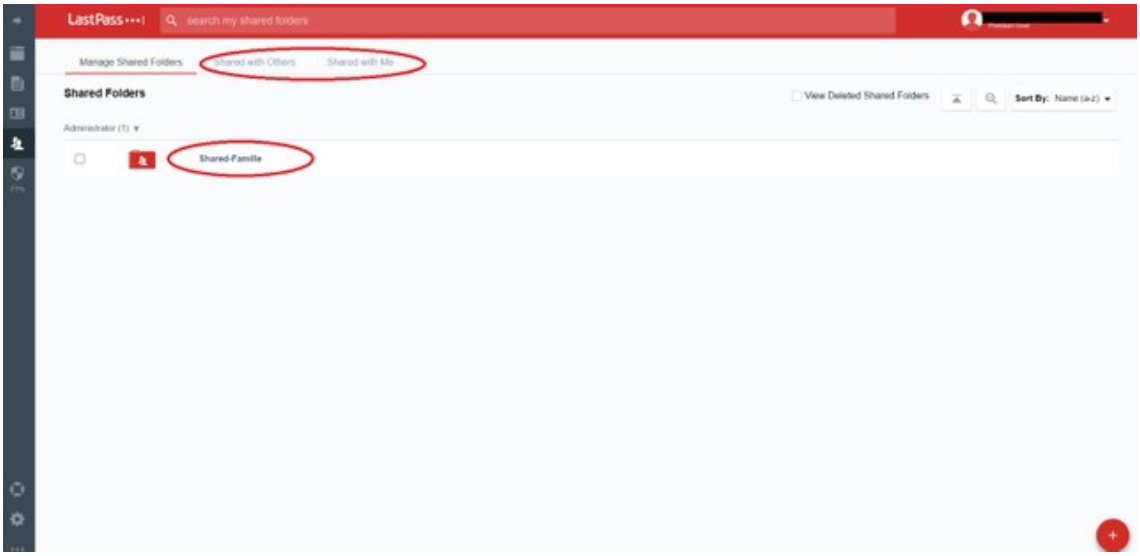
- Two-factor authentication provided.
- Enables password sharing.
- Includes a form filler option.

- Allows note storage.
- All features available at a very affordable price: $24 per user per year for the premium plan, while the team plan is priced at $29 per user per year. Also includes 1GB encrypted file storage.

6.2**Lastpass-Cons:**

- Offline mode: Vulnerable to physical theft since passwords can be stored on devices for offline access, although this can be disabled in the settings (note 1). Potentially susceptible to brute force attacks as all data is stored in user browsers, presenting a vulnerability exploitable by hackers.

6.3**Lastpass-Screenshots:**



Myki (07/13)

A relatively new password manager with lots of advanced features but some basic vulnerabilities.

7.1**Myki-Pros:**

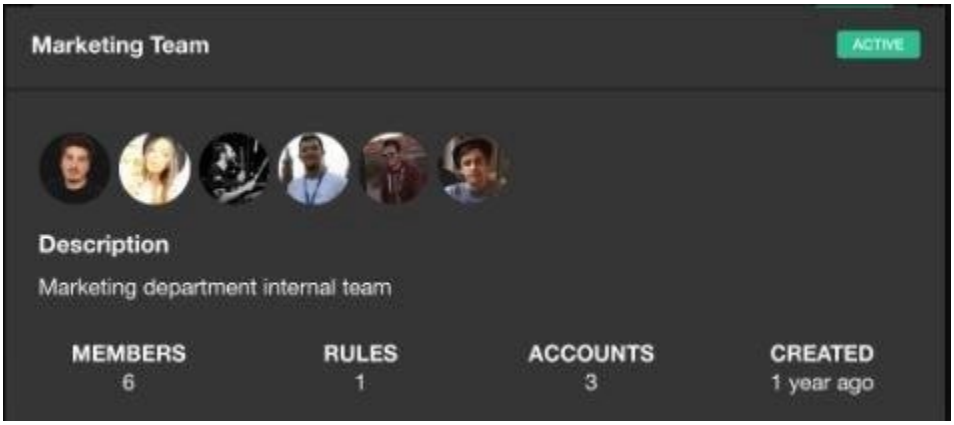
- Cost-effective for teams at $48 per 100 users per year.
- Provides provisional accounts,
- Facilitates management and access restrictions for multiple members simultaneously.
- Offers geographical access restrictions, allowing mapping to limit team members' account access.
- Incorporates IP address restricting/whitelisting
- Time-based access control.
- Features Browser Activity Monitoring (BAM) for real-time insights into users' interactions, down to their keystrokes, aiding in detecting malicious activity.
- Includes account sharing functionality to grant access without sharing credentials and supports two-factor authentication.

7.2**Myki-Cons:**

- Provides solely mobile app access, exposing vulnerability to device theft.
- Local storage of passwords on phones heightens susceptibility to device theft.

- The web interface is still under development,
- UI lacks polish.
- The digital wallet auto-fill feature is also susceptible to theft.

7.3**Myki-Screenshots:**



PassworkMe (08/13)

PassworkMe is a team-oriented password manager designed for companies and startups, with hosting based in the Netherlands.

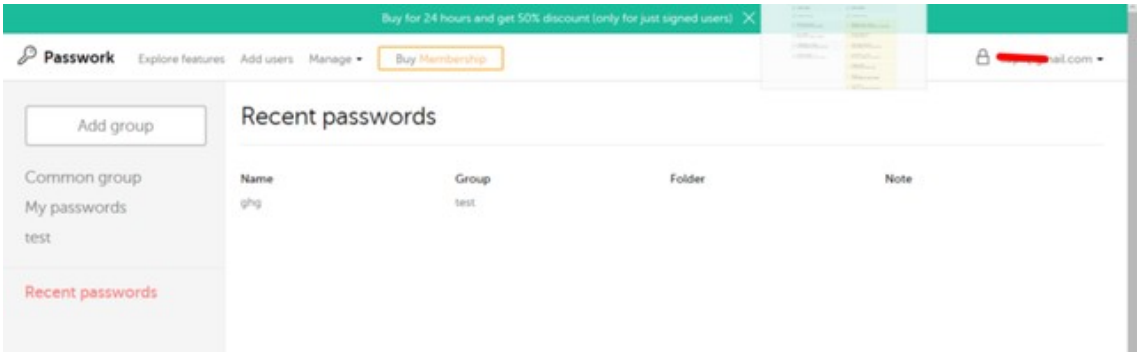
8.1**PassworkMe-Pros:**

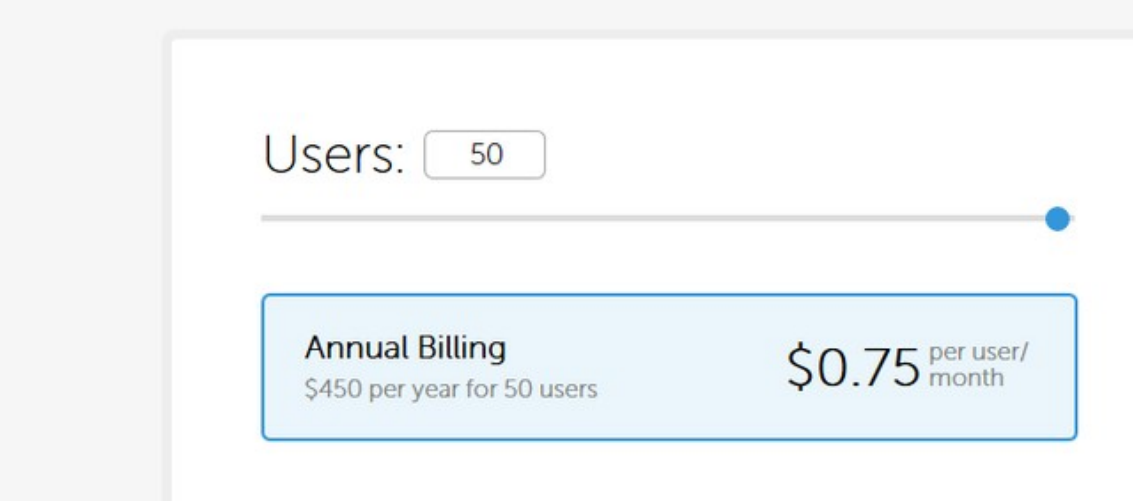
- RSA encrypted access.
- Priced at $18 per user per year.
- Flexible vaults are not stored locally.
- Password vaults are not stored locally.
- Includes IP address restricting/whitelisting.
- Facilitates secure password sharing.

8.2**PassworkMe-Cons:**

- Limited to 50 users.
- Lacks emergency access.
- No user restrictions.

8.3**PassworkMe-Screenshots:**





Roboform (09/13)

RoboForm claims the title of the world's top password manager and secured the second spot for our organization. Here's why:

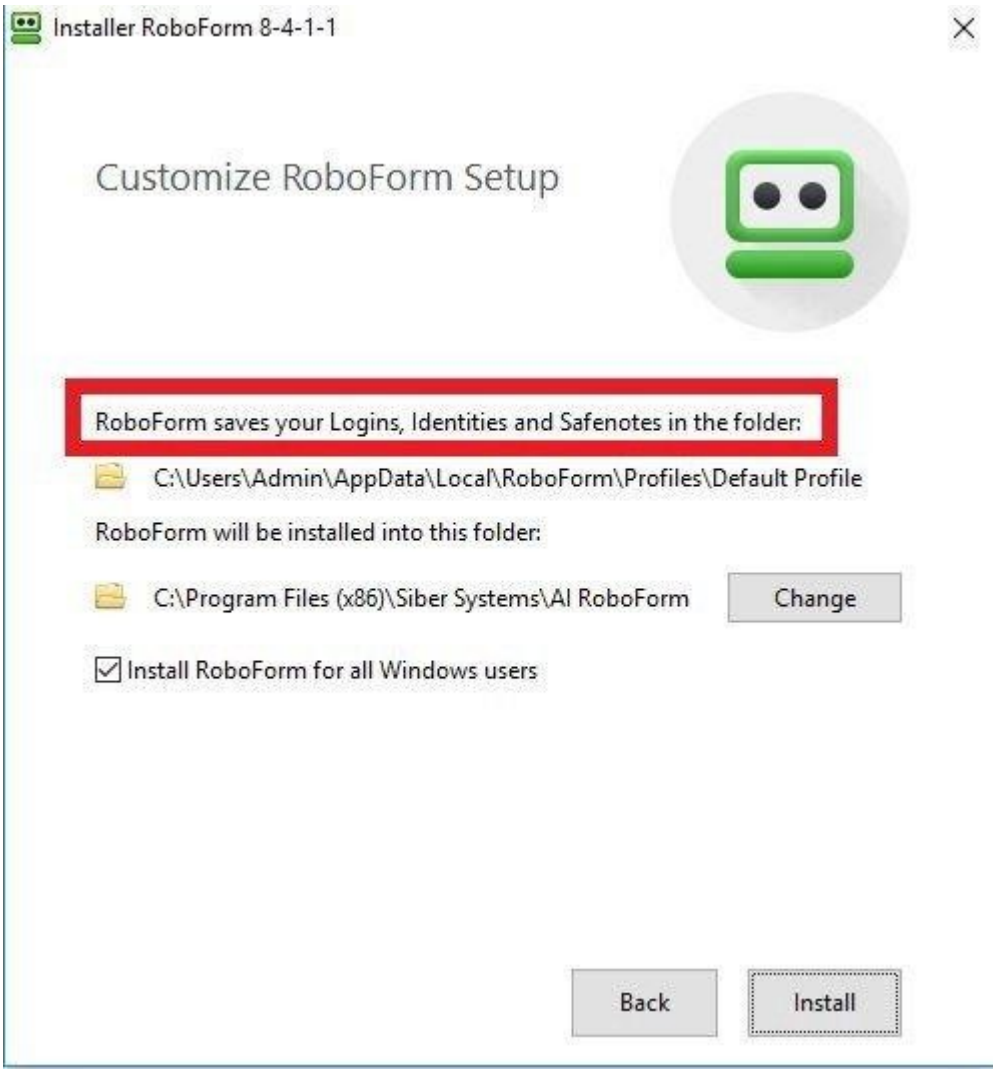
9.1**Roboform-Pros:**

- Enforces robust user policies.
- Features user-friendly interfaces.
- Includes IP address whitelisting.
- Incorporates a web session timeout feature.
- Provides a one-time password authentication option.
- Allows administrators to limit the number of password changes.
- Offers user login reports.
- Employs end-to-end encryption for password sharing.
- Facilitates the importation of browser bookmarks.
- Competitively priced at $25 per user per year for a business account.

9.2**Roboform-Cons:**

- Restricts password sharing to paid accounts.
- Requires most actions to be performed through installed software.
- Stores data locally.
- Poses challenges for users in terms of management.

9.3**Roboform-Screenshots:**



Safe in Cloud (10/13)

SafeInCloud is another leading password manager known for its simplicity, user-friendliness, and compatibility across major platforms and devices.

10.1**SafeInCloud-Pros:**

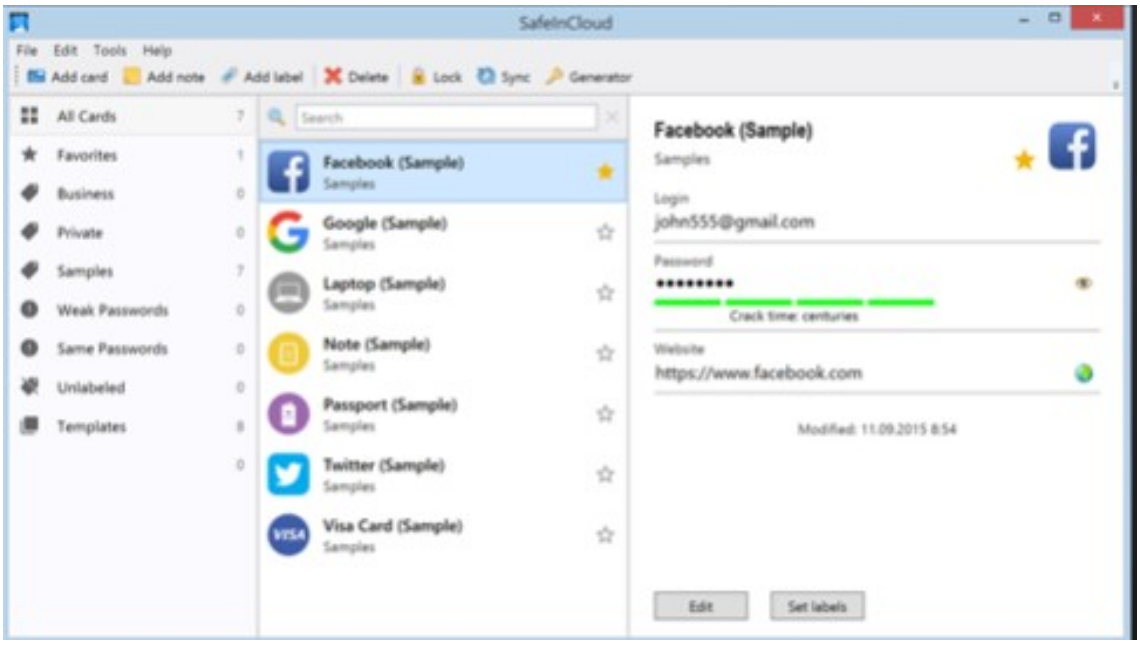
- Free.
- Facilitates password sharing.
- Includes a password generator and strength indicator.
- Offers cloud synchronization.
- Employs strong AES-256 encryption.
- Supports fingerprint authentication.

10.2**SafeInCloud-Cons:**

- Standalone solution: Requires local installation on devices.
- Lacks access or activity tracking.

- Automatically deletes the database if incorrect passwords are entered five times.

10.3**SafeInCloud-Screenshots:**



Sticky Password (11/13)

Sticky Password is a commendable password management solution for personal use. However, it is not recommended for teams, especially those operating in high-risk countries. Originally designed for personal usage, Sticky Password plans to introduce a new sharing feature in the coming months, enabling the sharing of selected accounts among Sticky Password users. This forthcoming feature will enhance the app's suitability for working teams.

11.1**StickyPassword-Pros:**

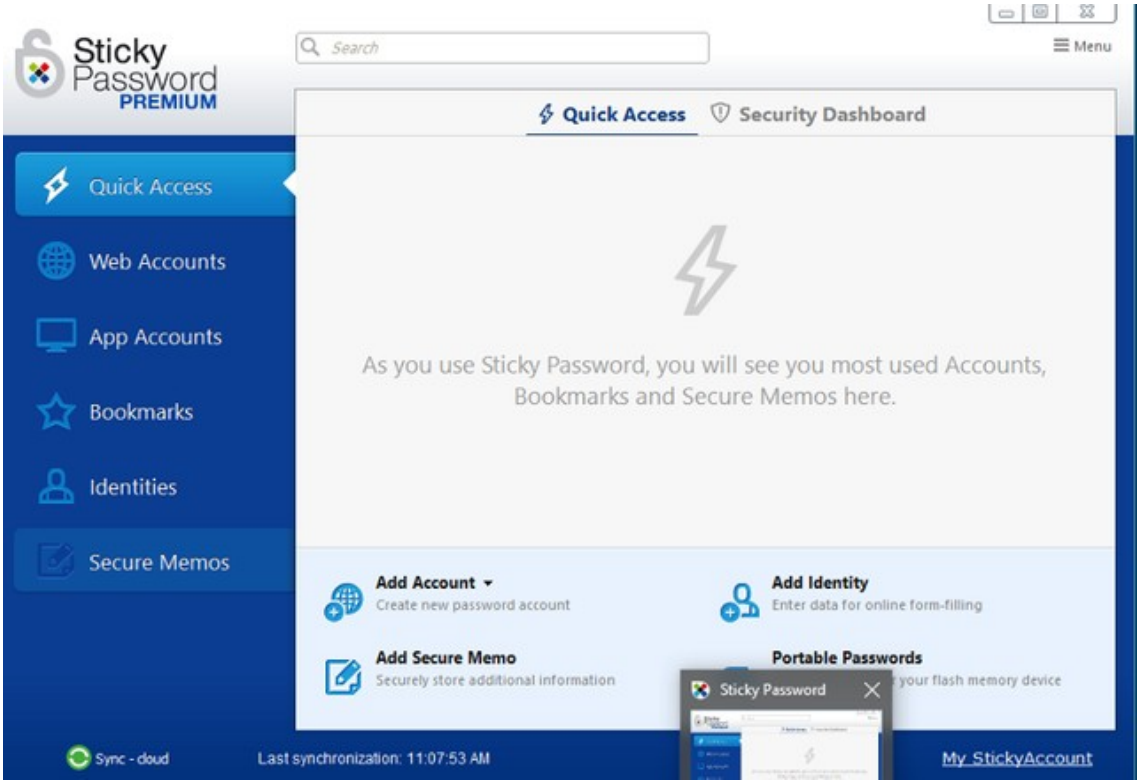
- AES-256 encryption ensures security.
- Fingerprint authentication enhances access control.
- Two-factor authentication adds protection.
- Cloud synchronization is available with the paid package for device connectivity.
- The lifetime access fee for the paid version is $150.
- Device whitelisting enhances security.
- Form filling streamlines data entry.

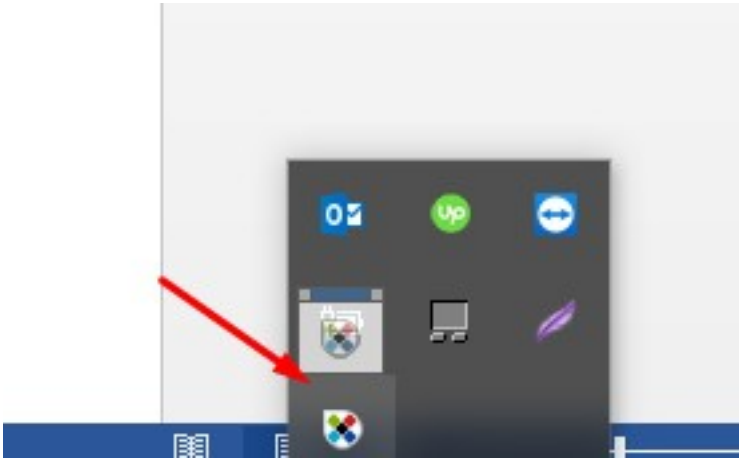
11.2**StickyPassword-Cons:**

- Standalone solution: locally installed on devices.
- Offline data synchronization may expose it to data theft.
- No password sharing.
- No access or activity tracking.
- Vulnerable to access from hacked emails.

- No recovery if the main password is lost.
- The application doesn't request a master password when closed and opened.

11.3**StickyPassword-Screenshots:**





SuperGenPass (12/13)

SuperGenPass is a unique password solution. Instead of storing passwords locally or online, vulnerable to theft and data loss, it employs a hash algorithm. This algorithm transforms a master password into unique, complex passwords for the websites you visit.

12.1**SuperGenPass-Pros:**

- It's free.

- Passwords are not stored online or offline.

12.2**SuperGenPass-Cons:**

- No password sharing.
- No access or activity tracking.
- No reporting.
- No IP address restricting/whitelisting.
- Very basic console feature.
- For personal use only.

12.3**SuperGenPass-Screenshots:**

ZOHO (13/13)

ZOHO provides diverse online services for businesses. Although we haven't tested all their offerings, we selected their password manager, and ultimately the one we choose. A key factor is that ZOHO Vault avoids local storage of passwords on devices or browsers. This feature ensures the invulnerability of passwords stored on ZOHO's password manager against theft and brute force attacks.

13.1**Zoho-Pros:**

- Web encrypted access.
- Tracks password access and activities.

- Secure password sharing.
- Passwords are not stored locally on devices (note 6).
- Access can be restricted to specific IP addresses.
- Strong users access restriction policies.
- Detailed reporting on every user activity, including password sharing.
- Break glass account for emergency access.
- Also, a free option is available, but without certain features.
- Transfer/acquire ownership of passwords.
- One-click auto logon.
- Two-factor authentication.

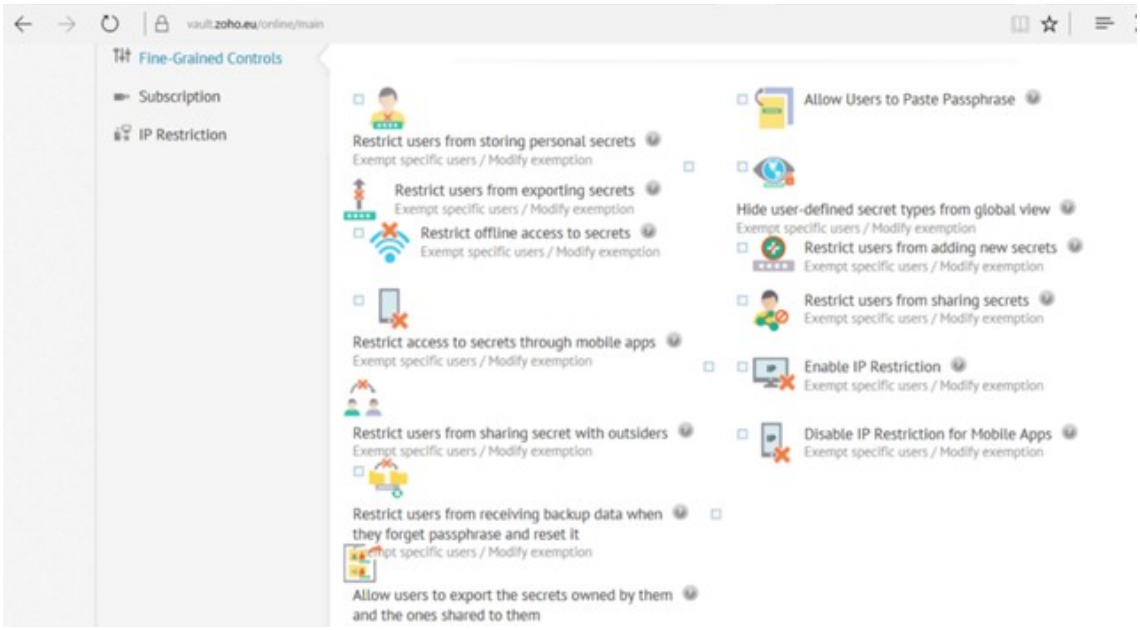
13.2**Zoho-Cons:**

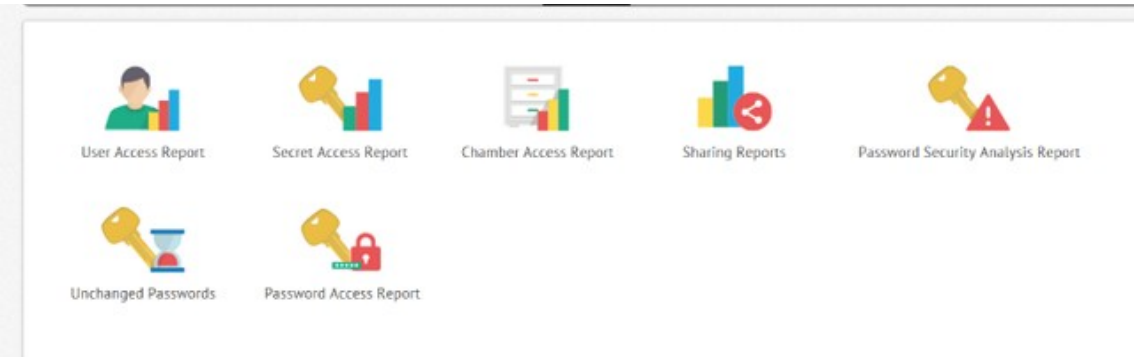
- Price of the professional package: €4/user/month.

-

- 13.3 Zoho-Screenshots:

-





1. Notes

(1) Certain software, such as Elcomsoft : *https://blog.elcomsoft.com/2017/08/one-password-to-rule-them-all-breaking-into-1password-keepass-lastpass-and-dashlane/* (https://blog.elcomsoft.com/2017/08/one-password-to-rule-them-all-breaking-into-1password-keepass-lastpass-and-dashlane/) is crafted to crack password managers. Among the tested providers, only Bitwarden, Keeper, PassworkMe, Supergenpass, and Zoho demonstrated security.

(2)Police, prosecutors, etc., engaging in "legal" crimes through corrupted state institutions pose a significant threat to individuals and countries. If involved in illegal activities, they can manipulate the system to cover it up. Seizing devices under false charges and gaining access to SMS and emails are common tactics. Utilizing encryption software, securing devices, and purchasing hardware from outside the operating country are essential precautions.

(3)Open source doesn't ensure thorough code audits for backdoors or weaknesses, yet it signals a commitment to transparency.

(4)Access passwords across devices and share specific passwords with agents globally. Must support iOS, Android, Windows, Linux, and Mac desktops. Windows phones and Blackberry are excluded due to limiting options and finding a solution becomes nearly impossible.

(5)Zero-knowledge encryption necessitates storing the key on the user’s device for protection against state-sponsored criminals. It doesn't prevent the provider from handing over plain text messages to the government but requires an active attack on the user to steal the necessary password.

(6)Upon logging into the Zoho Vault extension, all secrets are temporarily encrypted within the browser extension. When accessing secret details, editing secrets, or revealing passwords by clicking the “Show” button, the details are decrypted using the extension’s passphrase and displayed in plain text. Encrypted secret data in the extension is cleared upon logging out from Zoho Vault or when the passphrase is cleared after timeout. The browser extension supports offline access, requiring the passphrase for decryption.The Zoho Vault browser extension incorporates an offline access feature, requiring the passphrase for decryption. In offline mode, data persists even if the passphrase is cleared because there is no two-way connection with Zoho Vault servers to fetch secrets. Administrators can manage offline mode settings through fine-grained control. It's worth noting that these products underwent testing and review by Florjan Llapi, a Certified Ethical Hacker and System Administrator.

RESEARCH · 5 January 2018

Get Rid of Your Email

We elucidate the risks posed to your business and personal information by conventional email platforms, emphasizing their vulnerability to cyber attacks. We advocate for a transition to secure encryption messaging apps as a proactive measure to safeguard your assets.

Disclaimer:We have no affiliations with the mentioned companies, and there is no affiliate marketing associated with the provided links below for your convenience..

1. Stop Putting Your Security At Risk

The Internet has enhanced global business efficiency by facilitating streamlined communication and instant sharing of files and information. However, this convenience is accompanied by significant risks.

For those with malicious intent—be it criminals, competitors, or other individuals—storing and sharing valuable business information online creates an opportunity for hackers to exploit and cause severe damage to your organization.

In the realm of cybersecurity attacks, email stands out as one of the most vulnerable points of entry. "How to hack a Gmail account" is currently among the most searched topics related to account hacking on the Internet. Although email hacking, phishing, and spam are not novel practices, the increased online communication and the evolving sophistication of hackers amplify the risks for companies.

1. The Financial Cost Of Emailing

A security breach through email can inflict substantial financial losses on businesses, potentially costing millions of dollars in liability and lost revenue. In 2016, the average total cost of a security breach amounted to approximately $7.01 million. Understanding how these costs accumulate is crucial, and here are a few reasons why security breaches can be financially devastating to an organization:

- Remediation.
- Loss of Customers.
- Business Disruption.
- Regulatory Fines.
- Legal Costs.
- Public Relations.
- Breached Client Records.
- Direct Financial Loss.
- Notification Costs.
- Credit Card Reissues, Identity Theft Repair and Credit Monitoring.

Currently, there are 4.9 billion email addresses worldwide. Accordingto *Avatier’s timeline of email security breaches* (https://www.avatier.com/blog/email-security-breaches/), over two years, there have been 6,789 global email data breaches, compromising 886.5 million records—more than double the U.S. population.

In the dynamic business environment, email can pose a different kind of challenge—procrastination. How often have you dispatched an email, even flagging it as urgent, only to wait for an extended period for a response? Vital information may get buried in lengthy email threads involving multiple participants. Additionally, important files sent to you may end up in the wrong folder due to a rigorous spam filter or, worse, might be inadvertently deleted amid the effort to manage the constant influx of emails throughout the day.

Despite the perceived safety of a complex, secret email password, conversations lack end-to-end encryption, rendering them vulnerable to unethical interception. In the contemporary digital environment, email, integral to both business and personal life, has become outdated in providing the requisite security. For further insights, refer to our article on Data Privacy in the 21st century.

1. How To Safeguard Your Information.

The future of business messaging has arrived in the form of encrypted messaging apps. End-to-end encryption (E2EE) is a communication system where only the communicating users can read the messages, making it resistant to surveillance or tampering. This security measure ensures that no third party can decipher the communicated or stored data.

In practical terms, when two or more devices communicate through an app with this level of security, information is transmitted using a secret code rather than insecure plain text. For individuals and businesses seeking robust information protection, adopting this practice represents the way forward.

1. Login vs. email:

When signing up with an email provider, the standard procedure involves creating an email as the login and a password. It's common to use a password manager for generating a strong password, as discussed in our Password Manager article.

However, a security vulnerability arises when hackers, utilizing social engineering, assume the email as the login, especially when the email contains the provider's name like gmail, yahoo, outlook, yandex, etc. In such cases, gaining access becomes relatively easy through social engineering or brute force attacks on the password. To eliminate this weakness, it's advisable to create a login that is distinct from the communication email and is challenging to guess like urQP6V72EAuHzq3QF8fS7@tutanota.com . Utilizing a password manager allows for the creation of a secure login, ensuring heightened protection. with another difficult password all of that stored into a password manager. Then we create aliases to give round.

1. Use aliases to compartment

Spy servicescollaborate in sharing data, utilizing email addresses and phone numbers to interconnect profiles. If an individual consistently employs the same email across various platforms, especially with Prism program participants. And the person may find themselves ensnared in an internet bubble, where their searches lead to targeted advertisements, leading them to specific items or topics.

In the event of a database breach, the compromised email typically surfaces initially on the darknet before appearing on the clearnet. When, hackers exploit these exposed emails in attempts to gain access to associated mailboxes. By employing distinct aliases for each registration and using separate emails for various functions, in such a scenario, if a database is breached, only one email becomes compromised.

Many websites, including certain email providers, lack a delete account feature. To disengage from such platforms, users may need to deactivate the associated email. This is viable when utilizing one alias per website.

For general communications, consider creating an alias for each calendar year. Start afresh annually, providing a new email to those you wish to stay in touch with, and deactivate the previous year's email. This practice shields your privacy by limiting the scope of potential attacks and exposure.

Opt for open-source end-to-end encrypted email software or freemium hosted secure email services like Tutanota or Protonmail, prioritizing them over mainstream providers such as Gmail and Outlook. Consult our article on Tutanota vs Protonmail for budget-friendly guidance.

For users emphasizing security, explore apps like Threema, Wickr, and SafeUM. Our Threema article offers an in-depth understanding, including pros and cons for potential users.

These brands prioritize security and user privacy. Unlike some popular messaging apps claiming encryption, even Swiss-based Threema ensures server operators lack access to read your messages.

If privacy is paramount and you seek assurances against data sharing with third parties, these apps are the ideal choice. Download one today to rest assured that your information is securely encrypted.

REVIEW · 9 December 2017

Tutanota vs Protonmail

These are two encrypted email providers. We're using both of them. Here is our review:

Disclaimer: We are not affiliated with any of these companies. This article is entirely based on our independent findings, and there is no affiliate marketing associated with the links provided below for your convenience.

How we write our reviews: For an impartial and comprehensive review, all apps undergo the following testing criteria:

- Real-time usage on actual projects.
- Evaluation by diverse team members located in different countries.
- Testing on various devices and operating systems.
- Minimum testing duration of two weeks, averaging four.
- The article undergoes peer review by team members before being sent to the app's publisher for the final review.

Our specifications sheet:

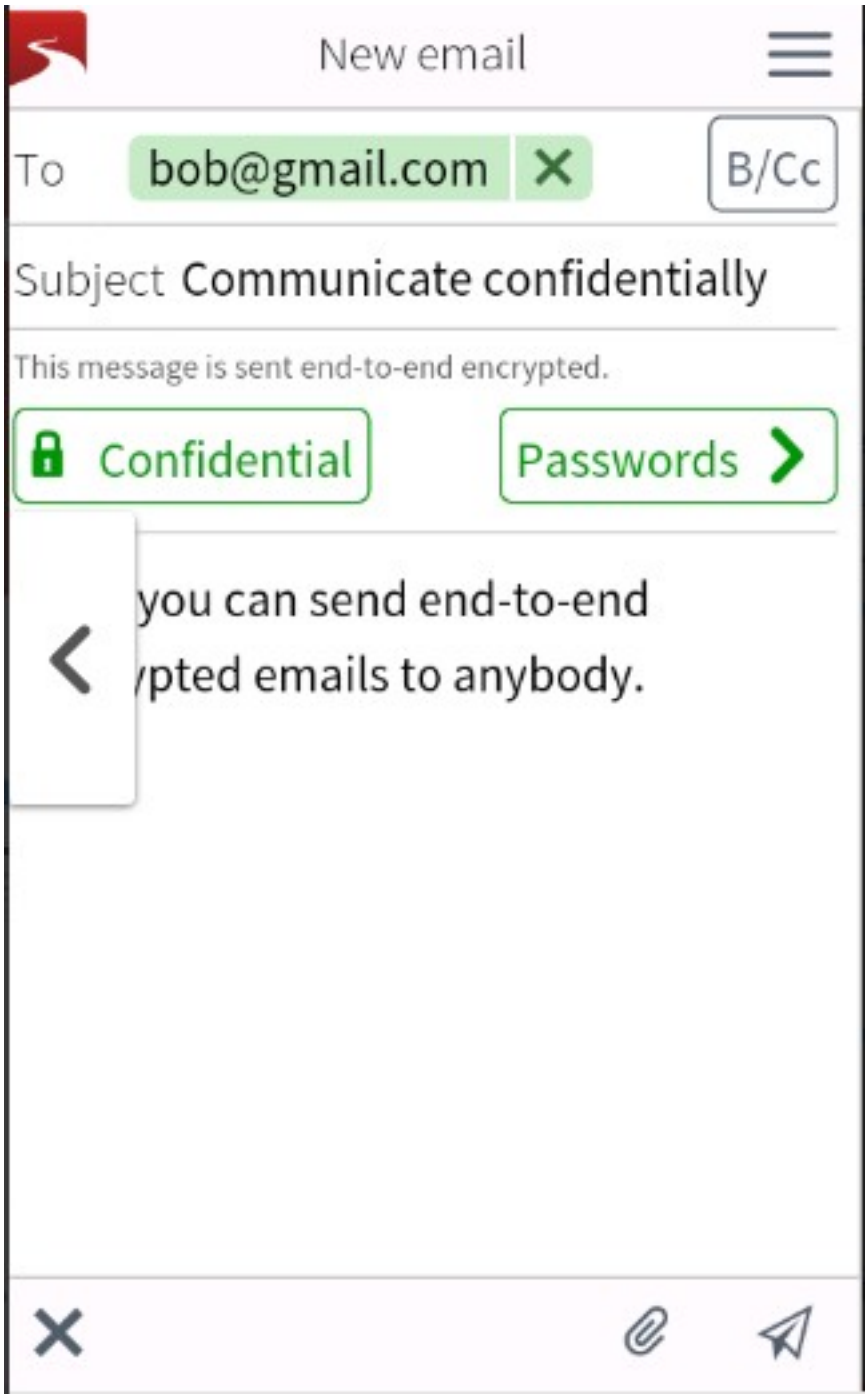
- End-to-end, zero-knowledge encryption (note 1).
- Open-source (note 7).
- Own business domain (note 2).
- User administration (note 3).
- Resistance to state-sponsored criminals (note 4).
- Cost-effective for a large user base (note 5).
- Multi-platform compatibility (note 6).
- Emergency support provided by the service provider.

From there, it’s easy to get a lot of solutions out of the list. Basically it quickly came down to Tutanota vs Protonmail. Interesting fact: The NSA requested a backdoor from them but they refused. We use both of them, but Tutanota is the one supporting our domain name with the Premium package. The main differences between Tutanota and Protonmail are the price and storage capacity (note 8).

1. Shared features between Tutanota Premium and Protonmail Plus:
    - End-to-end, zero-knowledge encryption (note 1).
    - Open source (note 7).
    - Own business domain (note 2).
    - Ability for each user to set up multiple aliases (note 3).
    - Multi-platform compatibility (note 6).
    - Web-based on desktops.
    - Password-protected emails for external users (note 10).

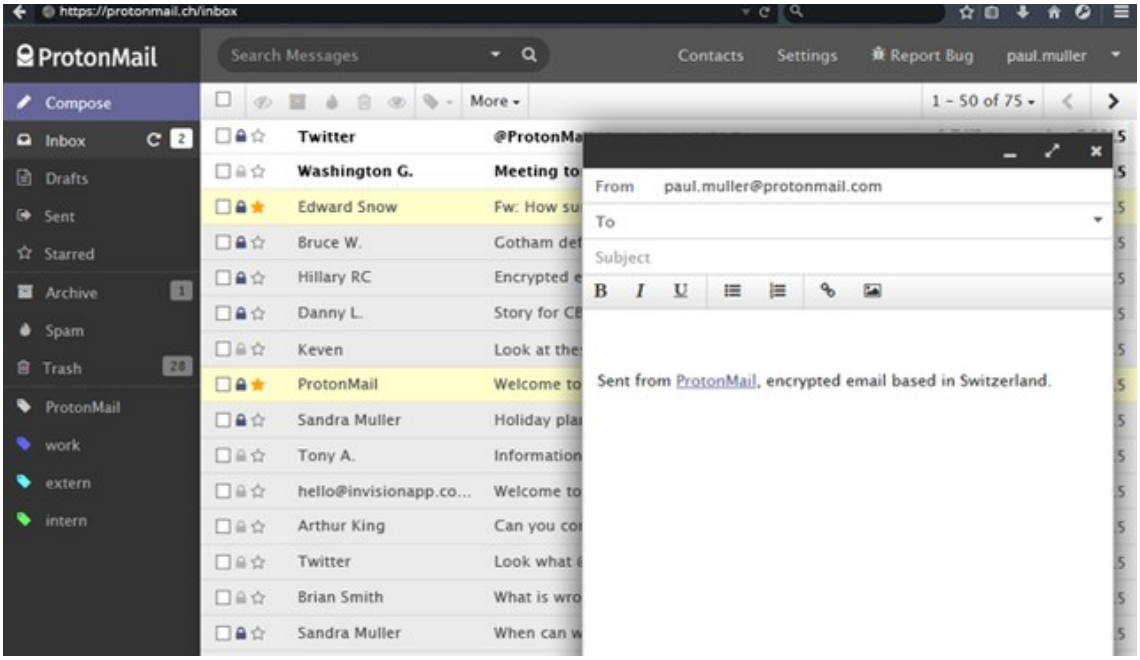
- No logging of users' data.
- Local encryption of data (note 13).
- Drag and drop messages (note 17).
- Bitcoin payments (note 20).
- Two-factor authentication (note 24).
- Professional plan with multi-user support (note 8).

1. Only with Tutanota:



- No recovery through email or SMS. However, administrators can recover for a user from the admin panel (note 9).
- Doesn't require a GSM phone number (note 19).
- Auto-synchronization with multiple devices and browsers.
- Servers are located in Germany, thus subject to German privacy protection laws (note 11). Read our article: Data Privacy in the 21st century: Germany vs Switzerland.
- Dual encryption mechanism (note 12).
- Utilizes DANE on top of SSL and PFS (note 23).
- Available as a desktop stand-alone application.

2. Only with Protonmail:



- Auto-destruct emails between ProtonMail users. Possible for external users if you set up a password-protected email.
- Notification on your recovery email for new emails.
- Option to disable recovery email.
- Requires a GSM phone number (note 19).
- PGP encryption available (note 14).
- Servers are located in Switzerland, subject to Swiss privacy protection laws (note 15). Read our article: Data Privacy in the 21st century: Germany vs Switzerland.
- Contacts import-export.
- Language support: French, German, Russian, Spanish, Polish, Turkish, Ukrainian, Dutch.
- Auto Unsubscribe (note 18).
- PIN protection for mobile apps.
- Auto-responder (note 22).

- Custom filters with Sieve (note 21).
- Desktop client bridge (note 25).
- IMAP support via extension (note 16).

3. Notes:

(1)In any case, end-to-end encryption applies exclusively to users within the same solution. PGP stands out as a universal method for sending encrypted emails to anyone, but its widespread adoption remains limited due to low user familiarity. With zero knowledge encryption, the key must be stored on the user's device to resist state-sponsored threats. While this doesn't guarantee immunity from providing plaintext messages to the government, it adds a layer of protection by necessitating active user attacks for password theft, a scenario that has not occurred so far and is unlikely in the foreseeable future. Additionally, if the password is lost, the provider is incapable of recovering or decrypting the data. Tutanota clarifies that, in the event of a valid German court order for criminal prosecution, if requested to hand over inboxes, all data, including encrypted Inbox rules, remains secure.

(2) The exposure to potential attacks by state-sponsored criminals through DNS records emphasizes the need to host your domain in a location that prioritizes access protection, preferably not in the same country as your email provider. Consider countries outside the fourteen eyes alliance with a reputation for respecting privacy and democracy. End-to-end protection serves as a safeguard in case emails are intercepted. Alternatively, you can opt to use the provider's domain,(Tutanota.com or Protonmail).

(3Multiple users can each possess multiple aliases. Each user maintains individual access credentials, including a unique username, password, and mailbox. Aliases function as email forwards to and from the original email address. For instance, if the original email is name.surname@yourdomain, aliases like blabla01@yourdomain, blabla02@yourdomain, etc., can be set up. Emails sent to any alias are then forwarded to the main name.surname@yourdomain address. This setup offers the advantage of easily creating and managing email addresses as needed.

(4)Police, prosecutors, and similar entities, when corrupting state institutions, engage in ostensibly "legal" crimes, posing significant dangers to individuals and the nation. Their capacity to conceal illegal activities allows them to cover up wrongdoings as they see fit. They can intercept and read IMAP, POP3, TLS, and SSL communications, spoof your email provider's SSL certificate, and gain access to your SMS and emails. This vulnerability often makes recovery options an easy target for potential attacks. Therefore, it is crucial to consistently employ encryption software, encrypt your devices, and procure hardware from locations outside the country of operation.

(5)With hundreds of contractors utilizing our emails, a synchronized and unified solution is imperative to minimize the risk of potential information leaks to third parties.

(6)It must be accessible from iOS, Android, Windows, Linux, and Mac desktops. We exclude Windows phones or Blackberry due to the significant limitations they impose, making it nearly impossible to find a suitable solution.

(7) While open source doesn't guarantee thorough code audits for backdoors or weaknesses, it does reflect a commitment to transparency. Tutanota asserts regular code audits and has undergone an extensive penetration test conducted by SySS GmbH, demonstrating their dedication to security.

(8)Tutanota's business plan is priced at $1/user/month, while Protonmail's business plan costs 6.25€/user/month, with a limitation of 5 users. Protonmail allows the creation of administrators for organizational management of regular users' accounts. Although Tutanota is more affordable than Protonmail, it offers less storage space (1GB vs. 5GB).

(9) In Protonmail it is possible to disable the email recovery feature.

(10) You need to send the password through another communication channel.

(11)We are uncertain about the implications of choosing Germany, a member of the Five Eyes. While NSA hardware is present on German soil, acting as a base for European surveillance, it also reflects a populace accustomed to resisting such actions. Tutanota asserts that they won't provide backdoors to these agencies and would consider relocating the company to another country if compelled by law to build backdoors.Here is their stand about the situation: *https://tutanota.com/blog/posts/data-protection-germany* (https://tutanota.com/blog/posts/data-protection-germany)

(12)Tutanota employs a dual encryption mechanism involving a private key and password. Upon registration, a private key is generated in the browser, serving the purpose of encryption and decryption. Subsequently, this private key undergoes encryption using the login password.

(13) Emails are stored encrypted locally on the devices.

(14) Tutanota is planning to develop an API to allow users to use PGP in a user friendly manner.

(15) By remaining outside of US and EU jurisdictions they provide a safer location to protect confidential data.

(16) IMAP and POP3 are not secure because they download emails locally unencrypted therefore they can be read in transit and/or on the devices.

(17) This feature enables efficient organization of your inbox by utilizing custom folders or labels. Simply hold down your message and drag it into the relevant folder or label for quick and easy categorization.

(18)The auto-unsubscribe feature simplifies the process of unsubscribing from email lists or newsletters you no longer wish to receive. It functions by identifying the unsubscribe link in the hidden header and making it accessible in the top right corner of your message. To remove your email address from mailing lists, simply click "Unsubscribe."

(19)ProtonMail insists on obtaining your GSM phone number, implying the alternative of completing a captcha. However, the captcha process is excessively time-consuming, leading many to abandon it. SMS, as a recovery option, is highly vulnerable to interception by state-sponsored criminals.

(20) You can now utilize Bitcoin for upgrading your ProtonMail and Tutanota mail accounts to premium plans, account top-ups, or making donations.

(21)ProtonMail's default filter options serve basic tasks efficiently and are easily implemented for maintaining a well-organized inbox. For advanced filtering, the custom filter with Sieve provides nearly limitless personalization capabilities. Sieve programming language, a global standard, underlies this advanced filtering feature, catering to power users and enhancing ProtonMail filters with unparalleled versatility.

(22)Users can now utilize the new auto-reply feature to set personalized responses to incoming messages. This functionality is particularly useful when on vacation or out of the office, allowing users to inform customers automatically about their absence.

(23)In addition to its automatic end-to-end encryption, Tutanota maximizes connection security by employing DNSSEC, DANE, DMARC, DKIM, PFS, and STARTTLS. The DANE protocol, specifically, serves as a robust defense against Man-in-the-Middle (MITM) attacks, and its adoption is recommended for all mail providers.

(24) Tutanota has introduced TOTP as an additional option for two-factor authentication in the beta client, following the recent inclusion of using a security device (U2F) for 2FA. TOTP enables users to utilize authenticator apps like Google Authenticator or Authy to generate codes. These codes, along with your password, serve as the second factor for logging into your Tutanota account. TOTP codes have a brief validity period, mitigating potential issues in case of code loss.

(25)The ProtonMail Bridge extends ProtonMail functionality by incorporating IMAP and SMTP support, accessible to all paid ProtonMail members. This feature enables the sending and receiving of encrypted emails directly from your preferred mail client. Compatible with Apple Mail, Thunderbird, Outlook 2011, and Outlook 2015 on macOS, as well as Thunderbird, Outlook 2010, Outlook 2013, and Outlook 2016 on Windows.

1. We've tested this and more:
    - bulletmail.org
    - chiaramailcorp.com
    - confidantmail.org
    - countermail.com
    - darkmail.info
    - invmail.io
    - mailbox.org
    - mailfence.com
    - msgsafe.io
    - mynigma.org
    - openmailbox.org
    - posteo.de
    - riseup.net
    - runbox.com
    - safe-mail.net
    - scryptmail.com
    - shazzlemail.com
    - unseen.is
    - virtru.com
    - zeromail (via zeronet)

- zwooky.com

REVIEW · 10 January 2020

Using Tutanota

Out of 20+ email providers we've tested. Basically it quickly came down to Tutanota vs Protonmail. We use both of them...

Disclaimer: We are not affiliated with these companies. This article is based entirely on our own research findings, and there is no affiliate marketing involved through the links provided below for your convenience.

How we write our reviews: For an impartial and comprehensive review, all apps undergo rigorous testing:

- Real-time usage on actual projects.
- Evaluation by diverse team members situated across various countries.
- Testing on a range of devices and operating systems.
- Minimum testing duration of two weeks, averaging four weeks.
- Peer review by team members precedes submission to the app's publisher for the final assessment.

1. Our specifications sheet:

End-to-end, zero-knowledge encryption (1),

Tailored to our business domain (2),

Efficient administration of users (3),

Resilience against state-sponsored threats (4),

Cost-effectiveness for a large user base (5),

Multi-platform compatibility (6),

Open-source nature (7),

Emergency support provided by the service provider.

This criteria swiftly narrowed down our choices, leading to a comparison between Tutanota and ProtonMail. Notably, both declined NSA's request for a backdoor. While we utilize both, Tutanota, with its Premium package, supports our domain name. Key distinctions lie in pricing and storage capacity (8).

1. Shared features between Tutanota and Protonmail:

- Open source.
- End-to-end encryption with keys stored on the user's computer (9).
- Android and iOS apps.
- Web-based add-ons for desktops.
- Password-protected emails for external users (10).
- Own domain.
- No logging of users' data.

> Two-factor authentication.

- Encrypted calendar.
- Encrypted contacts.

1. Only with Tutanota:
    - Administration of users.
    - No recovery via email or SMS (considered insecure), but through a Recovery Code generated during account creation. The admin retains the ability to recover for a user from the admin panel.
    - 1€/month/user.
    - 1 GB storage.
    - Servers located in Germany, subject to German privacy protection laws (11).
    - Dual encryption mechanism (12).
    - Local encryption (13).
1. Only with Protonmail:
    - Auto-destruct emails between ProtonMail users, with the option for external users when setting up a password-protected email.
    - Notification on the recovery email for new incoming emails.
    - 5€/month/user.
    - 5 GB storage.
    - Option to disable the recovery email.
    - PGP encryption available (11).
    - Servers located in Switzerland, subject to Swiss privacy protection laws (15).
    - IMAP/POP3 support (16).
1. Serious alternatives:
    - *Countermail* (https://countermail.com/)
    - *Virtru* (https://www.virtru.com/)
    - *Zeromail* (https://zeronet.io/)
1. Notes:

(1) End-to-end encryption is restricted to users within the same solution; PGP remains a universal method for sending encrypted emails to anyone, although its usage is limited due to awareness constraints. The encryption key's security is contingent on its storage on the user’s device, ensuring protection against state-sponsored threats. While this doesn't guarantee immunity from government requests for plain text messages, it does elevate the level of effort required, involving an active attack on the user to obtain the necessary password. As of now, such attacks have not occurred, and the likelihood of them happening in the foreseeable future remains low.

(2)This potential vulnerability could expose an attack opportunity for state-sponsored criminals through MX records. To mitigate this risk, it is advisable to host your domain in a location that prioritizes access protection, ideally in a country not affiliated with the fourteen eyes alliance. Consider states with a track record of respecting privacy and upholding democratic principles.

(3)Distinguishing between multiple users and multiple aliases is crucial. Each user possesses distinct access credentials, including a unique username, password, and mailbox. Aliases function as email forwarding mechanisms, directing emails to and from the original email address. For instance, the original email could be name.surname@yourdomain.com, with aliases like blabla01@yourdomain.com and blabla02@yourdomain.com. Emails sent to any alias are forwarded to the main name.surname@yourdomain.com address. While aliases offer the advantage of easy email creation and deletion, sharing the inbox requires admin access, an impracticality in a business environment.

(4)Law enforcement, prosecutors, etc., engaged in corrupt practices wield significant influence, rendering their actions seemingly legal. Such individuals pose a substantial threat, whether to an individual or a country. If involved in illicit activities, they can conceal them using various means, including intercepting and reading IMAP, POP3, TLS, SSL. Manipulating your email provider's SSL certificate and gaining access to your SMS and emails are potential exploits. Consequently, recovery options become vulnerable, making it crucial to consistently employ encryption software, secure devices, and procure hardware from external sources.

(5) For our numerous contractors utilizing our emails, a synchronized and unified solution is imperative to minimize potential information leaks to third parties.

(6) Accessibility is essential across iOS, Android, Windows, Linux, and Mac desktops. Excluding Windows phones and Blackberry is necessary to avoid undue restrictions on the available options, ensuring a feasible solution.

(7) Open source doesn't automatically ensure thorough code audits for potential backdoors or weaknesses, but it does reflect a commitment to transparency. Tutanota asserts regular code audits and has undergone a comprehensive penetration test conducted by SySS GmbH, showcasing their dedication to security.

(8) Tutanota, priced at 12 USD per year per user, is more economical than ProtonMail. Although it provides less storage space (1 vs. 5), our minimal storage requirements make pricing the decisive factor in our choice.

(9) It also means the provider is unable to recover (decrypt) data if password is lost.

(10) You need to send the password through another communication channel.

(11)The uncertainty arises as Germany is a member of the Five Eyes. While NSA hardware is present on German soil, acting as a surveillance hub for Europe, the resilience of the German people in resisting such activities is notable. Tutanota asserts a stance against providing backdoors to these agencies, adding a layer of assurance.

(12)Tutanota employs a dual encryption mechanism involving a private key and password. Upon registration, a private key is generated in the browser for encryption and decryption purposes. This private key is subsequently encrypted with the login password for added security.

(13) Emails are stored encrypted locally on the devices.

(14) Tutanota is planning to develop an API to allow users to use PGP in a user-friendly manner.

(15) By situating themselves outside US and EU jurisdictions, they establish a more secure location to safeguard confidential data.

(16)IMAP and POP3 are deemed insecure as they download emails locally without encryption, making them susceptible to being read in transit and/or on the devices.

1. We've tested this and more:
    - bulletmail.org (dead).
    - chiaramailcorp.com (dead).
    - *confidantmail.org* (http://confidantmail.org/)
    - *countermail.com* (https://countermail.com/)
    - *darkmail.info* (https://darkmail.info/)
    - invmail.io (dead).
    - *mailbox.org* (https://mailbox.org/)
    - *mailfence.com* (https://mailfence.com/)
    - *msgsafe.io* (https://www.msgsafe.io/)
    - mynigma.org (dead).
    - openmailbox.org (dead).
    - *posteo.de* (https://posteo.de/en)
    - *riseup.net* (https://riseup.net/)
    - *runbox.com* (https://runbox.com/)
    - *safe-mail.net* (http://safe-mail.net/)
    - scryptmail.com (dead).
    - *shazzlemail.com* (https://shazzlemail.com/)
    - unseen.is (dead).
    - *virtru.com* (https://www.virtru.com/)
    - *zeromail* (https://zeronet.io/) (via zeronet)
    - *zwooky.com* (https://www.zwooky.com/)

RESEARCH · 3 April 2018

Facial Recognition

The utilization of facial recognition software continues to expand, with various companies incorporating it into their operations. Gaining an understanding of how facial recognition software functions is crucial for comprehending potential actions that can be taken in response.

Disclaimer: We have no affiliations with the mentioned companies, and this article solely presents our independent findings. The provided links are for your convenience, and there is no affiliate marketing in place.

How we write our reviews: To guarantee an impartial and comprehensive review, all apps undergo testing in the following ways:

- In real-time, applied to actual projects.
- Evaluated by diverse team members situated in different countries.
- Tested on various devices and operating systems.
- Assessed for a minimum of two weeks, with an average duration of four weeks.
- The article undergoes peer review by team members before being submitted to the app developers for the final review.

Contents of this article.

1. What is Facial Recognition?
2. How Does The Software Work?
3. Commonly Used Facial Recognition Software.
4. Why it is used.
5. Safety Concerns.
6. Alternatives and Solutions.
7. Conclusion.
8. Sources.
9. What is Facial Recognition?

Facial recognition is a software that identifies individuals through digital images. This analysis system is employed by various companies, ranging from security systems and computer companies to social networks. The utilization of facial recognition software appears to be continually expanding, with different companies adopting this technology.

1. How does the Software Work?

Comprehending the functioning of facial recognition software is crucial to understanding potential actions one can take in response. When a person's photograph is uploaded into a database, whether through sharing on Facebook or captured by a security camera, the facial features are promptly compared to other facial images within that database. For instance, Facebook can identify matching features and pull up

additional photos of an individual when a new one is uploaded. This process involves scrutinizing common facial features such as shape, depth, color, and intricate details to establish matches with other pictures.

1. Commonly Used Facial Recognition Software.

Numerous major corporations, including Facebook, employ facial recognition software for various purposes. Facebook's DeepFace technology utilizes micro dust captured on camera lenses, boasting a remarkable 97 percent accuracy in recognizing faces, surpassing the FBI's Next Generation Identification system with an 85 percent accuracy rating. Despite varying privacy laws across countries, companies like Facebook seemingly employ this technology without public awareness. Facebook asserts its usage for connection purposes, yet the potential for undisclosed data utilization raises concerns, especially in targeted marketing.

Google has faced scrutiny for its facial recognition software integrated into Google Photos, demonstrating advanced programming capabilities, even in identifying animals. In the U.S., Google's Arts and Culture app, allowing users to match their selfies with artworks, raised privacy concerns as the data, though disclaimed as not saved, is transmitted to Google's system for matching.

Apple has incorporated facial recognition software to unlock its devices, showcasing an unprecedented level of precision that mitigates hacking concerns. Meanwhile, casinos employ facial recognition to track gamblers, ostensibly for managing gambling addiction, yet the potential for other uses, such as monitoring high spenders or card counters, remains.

Beyond entertainment, bars leverage facial recognition to identify patrons' drinking age, facilitating the expulsion of underage individuals, even if possessing fake IDs. Despite potential concerns about mislabeling, the accuracy of the software aligns more with security and law enforcement applications in crime-related incidents rather than commercial monitoring.

1. Why it is used?

Facial recognition software, originating in the 1960s, gained prominence in recent years. Initially utilized for security, it aimed to match criminals captured on security cameras with mugshots and identification cards. The advent of social media and the widespread use of smartphones further accelerated its adoption. Social media platforms facilitated constant photo-sharing, while smartphones enabled instant uploads.

The cultural shift toward individual photography and selfies, especially within millennial culture, has flooded online platforms with a remarkable number of facial images. This abundance of online pictures has streamlined the process for companies to extract user images for marketing and commercial purposes. By scrutinizing profiles and associating faces with social connections, locations, and activities, companies can construct personalized marketing profiles without individuals necessarily being aware of it.

1. Safety Concerns.

In the past, when facial recognition was employed to apprehend criminals, concerns regarding privacy and safety were often overlooked. These images, sourced from security footage, were primarily used to trace individuals posing potential threats to society. However, the advent of the internet and social media has heightened safety apprehensions. Companies now have the capability to track personal preferences, destinations, decisions, and even identify people in your life, constructing comprehensive profiles for targeted marketing.

Beyond marketing, governments can access these profiles and exploit the information to control individuals. For instance, in Shenzhen, China, facial recognition cameras identify jaywalkers, publicly shaming them on screens to enforce compliance—an erosion of public anonymity reminiscent of an Orwellian dystopia.

Online platforms like Alibaba offer the option to "pay with a smile," utilizing facial recognition for transactions. Smartphones and computers also employ facial recognition for unlocking. While marketed as convenient, the darker reality emerges as these technologies learn about users, documenting daily lives. Companies leveraging this data for marketing gain insights into habits, social class, and purchasing behaviors. Digital tags in stores adjust prices based on customer profiles, potentially exploiting consumer behavior.

Moreover, governments with access to this data can exert control, limiting personal choices. Authoritarian states may manipulate personal information to make decisions for individuals, eroding autonomy. Some software even attempts to recognize users from behind, heightening security risks. Living in a country suppressing diverse sexualities could lead to trouble if identified through such software, even for actions not officially recorded.

1. Alternatives and Solutions.

As the pervasive influence of facial recognition technology continues to grow, evading its reach may seem daunting, but there are practical measures to safeguard yourself against it. Here are some suggestions, varying in difficulty but all aimed at enhancing your privacy:

1.**Social Media:**Initiate your defense against facial recognition by addressing your social media presence. Remove existing pictures of yourself and abstain from uploading new ones. Opt for images of landscapes, animals, or inanimate objects to obscure your facial identity while still reflecting your preferences.

2.**Unlocking Devices:**Abstain from utilizing facial unlock features on devices such as phones, tablets, and computers. Opting for alternative unlocking methods helps maintain a discreet link between you and your devices.

3.**Payments:**Refrain from using facial payment options offered by various companies. Although it may seem convenient, the compromise in terms of privacy is too high a price to pay.

4.**Camera Finders:**Invest in a camera finder that alerts you to nearby security cameras, providing an opportunity to conceal your face before passing by. Avoid being unknowingly captured on camera.

5.**NIR LEDs:**Incorporate NIR LEDs, powerful lights that overload light sensors, into clothing or accessories. While some may be less conspicuous, this seemingly extreme measure proves useful, particularly depending on your location.

6.**Masks:**In locations where facial recognition poses a genuine concern, consider resorting to masks for added anonymity. Options range from surgical masks covering the lower part of your face to ski masks, or even more intricate prosthetic masks that mimic a person's appearance without revealing your true identity.

1. Conclusion.

As facial recognition software continues to proliferate, strategic considerations in evading it become imperative. Your face is increasingly identified in all facets of your personal life, leading to a

relinquishment of privacy and autonomy. Exercise judicious use of your facial data and remain vigilant. The prevalence of this software exceeds our collective awareness.

1. References.

Facial recognition system. En.wikipedia.org

- https://en.wikipedia.org/wiki/Facial_recognition_system

Face Recognition Software: Best-in-Class Enterprise Facial Recognition Security Platform. FaceFirst Face Recognition Software.

- https://www.facefirst.com/

Biometric Facial Recognition - FindBiometrics

- https://findbiometrics.com/solutions/facial-recognition/

Top 8 Ways Facial Recognition Software is Being Used Today - Tech Guru, LLC

- https://www.techguruit.com/top-8-ways-facial-recognition-software-used-today/

Facial Recognition Applications - Security, Retail, and Beyond: TechEmergence.

- https://www.techemergence.com/facial-recognition-applications/

Revealed: how facial recognition has invaded shops – and your privacy

the Guardian.

https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto

Hannah Williams. How is facial recognition used? Techworld.

- https://www.techworld.com/picture-gallery/tech-innovation/how-is-facial-recognition-used-3668674/

Home Garden. How Facial Recognition Systems Work. HowStuffWorks.

- https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition4.htm

Understanding Facial Recognition Software. The Franklin Institute.

- https://www.fi.edu/understanding-facial-recognition-software

RESEARCH · 9 December 2017

Data Privacy: Germany vs Switzerland

When evaluating data security among European countries, Germany and Switzerland emerge as standout choices. Here are the distinctions in terms of data security and related issues between these two nations:

Disclaimer: We are not affiliated with any of the mentioned companies; this article is based entirely on our independent findings. There is no affiliate marketing associated with the provided links below for your convenience.

How we write our reviews: For an impartial and comprehensive review, all apps undergo the following testing procedures:

- Real-time usage on actual projects.
- Evaluation by diverse team members situated in different countries.
- Testing on various devices and operating systems.
- A minimum of two weeks, with an average duration of four weeks.
- Peer review by multiple team members, followed by submission to the app's publisher for a final review.

In the current landscape, privacy has emerged as a contentious issue, with governments facing scrutiny for privacy infringements, and individuals or organizations illicitly obtaining sensitive information globally. Safeguarding this data has become imperative for businesses and individuals. The location of servers and service providers plays a pivotal role in ensuring the security of sensitive information. Given concerns about governmental monitoring in countries like America and China, many consider Europe as a preferable choice. In the realm of data security, turning to the developed world is often viewed as a prudent decision.

1. History, Culture and Mutual Agreements:

1.1 Germany:

1.1.1**Pros:**

- A troubled history marked by state surveillance, which remains prevalent within the government.
- A legacy of resistance against governmental oppression.
- A public stance firmly opposing the provision of information to foreign intelligence.

1.1.2**Cons:**

- Vulnerable to laws and pressures imposed by the EU.
- The German Intelligence Agencies are known for sharing data with other intelligence agencies.

1.2 Switzerland:

1.2.1**Pros:**

- Troubled history with pervasive state surveillance within the government.
- A culture of secrecy rooted in the banking sector.

- Not directly subjected to EU laws.

1.2.2**Cons:**

- Limited advancement in cyber-security legislation.
- Lack of specific legislation addressing cyber-security or cyber-crime.
- A history of government monitoring of private information of businesses and individuals.
- Switzerland maintains mutual legal assistance treaty relationships with the United States, obliging foreign governments to provide any information legally available to their local authorities upon request.

Germany has a severe history of state surveillance, leading to a pervasive wariness of government overreaches among generations of the German people. Switzerland also has a history with state surveillance, notably the secret files scandal of 1981. However, this scandal revealed mass surveillance rather than a prolonged experience of governmental oppression. Consequently, the impact of historical surveillance practices is more pronounced in Germany than in Switzerland.

1. National Laws:

2.1 Germany:

2.1.1**Pros:**

- Within the EU, data privacy regulations rank among the most stringent globally.
- The German Constitution guarantees citizens' right to privacy.
- Strict regulations mandate the storage of metadata only within the country.
- The Federal Data Protection Act (Bundesdatenschutzgesetz) is designed to ensure data security.
- General surveillance is prohibited by EU law.

2.1.2**Cons:**

- Laws allow data retention for up to 10 weeks, excluding emails.
- Specific statutes mandate the retention of business documents for 6–10 years.

2.2 Switzerland:

2.2.1**Pros:**

- Switzerland has generally stringent privacy laws.
- Not obligated by the EU to Pan-European agreements for data sharing.
- The Swiss Data Protection Act safeguards access to locally stored data.
- In cases where courts grant access to otherwise inaccessible data, parties must be notified and provided with an opportunity to contest.

2.2.2**Cons:**

- Swiss email providers are mandated to retain user data for a minimum of 6 months.In 2016, 65.5% of the Swiss voted in favor of a more stringent surveillance law.Switzerland is considering a revision to its data retention law (BÜPF) to extend the storage duration of all communication data (post, email, phone, text messages, IP addresses) to 12 months.

From a legal standpoint, Switzerland has established precedents that render communications and stored data there more sensitive to government and related party access. German laws are explicitly more protective of the privacy rights of individuals and organizations. In Switzerland, data security is more implicitly ingrained in the culture, subtle yet prevalent.

1. National Technology and Infrastructure:

3.1 Germany:

- Advanced IT infrastructure.

3.2 Switzerland:

Both Switzerland and Germany boast sophisticated IT infrastructures, with large areas dedicated to IT hosting. Switzerland, however, stands out with repurposed bunkers and underground tunnels providing impervious data storage. Additionally, Switzerland offers affordable electricity, resulting in lower overall costs, making it particularly appealing to larger organizations..

1. Sources

Secret files scandal:

- https://en.wikipedia.org/wiki/Secret_files_scandal

Switzerland votes in favor of greater surveillance:

- https://www.theguardian.com/world/2016/sep/25/switzerland-votes-in-favour-of-greater-surveillance

Telecommunications data retention:

- https://en.wikipedia.org/wiki/Telecommunications_data_retention#Switzerland

Federal data protection act in Germany:

- https://en.wikipedia.org/wiki/Bundesdatenschutzgesetz

Data Security in Switzerland:

- https://www.digitaltrends.com/computing/switzerland-data-security/

The EU's highest court rules against data retention:

- https://tutanota.com/blog/posts/eu-ruling-data-retention

MR. Robot uses Protonmail but it still isn't fully secure:

- https://www.wired.com/2015/10/mr-robot-uses-protonmail-still-isnt-fully-secure/

Swiss civil society struggles against digital surveillance laws:

- https://edri.org/swiss-civil-society-struggles-digital-surveillance-laws/

REVIEW · 7 July 2018

Myki Password Manager

Last Revised 07 July 2018.

Contents of this article.

1. Introduction.
2. What is Myki?
3. Pros.
4. Cons.
5. Conclusion.
6. Screenshots.
7. Criteria used for testing.
8. Introduction.

Managing multiple accounts across various platforms leads to the challenge of storing numerous passwords, causing significant frustration. Consequently, numerous password management services have emerged. Traditional password managers typically require online login to select and use a secret. However, Myki takes a unique approach by storing secrets directly on your phone, offering an added layer of security and convenience.

1. What is Myki?

Myki functions as an authenticator and password manager through its mobile app and compatible browser extension for Chrome, Opera, Safari, and Mozilla Firefox. To pair the app with the browser, users must scan a QR code. What distinguishes Myki from other password managers and authenticators is its unique approach: passwords are not stored on external servers or in the cloud; instead, they reside solely on your mobile device for added security.

Website: *https://myki.co/* (https://myki.co/)

1. Pros.

- Myki's interface is user-friendly and straightforward.
- Pair passwords with different computers via fingerprint or PIN code authentication.
- Myki refrains from storing browsing data, mouse, or keystroke logs (Testing Criteria: Zero-knowledge).
- Passwords are solely stored on your phone without any cloud backup (Testing Criteria: Zero-knowledge).
- Encryption secures all traffic between your phone, Myki servers, and browser extensions (Testing Criteria: End-to-end encryption and implementation).
- AES-256 encryption protects passwords exchanged between the phone and browser extension via QR code scan (Testing Criteria: End-to-end encryption and implementation).
- Public key cryptography authenticates users; the server verifies signed challenges unlocked by pin codes or fingerprint sensors (Testing Criteria: End-to-end encryption and implementation).
- Remote logout from computer accounts is possible through Myki's mobile app.
- Myki stores and auto-fills two-factor authentication tokens.
- In case of a data breach, Myki's lack of sensitive data storage prevents forced access (Testing Criteria: Zero-knowledge).
- No master passwords or passphrases are necessary.
- Unlimited pairing and login across various computers.
- Available on multiple devices - tablets, desktops, laptops (browser extensions), Android, and iOS (Testing Criteria: Multiplatform).
- Responsive customer support provided by Myki.
- Supports credit card integration for online autofill similar to password autofill.
- Encrypted password sharing among Myki users via peer-to-peer connection without revealing passwords (Testing Criteria: Zero-knowledge).
- Revocable access to shared passwords.
- App prevents screenshots during use.
- Chrome extension features a password creator for intricate and secure password generation.
- Multiple team accounts managed on one device with distinct permissions for agents, admins, departments, friends, or family, priced per user count within each team.

1. Cons.
    - Myki app inserts passwords into pages, potentially exposed to hacking or inspection by hackers, state-sponsored criminals, or knowledgeable users intercepting JavaScript execution for password retrieval.
    - Myki entails a high cost for usage.
    - Certain features are incompatible with older Android versions, such as the absence of the location feature in Android 6.0 Lollipop.
    - Screen recording applications pose a risk of capturing passwords or actions while using Myki.
    - Myki lacks open-source accessibility (Testing Criteria: open-source).

- Slow internet connections sometimes prevent saving newly created secrets from the dashboard.
- Unencrypted URLs are utilized for website icon retrieval, raising concerns about potential tracking activities.

1. Conclusion.

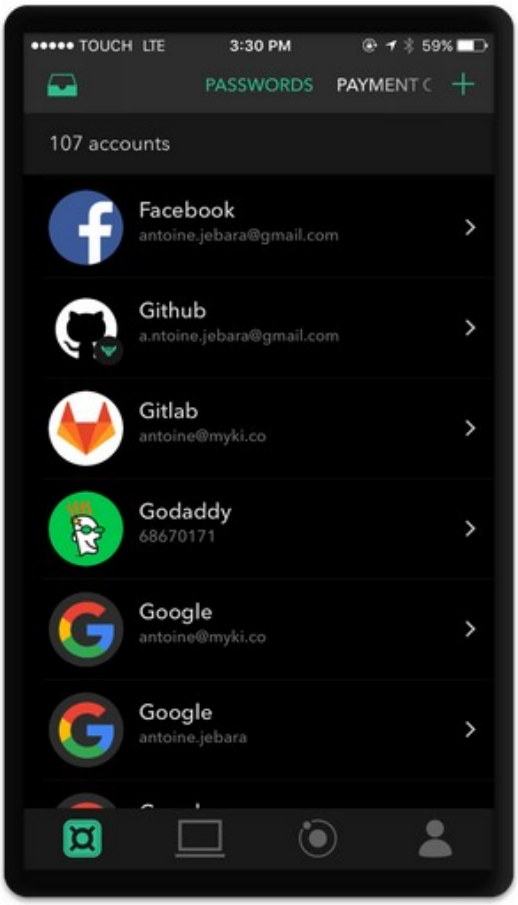
Myki effectively achieves its primary objective of ensuring passwords maintain a high level of complexity, making them challenging to decode, decrypt, hack, or access. The password manager's notable feature is its use of the phone to store passwords, providing assurance that sensitive information is not stored in the cloud or on remote servers vulnerable to breaches. This unique approach puts control directly in the user's hands.

Passwords can be easily viewed within the app, and users have the option to disable access even without physical contact with the phone. In the event of a lost or stolen phone, users can promptly revoke access to the device. However, a drawback is the lack of access to Myki's source code for independent review, as it is not open source.

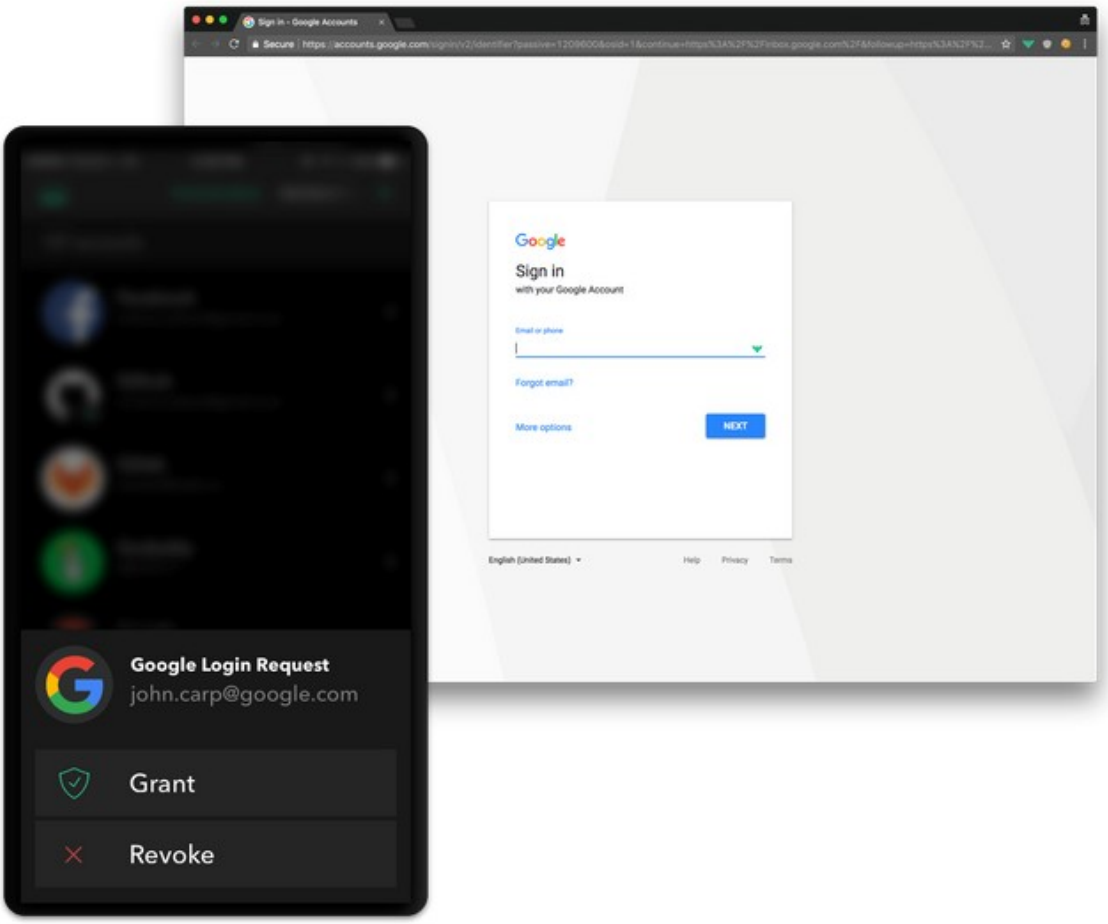
Myki also monitors various parameters such as physical addresses, IP addresses, geographic locations, login data, and battery levels through the administrative panel. This helps identify unusual activities or irregular behavior within the app. In the event of a potential hack, whether initiated by the user or external threats, Myki's administrators can swiftly perform a mass reset, issuing new passwords to all users. The app's responsive support staff promptly addresses reported bugs, further enhancing its reliability.

In conclusion, Myki receives high ratings and proves to be a suitable choice for both individuals and organizations.

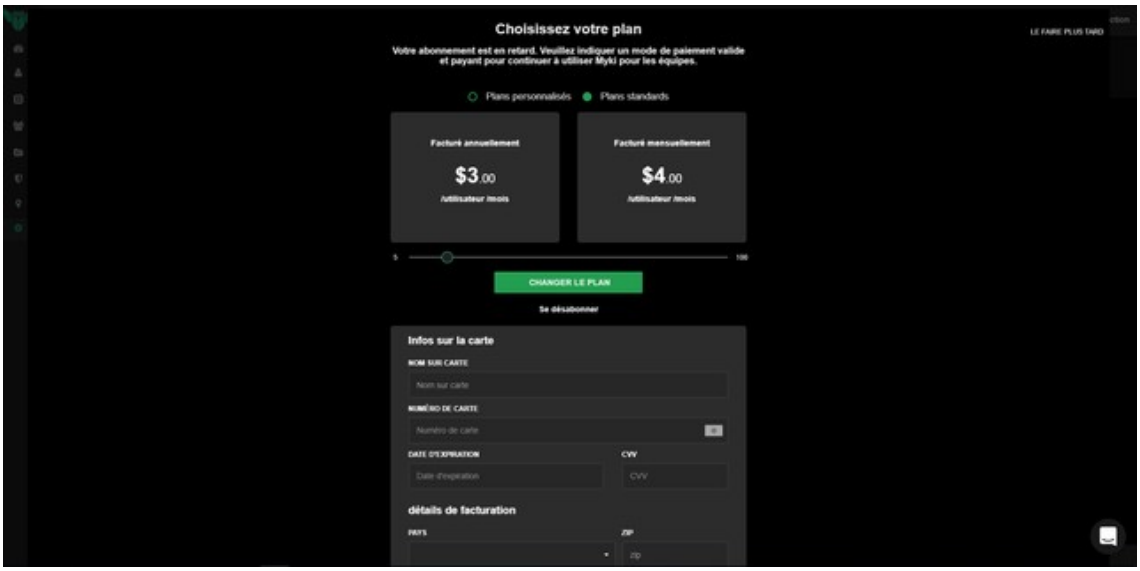
1. Screenshots.



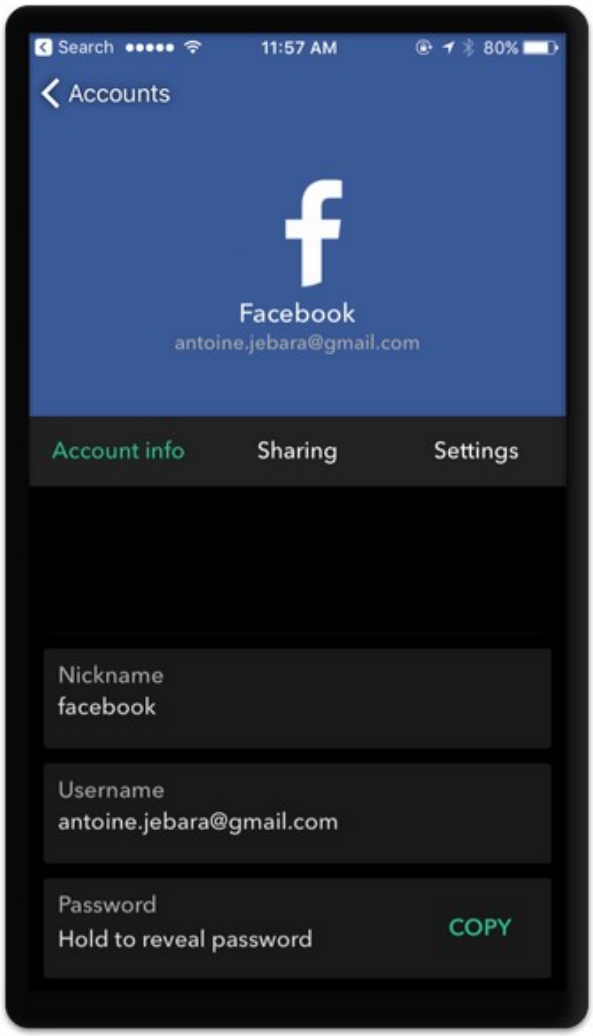
Screenshot 1: Myki UI.



Screenshot 2: Secret login request.



Screenshot 3: Sharing center.



Screenshot 4: Example of a secret.

2. Criteria used for testing:

• **Zero-knowledge:**Currently, Myki doesn't maintain complete zero-knowledge functionality. It retains metadata like auto-generated unique IDs for stored accounts, phone numbers for recovery, and shared account IDs for access revocation. However, Myki does not log browsing data, mouse movements, or keystrokes.

• **End-to-end-encryption and implementation:**Myki ensures robust end-to-end encryption by employing the AES256-CBC encryption algorithm, recognized as one of the most secure standards. This algorithm guarantees the safety of your data during transfers. The encryption key is shared exclusively between your mobile device and the browser extension via a QR code scanned through the Myki app's camera, ensuring that none of your encryption keys are transmitted over the web. The AES key, generated by your browser extension, establishes a visual connection with Myki. This method stands as a highly secure means to safeguard encryption keys.

• **Open-source:**Myki's lack of open-source accessibility stands as a significant drawback, limiting the ability to review or verify the contents of its source code.

• **Multiplatform:**Myki is accessible on mobile platforms, including iOS and Android. On desktops, it functions as an extension compatible with Google Chrome, Firefox, Safari, and Opera.

• **Resistance to state-sponsored criminals:**Individuals such as police officers and prosecutors, among others, pose a unique threat as their actions are often deemed legal due to corruption within state institutions, making them formidable criminals on both individual and national levels. Their ability to cover up illegal activities is concerning; they can intercept and read IMAP, POP3, TLS, and SSL communications. Additionally, they can spoof email provider SSL certificates and access SMS and emails, making recovery options vulnerable to exploitation. Therefore, it's crucial to utilize encryption software, encrypt devices, and consider purchasing hardware from locations outside the operational country.

1. Sources.

Myki For Teams - Product Hunt. (2018). Retrieved from: *https://www.producthunt.com/posts/myki-for-teams* (https://www.producthunt.com/posts/myki-for-teams)

Myki rolls out a password manager that locks all your info away on your phone. (2018). Retrieved from: *https://techcrunch.com/2016/09/13/myki-rolls-out-a-password-manager-that-locks-all-your-info-away-on-your-phone/* (https://techcrunch.com/2016/09/13/myki-rolls-out-a-password-manager-that-locks-all-your-info-away-on-your-phone/)

Password Fish - Product Hunt. (2018). Retrieved from: *https://www.producthunt.com/posts/password-fish* (https://www.producthunt.com/posts/password-fish)

Secure Offline Storage - Myki Password Manager. (2018). Retrieved from: *https://myki.co/features/offline-storage* (https://myki.co/features/offline-storage)

Solution, H. (2018). How Myki, with its cloudless solution, plans to be the death of the password. Retrieved from: *https://yourstory.com/2017/10/app-fridays-myki-death-to-passwords/* (https://yourstory.com/2017/10/app-fridays-myki-death-to-passwords/)

REVIEW · 4 December 2017

Seven 2FA Apps

We've tested 7 two-factor authentication apps. We need something that can be used across the organization.

Disclaimer: We are not affiliated with any of the mentioned companies. This article is exclusively based on our independent findings, and there is no affiliate marketing associated with the provided links below for your convenience. The apps are listed in alphabetical order.

How we write our reviews: For an impartial and comprehensive review, all apps undergo thorough testing:

- Real-time usage in actual projects.
- Evaluation by different team members across various countries.
- Testing on different devices and operating systems.
- A minimum of two weeks, typically four, trial periods.
- The article undergoes peer review by team members before being sent to the app's publisher for final review.

Background:

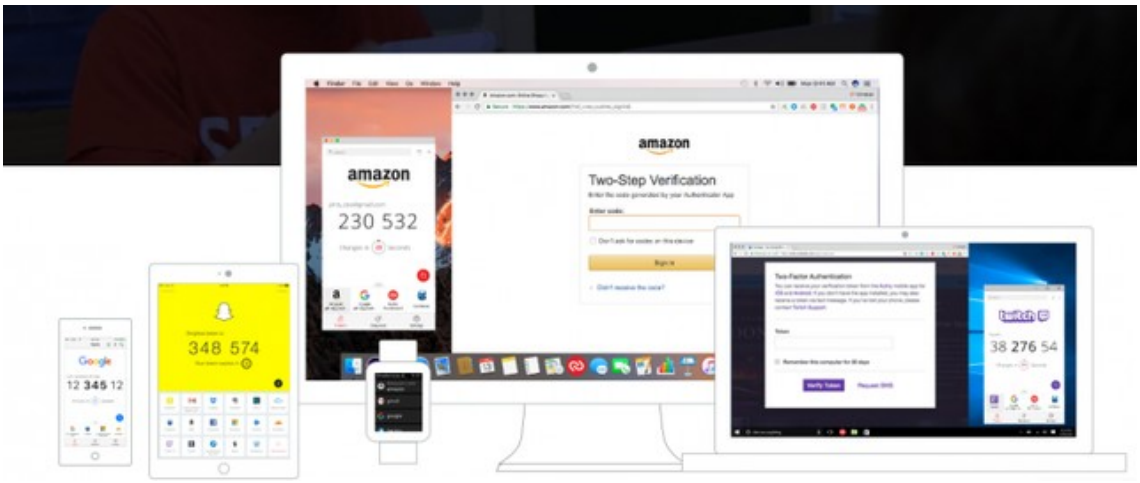
Two-factor authentication (2FA) is an advanced method for device or system authentication, employing two or more verification levels, as opposed to a single login-password. This single factor is vulnerable to hackers or state-sponsored criminals using brute force attacks. While many associate 2FA with one-time passwords via text messages, this method, if predominant for web services, poses high insecurity. Various, more secure approaches to achieve 2FA exist. It is akin to securing a door with two padlocks: one being the conventional login-password, and the second being an alternative method. While additional padlocks can be employed, it elongates the door-opening process, making it prudent to start with at least two.

Our specifications sheet:

- Ensure broad platform coverage (Windows, iOS, Android OS, Clouds, social media like Facebook, Twitter).
- Provide diverse 2FA options, including email authentication apps and hardware keys.
- Prioritize offline functionality.
- Allow disabling of less secure SMS 2FA, voice messages, and fingerprint options prone to interception or brute-force attacks by hackers and state-sponsored criminals.

01-Authy.

Authy is a free application designed to capture 2FA tokens from widely used web services. It also serves as a client for the Twilio 2FA API, streamlining the implementation of two-factor authentication for companies such as CloudFlare, Twitch, and SendGrid.



Website: *https://authy.com* (https://authy.com/)

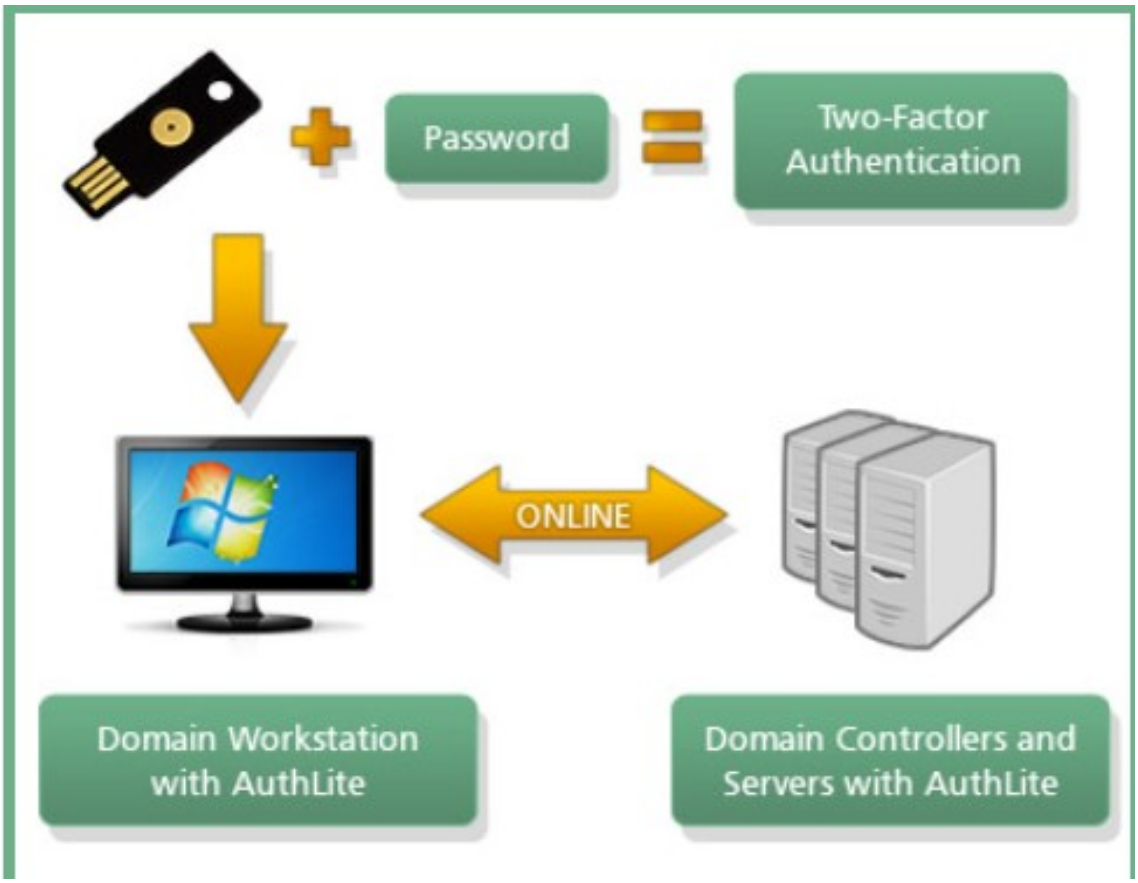
1.1 Pros:

- Authy is available on common platforms like iOS and Android, with a desktop client for Windows and Mac OS, and Linux support forthcoming.
- It captures 2FA tokens from popular services such as Facebook, Google, and Twitter
- Offering guides at authy.com/guides.
- The app collaborates with the Twilio 2FA API, providing codes and push-based authentication.
- Multiple device authentication is supported, allowing use across various devices. In case of loss or retirement, deauthorization and reauthorization are swift, via SMS/voice or more secure app methods.
- Backup tokens functionality prevents access loss if the authorized device is misplaced.
- The app allows disabling of SMS and voice call authentication, provides offline authentication, and ensures easy installation.

1.2 Cons:

- The app is free for use with services like Twitter and Snapchat. However, integrating a comprehensive 2FA solution into your application comes with a cost. The pricing is budget-friendly, with the first 100 authentications per month being free. Beyond that, you can opt for a pay-as-you-go model at $0.045 USD per authentication. For 300 authentications monthly, the cost is 13.5 USD.

02-Authlite.



Website: *http://www.authlite.com* (http://www.authlite.com/)

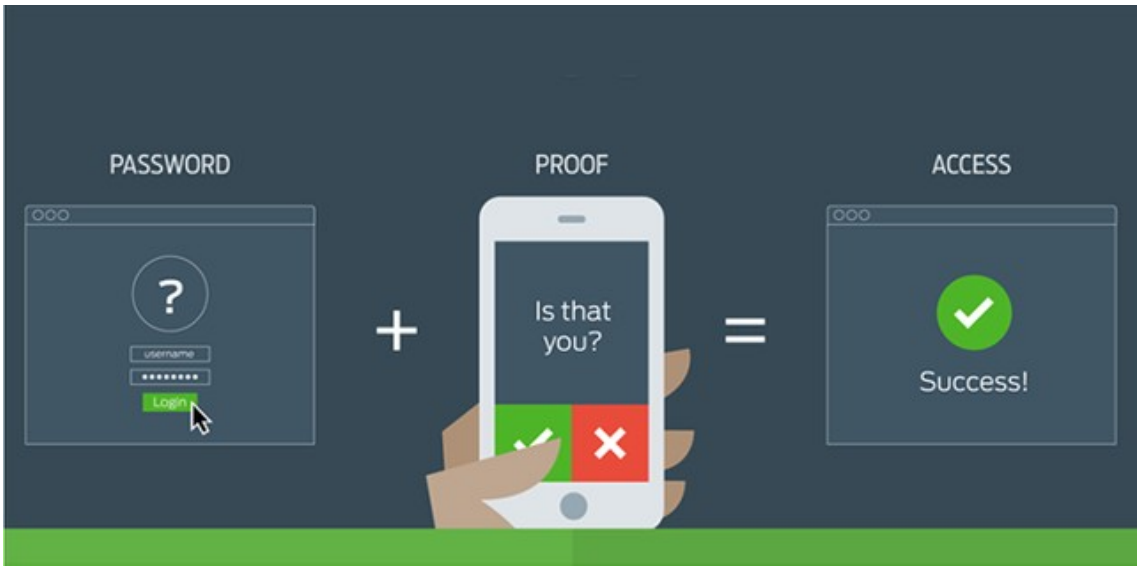
2.1 Pros:

- AuthLite provides offline authentication capabilities. It can utilize any OATH token, including smartphone soft token apps like Google Authenticator, potentially reducing costs compared to YubiKey usage. Especially for larger user volumes, the pricing is significantly lower than $48 per user. AuthLite can enforce two-factor authentication for any authentication linked to Active Directory, including systems utilizing ADFS for federation into AD.

2.2 Cons:

- AuthLite is a lightweight solution with a narrow focus on specific authentication types: Windows authentication, RDP authentication, and VPN. For two-factor authentication, a Yubikey USB stick is required. However, this may not be practical, as it poses the risk of being lost, potentially resulting in device access loss. The price is relatively high compared to the features offered, at 48 USD per user for a lifetime license and an additional 30 USD for the Yubico Key Token, totaling 70 USD.

03-Duo.



Website: *https://duo.com* (https://duo.com/)

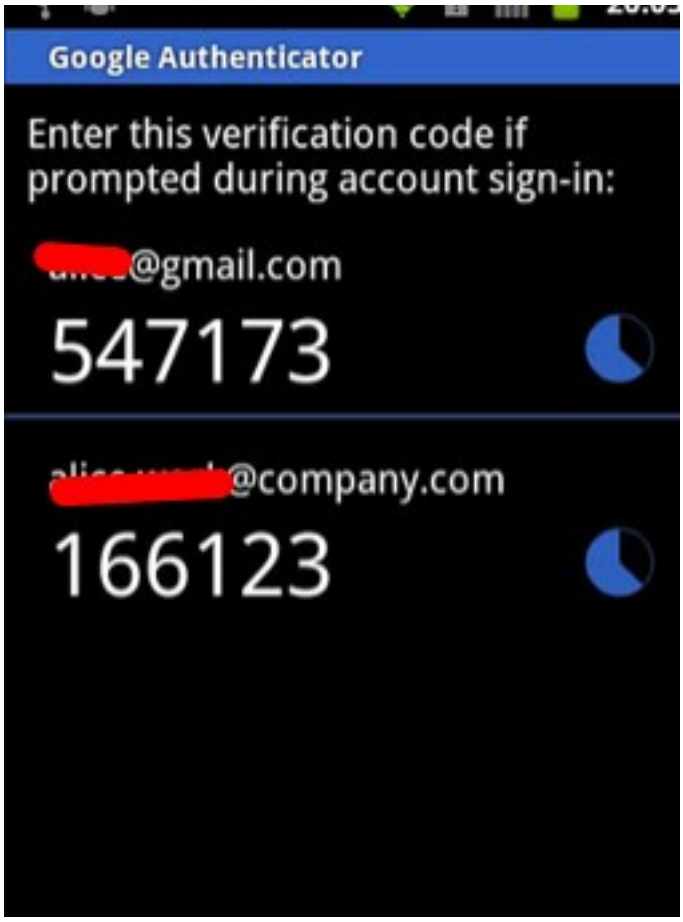
3.1 Pros:

- The application enjoys broad support across various platforms, including Windows, VPN, SSH, and Cloud. It features a robust centralized user console for effective user and device management. In case of a lost, stolen, or retired device, swift deauthorization can be done from any authorized device. The system offers multiple authentication forms and provides the option to disable SMS or voice call authentications.

3.2 Cons:

- The application lacks support for mobile operating systems such as Android and iOS for 2FA. The pricing for the package intended for use in high-risk countries is steep, at 6 USD per user per month. Additionally, the support team indicated that "offline authentication" doesn't function optimally, as devices need to be connected to the internet.

04-Google Authentication.



Website: *https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2* (https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2)

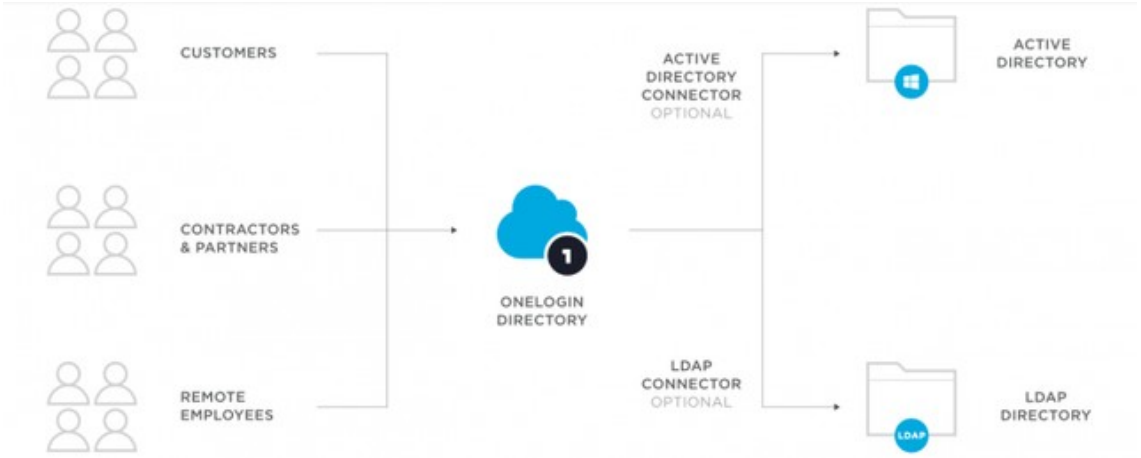
4.1 Pros:

- The system offers 2-Step Verification through SMS text message or Voice call. It allows code generation using a mobile device and supports offline authentication through the Google Authenticator app, ensuring receipt of codes even without an internet connection or mobile service. The service is available for free.

4.2 Cons:

- The authentication tool is utilized for signing into various accounts, including Google, Facebook, Tumblr, Dropbox, vk.com, and WordPress. For Windows logins, a third-party application integrated with Google Auth must be sought. Limited to one device per account, it lacks a backup recovery option in case of mobile loss or confiscation by law enforcement.

05-Onelogin.



Website: *https://www.onelogin.com* (https://www.onelogin.com/)

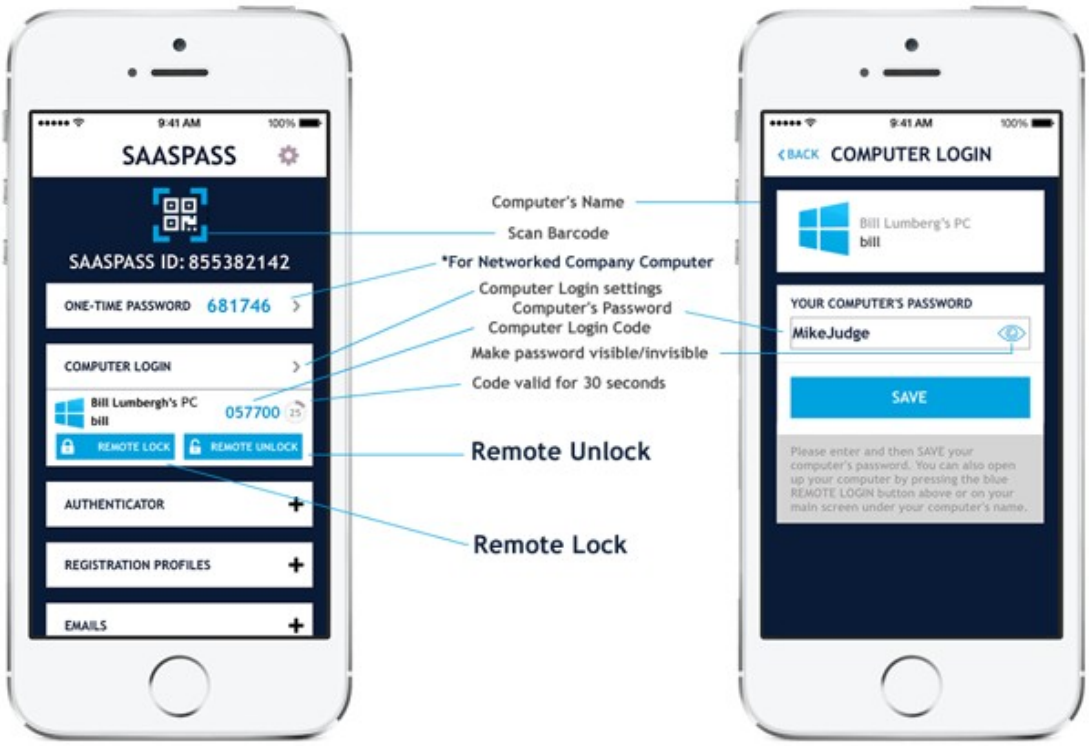
5.1 Pros:

- Price is affordable.
- It has a centralized reporting for the users 48 USD/year.

5.2 Cons:

- This solution operates as a centralized IT system, requiring an in-house IT staff and integration with an Active Directory, achievable with a single click. However, for our globally dispersed agents without a centralized setup, this becomes a drawback. The availability of offline authentication is not explicitly mentioned. It appears to primarily support desktop operating systems (Windows and Mac OS) and applications.

06-SAASPASS.

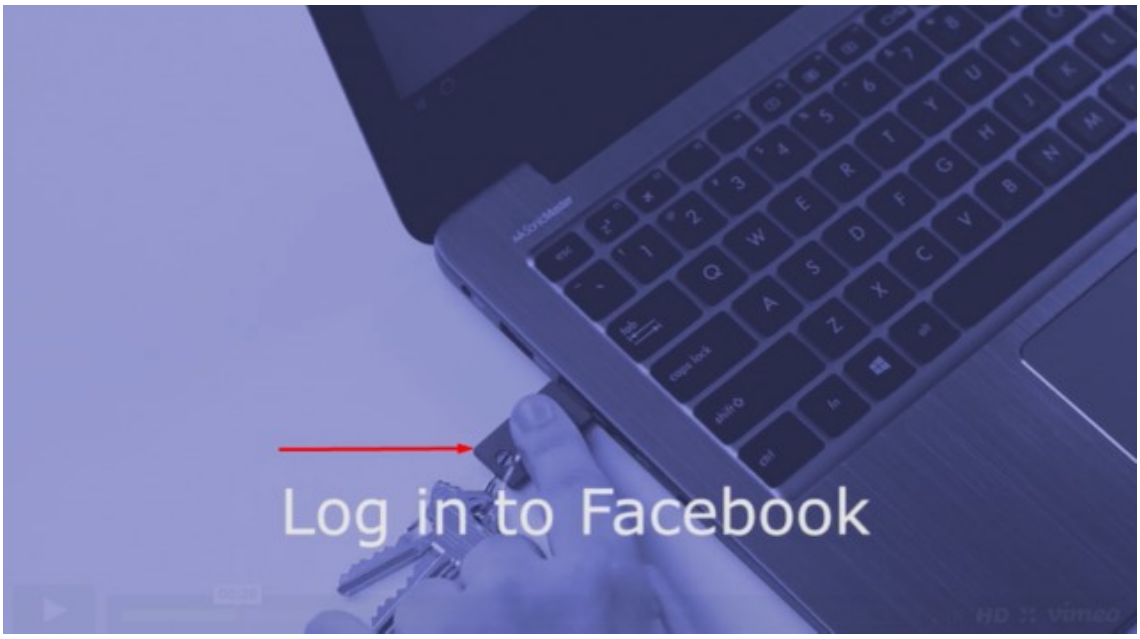


Website: *https://saaspass.com* (https://saaspass.com/)

6.1 Pros:

- Covering an extensive range of platforms, it requires a smartphone for operation, including iPhone, Android, Apple Watch, Android Wear, Blackberry, Windows Phone, Java ME, iPad, iPad Mini, Android Tablet, Windows Tablet, Mac OSX, Windows OS, Mac Mini, Wearables, Google Glass, and Kindle. This solution supports numerous platforms and applications for 2FA, facilitating multiple device authentications. Swift deauthorization is possible for lost, stolen, or retired devices. It provides token backup to prevent access loss due to device misplacement. With multiple authentication forms, including Touch ID, it offers options to disable SMS, Voice call, and fingerprint authentication. Offline authentication is supported. The pricing is more economical than other solutions, with a free package available, albeit with limited features. For a high-security profile with globally dispersed agents, packages costing around 20 USD/year and 40 USD/year are available. Installation is straightforward.

07-Yubico (Yubikey).



Website: *https://www.yubico.com* (https://www.yubico.com/)

7.1 Pros:

- This solution spans various platforms, including Windows desktops (with Linux support coming soon), iOS, Android OS, selected cloud storages, and web platforms like Facebook and Twitter. It facilitates multiple device logins and offers offline authentication. The cost is budget-friendly, approximately 50 USD per USB token (Yubikey). Installation is straightforward.

7.2 Cons:

- This solution relies solely on USB authentication using Yubikey. If the Yubikey is lost, stolen, or confiscated by the government, there is a significant risk of losing access to both applications and devices such as computers and mobiles. Unfortunately, there is no option to backup tokens.

1. Conclusion:

Two-factor authentication significantly mitigates threats by necessitating more than just password access, making it unlikely for attackers, including state criminals, to possess the associated physical device. The added layers of authentication enhance system security.

Among the mentioned apps, all excel in providing an extra layer of protection. They support mobile tokens, offer diverse flexible authentication methods, and undergo additional analysis for some. Differences emerge in pricing, packaging, multi-device installation, offline authentication, app support, user-friendliness, and SMS option disablement. Considering these factors, SAASPASS stands out as the primary solution, followed by Authy as the secondary choice.

REVIEW · 12 November 2017

Encryptr App

There are specific use cases where Encryptr is the best solution. We explain this in this article.

Disclaimer:We have no affiliations with the mentioned companies; this article is entirely based on our independent findings. There is no affiliate marketing associated with the provided links for your convenience.

How we write our reviews: For an impartial and comprehensive review, all apps undergo rigorous testing:

- Real-time usage on actual projects.
- Evaluation by team members from diverse locations.
- Testing across various devices and operating systems.
- Minimum two-week, typically four-week, trial periods.
- Peer review by team members, followed by submission to the app's publisher for final review.

In our article evaluating password managers for business use, we included Encryptr, despite its limitation of lacking a sharing feature suitable for groups. A detailed description of Encryptr can be found on Spideroak's website. It's essential to note that while Encryptr may not be suitable for group usage, there are specific use cases where it stands out as the best solution.

1. Use cases:

- To transmit data anonymously.
- To back up selected credentials not intended for inclusion in your primary password manager without registering with an additional provider.
- To synchronize specific data across your devices.
- 2. Specifications of Encryptr:
- End-to-end, zero-knowledge encryption (Note 01).
- Open source (Note 02).
- Auto log off.
- Intuitive.
- Free.
- Cross-platform (Note 03).
- Can share notes as well.
- No recovery option.
- Offline access which is sensitive to device theft as it stores data on APPDATA folder (Note 05).

1. Example for passing on data anonymously:

Step 1:

- Create a specific login-password combination for the data you want to pass on.

Step 2:

- Give this combination to your addressee.

Step 3:

- Once the addressee has confirmed he/she has access to the Encryptr, delete it from your computer.

1. Pros and Cons in this use case:

4.1 Pros:

- Your recipient is not required to create an account with a password manager provider.
- The application is user-friendly, requiring no learning curve for your recipient.
- Encryptr is downloadable at no cost and anonymously, eliminating the need for registration with SpiderOak.
- Being cross-platform allows usage with individuals irrespective of their computer preferences.
- Not only can login credentials be shared, but also notes.
- The transfer lacks direct real-time communication between parties, reducing interception risk by minimizing communication events.
- The absence of recovery options (SMS or email) decreases the attack surface for state-sponsored criminals (Note 04).

4.2 Cons:

- Data is stored locally on your computer, which poses a potential hacking risk (Note 05). Ensure your hard drive is consistently encrypted. After concluding use with Encryptr, delete it by accessing the APPDATA folder and utilizing a freeware tool like Privazr for Windows.

1. Notes:

(1) Zero knowledge encryption necessitates storing the key on the user's device to ensure protection against state-sponsored criminals. While this doesn't eliminate the possibility of government access to plain text messages, it would require active hacking of the user to obtain the necessary password.

(2) While open source doesn't guarantee a thorough code audit for backdoors or weaknesses, it does demonstrate a commitment to transparency. The source code of Encryptr is accessible..

(3)Must be accessible across iOS, Android, Windows, Linux, and Mac desktops. Exclusion of Windows phones and Blackberry is due to limiting options, as finding a compatible solution for these platforms is nearly impossible.

(4)Police, prosecutors, and similar officials can engage in ostensibly "legal" crimes by corrupting state institutions, posing a significant threat to individuals and nations. Their ability to conceal illegal actions is concerning, including the interception and reading of IMAP, POP3, TLS, and SSL. They can also spoof your email provider's SSL certificate and access your SMS and emails, turning recovery options into easy attack possibilities. Therefore, it's crucial to consistently use encryption software, secure your devices, and obtain hardware from outside your operating country.

(5) There are specific software designed to crack these password managers, for example Elcomsoft: *https://blog.elcomsoft.com/2017/08/one-password-to-rule-them-all-breaking-into-1password-keepass-

lastpass-and-dashlane/* (https://blog.elcomsoft.com/2017/08/one-password-to-rule-them-all-breaking-into-1password-keepass-lastpass-and-dashlane/)

GUIDE · 11 January 2024

Privacy Upgrade

A list of easy to use software to preserve your online privacy:

Hard Drives: The Samsung 850 Evo Pro Self-Encrypting SSD serves a specific purpose: instant Bitlocker activation. Without it, encrypting a new drive could take approximately 3 days per terabyte. However, caution is necessary—a Self-Encrypting Drive (SED) must comply with TCG Opal standards for Bitlocker compatibility. Even with compliance, specific software is essential. Exclusive to the 850 Pro model, utilizing Samsung Magician in e-drive mode offers the unique capability of activating Bitlocker immediately upon unboxing.

OS for beginners: Windows 10 Pro offers easy upgradability in just three clicks and comes equipped with Bitlocker, ready for activation on drives and thumb drives. Activation isn't mandatory to use Bitlocker, although it prompts an occasional overlay at the bottom right of your screen, which can be somewhat bothersome.

OS for advanced users: Kodachi (Linux) stands out as the optimal operating system for privacy, and it's entirely free. It's built on Linux Ubuntu, offering the advantage of encrypting the entire hard drive during the installation process.

Windows Antispy: WPD (Windows Privacy Dashboard) is a convenient tool for several reasons: it automatically updates, is free, user-friendly, offers IP-based firewall rules, includes an App uninstaller, and doesn't require installation on your computer.

Firewall: GlassWire's paid version provides a compelling feature: the "Ask to Block" function, granting absolute one-click control over your traffic. However, it's crucial to note that due to its utilization of the Windows firewall, the paid version might not be compatible with antivirus software that incorporates its own firewalls, such as Bitdefender.

Email: Tutanota (freemium) Why: Read our article: Tutanota vs Protonmail. Alternatively: Protonmail.

VPN: ExpressVPN is renowned for its speed and operates from RAM memory, ensuring no logs are retained. Additionally, it seamlessly integrates with DDWRT routers, safeguarding all traffic across your entire home network.

Primary Browser: Firefox, Waterfox, Opera GX. You can enable DNS-over-HTTPS.

Password manager: Zoho Vault (freemium). To understand why we use it, Read our article: 13 password managers.

Messaging, Voice and video calls: Threema, available on a freemium model, stands out due to its open-source, end-to-end encryption and zero-knowledge policy. It's resilient against state-sponsored threats and operates from Switzerland (unlike Wire and Wickr, which are currently based in the US). For further insights, we recommend exploring our article outlining Threema's pros and cons.

SMS: Don’t. If you have no choice, use Silence on Android (free). It offers encryption over GSM network.

File sharing: through links (think dropbox): sync.com (free). It offers end-to-end, zero knowledge encryption. Granular control with the paid version.

File Synchronization Inter-device synchronization is efficiently managed through Resilio Home (freemium). It excels in supporting encrypted read-write folders, ensuring secure synchronization with both home and off-site servers for your data, which remains fully encrypted throughout the process.

Disk Cleaning: Bleachit is versatile, functioning seamlessly on both Windows and Linux platforms. Alternatively, Privazer (free) is an excellent choice, specifically for Windows users. Privazer offers a one-click solution to thoroughly clean your entire system.

Anonymous Browser:TOR (free). We recommend you use this as your primary browser.

Anonymous Chat App: Briar, available exclusively for Android, stands out for its exclusive use of the TOR network. Additionally, it boasts the capability to host both forums and blogs within its platform.

Useful Links:

- https://prism-break.org/en/
- https://privacytoolsio.github.io/privacytools.io/
- CIA tools released by Wikileaks: https://wikileaks.org/vault7/
- NSA tools released by Shadowbroker: https://github.com/misterch0c/shadowbroker
- Scanning Service against NSA's Doublepulsar malware: https://doublepulsar.below0day.com/

GUIDE · 5 February 2015

Pseudo-anonymous Google Account

Pre-requisites:

1. Use a disposable GSM phone to receive SMS validation codes.
2. Use an anonymous and secure email service provider like Tutanota.
3. Employ a password manager to enhance security.
4. Ensure secure internet browsing by using a VPN for your connection.

Step 1. Get ready:

Get your desktop ready, do not attempt this from an Android device (note 5).

- Have your VPN active.
- Have a notepad open.
- Now move on to step 2.

Step 2. Sign up:

- Please note down the following in your notepad: date, time, and VPN location (note 3).
- Proceed to Google's signup page: https://accounts.google.com/SignUp?hl=en
- Enter a fictitious first name.
- Enter a fictitious last name.
- Select "I prefer to use my email" and input your Tutanota email.
- Create a robust password; exceeding 24 characters.
- Store this in your password manager, clipboard, or notepad.
- Provide a Birthdate: 01 January 1980 or a date more than 18 years ago.
- Choose "rather not say" for Gender.
- Input your burner GSM cell phone number for the Phone field.
- Leave the Location field as is; it may differ from your VPN or burner GSM phone location, which is inconsequential.
- Validate the validation code sent by Google via SMS.
- Validate the email verification sent to your Tutanota email by Google.
- Add to your notepad: date, time, VPN location.
- Save your notepad.
- Save all information in your password vault manager.

-

Step 3. Remove number from account:

- Access "My account" located in the upper right corner.

- Navigate to "Your personal info" within the Personal info & privacy section.
- Select the "Phone" field.
- Click on the edit icon (pen) situated next to the phone number.
- Re-enter your password when prompted.
- Click the edit icon (pen) once more.
- Choose "Remove phone number" and confirm the action by clicking again.
- Expect to receive an email from Google as a security measure; you can disregard this email.
- Now, your cell phone is available for activating another Google account.

Step 4. Deactivate tracking features:

- Do the Privacy Checkup. Deactivate everything.
- Shared endorsement.
- Ads settings.

Step 5. Deactivate Google and Tutanota:

- Upon completion of tasks with your Google account, deactivate it via My Account -> Account Preferences -> delete your account or services.
- Additionally, deactivate your linked Tutanota account to thwart potential Social engineering attacks.

Notes:

(1) In the current landscape, Google frequently requests a phone number. It's crucial to recognize that to Google, users serve as the product. To safeguard your privacy and outmanoeuvre Google's algorithms, frequent changes to your Google account and avoiding its association with your phone number are advisable strategies.

Maintaining separate Google accounts simplifies the management of multiple devices. When using burner phones, creating a corresponding burner Google account becomes necessary. This account should also be applicable for platforms like Facebook, Twitter, LinkedIn, etc. Moreover, Android phones require a Google account for access to the Play Store.

(2) Disposable email services have a limited validity of 48 hours, posing issues particularly when using VPNs. Google often restricts access for security purposes and sends security codes to recovery email addresses. We recommend opting for Tutanota due to its resilience against state-sponsored threats and its non-reliance on GSM numbers. Supporting Tutanota through a premium account, even for burner emails, is encouraged.

(3) Creating strong credentials necessitates using a password generator. Remembering all signup details is crucial as Google might request them during account recovery processes.

(4) Utilizing services that conceal your IP address is essential to safeguard your location and identity. Protonmail (https://protonvpn.com/about) is a reputable option available for purchase online.

(5) Activating from an Android device might prompt a Gmail email requirement, which compromises privacy. Moreover, obtaining a VPN on the device without Google Play poses challenges in creating a strong password and other security measures.

Part II

Secure & Encrypted Communications

RESEARCH · 8 December 2017

SIM, Backdoors and Security

How to safeguard your phone from state-sponsored criminal attacks: This article covers essential information on defending against SIM backdoors.

Disclaimer:We are not affiliated with any of these companies; this article is solely based on our findings. There is no affiliate marketing through the links provided below for your convenience.

How we write our reviews: For an unbiased and comprehensive review, all apps undergo testing in the following ways:

- In real time, actively used on genuine projects.
- By various team members across different countries.
- On different devices and operating systems.
- For a minimum of two weeks, typically four weeks on average.
- The article undergoes peer review by team members and is then sent to the app's publisher for final review.

1. This is an informational guide for:
    - Security concerns regarding SIM cards in your mobile device.
    - Explore SIM attacks and their occurrence.
    - Learn how your SIM card can serve as a gateway for spying or information theft.
    - Discover preventive measures against data acquisition by state-sponsored criminals.

1. Reviewing SIM security concerns and attacks

SIM cards are susceptible to attacks from both your phone carrier and external sources, posing a risk to much of your information if access falls into the wrong hands.

- Billing information may be accessed or tampered with.
- Malware or malicious apps might be uploaded to your mobile device from external sources.
- State-sponsored criminals can exploit your SIM to track you, access your data, or inject unwanted advertisements and apps onto your device.
- Similarly, information and apps can be removed from your device without your knowledge or consent.
- SIMs typically have a predictable default PIN, making them susceptible to hackers.

> Your phone’s lock does not keep criminals from being able to access your SIM and tamper with your mobile device.

- The frequency of robocalls and spam calls has surged in the past year, showing no signs of slowing down. This increased volume makes your device more vulnerable to computerized calls that could attempt to access your data and personal information.

1. How your SIM can also be compromised

- Your SIM can be compromised through text messages and missed calls, even on a non-Android or iOS device, using Flash SMS or silent SMS (note 1).
- If you miss a call from an unknown number with a different country code, refrain from calling back to prevent potential SIM cloning by criminals in other countries.
- A cloned SIM can exploit your data plan, escalating your plan costs and using it illicitly for other purposes.
- The text message SIM concern, exposed in 2013, persists; avoid responding to text messages from users claiming to be your service provider.
- Changing wireless providers also poses risks; while SIM cards are configured with the original provider, the APN (note 3) can be altered by the new carrier using OTA (note 2).
- When your SIM is transferred to a new carrier, the original carrier retains your SIM's information, meaning the company can still be maintaining access even without an active contract or service plan.
- This allows the former carrier to track your current data plan, sending marketing materials and advertisements to entice you back. They may even contact you directly to inquire about the switch. Additionally, the previous carrier could tamper with your device's applications or upload software without your knowledge or permission (note 3).

1. Protecting your SIM card

4.1 Replace your SIM card.

- Consider using burner phones; refer to our article on GSM burner phones GSM burner phones.
- Information may take months to reach the SIM card registry.
- Cheap SIM cards are available for purchase online.
- In the US, this method is limited, as only certain carriers use removable SIM cards.
- Regularly replacing your SIM card makes it challenging for state-sponsored criminals to link you to your mobile device.
- Contact your carrier to transfer your phone number to the new SIM card, or consider obtaining a new number.

4.2 Do not click on anything suspicious.

- Mobile technology advancements have transformed phones into pocket computers. Cellphones, due to users not taking equivalent precautions as with computers, have become prime targets for hackers. Avoid clicking on phone pop-ups or alerts stating phone compromise. Refrain from responding to suspicious or unknown text messages or phone calls, especially those claiming to be from a company.

4.3 Pay attention to the apps you download.

- Download apps exclusively from reputable developers; unknown or recently emerged developers pose unnecessary risks. If an app requests illogical permissions on your phone, it raises security concerns. For example, a photo app seeking picture access is logical, but access to contacts is questionable. If an unfamiliar app appears on your device, check with your carrier to verify if it's a service update (note 2); otherwise, your SIM may be compromised. Google and Android devices are more vulnerable due to open app stores; Apple's restricted app accessibility limits potential malware

downloads. Exercise caution with pop-ups or downloads on your mobile device, similar to your approach on a standard PC or laptop.

4.4 Watch out for public Wi-Fi.

- Connecting to public Wi-Fi exposes your mobile device to potential hackers. With your phone's GPS signal indicating your location at any moment, state-sponsored criminals, including your current or previous mobile provider, can track you. Password-protected public Wi-Fi, with several strangers using it simultaneously, poses risks. Even novice hackers can identify users on the network, jeopardizing your device and information.

4.5 Update your device.

- Carriers regularly update security information upon discovering new malware, enhancing device security.
- Promptly installing security updates from your provider is crucial.
- Avoid delaying or ignoring updates to prevent potential attacks on your device.
- New devices are equipped with the latest protections against criminals.
- However, as criminals keep abreast of security updates, they continually devise new methods to target mobile device users.

4.6. Lock your SIM card.

- Locking your phone is distinct from securing your SIM card.
- The SIM card holds vital data, including your phone number, billing information, security data, and other details about you and your phone activity.
- Merely removing the SIM card is ineffective, as your phone won't function without it.
- To secure your SIM card, refer to the information below.

4.6.1 How you can lock your SIM Card.

Step 1:

Depending on your provider, you need to locate your PIN Unlock Key (PUK).

For AT&T users:

1. Access your AT&T account in a browser.
2. Navigate to the myAT&T tab.
3. Click on your mobile device.
4. Choose "Unblock SIM Card."
5. You will then be directed to a new page where your PUK is listed.

For Verizon users:

1. Access your Verizon account in a browser.
2. Choose the "I Want To" section,
3. Then click on the "More Actions" button.
4. Navigate to "Phone Details" under devices.

5. Select "Unlock SIM," where your PUK and the card's default PIN should be displayed.

For other carriers, check your account online or contact them to obtain your PUK and default PIN for the SIM. While many default PINs are either 0000 or 1111, variations exist. The PUK becomes necessary only if you incorrectly enter the PIN three times.

Step 2:

> Now, you can secure your SIM:

> 1. In your mobile device’s settings, access the security option.

> 2. Find the "Setup SIM card lock" option.

> 3. Choose "Lock SIM card."

> 4. Input the default PIN.

> 5. Select "Change SIM PIN."

> 6. Reenter the default PIN and confirm.

> 7. Enter a new 4-digit PIN.

> 8. Confirm the new PIN.

> 9. Restart your mobile device and input the SIM PIN when prompted.

4.6.2 Locking a SIM on an iPhone.

SIM cards on iPhones appear differently than on other mobile devices but can still be secured. Follow these steps:

1. Open the Settings app and go to Phone.
2. Scroll down to SIM PIN.
3. Enter the default SIM PIN provided by your carrier.

By taking these steps, you make your SIM's identity inaccessible, preventing unauthorized access to your SIM or phone information. This safeguards against a previous carrier accessing your SIM to gather information about your current carrier or extract personal data. Note that this protection does not extend to your current carrier, which retains access to your information.

A workaround to prevent a previous carrier's access is to use a dumb phone with a secured SIM, limiting external access to your phone. Caution: Incorrectly entering your SIM card’s PIN three times or entering the wrong PUK may permanently lock your SIM. Without a functional SIM, your mobile device won't operate, as the carrier can't verify a service plan. If a breach is detected, your carrier may shut down your SIM to protect your information even if you trying to access it. In such cases, visit the nearest carrier location to replace your SIM, and obtain your SIM’s PIN and PUK to avoid future issues.

1. Notes

(1) A Flash SMS is a type of SMS that directly appears on the main screen without requiring user interaction and is not automatically stored in the inbox. This feature proves useful in emergencies, such as fire alarms, or in cases where confidentiality is crucial, such as delivering one-time passwords.

(2) OTA, or over-the-air update, on modern mobile devices like smartphones, refers to a software update distributed over Wi-Fi or mobile broadband. This update is facilitated by a function embedded in the operating system, eliminating the need for the user to connect the device to a computer via USB for the update. The "over-the-air" aspect highlights its reliance on wireless internet connectivity.

(3)An Access Point Name (APN) is the gateway name connecting a GSM, GPRS, 3G, or 4G mobile network to another computer network, often the public Internet. For a mobile device to establish a data connection, it must be configured with an APN, which it presents to the carrier. The carrier then assesses this identifier to determine the specifics of the network connection to be established. This includes assigning IP addresses to the wireless device, deciding on security methods, and determining whether and how it should connect to a private customer network.

RESEARCH · 28 November 2017

SIM Attacks

The truth about real-life SIM attacks.

We frequently encounter accounts recounting security breaches affecting mobile users, resulting in infringements upon their privacy. The challenge lies in the dissemination of these narratives, which often undergo multiple retellings, ultimately leading to their distortion into urban legends or exaggerated versions of the original events. Unfortunately, the perception of these incidents as mythological has enabled telecommunication companies and state-sponsored actors to exploit privacy vulnerabilities without facing consequences.

We have curated a selection of genuine accounts that underscore the susceptibility of mobile users' SIM cards to breaches. It is essential to acknowledge that SIM cards store sensitive information, including call records, personal data, and geolocation. Presented below are illustrative examples that emphasize the necessity for heightened vigilance in understanding the extent to which our privacy is compromised on a recurring basis.

1. Data Uploading While Device is Off: The Background

In this instance, a user residing in France possessed an iPad Air LTE equipped with a SIM card. The national mobile carrier in France, Orange, was the service provider for this individual, making this scenario relevant to any Orange subscriber.

The user encountered connectivity issues while vacationing in Spain, unable to access the local 4G signal despite expectations set by the carrier. Upon returning to France, the problem persisted as the iPad failed to connect to the French network. Consequently, the user sought assistance from Orange customer service.

Upon contacting Orange, the user was advised to power off the device to facilitate the uploading of the appropriate SIM settings. Following this instruction, the device successfully connected to the network upon rebooting.

1.1 Conclusion

In this situation, it was discovered that the carrier had access to the user's SIM card even when the device was powered off. This indicates that some form of signal is emitted even when the device is not operational. The concerning aspect of this is that both the carrier and potentially state-sponsored criminals could access the user's SIM card without permission or knowledge, even on an iOS device.

Unfortunately, much of the information stored on a SIM card cannot be altered or removed as it is part of the carrier network. However, there are some measures that users can take to exert control over their SIM card's security.

One option is to purchase a SIM reader, a USB device that plugs into your computer, allowing you to view the contents of your SIM card and delete any non-essential stored information.

Additionally, users can directly contact their carrier and request that their SIM card be locked. This prevents unauthorized access to the card, but also renders it unusable on any other device.2.

2. Disappearing text messages: The Background

In this scenario, the user was expecting a new credit card from their bank. The bank informed them that the PIN number for the new card would be sent via text message after the card was registered, and that the message would automatically disappear after three days. True to their word, the text message vanished after the three-day period had passed.

2.1 Conclusion

This situation highlights that not only mobile carriers, but also banks, have the capability to delete messages from your phone or device. Specifically, the type of message that can disappear is known as a Flash SMS. Unlike regular text messages, Flash SMS messages are not stored in your message inbox. Instead, they are typically used to grab the user's attention for marketing purposes. While the fact that these messages are not stored can be seen as a positive, companies can exploit the flash method to intrude on the user's device by sending spam messages.

Fortunately, if you're being bothered by Flash SMS messages, there are ways to block them. Depending on your device, there should be an option to disable flash message spam, preventing them from appearing on your device. However, if your bank is attempting to send you important information through this method, you may not be able to receive it.

3. Changing device settings: The Background

A user recently acquired a new smartphone but wished to retain their old SIM card to transfer their phone number and contacts stored on it. However, upon setting up the new phone, they encountered an issue where the internet was not functioning. As a result, they reached out to their carrier for assistance. Following their contact with the carrier, a text message was sent to the user. Upon opening the text message, the internet began to function properly on the phone.

3.1 Conclusion

This scenario demonstrates that carriers have the capability to remotely modify a device's settings through the SIM card, without requiring physical access to the device. This method can be used by carriers to update a device's firmware, configure handsets remotely, or even lock devices.

Researchers Mathew Solnik and Marc Blanchou conducted tests revealing that nearly all devices are vulnerable when it comes to accessing settings on a mobile device. Depending on the skill level of a hacker, significant portions of a user's phone could potentially be altered remotely. Although there have

been no reported incidents of hackers or state-sponsored criminals exploiting this vulnerability, the risk remains present.

4. Locating you with your device: The Background

A user with a basic feature phone found themselves involved in a crime when the police contacted them regarding an incident that occurred nearby. The police had accessed information that displayed all mobile numbers in the vicinity at the time of the crime. As a result, the individual was interviewed by the authorities for information related to the incident, facilitated by the knowledge of their device's location.

4.1 Conclusion

Your device's location can generally be tracked whenever it's in proximity to a cell tower. To provide you with internet or cellular access, your carrier triangulates your signal approximately every 10 seconds. While this facilitates connectivity, it also means that your location can be traced whenever your phone or device is with you.

It's important to understand that this triangulation provides a general location rather than an exact one. However, if you wish to use a mobile device, there's no way to avoid this tracking, as towers need to provide signal for usage. Unfortunately, this also means that state-sponsored criminals could exploit this information. Your only protection in such cases is to either remove the battery from your device or be in a remote area where there's no carrier signal.

5. Finding you with a new SIM: The Background

In this scenario, a user switched to a new carrier and obtained a new SIM card, resulting in a new phone number. Despite the change, they continued to use the same phone. However, one day, the user received a call from their previous carrier on their new number, inquiring about the reason for the switch. This was surprising, as the previous carrier should not have had any record of the user's new phone number.

5.1 Conclusion

In this instance, despite the change in SIM cards, the individual's new information was still traceable. Both your phone and SIM card hold distinct identifiers. Even if the SIM is replaced, the phone's unique identification can still be utilized to trace the individual. In this scenario, the previous carrier used the phone's identifier to discover the new phone number.

If a state-sponsored criminal or hacker sought to track this individual, they could potentially trace them even with a new phone number, provided they have access to the phone's identifying information. To prevent this kind of intrusion, one effective measure would be to purchase a new phone when changing SIM cards, effectively severing the link from the previous SIM card.

6. How to stay safe

The key lesson from these incidents is that your SIM card holds information that could potentially be accessed by state-sponsored criminals. To safeguard yourself, it's advisable to acquire a SIM reader to ensure your SIM remains free of unwanted data in case it's lost or accessed by unauthorized individuals.

Simply changing your SIM card isn't sufficient for a complete break from your carrier; you'll also need to switch phones and carriers to prevent your previous carrier from tracking you.

Unfortunately, it's difficult to prevent your general location from being tracked, as carriers need to provide you with signal. However, you can mitigate this risk by removing the battery from your device when necessary. Stay vigilant about the privacy risks associated with your SIM card and take steps to protect your personal information accordingly.

RESEARCH · 28 November 2017

GPS Tracking

Your phone company can track your GPS location anytime, even if you've turned off location services, which can jeopardize your privacy.

1. This is an informational guide for:

- Understanding mobile GPS functionality.
- Unauthorized actions by your cell phone provider.
- The potential for SIM card exploitation in tracking your location.
- Finding ways to thwart state-sponsored criminals from tracing your mobile.

2. Reviewing SIM backdoors and location security:

- • Your mobile provider constantly has access to your GPS location.
- • Unauthorized tracking by government entities through your mobile device is possible.
- • Locking your phone or turning off location services won't stop location tracking.
- • Apple's privacy terms state that your iPhone's location data might assist emergency response efforts during emergency calls, regardless of Location Services settings.
- • All phones, even those without SIM cards, can make emergency calls.
- • Emergency services' ability to locate you during calls means even a phone without a SIM card can be traced using geo-location.

3. How your GPS is used on your mobile device:

- • iOS and Apple device users can disable Location Services for everything except emergency calls.
- • Android users can choose between High Accuracy, Power Saving, or GPS only modes and can select which apps have GPS access, but they cannot completely turn off Location Services.
- • Your phone's location is triangulated approximately every 10 seconds to determine the nearest cell tower, aiding emergency services in locating you.
- • Since emergency services can easily locate you, there's nothing preventing state-sponsored criminals from doing the same.
- • Removing your SIM card won't prevent your phone from being traced because the trace relies on the connection to the cell tower.
- • If spyware is installed on your device, criminals and hackers could access your location.
- • Spyware isn't limited to location tracking; it can also take control of your device's camera, contacts, text messages, and eavesdrop on your conversations.

4. Why tracing you without permission is wrong:

- • Emergency services may use it for locating you during emergencies, but the accuracy varies.
- • If emergency responders can't effectively use phone location options, it serves little purpose.

- • You should have the choice to control whether your provider accesses your location due to privacy concerns.
- • State-sponsored criminals might exploit your location as incriminating evidence to place you at a specific location.
- • Since the tracing isn't precise, the data used by state-sponsored criminals could be inaccurate.
- • Despite inaccuracies, such information might still be presented as factual.
- • Your whereabouts shouldn't be accessible to others.
- • Tracking people mirrors Orwell's concept of "Big Brother."
- • Software like Wireshark, utilizing SS7 and OpenstreetMap, can locate users on the network, blurring the line between legality and illegality, complicating prosecution of abusers.

5. How can you protect your location privacy:

- • Refrain from granting permission for geo-location requests online.
- • Maximize security by locking down location services on your phone, although this might be challenging depending on your device and operating system.
- • Disable your device's ability to store location history and clear any existing data if necessary.
- • Prevent location tracking by configuring your browser to include a Do Not Track (DNT) HTTP header.
- • Note that while most browsers recognize DNT requests, not all websites honor them, as the browser cannot enforce compliance.
- • Utilize encrypted networks whenever feasible.
- • Disable cookies in your browser settings to prevent marketing teams from tracking your internet activity.
- • Recognize that state-sponsored criminals could exploit the same tracking information used by marketers.
- • Install anti-tracking apps or software on your mobile device to detect and prevent spying attempts.
- • Don’t use Google services due to its pervasive tracking capabilities.
- • Employ apps or add-ons like Location Guard to thwart Google's location tracking.
- • Ensure that Web Real Time Configuration (RTC) is deactivated to prevent servers from requesting device information that could disclose your location.
- • Enhance mobile security with a Virtual Private Network (VPN), which encrypts data transmission and hides your IP address. Consider using Protonmail VPN for added protection.

6. Conclusion:

All mobile devices possess inherent location tracking capabilities, even though the accuracy of this tracking isn't always reliable. Despite being promoted as beneficial for emergencies, the inaccuracy of location services raises concerns about their necessity. If emergency responders can access a rough location, it opens a similar path for state-sponsored criminals to trace you.

Simply disabling Location Services on mobile devices doesn't entirely eliminate tracking capabilities. However, a pragmatic step involves minimizing Location Services to the extent possible. Using a mobile VPN, such as Le VPN, becomes crucial to encrypt your location data, rendering it inaccessible to unauthorized entities, including state-sponsored criminals.

As mobile phones must connect to cell towers for operation, your location is constantly being identified whenever the device is in use. Whether this tower can pinpoint your specific device relies on your ability to use a VPN for signal encryption.

GUIDE · 11 January 2024

Matrix Encrypted Chat Server

Matrix is a decentralized real-time communication protocol operating as an open standard. Implemented through distributed home servers across the internet, it ensures the absence of a single point of control or failure.

Contents of this article.

1. Matrix server installation guide.
2. DNS settings.
3. Installing Synapse.
4. Adding encryption support.
5. Configuring nginx.
6. Fine-tuning Synapse.
7. Run Synapse.
8. Register your first Matrix user.
9. Enabling self-service user registrations.
10. Running Riot.
11. Pros of running your own server.
12. Cons of running your own server.
13. Matrix server installation guide.

Matrix functions as an open standard communication protocol for decentralized real-time communication, executed through distributed home servers across the internet, eliminating any single point of control or failure. It provides a RESTful HTTP API for the creation and management of distributed chat servers, encompassing tasks like sending and receiving messages, inviting and overseeing chat room members, managing user accounts, and offering advanced features such as VoIP and video calls. Matrix ensures secure synchronization between globally distributed home servers.

Synapse, developed by the Matrix team, serves as the implementation of the Matrix home server. The Matrix ecosystem encompasses a network of federated home servers worldwide. Users employ a chat client to connect to the home server, which, in turn, links to the Matrix network. The home server stores the chat history and login information for each user.

The subsequent section will guide you through the installation of your Matrix reference server and its connection to your initial user(s).

There are two basic things you need to run your private Matrix service:

- Domain name (e.g. ubinodes.org).
- A virtual server running Debian 8 on a cloud service (AWS, DigitalOcean, Vultr, etc.) or a physical server.
- Basic knowledge of the Linux CLI.

For this guide, we will use**ubinodes.org.**

1. DNS settings.

First, you have to register a domain name and fire up your DNS admin panel. You need to create a DNS record like this:

ubinodes.org 300 IN A 1.2.3.4

1. Installing Synapse.

After completing the above step, the following guide helps you set up Synapse, which is Matrix's reference home server implementation.

3.1 Prepare your server.

- Launch a virtual machine running**Debian 8**on your preferred cloud provider and SSH into the host. The instructions below assume that you are root on the server.
- As Matrix/Synapse package lives in a non-standard repository, we are going to add the repo to our machine's package repository:

```
# echo 'deb http://ftp.debian.org/debian jessie-backports main' >> /etc/apt/sources.list
```

- And then we need to make sure that Debian knows that the repo is there:

```
# apt-get update && apt-get dist-upgrade -y
```

- Next, we need to install a few packages that would be useful later. Our VM's are set to basics by default. So, you need to run the following:

```
# apt-get install -y apt-transport-https lsof curl python python-pip
```

```
# apt-get install -y certbot -t jessie-backports
```

- At this point, we need to add another software repository. Create /etc/apt/sources.list.d/matrix.list and open this up in your preferred text editor.
- Inside /etc/apt/sources.list.d/matrix.list, add the following two lines:

```
deb https://matrix.org/packages/debian/ jessie main
```

```
deb-src https://matrix.org/packages/debian/ jessie main
```

3.2 Installing Synapse.

- With that out of the way, it's time to actually install Matrix. Run the following:

```
# curl https://matrix.org/packages/debian/repo-key.asc | apt-key add -
```

```
# apt-get update
```

```
# apt-get install matrix-synapse -y
```

• If the package installs without hiccups along the way move to the next section "Adding encryption support".

- If python-cffi is broken, you might get a python-cffi package conflict error at this point, which will cause the matrix-synapse install to fail.
- Simply run this command to install python-cffi from backports:

apt install python-cffi/jessie-backports

- Once the backported package is installed, try installing Synapse again:

apt-get install matrix-synapse -y

- You will be asked to provide a host name for your server, which in this tutorial we used myserver.example.com

1. Adding encryption support.

- Synapse should expose the Matrix service over SSL, so we need to request for a new certificate. You may reuse your existing SSL certificate if you already have one. For myserver.example.com. Otherwise, you can get a new one from *Let's Encrypt* (https://letsencrypt.org/).
- The next step is to use certbot to generate a Let's Encrypt certificate.

certbot certonly

- Choose the**"spin up a temporary web server"**option.
- The certificate is valid for three months. To configure auto-renewal, we need to add certbot to the system crontab file:

crontab -e

- Insert the following line:

@daily certbot renew --quiet --post-hook "systemctl reload nginx"

1. Configuring nginx.

- To make this HTTPS-ready, we need to configure a reverse proxy. We will use nginx for this, so install it:

apt-get install nginx -y

- Then add the following configuration to /etc/nginx/conf.d/matrix.conf:

server {

listen 443 ssl;

server_name love4aviation.fr;

ssl_certificate /etc/letsencrypt/live/love4aviation.fr/fullchain.pem;

ssl_certificate_key /etc/letsencrypt/live/love4aviation.fr/privkey.pem;

ssl_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl_ciphers HIGH:!aNULL:!MD5;

location /_matrix {

proxy_pass http://localhost:8008;

proxy_set_header X-Forwarded-For $remote_addr;

}

}

- Make sure you replace ubinodes.org with the relevant server name.
- Once that's saved, restart nginx by running:

systemctl restart nginx

1. Fine-tuning Synapse.
    - Add a shared secret to the config file at /etc/matrix-synapse/homeserver.yaml:

Registration_shared_secret: <add random characters here, whatever you want your secret to be>

- Synapse caches conversation information in RAM where possible, and will use as much as you allow. For small implementations, (>50 users), you probably need about 512MB of RAM.
- You can configure this by adding the SYNAPSE_CACHE_FACTOR environment variable to /etc/default/matrix-synapse

`SYNAPSE_CACHE_FACTOR 0.02``

1. Run Synapse.
    - Apply the settings by enabling and restarting the Synapse service:

systemctl restart matrix-synapse

systemctl enable matrix-synapse

1. Register your first Matrix user.

One of the major things you probably want this chat server for is a secure means of communication for your business. To do that, we need some user accounts, let’s start by creating your own.

- Create a new user by running the following, and answering the prompts:

register_new_matrix_user -c /etc/matrix-synapse/homeserver.yaml https://localhost

- New user localpart [root]: {add your name/handle here}
- Password:
- Confirm password:
- Make admin [no]: yes
- Sending registration request…
- Success.

1. Enabling self-service user registrations.

Optional:to avoid having to register new users via CLI on your server every time, you can enable GUI user registration through the Riot client by editing /etc/matrix-synapse/homeserver.yaml and changing the following setting:

enable_registration: true

Otherwise, to register additional users, run register_new_matrix_user -c /etc/matrix-synapse/homeserver.yaml https://localhost again to manually configure more accounts. Make sure you don’t set them all as admins.

Run your end-to-end encrypted chat server using Matrix and Riot.

1. Running Riot.

Riot is the front-end client for the server we just set up. If you don't have it already, you can download the app for your OS of choice at *https://riot.im/* (https://riot.im/)

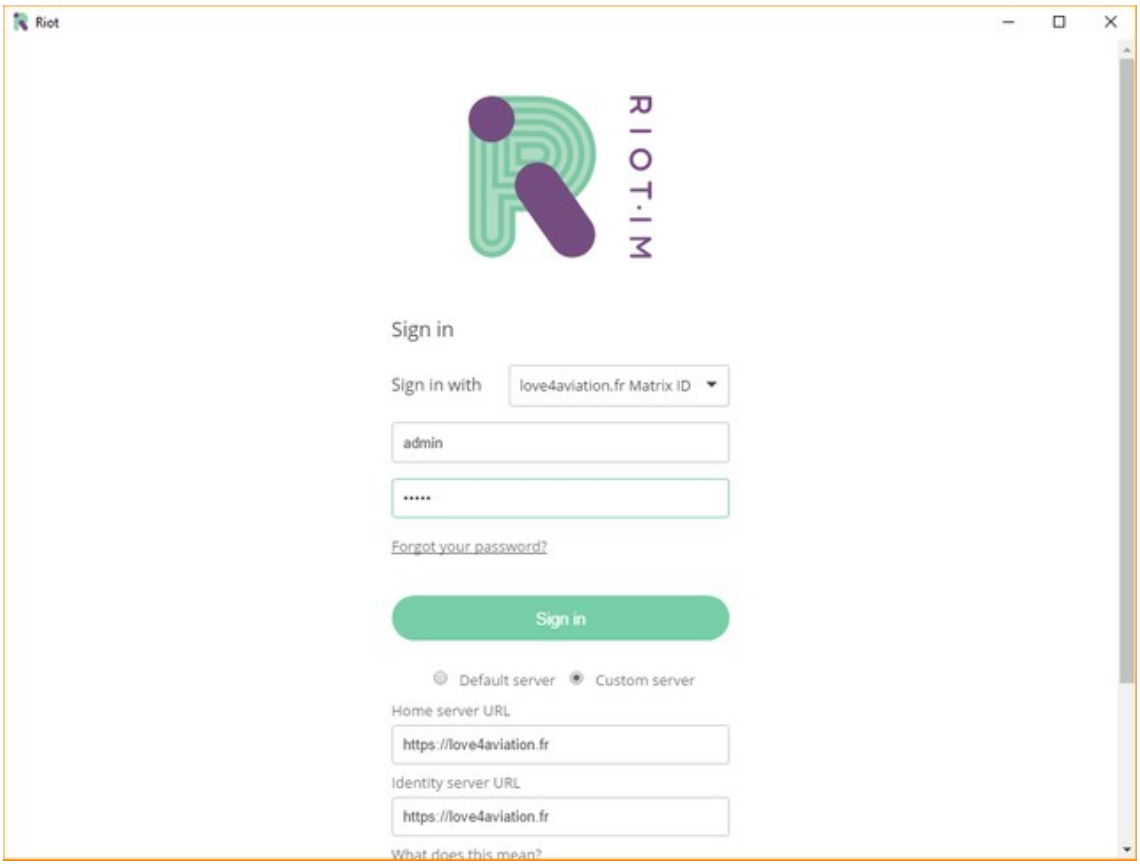
Riot may try to auto-connect you to their default servers. If this happens, log out. We want the Riot login screen for the next part.

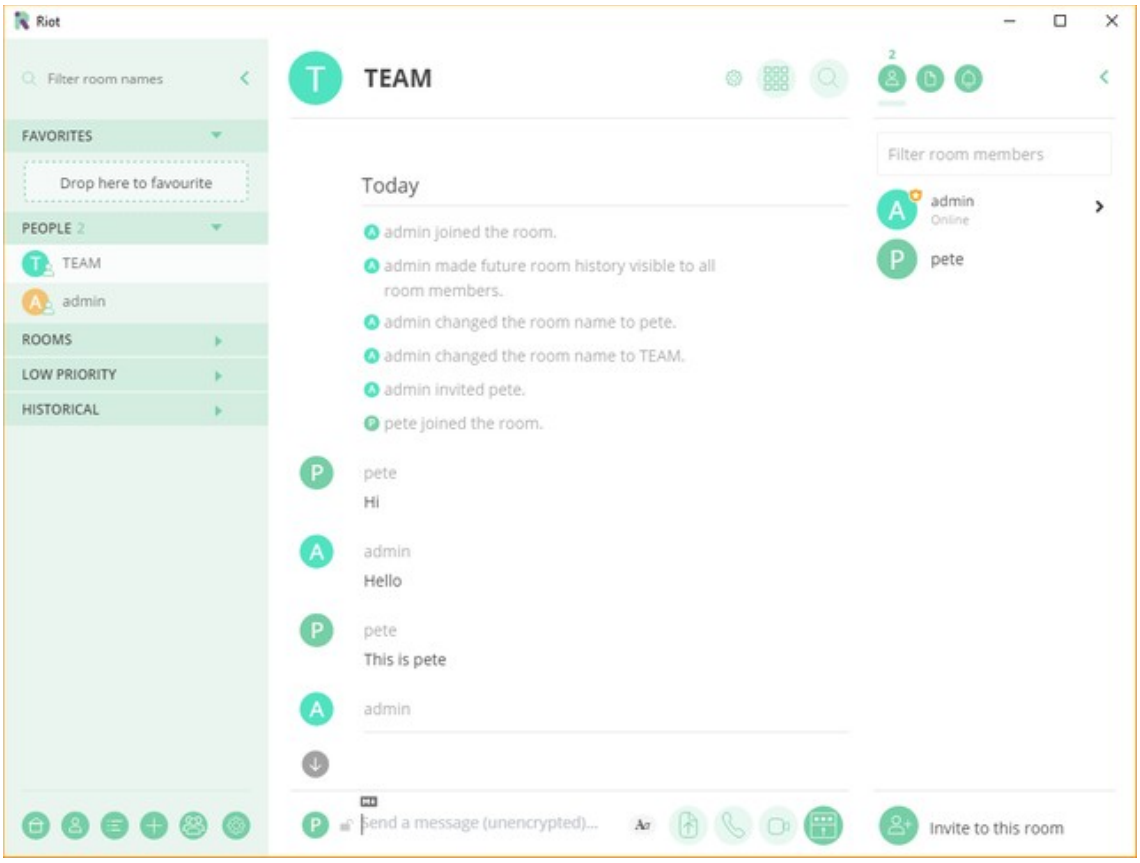
Let's connect Riot to the server we just configured.

Add your hostname (either your BYO hostname or the here's-what-we-prepared-earlier hostname on your handout):

Home server URL: https://ubinodes.org

Identity server URL: https://ubinodes.org





You can now join any room on the Matrix network. Here is our public room:**#foo:Ubinodes.org.**

1. Pros of running your own server.
    - Retain control over your data by executing a script to tidy up deleted rooms at your discretion.
    - Enjoy enhanced privacy settings, allowing you to determine what information you share, a distinct advantage compared to vector.im users.
    - Opt for a personal server for identity, avoiding reliance on vector.im's server. This permits the use of your domain name for team member identification or LDAP integration. An example of such an identity service is mxisd:
    - Demonstrates notably faster performance than utilizing Matrix's free server.
    - Enables businesses to authenticate users with their own domain, enhancing security. In public rooms with diverse participants, restricting registrations to the organization's domain helps thwart social engineering by ensuring that only team members can register with their associated domain.
1. Cons of running your own server.
    - Challenging to set up, requiring meticulous firewall configuration, and necessitating a skilled system administrator for ongoing server maintenance.
    - Despite claiming decentralization, it operates on a federated model. To achieve redundancy, a minimum of two servers is essential—one for hosting rooms and another as the user gateway. This configuration ensures data from the central room is pushed to edge rooms, creating redundancy. However, if the central room experiences downtime, other rooms will be affected.

- Operating your identity server necessitates connection with vector.im. If the server encounters issues, users won't be able to reuse their ID to reconnect to Matrix.
- Managing your ID server involves setting up and maintaining your plugin, as opposed to using Vector.im directly, which may not be a worthwhile endeavor.

1. Conclusion.

Running Matrix home servers on a dedicated domain is crucial to restrict potential attacks on web applications hosted on the same domain by limiting malicious user-generated content served through a Matrix API. This recommendation holds particular significance when both a Matrix web client and server are shared on the same domain.

REVIEW · 11 January 2021

Threema App

Threema is a commendable app that could have become a top encrypted messaging platform if it had open-source code and a desktop application. Its well-designed and user-friendly interface makes setup, installation, and usage easy, even offering a free version.

Disclaimer: We are completely independent of these companies; this article only reflects our findings. The links below are for your convenience, and there is no affiliate marketing involved.

How we write our reviews: For an impartial and comprehensive review, all apps undergo rigorous testing:

- Real-time usage on actual projects.
- Assessment by team members across diverse locations.
- Evaluation on various devices and operating systems.
- Minimum two weeks of testing, averaging four.
- Peer review by team members precedes submission to the app's publisher for final review.

Contents of this article:

1. Pros of Threema
2. Cons of Threema.
3. Conclusion.
4. Screenshots.
5. Criteria used for testing:
    - Encryption Implementation.
    - End-to-end Encryption
    - Zero-knowledge
    - Server location.
    - Suitable for business use.
    - User administration.
    - Resistance to state-sponsored criminals.
    - Multi-platform.

1. Notes.
2. Sources.

1. Pros of Threema:

Threema encrypts all messages and multimedia, ensuring complete security. The app prioritizes anonymity by not requiring phone numbers or email addresses; instead, it generates a random ID at startup. Threema's servers are located in Switzerland, a neutral country outside the jurisdictions of the 9 Eyes, US, and EU, enhancing user privacy.

Threema is suitable for both personal and business use, with Threema Work recommended for professional communication. Threema Work offers a secure, user-friendly platform with features such as text and voice messages, calls, shared media, group chats for up to 100 members, polls, appointment scheduling, and integration with personal software. Group members can be easily managed.

Messages are stored only on one device and cannot be accessed from another device, even if logged into the same user account, maintaining security in case of a breach on one device. This device-specific storage ensures data confidentiality. Groups communicate without server involvement, ensuring zero knowledge, as servers remain unaware of user identities. Threema utilizes standard push notification services provided by the operating system.

Users can easily discontinue app usage by revoking their ID through the emergency feature at *this link* (https://myid.threema.ch/revoke). Threema's web client code is fully open source.

The app offers seamless functionality across various platforms, including Android, iOS, tablets, Blackberry, smartwatches, and Desktop. Contact synchronization is optional, and messages can be quoted for specific replies within a chat. Text formatting options include bold, italic, and strikethrough.

Threema provides an "agree or disagree" feature for discreetly expressing feelings towards incoming messages. Even under legal pressure, message decryption remains impossible. The app safeguards against man-in-the-middle (MITM) attacks by enabling ID verification for communication partners.

Compliant with the European General Data Protection Regulation (GDPR), Threema allows data transfer to a new phone within the same operating system. Privacy settings include disabling "message read" and "typing" displays.

The app supports GPS position sharing with Google Maps integration on both Android and iOS. Bitcoin offers an anonymous payment option. On Android, a passphrase can be set for app exit or phone sleep. Threema's code is open source.

2. Cons of Threema.

 Re-entering the app without a password request after exiting or phone sleep poses a risk of unauthorized access.

 PayPal, one of the payment options, is susceptible to data breaches and user fund cessation.

 Certain features, such as message quoting, text formatting, voice calls, and file sending, are absent on Windows phones.

 Threema's desktop version is compatible with Android and iOS but lacks a web app.

 Chat rooms are capped at 100 participants, and the app struggles to connect during slow internet connections.

The distribution list feature is available on Android and the web app but not on iOS.

3. Conclusions.

Threema is an impressive app that could have been one of the finest encrypted messaging platforms with the inclusion of a desktop version. Well-crafted,

intuitive, and easy to set up, install, and use, it also offers a free version. Even in the rare instance of a server compromise, your messages remain fully encrypted, stored nowhere, and utterly unreadable. The app's exceptional quality was recognized with the prestigious 2015 App of the Year award.

When evaluated against established testing criteria, Threema performed exceptionally well, earning a high rating. It is suitable for individuals and businesses that value data security and privacy.

4. Screenshots:

[]{.image .placeholder original-image-src="media/image1.png" original-image-title="" width="6.66614in" height="4.21811in"} []{.image .placeholder original-image-src="media/image2.png" original-image-title="" width="5.4311in" height="9.72441in"} []{.image .placeholder original-image-src="media/image3.png" original-image-title="" width="5.55472in" height="9.95709in"}

5. Criteria used for testing:

Encryption Implementation

Threema employs advanced asymmetric cryptography to secure messages, calls, and communication between the app and servers. It uses the "Box" model from the NaCl Networking and Cryptography Library for both encryption and authentication.

End-to-End Encryption

Threema ensures the security of messages with dual encryption layers: end-to-end encryption and transport layer encryption. All messages exchanged between users, including text, videos, images, and audio recordings, are encrypted for enhanced security.

Zero-Knowledge

Threema guarantees complete privacy by maintaining zero knowledge of message contents, user identities, or security keys. User keys are stored exclusively on individual devices, providing full anonymity.

Server Location

To prevent interference from state-sponsored entities, Threema's servers are located in "neutral countries" outside the jurisdictions of the United States and the European Union. These locations are immune to coercion for data disclosure.

Suitable for Business Use

Threema is an excellent tool for private users, businesses, and organizations. Threema Work is specifically designed to meet business data needs, with a trial version available for testing.

User Administration

Group admins have exclusive rights to add or remove members from a group.

Resistance to State-Sponsored Criminals

Threema refuses to decrypt messages, even under legal compulsion, because it does not possess the keys, which are stored solely on users' devices. State-sponsored entities, such as police or prosecutors, may have the technical capability to intercept and read various protocols and manipulate SSL certificates. To counteract such threats, it is crucial to consistently use encryption software, secure all devices through encryption, and consider purchasing hardware from locations outside your residing country.

Multi-Platform Availability

Threema is available across major platforms, including Android, iOS, and Windows Phone.

6. Notes

Threema is available for download on the Google Play Store and Apple Store but does not have a dedicated desktop application. To use it as a desktop app on Windows, you need to install Bluestacks, an Android emulator that allows you to run Android apps on the Windows platform. Here's a brief guide on how to proceed:

1. Download Bluestacks from *this link* (https://www.bluestacks.com/).
2. Establish a Google account, preferably using a burner phone.
3. Obtain the Threema APK.
4. Install the APK on Bluestacks by selecting the downloaded Threema file and installing it through Bluestacks.
5. Launch Threema from Bluestacks and input your details to start using the app.

7. Sources.

1. En.wikipedia.org. (2018). Threema. [online] Available at: https://en.wikipedia.org/wiki/Threema [Accessed 4 Apr. 2018].
2. Threema.ch. (2018). [online] Available at: https://threema.ch/press-files/cryptography_whitepaper.pdf [Accessed 4 Apr. 2018].
3. Threema.ch. (2018). Frequently asked questions - Threema. [online] Available at: https://threema.ch/en/faq [Accessed 4 Apr. 2018].
4. Threema.ch. (2018). What are distribution lists? - Threema. [online] Available at: https://threema.ch/en/faq/distribution_lists [Accessed 4 Apr. 2018].
5. Work.threema.ch. (2018). Threema Work - The messenger for organizations. [online] Available at: https://work.threema.ch/en [Accessed 4 Apr. 2018].
6. Open-Source: https://threema.ch/en/open-source

REVIEW · 8 December 2017

Semaphor App

The Semaphor app, developed by SpiderOak, enables users to securely message, chat, or share files through encryption, guaranteeing no risk of eavesdropping on the information transfer.

Disclaimer:We are not affiliated with these companies. This article is entirely based on our independent findings, and there is no affiliate marketing associated with the links provided below for your convenience.

How we write our reviews: To guarantee an unbiased and comprehensive review, all apps undergo testing:

- In real time, meaning they are used on real projects.
- By various team members situated in different countries.
- Across different devices and operating systems.
- For a minimum of two weeks, with an average duration of four weeks.
- The article undergoes peer review by other team members before being sent to the app's publisher for the final review.

1. Our specifications sheet:
    - End to end, zero knowledge encryption (note 01).
    - OpenSource (note 02).
    - Administration of users (note 03).
    - Resistance to state-sponsored criminals (note 04).
    - Cost Effective for a large user base (note 05).
    - Multiplatform (note 06).
    - Own business domain (note 07).

Semaphor, a leading collaboration tool for groups, whether personal or business related, is developed by SpiderOak, its parent company. SpiderOak has maintained a strong presence in the market for users concerned about spyware or malware. The key factor contributing to this reputation is its dependable encryption.

1. Advantages of using Semaphor:
    - It features a zero knowledge central server, encrypting data as it passes through (note 01).
    - No passwords are required for ease of use.
    - Every message and shared file is securely encrypted; the chat is encrypted before reaching other users (note 01).
    - The source code is open for review (note 02 and screenshot 01).

-

    - It offers unlimited teams and channels (note 03 and screenshot 02), enabling simultaneous uploading of multiple files.

- Users can begin downloading a file even before it completes uploading from another user's device.
- Access to channels is invitation based, and users only see channels they are invited to (note 03 and screenshot 03).
- Channel members can be removed as needed (Screenshot 04).
- The app is accessible on both desktop and mobile devices (note 06). Users can create public groups and set auto accept for join requests (note 03 and screenshot 05).
- Users can remain anonymous by joining with either an email address or a username. The platform retains messages for 30 days before automatic deletion.
- Bots and integrations are supported based on user needs.
- A builtin search engine is provided (note 08 and screenshot 06).
- Adding a new device is convenient with the bar code scanning feature (note 09 and screenshot 07).
- Verification of addressees is facilitated through device fingerprinting (note 10 and screenshot 08).
- Updating profile settings reflects across all devices (Screenshot 09).
- It ensures consistent features across all operating systems, eliminating the need for adaptation when switching (note 11).
- Semaphor offers mobile and desktop apps for Windows, iOS, and Android operating systems.

1. Disadvantages of using Sempahor:
    - It lacks app locks, making it not password-protected if another user picks up the device; fingerprinting provides a solution.
    - However, at $9 per user/month, it can be expensive, particularly for large groups (note 05).
    - There's a limited 2 GB file support, and no notifications for join requests; users must check for new requests by navigating to "team settings."
    - To notify a specific group member, you need to tag them using*@username* (https://steemit.com/@username) in
    - the message.
    - The desktop app supports message notifications, but the mobile app lacks push notifications for incoming messages; users must enter the app to check for new notifications.
    - The app may not perform well on slower internet connections, potentially resulting in multiple postings of a single message.
    - It is not consistently userfriendly; if the screen is not refreshed, it may display members from the previous channel instead of the current one.
    - While SpiderOak emphasizes "zero knowledge," this does not extend to zero knowledge web browsing or zero knowledge backup from mobile devices. Moreover, picture uploads lack endtoend encryption, and editing them from a mobile device is not supported. The iPad app is restricted to portrait mode and does not rotate to landscape.
1. How the Security Works:

- Semaphor employs a key instead of a password, mitigating the risk of user forgetfulness or external hacking, including threats from state-funded criminals. The key, consisting of randomly generated words, enhances security by eliminating the vulnerability associated with passwords.
- Instant encryption is a distinctive feature, ensuring that messages are encrypted prior to departing the original device. This signifies that the encryption process occurs directly on the device itself.
- The key allows you to monitor the devices that have accessed your account. SpiderOak, committed to user privacy, refrains from retaining any user information, rendering their system invulnerable to hacking attempts. The service does not store data; instead, it encrypts all information or files exchanged between users.
- In the event of an account attack by an individual or malware, the assailant will be barred from all accounts associated with your organization, extending beyond the ones you personally access. This precautionary measure ensures that the attacker cannot compromise any other accounts. Semaphor's encryption surpasses the security of data stored in a cloud. Unlike a cloud, which is a remote server retaining your data, this app does not retain any user data but secures transmitted data directly through your device.
- Access is limited to channels to which you've been invited, safeguarding the privacy of other channels. Your identity can remain anonymous, as you are identified only by a username depending on the group type. This means other members in the same channel won't know your personal details unless disclosed by you.
- The encryption ensures that even state-sponsored criminals, who might attempt illegal access, cannot compromise your data.

1. Other ways you can protect your information:

- Utilize your own web domain to initiate online activities. Ensure that your VPN is not within the 14 Eyes alliance, safeguarding against surveillance by your nation or any participating in the UK-USA Agreement. These countries engage in clandestine data collection worldwide. Although your data may transit through their servers, commencing traffic elsewhere enhances your protection. The 14 Eyes consist of: United Kingdom, United States, Australia, Canada, New Zealand, Denmark, France, The Netherlands, Norway, Germany, Belgium, Italy, Spain, Sweden.
- Opt for private browsing, available on major web browsers. This setting erases cookies, temporary files, and browsing history upon window closure, severing ties to online activities.

-

- Conceal your IP address using a VPN for encrypted anonymity. Avoid divulging comprehensive personal information on social networks, minimizing the risk of exposure.

1. Alternatives to Semaphor:

Alternative apps exist in the market, but none have demonstrated the same level of safety as Semaphor. Notably, many of these apps are open source, allowing for potential modification of the original source code. While open source provides the flexibility to customize the app according to specific needs, it also introduces the possibility of security enhancements based on the user's ability to modify the code.

1.**Slack:**Initially a popular secure group chat forum and still available, but lacks the "zero knowledge" cloud associated with SpiderOak**.**

2.**Riot:**Formerly known as Vector, Riot is an open source app compatible with major operating systems. It provides both public and private messaging, featuring end to end encryption and a decentralized structure.

3.**HipChat:**A freemium service akin to Semaphor and Slack, designed for team communication within companies. It includes chat history search, chat rooms, and file sharing.

4.**Mattermost:**Modelled after Slack, Mattermost is an open source platform positioned as a cost effective alternative. It markets itself as a Slack substitute with similar features at a lower cost.

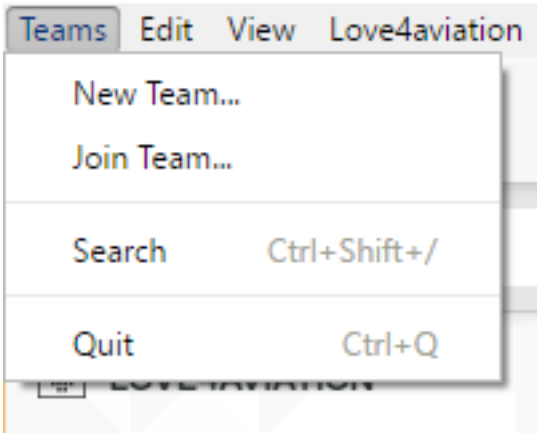
5.**RocketChat:**Essentially a younger, open source clone of Mattermost and Slack, still in its development stages.

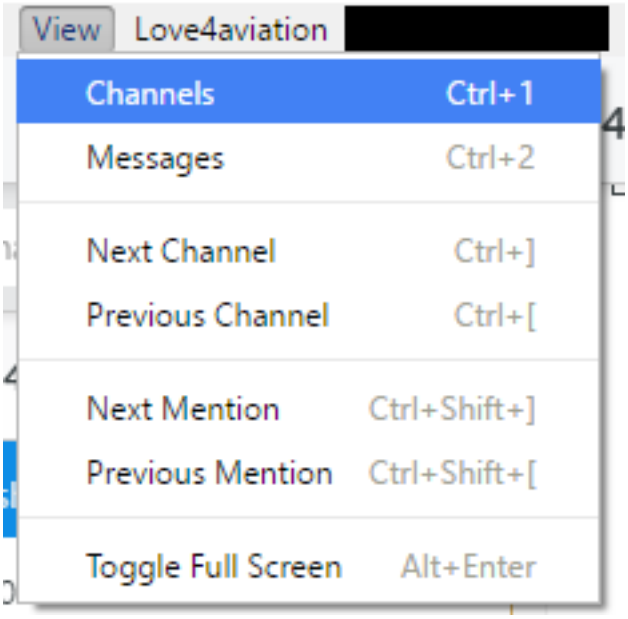
The alternative apps offer encrypted data options but lack the "zero knowledge" cloud provided by SpiderOak. A "zero knowledge" cloud ensures that even SpiderOak cannot decrypt any data passing through it. This guarantees that the data is only readable between the sender and the recipient, not by the channels it traverses. Semaphor, by not having the ability to read any transmitted data, stands out as the safest among encrypted chat apps, safeguarding both messages and shared files between users.

1. Screenshots:

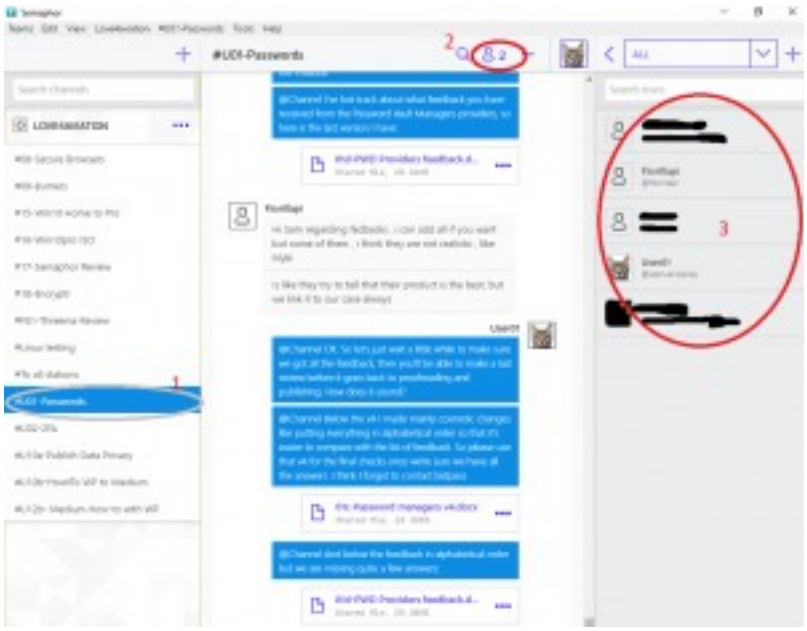
01: Source code is also reviewable.

02: Unlimited teams and unlimited available channels.

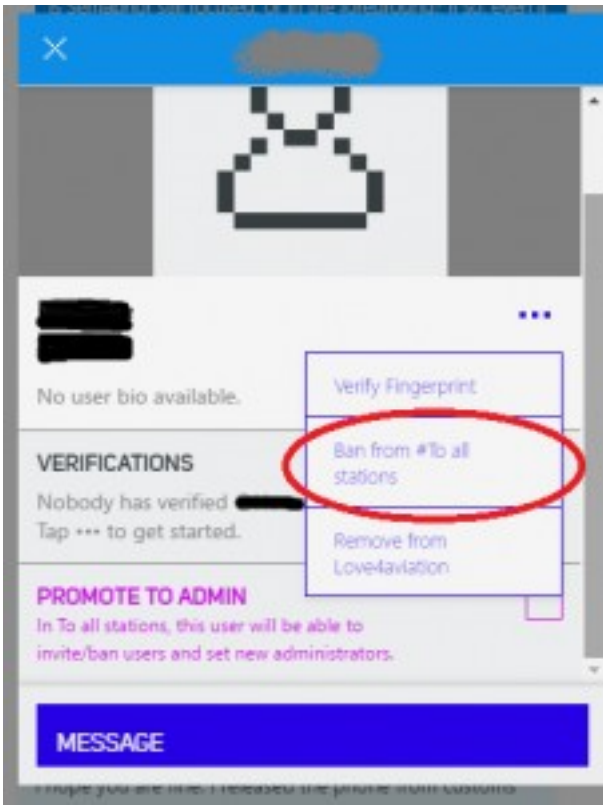




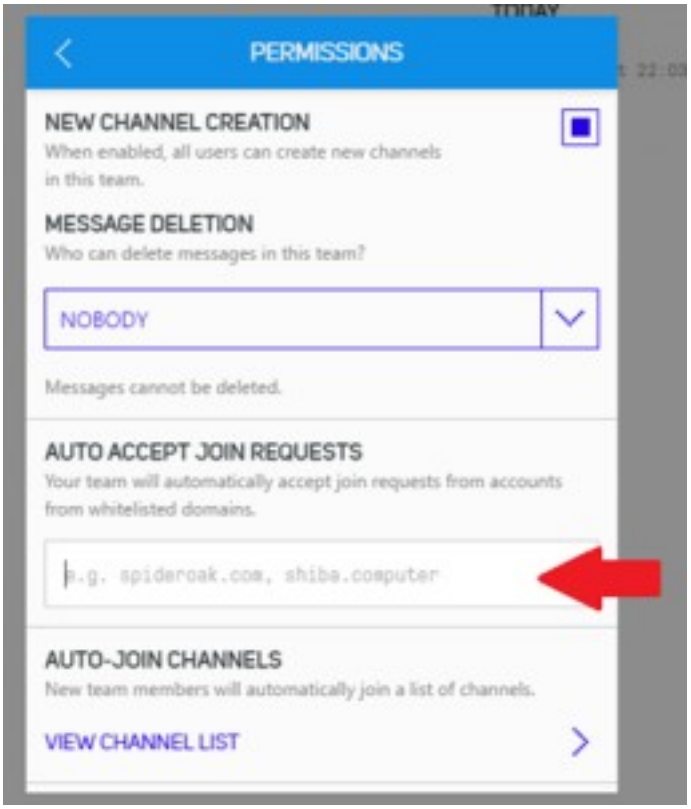
03: A user does not see all of the channels.



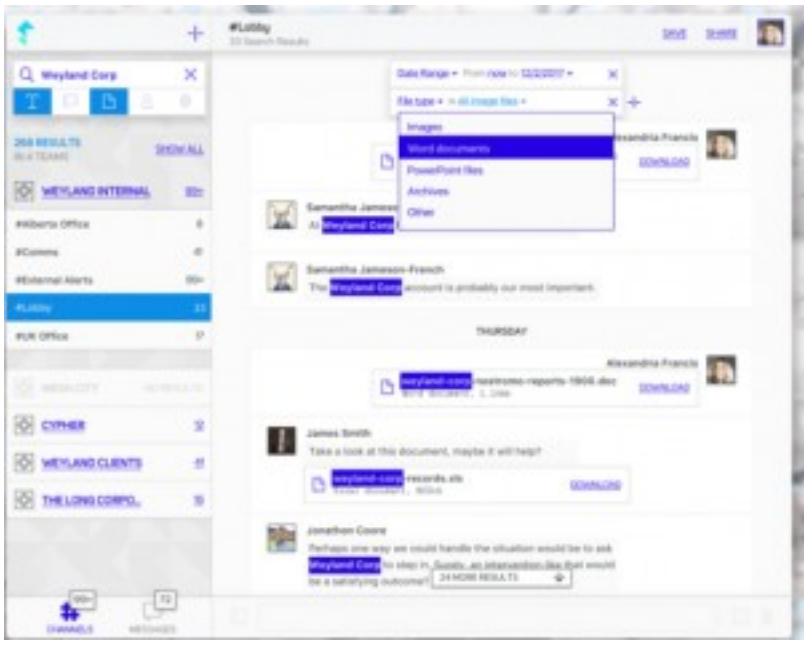
04: Remove members from a channel.



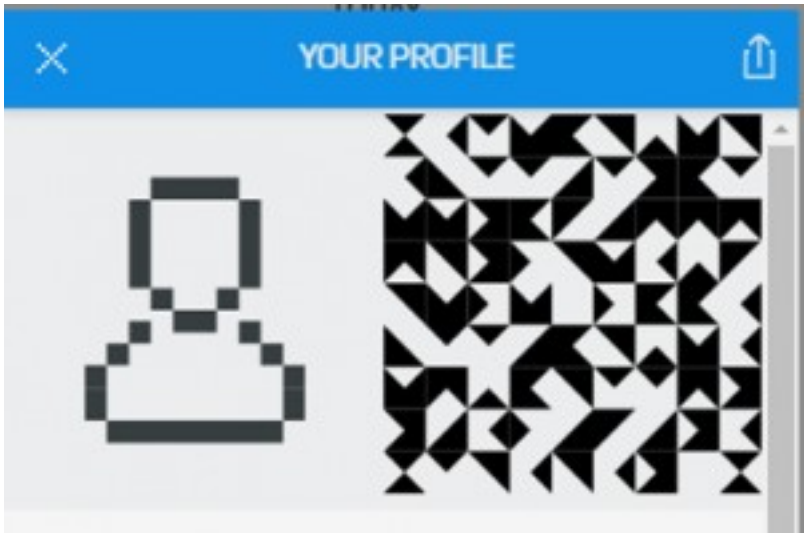
05: Allows you to create public groups as well as autoaccept any join requests.



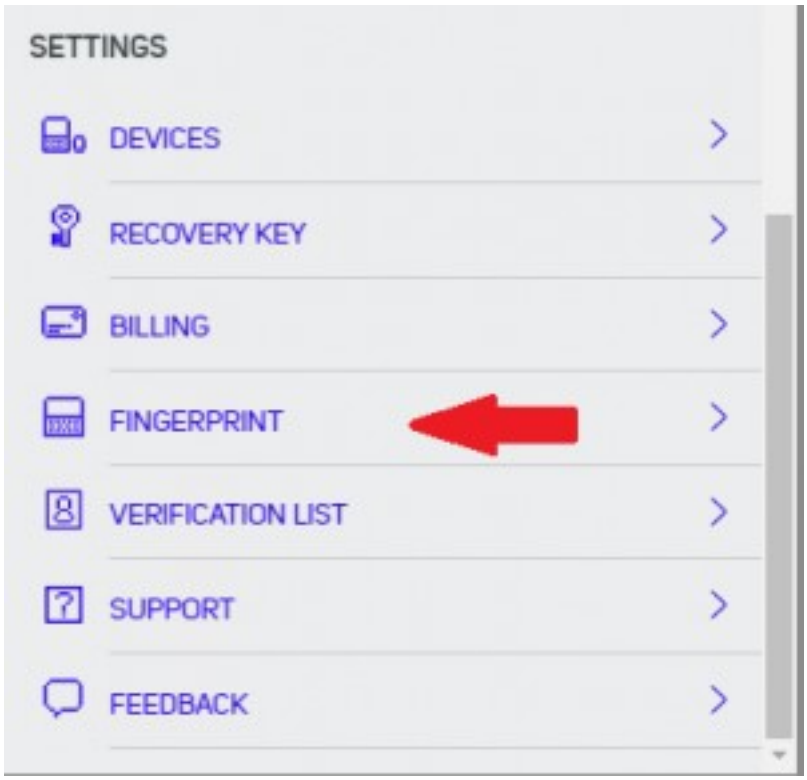
06: Builtin search engine.



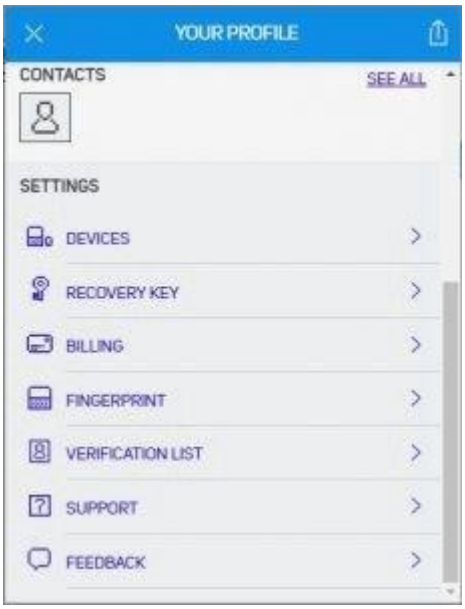
07: Add a new device with its bar code.



08: Verify addresses by fingerprinting.



09: Change your profile settings.



1. Notes:

(1) Endtoend encryption is achieved as:

- No central server, data is downloaded to devices.
- Every message & file is cryptographically secure.

(2) Open source code: Go to: *https://spideroak.com/solutions/semaphor/source* (https://spideroak.com/solutions/semaphor/source)

(3) Administration of users:

- Create a new team or join an existing one.
- Establish multiple channels and navigate seamlessly between them.
- Users can only view channels to which they are invited.
- Create public teams and enable auto acceptance of join requests.
- Access the "Manage Team" section and navigate to "Permissions."

(4) Resistance to statesponsored criminals: Police, prosecutors, etc., can engage in "legal" crimes by corrupting state institutions, posing a severe threat to individuals and countries. If they commit illegal acts, they can easily cover them up, intercepting and reading IMAP, POP3, TLS, and SSL. They can spoof your email provider's SSL certificate, gaining access to SMS and emails, making recovery options vulnerable. Always use encryption software, secure your devices, and buy hardware from abroad.

(5) Costeffective for large user base: Don’t meet. $9 per user/month is expensive for big teams (5).

(6) Multiplatform: For Desktop, Go to: *https://spideroak.com/personal/semaphor* (https://spideroak.com/personal/semaphor) For Android, you can find it in Google play.

(7) Own business domain: To mitigate the risk of attack by state-sponsored criminals through DNS records, host your domain in a location that prioritizes access protection, avoiding the same country as your email provider. Choose a country outside the fourteen eyes alliance, known for respecting privacy and democracy. Employ end-to-end protection to secure your emails in case of interception.

(8) Built in search engine: Works even offline.

(9) Easy to add new device with bar code scanning: No need to reenter credentials.

(10) Can verify addressees by fingerprinting devices: List of verified addressees in the apps settings.

(11) Same features on all types of operating systems: For example you can accept join request from a mobile device, you don’t need to use the desktop app to get some admin features.

REVIEW · 25 April 2018

SID Messenger App

SID is a messenger platform that purportedly utilizes end-to-end encryption. However, our investigation revealed that all traffic between users bypassed international routes and instead was routed directly to servers located in Madrid, where SID's servers are based. This contrasts with the expectation that traffic would travel between countries where our consultants were conducting tests.

Disclaimer: We have no affiliation with these companies. The information presented in this article is solely based on our independent findings. The provided links are solely for your convenience, and no affiliate marketing is involved.

How we write our reviews: For an impartial and comprehensive review, all apps undergo the following testing criteria:

- Real-time usage on genuine projects.
- Evaluation by diverse team members across various countries.
- Testing on different devices and operating systems.
- Minimum testing duration of two weeks, typically spanning four weeks.
- Peer review by team members precedes the final review sent to the app's publisher.

Contents of this article.

1. What is SID?
2. Pros.
3. Cons.
4. Conclusion.
5. Screenshots.
6. Criteria used for testing.

> • Zero knowledge.

> • End to end encryption.

> • Encryption implementation.

> • Peer to peer file transfer.

> • Sid address.

> • Open source.

> • Multiplatform.

> • Resistance to state sponsored criminals.

1. Sources.

Have you ever questioned the true security and encryption of the apps you use? With numerous revelations about big tech companies storing and exploiting user data, it's crucial to prioritize privacy and security, whether for personal or business purposes.

How can we verify claims of app security and ensure they deliver on their promises, rather than being deceptive tools created by malicious actors? We dedicated time to researching various encrypted apps, subjecting them to thorough reviews and tests across different devices. One such app we examined is SID, and our findings were startling. Before delving into specifics, let's first take a brief overview of the app.

1. What is SID?

SID is a messenger application that purportedly employs end-to-end encryption, making team communication simple, efficient, and secure. Users have the option to communicate via group chats or one-on-one chats, and securely send files between team members without concern for data compromise. Additionally, when new team members join, their contacts are automatically exchanged.

Users can create dedicated channels to organize and structure their communication with their team, with the flexibility to customize and edit them as needed. The primary selling point of SID lies in its emphasis on security and privacy. The platform is purportedly structured and designed to prioritize these aspects, ensuring that private messages remain solely accessible to the intended user. SID's philosophy is centered around safeguarding user privacy, aiming to prevent interception of messages by state-sponsored criminals.

Website: *http://sid.co/* (http://sid.co/)

-

1. Pros:

SID is free to use.

Stream encryption for SID cannot be turned off and is always in place.

Fast file transfer of any size makes it convenient to send large files, especially on local networks (Peer-to-peer transfer criteria).

No personal information about the user is entered on SID (Zero knowledge criteria).

The app is suitable for individuals and businesses that prioritize data security and privacy.

SID is compatible with major devices in the market, including iOS, Android, Linux, and desktop (Multiplatform criteria).

Users can create and customize groups and multiple chat rooms on SID.

Users can leave groups when they are no longer needed.

Various members can be added to a group chat as desired.

SID utilizes the BitTorrent protocol with a central server for offline chat, eliminating a central point of failure.

When installing on a new device, SID prompts users to enter their ID and confirm the new device from another active device, without the need for login/password. Previous conversations may not be visible on the new device, but all chat rooms remain accessible (SID address criteria).

1. Cons:
    - Voice/video chat unavailable.

Documents lack peer-to-peer synchronization and updates. Only you possess access to files sent to you, without the harmonization and synchronization found in tools like Resilio and SyncThing. This drawback is particularly significant for teams, companies, and organizations aiming to securely collaborate on files.

- Absence of an in-app support panel.
- SID's code remains unpublished, rendering it not open source at the time of writing (Refer to Testing Criteria: Open source).
- Specific image sizes required for chat room thumbnails; smaller images won't upload.
- Message syncing across devices isn't immediate; reading a message on one device doesn't instantly reflect on others until the app is reopened.
- No read receipts available to confirm message viewing by recipients.
- Lack of message quoting, hindering coherent conversation tracking.
- Servers based in Madrid, part of the 9 eyes alliance (Refer to Testing Criteria: Resistance to state-sponsored criminals).
- For offline use, encrypted messages stored on servers could potentially be intercepted by state-sponsored entities (Refer to Testing Criteria: Resistance to state-sponsored criminals).
- Deleting messages during chats removes them only from the sender's end, not the receiver's.
- Absence of ephemeral (self-destructing) messages.
- All files sent/received on SID can be accessed from the installation folder, compromising app security if the hard drive isn't encrypted, potentially accessible by state-sponsored entities.

Note: For comprehensive details, refer to the elaborated explanations in the Criteria used for testing section below.

1. Conclusions.

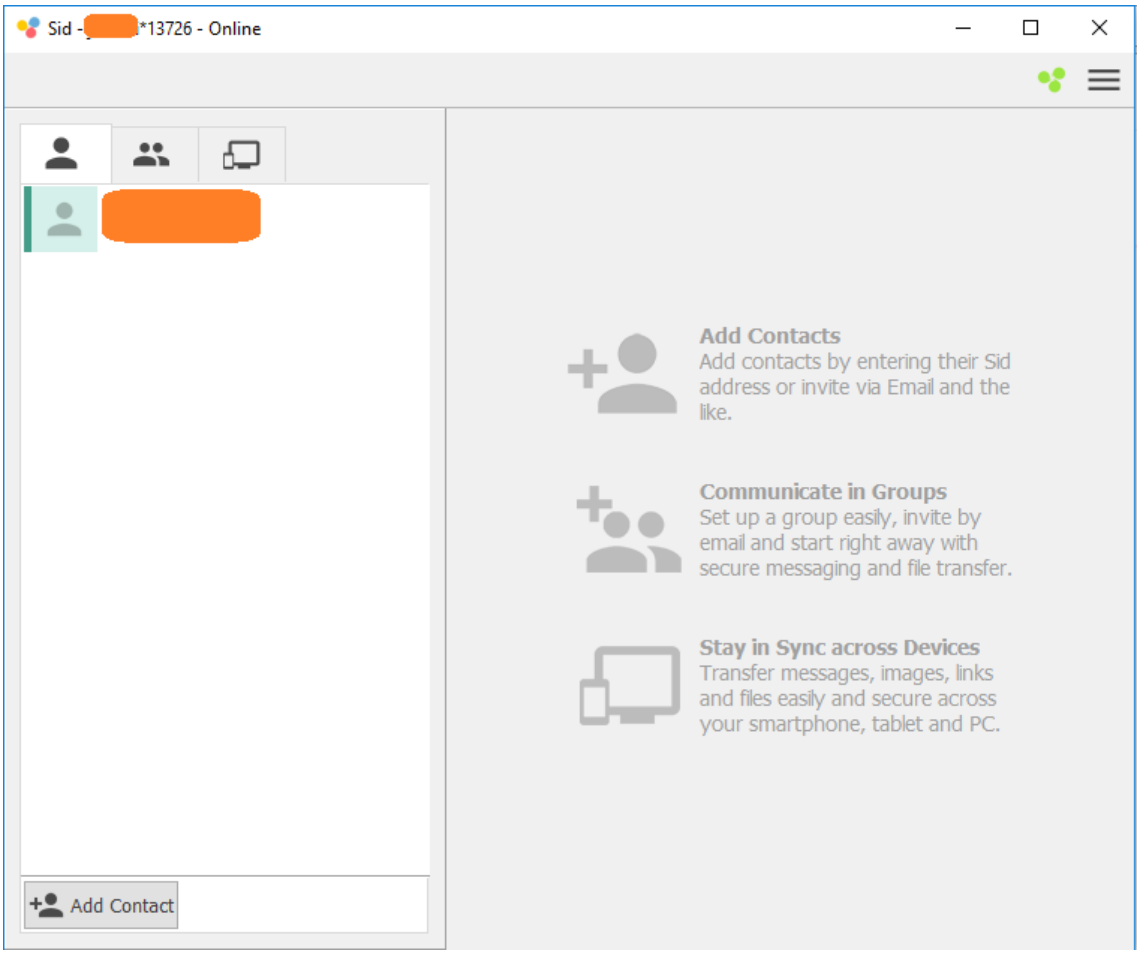
After conducting comprehensive testing of the Sid app with various consultants in different countries using diverse devices and operating systems, including the utilization of Wireshark for peer-to-peer encryption verification, we made several significant findings.

Firstly, our analysis revealed that all traffic between users was directed straight to Madrid, where Sid servers are based, rather than being routed between the countries where our consultants were conducting tests. This observation suggests that Sid stores messages on a central server, contradicting their claim of not storing user data.

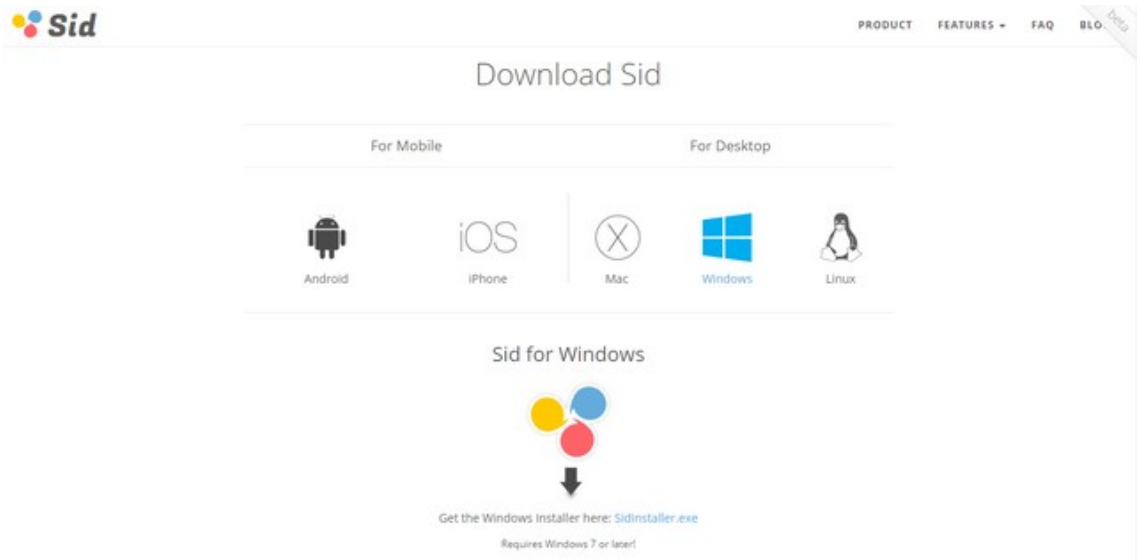
Additionally, a notable drawback is the lack of open-source availability for the app's source code, which prevents independent verification of claims regarding end-to-end encryption and zero-knowledge principles. Moreover, the location of Sid's servers in Madrid, a country that is part of the 9 Eyes alliance, raises concerns about data privacy and security. Ideally, locating servers in a neutral country with no affiliation to the US or EU would be preferable.

We forwarded our research findings to Sid support for review; however, as of the time of publication, we have not received their feedback.

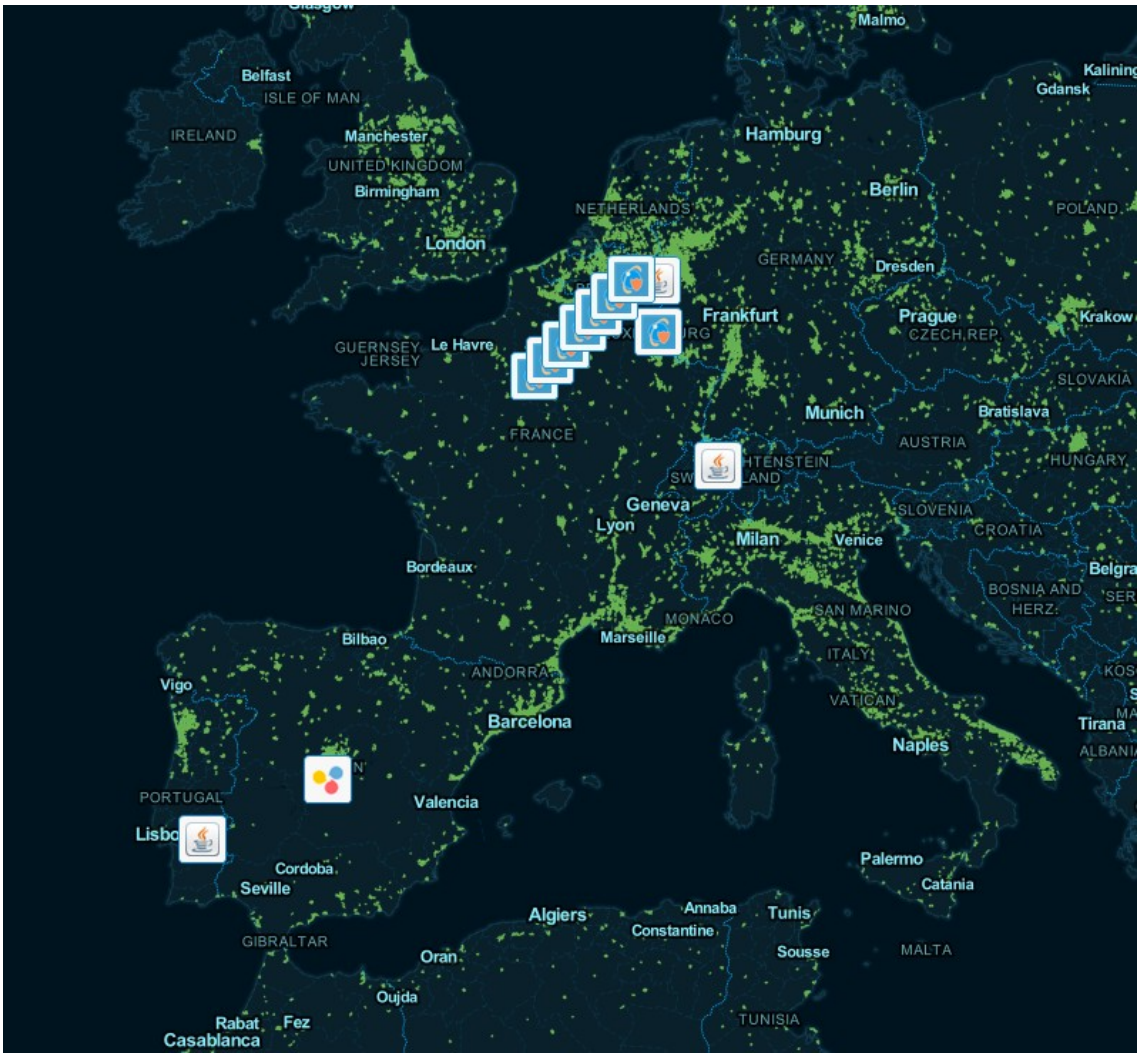
1. Screenshots:



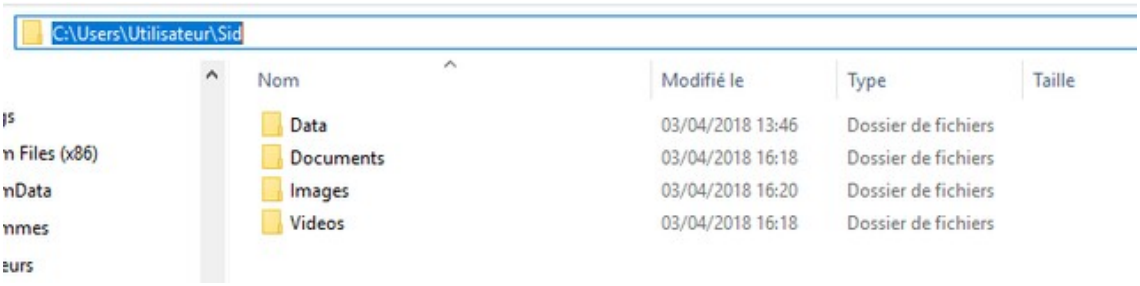
SID app interface



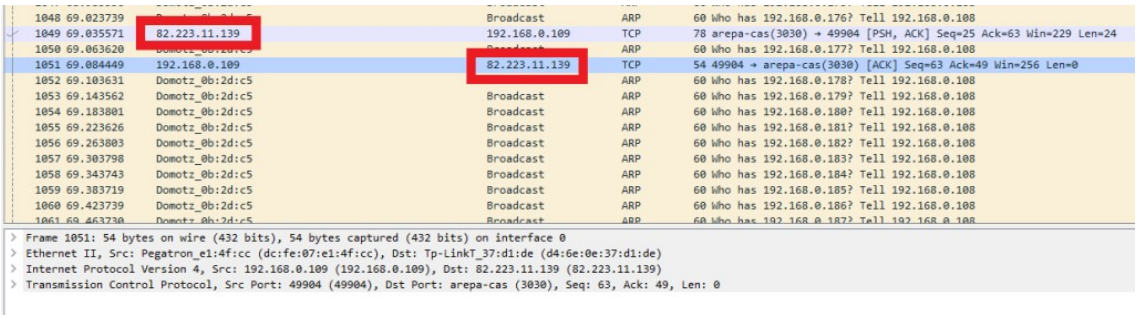
Downloading SID



SID servers in Madrid



Installation folder on PC



Testing SID with WireShark

2. Criteria used for testing.

• **Zero knowledge:**The Sid app ensures that only the sender and receiver have access to their data. In cases where data is stored on offline servers for backup or offline delivery purposes, it is encrypted and can only be decrypted by those who possess the keys on their devices, specifically the sender and receiver of the information. It's important to note that the sent data is not altered, read, or analysed for any purpose whatsoever.

• **End-to-End encryption:**According to SID Messenger, they utilize a trusted and robust encryption method that fully encodes the entire transfer chain, unlike HTTPS (Secure Hypertext Transfer Protocol), which is commonly used for secure web server solutions. For users of HTTPS, it means that when a device is connected via HTTPS, only the connection from the device to the server is encrypted. The concern with this setup is that the transferred data is available in plain text on the server side, which means that your service provider or any other entity with access to the cloud system can potentially access and read your data.

• **Encryption implementation:**On SID, you have the capability to send files such as documents, videos, and photos of all sizes. When you send a file to an individual contact on SID, it is transmitted directly to the receiver's device. However, if you send a file to a group on SID, all devices within the group network are utilized as senders to ensure backup network availability. Additionally, when sending files using a local network, such as within an office, school, or organization, the files are transmitted at the fastest speeds possible, thereby avoiding potential issues related to internet connectivity with ease.

• **Peer-to-peer file transfer:**On SID, you have the capability to send files such as documents, videos, and photos of all sizes. When you send a file to an individual contact on SID, it is transmitted directly to the receiver's device. However, if you send a file to a group on SID, all devices within the group network are utilized as senders to ensure backup network availability. Additionally, when sending files using a local network, such as within an office, school, or organization, the files are transmitted at the fastest speeds possible, thereby avoiding potential issues related to internet connectivity with ease.

• **SID address:**When signing up for SID, there's no requirement to provide any personal data such as email addresses, phone numbers, or physical addresses. SID utilizes its unique address system, which consists of a username appended with an asterisk (*) and a 5-digit unique number. This approach allows users to use their preferred username and choose who they wish to make contact with. Moreover, it serves as an effective preventive measure against spam.

• **Open source:**When signing up for SID, there's no requirement to provide any personal data such as email addresses, phone numbers, or physical addresses. SID utilizes its unique address system, which

consists of a username appended with an asterisk (*) and a 5-digit unique number. This approach allows users to use their preferred username and choose who they wish to make contact with. Moreover, it serves as an effective preventive measure against spam.

• **Multiplatform:******SID is available on desktop, Windows, Mac, Linux, iOS and Android.

• **Resistance to state-sponsored criminals:**These individuals, including police and prosecutors, operate with impunity, as state institutions have been corrupted and lack oversight. Their actions, though illegal, are considered legal due to the compromised state of governance. They pose a significant threat, both to individuals and to the integrity of a country. They possess the capability to intercept and read various communication protocols such as IMAP, POP3, TLS, and SSL. Additionally, they can spoof SSL certificates of email providers, gaining unauthorized access to SMS and emails. Recovery options often serve as easy targets for their attacks. To safeguard against such threats, it's essential to utilize encryption software, secure devices with encryption, and procure hardware from sources outside the jurisdiction where they operate.

1. Sources.

- Download.com. (2018). Sid. [online] Available at: http://download.cnet.com/Sid/3000-2654_4-76641095.html [Accessed 28 Mar. 2018].
- Sid. (2018). Sid | End-to-End Secure Team Communication. [online] Available at: https://sid.co/en/security-by-design [Accessed 28 Mar. 2018].

Part III

Web, Publishing & Social Media

GUIDE · 14 May 2021

WordPress: Build a Website from Scratch

What is this?

This is a "Step-by-Step" type article on the use of the WordPress Content Management System, to start a website from scratch and get it online within a day.

Why do we need this?

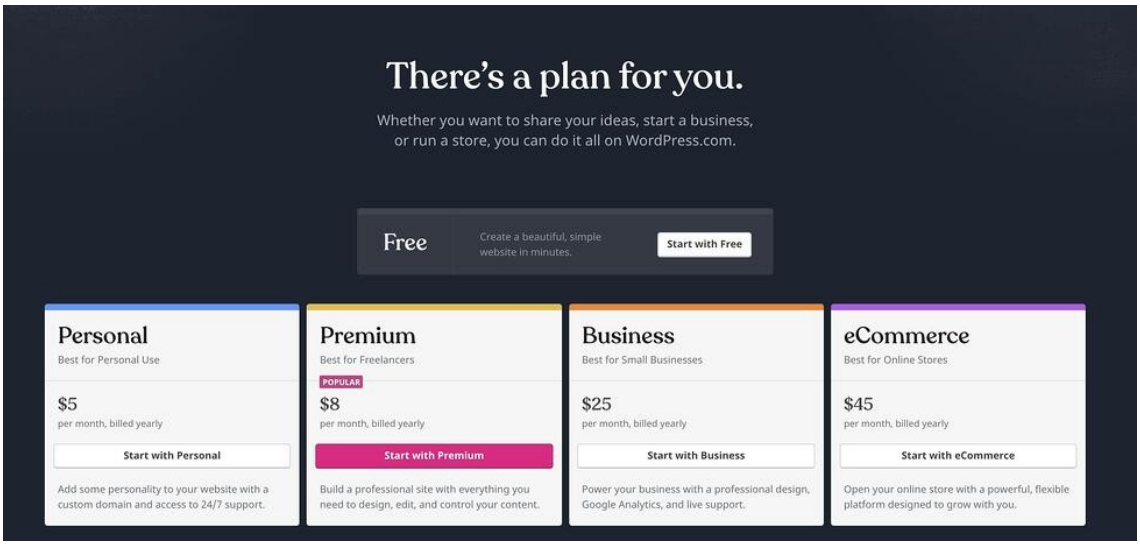
Ubinodes being an international marketing agency, we need to help our clients quickly and easily have a local internet presence in their target locations. This article helps us be on the same page when we start coaching them on efficiently using WordPress.

Contents for this article.

1. Select a WordPress plan (WordPress.com only).
2. Set up your domain name and hosting provider.
3. Install WordPress.
4. Choose your theme.
5. Post to your website.
6. Customize your website.
7. Installing plugins.
8. Shortcode.
9. Sources.

1- Select a WordPress plan (WordPress.com only).

At the beginning of creating your website, you need to select a plan from WordPress.com. There are five plans they have to offer one is free, two is personal, three is premium, four is business, and five is business. Each of these plans ranges from free to 45 dollars a month (See picture below).



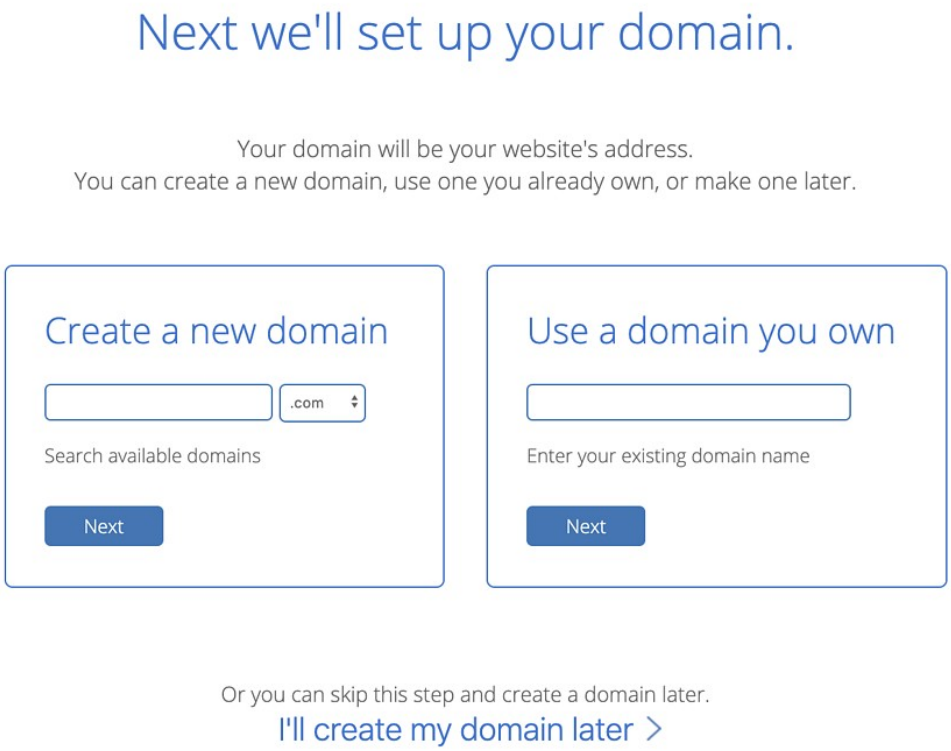
The main difference between all of these websites is monthly fees, site customization, and better access to marketing tools.

Warning* WordPress.orgrequires***you to create your domain and find a third-party hosting provider for your website. WordPress.com is better suited for first-time creators of a website because it is all-inclusive with domains and hosting providers.**

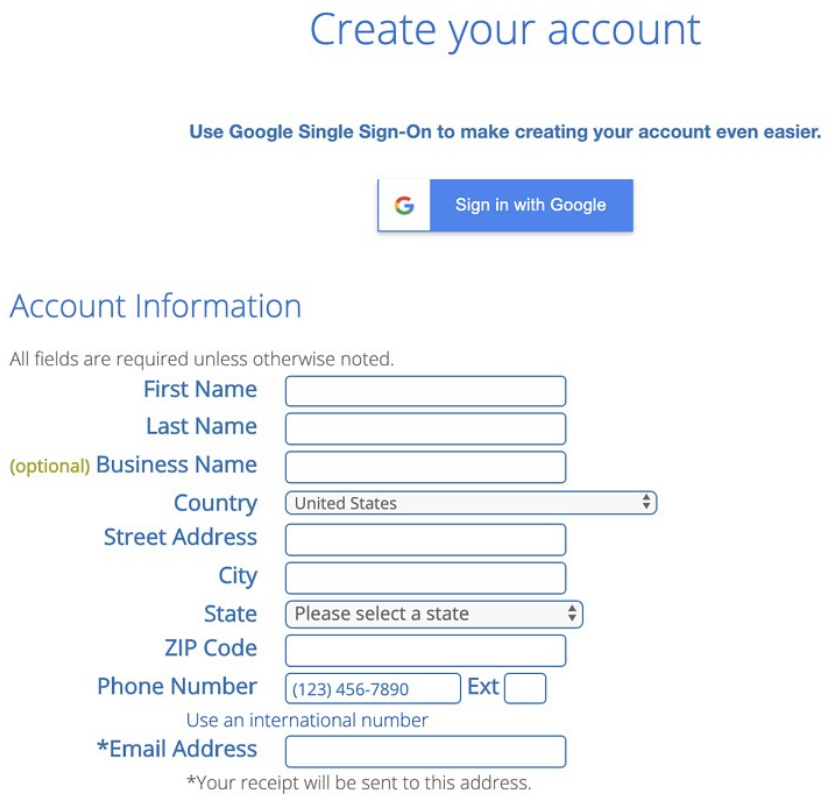
2- Setting up your domain name and hosting provider.

Setting up and choosing your domain and hosting provider should happen around the same time during the website creation. Think of the Domain as a home address and the Hosting provider is the actual home. The home address is how visitors find your website on the internet. The hosting provider is the part of your website that files are stored. Without both the domain and hosting provider the website would not work. Luckily WordPress.com allows you to decide whether or not you want a custom domain depending on the plan you choose, but it takes care of the hosting for you. Choose WordPress.com for this Step by Step.

2.1- Once have selected a plan it will take you to a page where you can set up your domain.

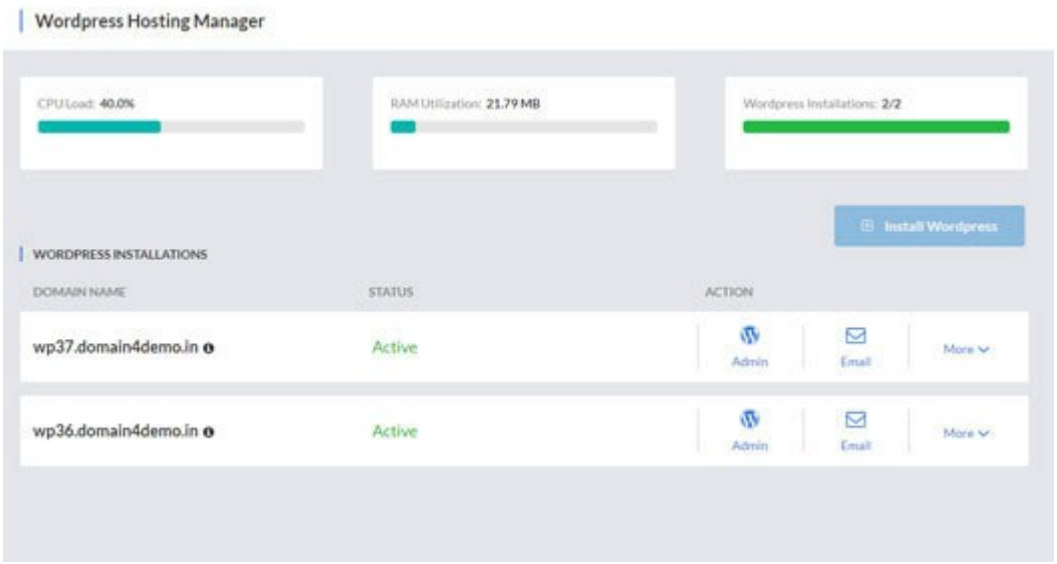


2.2- Once you have created a domain you will be brought to complete an account and billing information for your purchase.



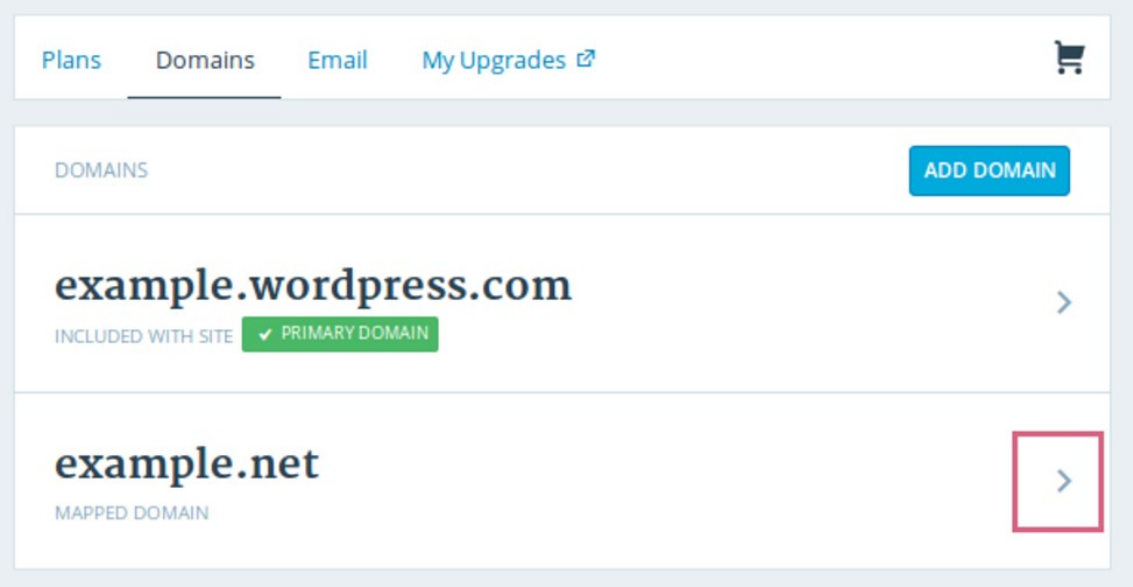
3- Installation.

3.1 After creating a domain and account you will gain access to the hosting dashboard and be able to Install WordPress CMS (Content Management Systems).

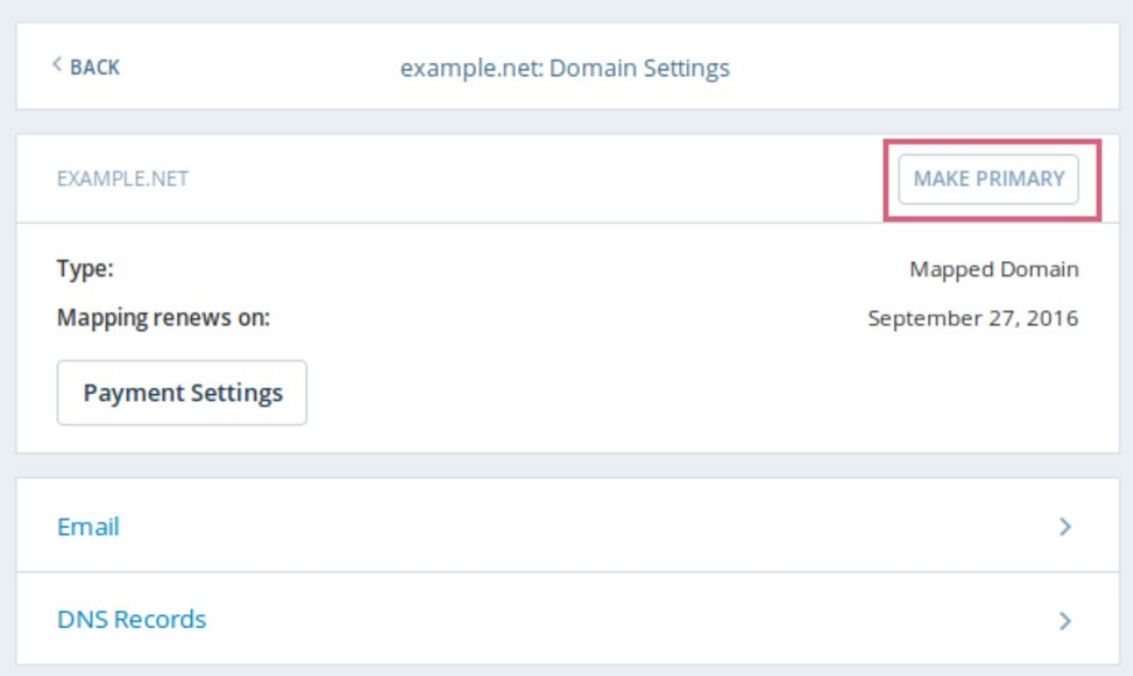


After Installing your WordPress you will have to answer a few questions about the domain you would like to use and the directory of where you want to install WordPress, and admin information. It can take some time for this process.

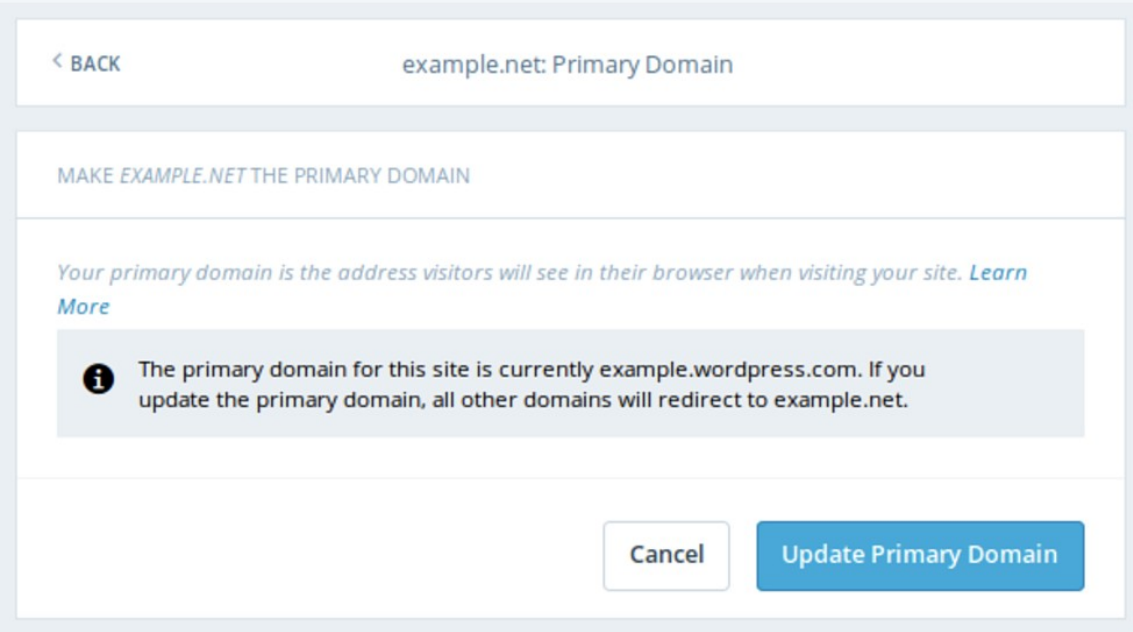
3.2 In WordPress go to My Site and click on Domains. From there you can select a custom domain you want as the primary domain.



Then click on make primary.



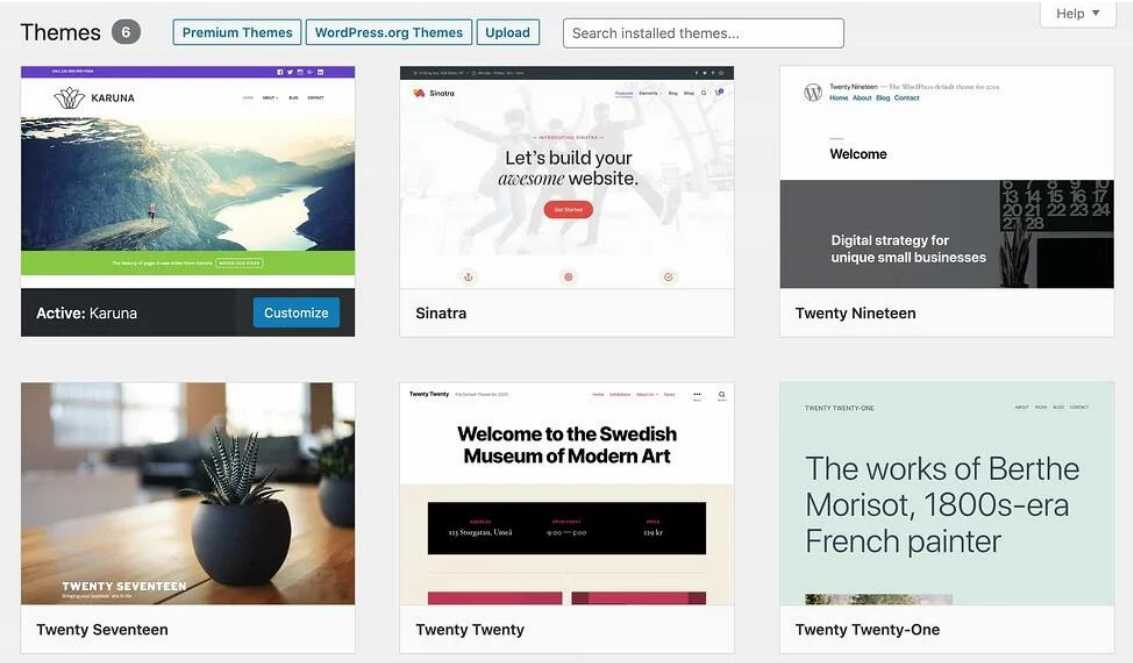
Then click on Update Primary Domain.



It has now been successfully updated and should say in green Primary Domain.

4- Choose your theme.

In WordPress, you can customize the website using many themes and templates offered by them. WordPress will automatically start a default theme that looks plain to start. A custom theme free or paid for will help your website look and stand out from other professional websites (See samples below).

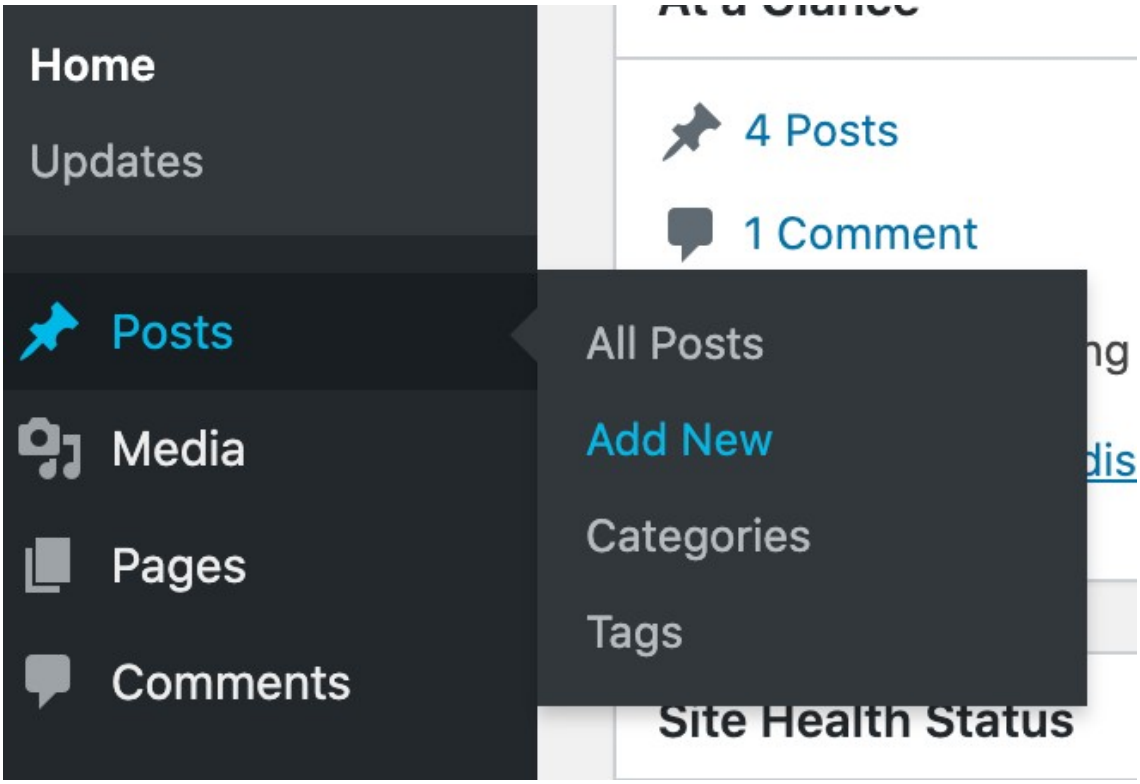


Once you have found the perfect theme and install it. Each theme will have a different process and steps required for the customization process.

5- Post to your Website.

Adding content to your website will be in the form or displayed as posts and pages.

A post is used for blogs and portfolios because they will automatically place the newest content at the top of the website. You can add different pages to your website and post to those pages so that it doesn't clutter the home page. Adding a new post should look something like this.



You can add a title for the post, change the formatting, insert page elements such as blocks, paste photos, and even use shortcode which I will explain in a separate paragraph. While you are making a post or page you can save it as a Draft and come back to it later or Preview it to see what the final product would look like on the page. On the portfolio tab, you can organize all of your posts by category, as well as see relevant information regarding your posts such as the date of the last update, recent changes, etc.

The same option will come up for pages when you want to post a new page except for the categories and tag lines.

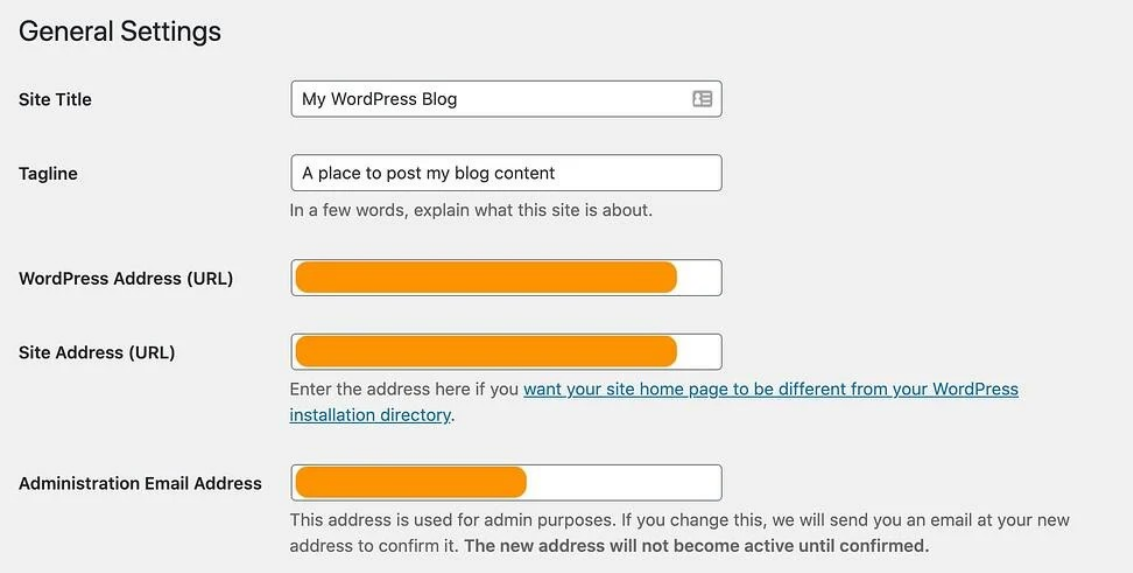
5.1 Portfolio.

Later, when there are categories within your website and you are adding new articles, you can add them without sending an alert, by posting through the "Portfolio" tab. This is preferable for posts that are constantly being updated, and when it is ready to be released, you can make a post about it.

6- Customize your website.

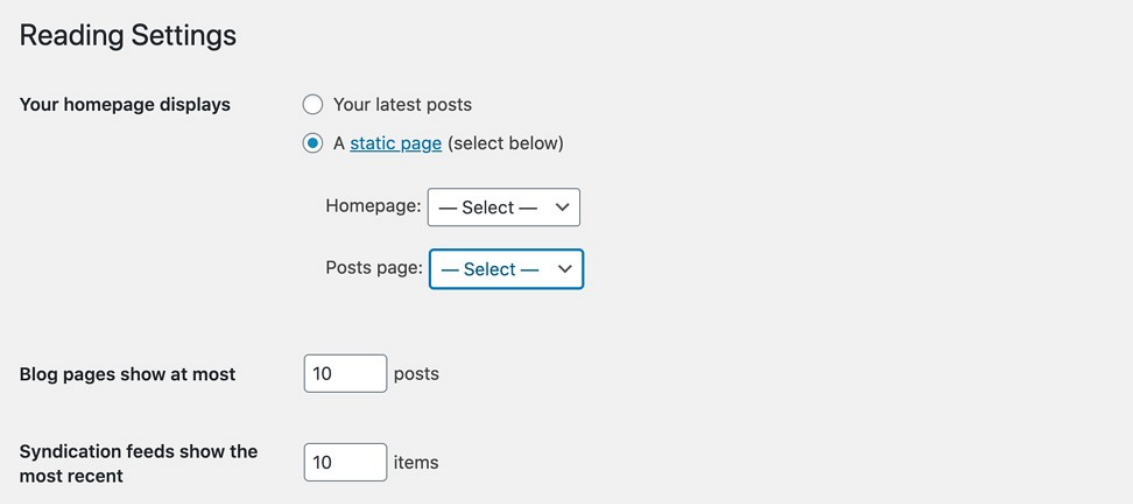
There is so much more than just themes when it comes to customizing your website, there are many options to choose from in this post.

To start, we can customize titles. From your admin dashboard select**Settings**and then**General**. From here you can add a website title and taglines as well as toggle other basic site information such as URL, email, time zone, and more (See picture below).



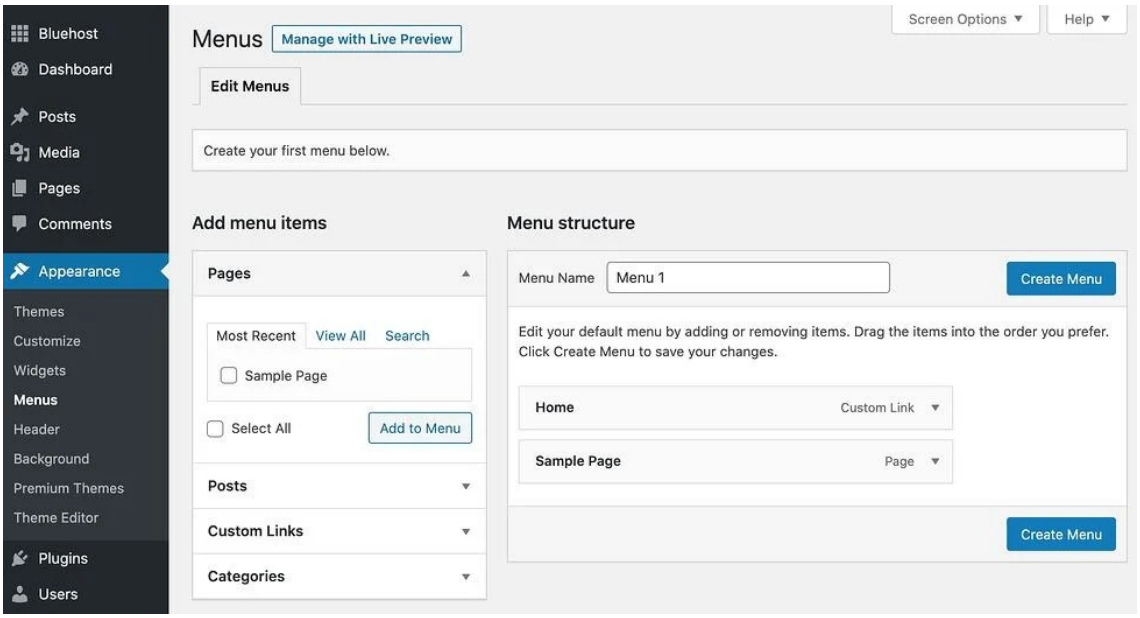
As you can see from these settings you can customize a lot. Next, we will look at the reading sections. Click on**Settings**once again and go to**Reading**. From here you will have options such as changing your home page to a static page.

A static page is a homepage that doesn't contain blog posts or other regularly updated content. Instead, it's “static,” or unchanging. A static front page, also known as a “splash page” or “custom homepage,” can feature whatever you want.



This site should be considered by business owners who prefer having content remain in one place on the website. For a blogger, you should consider a more dynamic approach like having the newest content appear at the top of the page.

Another customization that an admin could add is the**Navigation Bar**. To add this you have to go to the admin dashboard and click**Appearance**and then**Menu**(See picture below).



In the menu, you have the option to make the bar how you want to look, how many pages are included, the titles of the pages, and what the order of them are. I would highly recommend this for users that want to do more with their website to have it stand out.

7- Optimize your website.

When it comes to optimizing your website you need to make the user experience friendly. The page may be taking too long to load and that will make visitors move on to another side very quickly. Slow speeds are not good for your website. How you can improve on this is by enabling feature caching which is the process of temporarily storing the website's data on the visitor's browser. This will help your website's speed because the content does not need to be sent from the webserver for it to appear in the browser.

WordPress has an internal caching system that includes several subsystems. The WordPress core allows plugins to control this caching system to reduce the number of database calls.

8- Shortcode.

Shortcodes in WordPress are little bits of code that allow you to do various things with little effort. They were introduced in WordPress 2.5, and the reason to introduce them was to allow people to execute code inside WordPress posts, pages, and widgets without writing any code directly.

Examples of Shortcode:

A trivial shortcode for a gallery looks like this:

```
[gallery]
```

Shortcodes can also be used with additional *attributes* as the following example shows:

```
[gallery id="123" size="medium"]
```

9- Sources.

- WordPress website. WordPress.com: Create a Free Website or Blog (https://wordpress.com/)
- Ultimate Guide: How to Make a Website in 2021 – Step by Step Guide (Free). How to Make a WordPress Website - Easy Tutorial - Create Website (2021) (wpbeginner.com) (https://www.wpbeginner.com/guides/)
- How to Use WordPress – Tutorial for Beginners 2021. WordPress Tutorial 2021: Learn How to Use WordPress (Free) (firstsiteguide.com) (https://firstsiteguide.com/learn-wordpress/)
- Types of WordPress Caching. <https://www.interserver.net/tips/kb/types-wordpress-caching/#:~:text=WordPress%20has%20an%20internal%20caching,the%20number%20of%20database%20calls>
- Codex. <https://codex.wordpress.org/Shortcode>

GUIDE · 17 June 2021

Social Media for Business

What is this?

This article is a guide to help businesses start an online presence and remain private while doing so.

Why do we need this?

In the evolving digital landscape, social media has expanded its role beyond social networking, extending into crucial business activities like marketing. Its cost-effectiveness compared to traditional advertising campaigns and its global reach at the click of a button make it an integral tool. Leveraging social media enhances our efficiency in discovering new connections, be they potential clients or candidates.

However, with an amplified online presence comes increased vulnerability of information. Safeguarding data is crucial as government agencies have been known to manipulate seemingly innocuous details to their advantage. Therefore, minimizing information sharing whenever possible is advisable, and this article aims to guide you in doing so. Given that essential information is required to create a social media account, the focus will begin with securing this sensitive data.

Contents of this article.

1. Privacy.
2. Choosing the platform.
3. Relevant platforms.
4. Creating the profile.
5. LinkedIn and further.
6. Scripting LinkedIn.
7. Syncing contacts to LinkedIn.
8. Twitter and further.
9. Creating a marketing strategy.
10. Importing contacts to Google.
11. Conclusion.
12. Notes.
13. Sources.
14. Privacy.

Before establishing a social media presence, it's crucial to recognize the unrestricted flow of information, susceptible to ending up in unintended hands. Therefore, we'll provide techniques to safeguard your personal data. Employing a VPN for your internet connection is essential, as it conceals your IP, safeguarding your location and identity. Additionally, using a password generator for creating passwords is highly recommended.

01.1 Burner phone.

Prerequisite:

A VPN for your internet connection (note 1).

Setting up:

-**Step 1:**Get a standard GSM phone (preferably not a smartphone) that has never been used with a SIM card under your name (note 4).

-**Step 2:**Get a prepaid SIM card bought with cash in a drug store, do not use credit cards. Choose one that has no expiry date (note 2).

-**Step 3:**Initiate SIM activation via SMS. If online activation is unavoidable, refer to note 2. Typically, with anonymous SMS activation, the SIM can be used immediately for two weeks before online registration becomes necessary. If you require temporary Google or Facebook accounts, create them before registering your SIM online.

-**Step 4:**Activate the carrier's account online (note 2).

01.2 Burner Gmail.

To use the Google Web store in Bluestacks and importing contacts, you will need a burner Gmail account. Sign up using fabricated details and a generated password—no phone number or backup account submission is necessary. Once used for Bluestacks, promptly delete this account. If needed again, you can easily create another free account later.

1. Choosing the platform.

Choosing the right platform hinges on its value to your business and its ability to cater to your prospective customers' needs. The crucial features we seek are:

- Sync contacts via emails, a necessity for business to connect with our existing client base through social media, contrary to personal usage preferences. But as a business we have an existing list of clients and we want to be able to connect with them through social media.
- Display app users within our contact list, enabling us to follow them directly, bypassing reliance on app generated suggestions.

> As an illustration, Instagram will specifically disclose which of your contacts are using the app, whereas Twitter does not provide this information.

- Provide a feature to show users that are reciprocally following us. This enables us to streamline our following list by identifying those we've followed but who haven't followed back, ensuring a balanced ratio of followers to followed accounts. Twitter excels in this aspect by explicitly showing followers, whereas Instagram's process is cumbersome, requiring manual comparison of followers and followed accounts to remove inactive users.
- Enable sending and receiving direct messages, a crucial feature for initiating new conversations. Shapr's Tinderlike approach offers a convenient way to start conversations through matches, whereas other apps may require initiating conversations without a prior connection.
- Facilitate group creation and contact invitations, essential for hosting online presentations and meetings on diverse topics, providing a valuable engagement opportunity for our contacts.

1. Relevant platforms.

Syncing with your contact through emails:

- LinkedIn.
- Facebook (Note 5).
- Instagram.
- Twitter.
- Viber.
- Reddit (Note 6).
- TikTok.
- VK (Note 7 sync with Gmail and Facebook).
- OK.
- Facebook messenger.

Not syncing with your contacts:

- Shapr.
- Meetup (Note 8).
- Google Chat.
- Discord.
- Twitch.

Syncing with your contacts but only through phone numbers:

- Telegram.
- WhatsApp.

Allowing direct messages:

- Twitter.
- Instagram.
- Reddit.
- LinkedIn.
- Facebook.
- Viber.
- VK.
- OK.
- Facebook messenger.

Allowing the creation of group chats:

- Facebook.
- Facebook Messenger.
- OK.
- VK.

The subsequent section will outline four prominent platforms, along with brief insights into their user base, common corporate utilization, and possible drawbacks. Please note that these platforms are not presented in any specific ranking order.

02.1 Facebook.

Facebook boasts a staggering 2.74 billion monthly active users, dominating global teen engagement and encompassing users of all age brackets, positioning it as a cornerstone for social media marketing. Despite an aging user base, Facebook remains unparalleled in its extensive reach across all demographics. It's a preferred platform for companies aiming at customer engagement, fostering feedback and conversations. Leveraging the Facebook messenger app enhances the ability to connect with potential clients on an individual level. Nevertheless, the platform's vastness poses challenges, more suitable for customer retention rather than acquisition (Note 9).

Facebook's network effect is unparalleled; it swiftly garners followers. Group creation allows inviting all Facebook contacts. However, the need to periodically reset social media accounts every six months arises due to Facebook's tendency to confine users within an unproductive cluster of irrelevant profiles. It often results in connections from regions lacking business relevance.

02.2 Instagram.

Instagram, a subsidiary of Facebook, boasts a daily user base of 500 million, with 88% of its users located outside the United States. What sets it apart from Facebook is its emphasis on "organic" marketing. Unlike Facebook, Instagram does not rely heavily on paid promotion; instead, your follower count is influenced by the effectiveness of your own post marketing efforts (see Note 10). Moreover, its combination of visual imagery and text makes it particularly suitable for businesses aiming to showcase their products or services in a visually appealing manner.

When posting updates like website changes or new sponsored projects on Open Collective, including an image with your post is essential. Unlike Twitter, Instagram does not automatically generate a preview of the linked content. It's advisable to use a disposable or temporary photo for this purpose.

However, for a website update, you'll need to create an image:

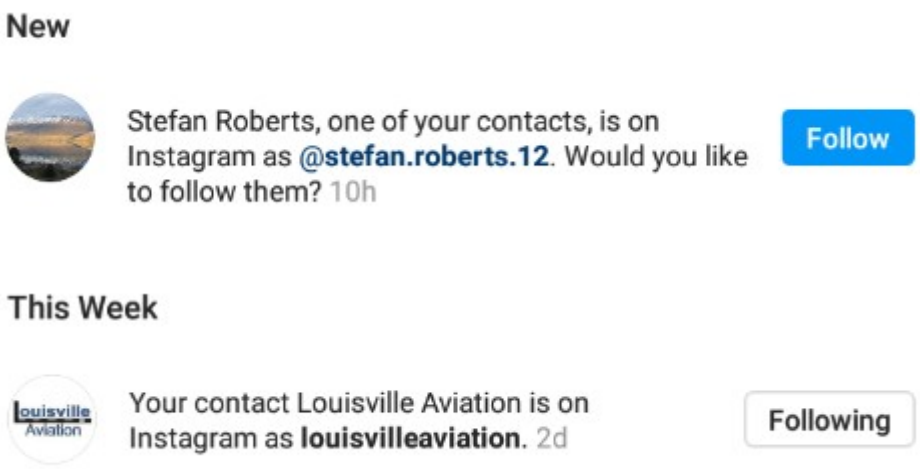
1. Using Libre Office Draw, go to "insert text box" and write your text. An example title: "website update 20 June 2021, use size 60 pt. font, align center, center vertically, and give it some colour.
2. If text is inserted into the image: Size 20 pt. is good.
3. Export as a JPEG, not as GIF because the background will be transparent instead of white.
4. Edit with paint 3D, crop as 1:1 image (square).
5. Import into android emulator.

Posts created on Instagram with the same account ID as Facebook can be shared. However, Instagram posts will appear on your timeline, not in groups. Unfortunately, Instagram posts do not support clickable hyperlinks, limiting website traffic (Note 11). Instagram seemingly aims to confine users to the app, encouraging businesses to pay for inapp advertising and sales. As a result, it caters to a specific set of businesses, more suited for showcasing visually appealing products like watches or fashion.

In this scenario, consider embedding the entire text directly into the image rather than relying on the comment or caption section. However, if you intend to share the post on Facebook as well, it's advisable

to place the entire text and hyperlink within the comments. This ensures that the content appears on your Facebook timeline with clickable hyperlinks. Keep in mind that you'll need to manually share the post in your Facebook groups.

We import email lists into our contact app to "jump start" the network effect, leveraging algorithms to our advantage. This approach also helps us avoid being flagged or blocked since following our own contacts is not considered suspicious. Once you've uploaded a contact list and permitted Instagram to synchronize, you should begin receiving suggestions of people to follow along with accompanying text.



"Your contact, xyz, is on Instagram as zyx," or "xyz, one of your contacts, is on Instagram as @zyx. Would you like to follow them?" Accompanied by a 'Follow' button, this prompts these contacts to receive a similar suggestion to follow you, increasing the likelihood of reciprocal follow backs.

One limitation from a business standpoint is the inability to repost or retweet posts from those you follow onto your own timeline. This restriction hinders the broadcast of information posted by other users within your network.

02.3 Twitter.

In terms of engaging with customers, Twitter stands out as a primary platform. Businesses can use the "hashtag" system not only to share updates, facilitating brand visibility, but also to interact individually with users when necessary. With a user base exceeding 350 million, comprising 70% male users and nearly 30% aged between 2534, Twitter users are known for their prompt responses, inclination to share, and swift dissemination of thoughts. For rapid feedback, Twitter proves to be an ideal choice. A guide for setting up a private business Twitter is provided below.

Even after cycling through contacts multiple times, I noticed that when attempting to add new people to follow based on suggestions, I consistently received recommendations from the initial imported list. To address this issue between importing new lists, it's necessary to take the following steps:

1. Go to Settings -> Privacy and Safety -> Discoverability and Contacts.
2. Untick "Sync Address Book Contacts."
3. Click on "Remove All Contacts."

4. Allow 48 hours for the changes to take effect.
5. Upload a new list of contacts and reactivate contact synchronization.

This process ensures that Twitter starts fresh with your new list, providing you with updated suggestions and, more importantly, increasing the likelihood of appearing in the suggestions of your contacts.

02.4 LinkedIn.

Taking a significant departure from the previous options, LinkedIn offers a more professional platform. With a user base of 722 million people, 76% of whom reside outside the U.S., and nearly 60% falling within the 25-34 age bracket, LinkedIn presents a compelling demographic. Notably, 40 million individuals use the platform weekly to seek job opportunities, with over 55 million companies listed. For businesses aiming to connect with young professionals, recruit talent, or explore potential partnerships, LinkedIn emerges as a primary choice. Further details on leveraging LinkedIn for business will be discussed in-depth later in this article.

02.5 OK.

This application originates from Russia and exhibits a degree of network effect. Within its "add friend" feature, there is an "import friend" option offering various choices, each yielding different outcomes.

-**Phone contacts**Unable to find the contacts.

-**VK contacts**Unable to find anything, meaning VK contacts won't work.

-**Search by photo**You need to take a photo of yourself.

-**People online**It shows you a list of people you don't know. After some time you will get a notification "You are sending a lot of invitations. Please take a little break".

02.6 VK.

Much like OK, this platform exhibits a network effect. Within its "add friend" feature, there is an "import friend" option, providing choices for importing contacts.

-**Phone Contacts**Doesn't work.

-**OK app**Pulls same contacts from OK.

-**Gmail**You must provide a Gmail account with relevant contacts then.

-**Facebook**Doesn't work well with LDplayer.

02.7 Shapr.

Shapr lacks a network effect and doesn't sync contacts. Nevertheless, it's an excellent tool for connecting with professionals. It's impractical to retain inactive contacts within the app. Moreover, an excessive number of contacts might restrict new matches. Clearing inactive contacts often leads to new and relevant connections. After removing contacts you have plenty new "matches".

But before unfollowing them ask them to follow us on social media.

Ubinodes on Twitter: @Ubinodes

Love4aviation on Twitter: @Love4aviation

Love4aviation on Instagram: Love4aviation_Official

02.8 MeetUp.

Pro: You have the option to share your events on your Twitter account.

Con: You cannot delete a group that you've created, which can be frustrating. If you want to deactivate a group, you need to follow these steps:

Remove all participants.

1. Completely clear the participant list.
2. Modify the group title and description to indicate its closure. For example, you can change the title to "This group is closed" and craft a description with a minimum of 50 characters, such as "This group is closed. Deleting a group on MeetUp is not an option. It's an odd requirement, but now a unique 50+ character description is necessary."

02.9 Opportunity.

Link: https://www.myopportunity.com/

Pros:

- Synchronizes with contacts
- Presents you with potential contacts called "leads", in a manner similar to Shapr, making it easier to cold contact people.

Cons:

- Seems that most users are service providers, so it may be harder to find manufacturers but may allow us to find good candidates.

02.10 SilentPhone.

The app allows contact discovery by syncing with your phone. Initiating cold contacts directly through the app isn't advisable. Yet, using emails from the app for targeted campaigns like IT security or Sponsored Projects is a viable option.

If you're not using SilentPhone, you can send your email list to a Node user who is using it. This will allow them to identify other users of the app and extract their emails for potential targeted email campaigns in the future. Additionally, you have the option to create "communities" on Node, similar to Facebook. These communities can be categorized as Business, Thematic Community, Brand or Organization, Interest Group, Public Page, or Event, depending on your preferences and objectives.

Test:

For starters, we created a public page, but inviting "friends" to join your group isn't feasible without paying on VK. Later, we formed an "interest" group named "France Export Import," functioning akin to a chat group. This allows inviting your VK contacts to join.

P**ros:**

- Ability to create groups on Node.
- Various settings available for managing groups, including the option to designate administrators.

- When composing a post with a hyperlink, Node offers the feature to select an image directly from the linked webpage, streamlining the process without requiring the import of an image into the emulator.

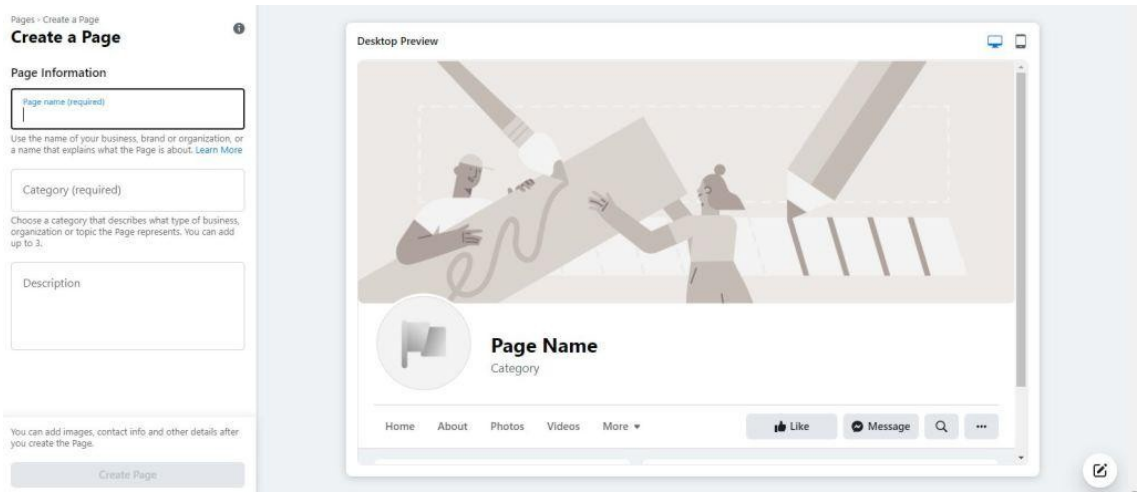
1. Creating the profile.

Now that you've decided which platform to use, it's time to create your profile. Make sure to use dummy information as we've discussed so far.

04.1 Facebook profile.

- Step 1: Go to this page: *facebook.com/pages/create* (https://www.facebook.com/pages/create). You must have a personal account beforehand, if necessary, create a new professional one.

> Step 2: Click "Get Started" under business and brand, you should see this page:



Step 3: Use your business or brand name as the page title.

Step 4: Select the category that best aligns with your business/brand offerings.

Step 5: Include a concise summary of your business/brand in the description section.

Step 6: Incorporate images to visually represent your brand for potential viewers.

Step 7: Verify both desktop and phone previews on Facebook, revisiting them frequently.

Step 8: Ensure you complete all available sections, then launch the page.

Step 9: Create your first post and start adding connections.

04.2 Instagram profile.

Step 1: Just like on Facebook, an existing account is necessary; the process involves converting it to a business account.

Step 2: Navigate to settings, locate the account section, and choose "switch to business account" at the bottom.

Step 3: Choose an appropriate business category and proceed to the next step.

Step 4: Enter your contact details and personalize your profile to reflect your business.

Step 5: Start posting images accompanied by relevant hashtags to build a follower base.

04.3 Twitter profile.

Step 1: Register an account at https://twitter.com/i/flow/signup (Note 12).

Step 2: Upload a profile photo (typically your logo) and header images (media showcasing your content).

Step 3: Set a display name (e.g., "@name") to enable tagging in other posts.

Step 4: Add a descriptive summary outlining your business and objectives.

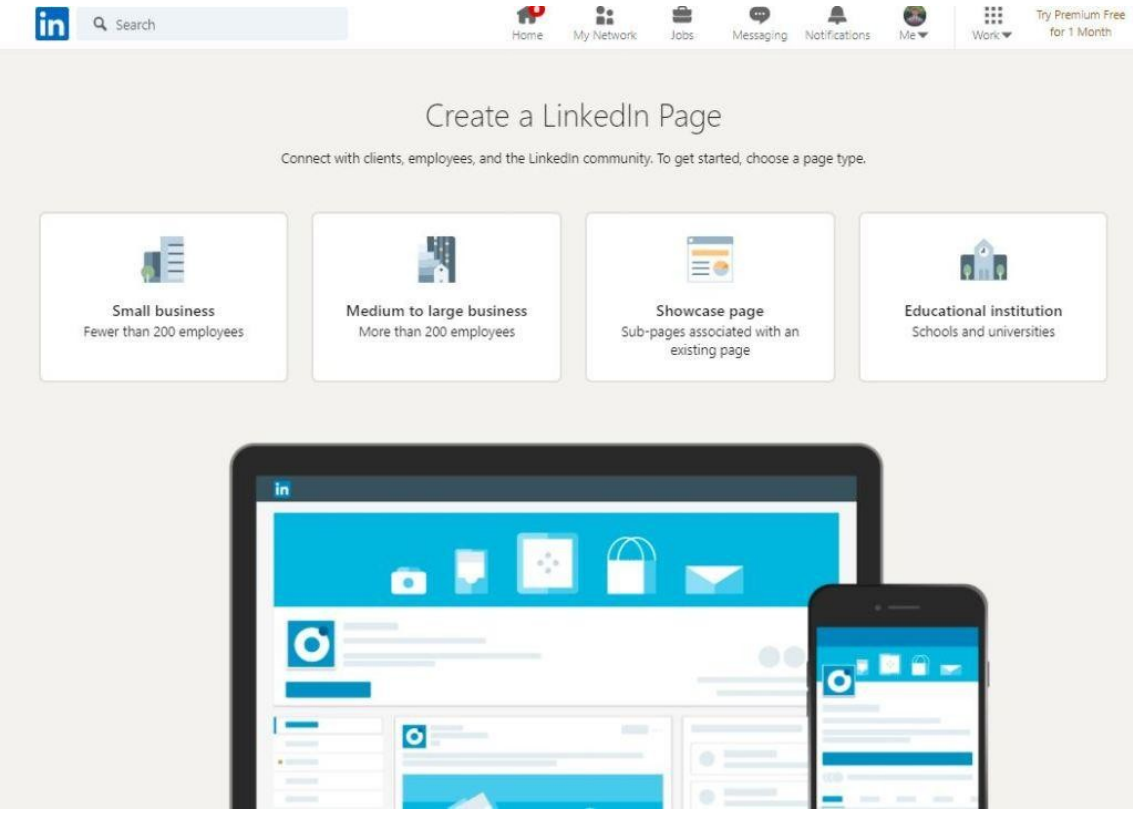
Step 5: Incorporate additional pertinent details about your business, such as hours, contact information, and location.

Step 6: Start posting, and pin an impactful post to attract viewer attention.

04.4 LinkedIn profile.

Step 1: Visit the following site: https://www.linkedin.com/company/setup/new/ (Note 13).

Step 2: Choose the option that most accurately aligns with your business size, ranging from small to large.



Step 3: Add all relevant profile information and ensure you verify your connection with the company.

Step 4: Select "Create Page" to start posting, establish connections, and actively engage with your community!

1. LinkedIn and further.

We prioritize LinkedIn as our primary social media account due to several reasons:

1. It serves as our primary business channel, offering a professional platform for business interactions.
2. Its functionality enables contact searches based on specific criteria like country or industry.
3. LinkedIn allows you to connect with people by synchronizing contacts or uploading email lists. On the other hand, Twitter only provides suggestions of people to follow, making it a less direct process that takes more time to grow your network and have your posts read by a significant number of people.

05.1 Android and iOS.

This manual primarily focuses on Android, given its prevalence as the primary OS for mobile devices. Nevertheless, the processes outlined here are equally applicable and functional on iOS devices. The only difference lies in the method for contact synchronization on your mobile device. For iOS users, we recommend using Woelkli, a CarDav compatible service, instead of Owncloud. Detailed iOS settings can be found here: *https://woelkli.com/en* (https://woelkli.com/en).

05.2 Android emulator.

We will use an Android emulator, Bluestacks, to access applications like Tutanota, Linkedin, and Twitter for this manual. However, if you possess an extra Android device lacking a SIM card, it can serve this purpose as well. It's crucial to emphasize that this device should be dedicated solely for this purpose. Under no circumstances should personal contacts be stored on this device, as platforms like Linkedin and Twitter may potentially retain and store these contacts on their servers indefinitely.

Pros and cons of using Bluestacks versus a separate android device:

Pros:

- More cost-effective; no need for an additional device.
- Enhanced privacy by routing all internet traffic through a VPN (like a router: https://www.expressvpn.com/vpnsoftware/vpnrouter) and using a burner phone. Android devices can track you even without a SIM card and in flight mode: https://www.youtube.com/watch?v=S0G6mUyIgyg
- Simplified message writing with a physical keyboard.
- Simultaneous multi instances support, enabling multiple accounts on the same computer. However, creating multiple accounts may require several burner phones or sharing them with other nodes. You can use the same Google account across multiple instances. When creating a new instance, refrain from cloning a previous one as it imports existing accounts; instead, create a fresh instance and reinstall all apps.

Cons:

- Not compatible with Linux operating systems.
- Requires staying at the computer to respond to messages.
- Limited ability to delete all contacts at once; manual deletion is necessary, making Owncloud the preferred option.

- In multi-instance mode, contacts are shared among all instances. Therefore, caution is needed when syncing contacts with apps; ensure the feature is set to manual for contact management between synchronizations.
- Exercise caution when simultaneously logging into multiple LinkedIn accounts, as it might flag shared IP usage as suspicious and lead to account blocking.
- Lacks a robust contact app; consider installing a different one. The default contact app in Bluestacks doesn't support selecting all contacts for mass deletion, a necessary function. Avoid installing the Google app, as it can cause confusion with Bluestacks' native app.
- Inability to directly copy-paste from the clipboard into Bluestacks. Therefore, create easily typable passwords for convenience.

Multi-instance:

We recommend you install these necessary apps on each instance for ease of use in the Google Play store:

- Tutanota.
- Cardavsyncfree.
- Linkedin.
- Twitter.
- Contacts.

05.3 About the email lists.

Exclusively for social media use: Email lists serve solely to connect with manufacturers and candidates through social media. Avoid any other utilization, particularly mass emailing.

List deletion protocol: Lists are used once per channel and then erased to evade algorithmic detection.

Categorized by country and volume: Thousands of emails are segmented into smaller lists based on intended usage: Desktop imports, Owncloud synchronizations, etc. Organization may also involve sorting by country through domain names and internet providers.

Leveraging LinkedIn's algorithms: To optimize efficiency, allow a 48hour interval between imports for the algorithms to process contacts and invitations.

Caution with LinkedIn suggestions: When importing, say, 50 emails from France, mainly from the aviation industry, resulting contact suggestions tend to align with approved invitations. Initially, selecting the same country and industry might be necessary to expand contacts. However, this initial choice could confine interactions within a specific industry. As contacts increase, diversify by choosing contacts from varied countries and industries to widen connections.

05.4 Share accounts.

Create a designated folder to store a text file containing all credentials and the profile photo. This allows seamless transfer of social media accounts, if required, use Resilio for sharing purposes. Feel free to request a template from a senior node.

Twitter: When transferring a Twitter account, modify the phone number in the settings since it's crucial for security and often used for account verification. The new user should insert their burner phone number into the account for continuity.

05.5 Profile photo.

To set the profile photo, opt for fake images accessible on Resilio or choose an avatar (such as an animal or an object) representing the node (you) across all platforms. However, as it's a personal social media account, the ultimate decision rests with you, even if it's employed for business objectives. If importing a photo, verify its uniqueness through TinEye Reverse Image Check at https://tineye.com/ to ensure it hasn't been previously used elsewhere.

05.6 Tutanota email.

Create a Tutanota email exclusively from your PC, using a mobilefriendly password. Note that Tutanota might temporarily freeze the account for 48 hours initially due to antispam measures; this is a standard procedure.

Consider upgrading to Tutanota Business. Your contribution supports service development and offers the ability to generate email aliases. This feature proves beneficial when regularly discarding social media accounts (without sharing them). With aliases, you can use the same inbox, creating a new alias for each social media account and discarding it when no longer needed.

05.7 Buffer.

- We use the SAAS Buffer for scheduling and simultaneous posting on Linkedin and Twitter: <https://buffer.com/>
- Create separate accounts for each instance, yet you can use the same Tutanota email for Linkedin and set a new password.
- Each Buffer account is linked to one Linkedin and one Twitter account.
- With the free plan, scheduling allows up to 10 posts daily.
- Given Twitter's 140character limit, concise writing is necessary for duplicating content. For different channels, longer content can be crafted specifically for Linkedin.

05.8 Delete every 6 months.

1. In a world of unstoppable global surveillance, the imperative solution is to minimize our data footprint.
2. The purpose of creating dedicated new social media accounts for Ubinodes is to:
    - Establish brand awareness for Ubinodes.
    - Promote our services to manufacturers.
    - Recruit diverse nodes from various countries and backgrounds.

We recommend deleting social media accounts every six months and creating new ones. Within this period, most contacts would likely be informed about Ubinodes, and interactions with manufacturers or candidates may have occurred. Past six months, social media algorithms tend to confine users by suggesting contacts with similar profiles, industries, or countries. For increased productivity and efficiency, it's advisable for nodes to regenerate accounts and upload new contacts every six months. After this period, an existing account serves little purpose beyond narrowing connections. Should you

wish to maintain long-term contact with social media connections, it's advisable to create another personal account, distinct from Ubinodes.

05.9 Next steps.

Step 1: Initiate a new folder on your computer labeled "3VLevel 4 Lists for Linkedin." Confirm this title to ensure recent changes haven’t altered it. Request the ReadWrite (RW) key and synchronize this folder with the team to share email lists.

Step 2: Follow the manuals precisely to create social media accounts as outlined below.

Step 3: On Linkedin, send invitations to other nodes; on Twitter, follow other nodes to enable sharing/retweeting of their posts. Locate them within the apps by searching for "Ubinodes."

Step 4: Set up a Buffer account and integrate your Linkedin and Twitter profiles.

Step 5:use Buffer to publish posts on your new profiles, promoting our previous articles and services to the audience.

Step 6: Maintain an active profile by regularly posting updates, exploring new manufacturers and nodes, synchronizing new contacts, and sending daily connection invitations.

1. Syncing contacts to LinkedIn.

06.1 Create an OwnCloud instance (desktop)

Open a free OwnCloud server: https://en.ocloud.de/product/owncloud.html

Note: you can't connect using a VPN.

Or you can use the one we share, via Zoho, make sure it's not being used by another Node, delete all previous contacts you may find in it.

IOS: owncloud isn’t free on iOS, you can use Woelkli instead. Then simply add the Cardav account in the iOS settings. Download: https://woelkli.com/en

06.2 Install CSV to VCF.

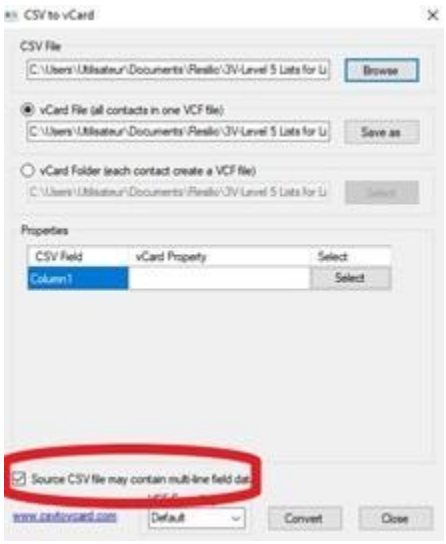
Download and install CSV to VCF converter: http://www.csvtovcard.com/

06.3 Prepare CSV file.

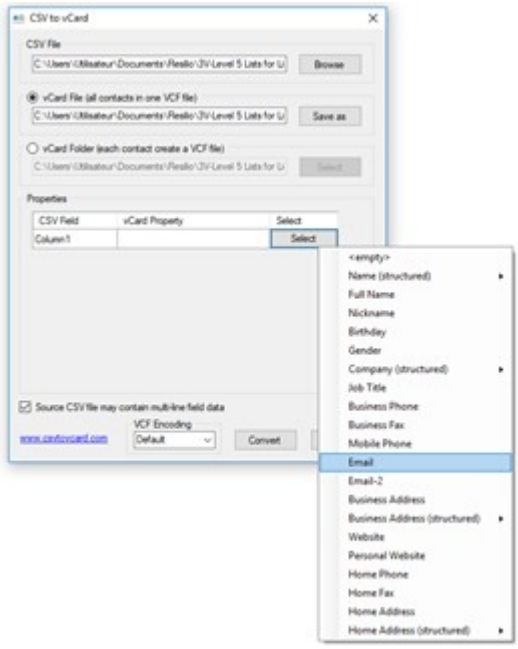
In the Resilio "3VLevel 5 Lists for LinkedIn", choose a .csv file, add a blank line at the top of the list, otherwise the first email won't be imported.

06.4 Convert the CSV to VCF file.

Step 1: Tick the box "Source CSV file may contain multiline field data".



Step 2: In the properties define the field as email.



06.5 Upload to OwnCloud.

Import your VCF file into your contacts by referring to the user manual: https://doc.owncloud.org/server/8.0/user_manual/pim/contacts.html

We recommend uploading approximately 1000 contacts. Note that in step 10, you can sync numerous contacts by repeating the process. It has been tested with over 7000+ emails successfully. However, while attempting with 9000+ emails, the account got blocked, and LinkedIn requested an ID to unlock the account, resulting in the loss of the account.

Make sure you always delete the imported files to prevent their use by another node or for alternative purposes.

06.6 Get link.

Access the settings on the bottom left of your Owncloud contacts page via the website. Locate the link provided for syncing contacts. Copy this URL into a .txt file.

Upload the .txt file onto your Owncloud's file page. This action enables easy access to the file from your device.

06.7 Install Cardavsyncfree on Android.

Play Store Link: https://play.google.com/store/apps/details?id=org.dmfs.carddav.sync

Grant authorization for Carddav to access Android's system.

use the URL and credentials from Owncloud to establish a connection with Carddav, enabling the synchronization of contacts.

Ensure to sync all contacts. It's crucial to use a burner smartphone to prevent the application from accessing and transmitting your private contacts to Linkedin's servers.

06.8 Install LinkedIn on Android.

Download the Linkedin app and create a fictitious profile using a Tutanota email and a burner phone: https://mobile.linkedin.com/

Before importing a photo, verify it using TinEye Reverse Image Check to ensure it hasn't been previously used: https://tineye.com/

Within the app, navigate to "add contacts" and grant authorization for the app to access and read your phone's contacts.

06.9 Invite people.

The Linkedin app will automatically send invitations to individuals on their network using the uploaded emails. This method enables you to send numerous invitations simultaneously without risking being blocked by Linkedin, as the app manages the process.

It's important to bear in mind that the contacts are uploaded to Linkedin's servers. Therefore, it's crucial to delete the files that have been used to ensure that no other node uses the same lists.

06.10 Add more.

You can expand your connections on Linkedin by repeating the process. Simply add new contacts to Owncloud and repeat the sync process.

1. In the LinkedIn app, navigate to your profile's settings → “Sync contacts” → Untick “Sync contacts from this device.”

> 2. Disable the "Sync contacts from this device" option.

> 3. Once you've uploaded a new VCF file in Owncloud, resync your device's contacts using opensync.

> 4. Return to the LinkedIn app's settings and reenable the "Sync contacts from this device" option. The app will prompt you to find contacts and send invitations.

1. Scripting LinkedIn.

There are two scripts you can use, depending on your purposes:

1^st^script.

Connects with all the users on the “People you may know” list.

```
setInterval(() => {
$('button[datacontrolname="invite"]').each((i, el) => el.click())
window.scrollTo(0, document.body.scrollHeight)
window.scrollTo(document.body.scrollHeight, 0)
window.scrollTo(0, document.body.scrollHeight)
}, 5e3)
```

2^nd^script.

Connects with a number of users you want. You just have to edit the number at the end of the script “*Here is the only change you have to do: Change the number 10 with the number of connections you want to do”.*

```
let arrUsers = [];
var numberOfUsers = 0;
var intervalUsers;
var lastWindowHeight = 1;
function startScript(numberOfCon){
numberOfUsers = numberOfCon;
connectWith();
}
function connectWith(){
runInterval().then(value => sendConnections());
}
function runInterval() {
return new Promise((resolve, reject) => {
intervalUsers = setInterval(function(){
window.scrollTo(0, document.body.scrollHeight);
if(numberOfUsers<=arrUsers.length || document.body.scrollHeight == lastWindowHeight){
console.log("Finishing interval, we already got enough users or we can not find anymore...");
clearInterval(intervalUsers);
resolve(1);
```

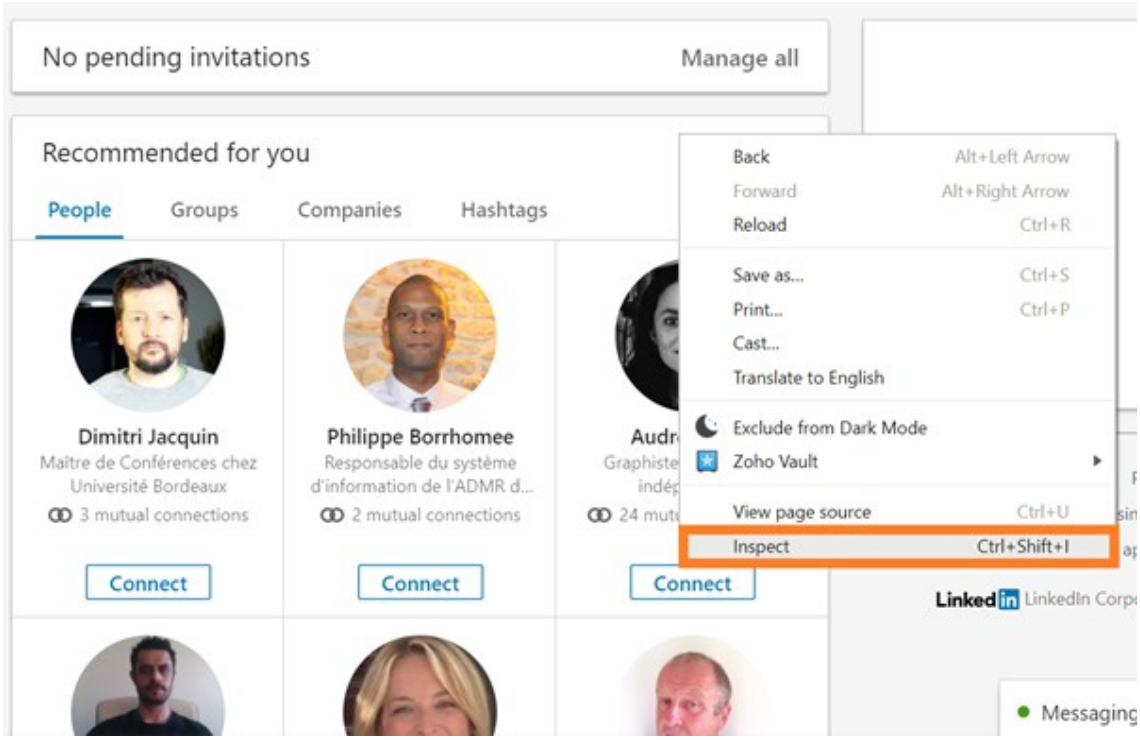
```
}
arrUsers = document.querySelectorAll('button[datacontrolname="invite"]');
console.log("We got " + arrUsers.length + " users (for now)...");
lastWindowsHeight = document.body.scrollHeight;
}, 2000);
})
}
function sendConnections(){
var totalConnectionsSent = 0;
for (let usr of arrUsers) {
if (totalConnectionsSent >= numberOfUsers) {
break;
}
usr.click();
totalConnectionsSent += 1;
}
console.log("FINISHED!");
console.log("Sent " + totalConnectionsSent + " connections.");
console.log("Developed by @Naulex (see me on BlackHatWorld forum)");
alert("FINISHED!nnSent " + totalConnectionsSent + " connections.nDeveloped by @Naulex (see me on BlackHatWorld forum)");
}
//
// Here is the only change you have to do: Change the number 10 with the number of connections you want to do: 1, 10, 37, 2184... and press enter.
StartScript(10);
```

07.1 How to use script.

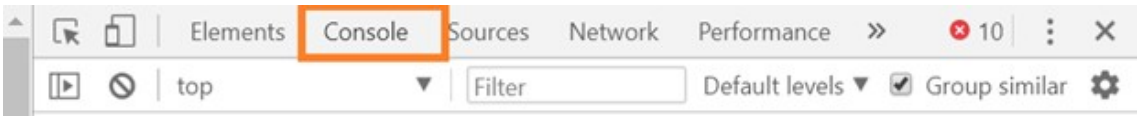
This example uses Iridium browser (Google Chrome based).

Go to: https://www.linkedin.com/mynetwork

- Rightclick on the area called “Recommended for you”. Then click on “Inspect”.

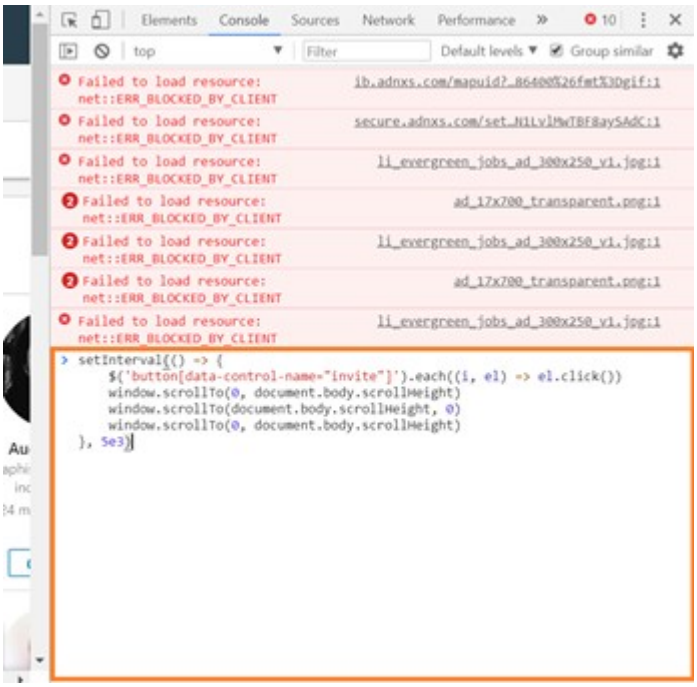


On the right a box will open. At upper part of that is a tab named “Console”, click on it.



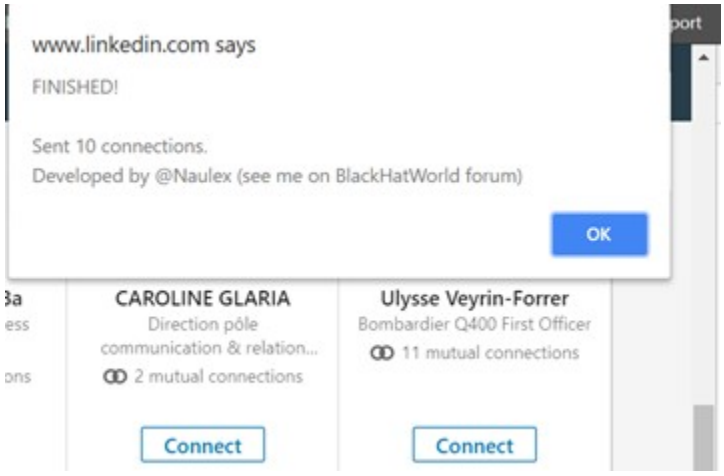
- Copypaste one of these two scripts, mentioned in the title “Scripts” in the box after this icon: > , as shown on the screenshot. Then click on enter.

The script will start scrolling the page and clicking on “Connect”. Just wait until the amount set by you connections are being invited or the limit of invites gets full, depending on which script you used.

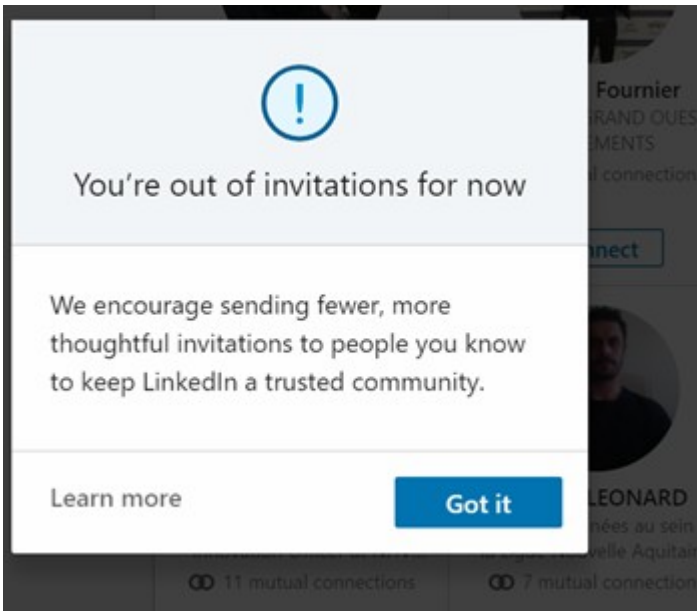


- When you are using 1^st^ script you'll see that it's sending out invites.

- When you are using 2^nd^ script you'll see this. Just click on "OK".



- If you have passed your invitations limit you'll see this message. Click on "Got it".



- Then, close the console from "X" and refresh the page so the script stops.

1. Twitter and further.

The rationale behind choosing Twitter for our social media strategy over other platforms is multifaceted:

using Twitter Deck allows granting access to Nodes for posting on the Ubinodes account.

This makes it simpler to monitor reciprocal follows, maintaining a balanced follower-following ratio. Additionally, you can usefllwrs http://fllwrs.com/faq

In contrast, on Instagram, determining who is following you back requires manual list comparison, posing long-term viability challenges. Facebook, on the other hand, is not suitable for business.

1. Dedicated mobile Android device: Install scrcpy: https://github.com/Genymobile/scrcpy for mobile use.

Pros: Mobility and connection with social media contacts.

Cons: Need another device. Not good for Communication Mantra as you may be interrupted by notifications all day long.

1. Android emulator: Use 32bit Bluestacks or LDplayer; *https://www.ldplayer.net/* (https://www.ldplayer.net/)

You can use any other Android Emulator. LDplayer has two benefits:

- Contact app ready to be used. No need to download one.
- GPS location spoofing ready to be used.

Pros: No additional device required. Optimal for safeguarding private data and preventing tracking, ensuring protection for your IMEI, IP (when using a VPN), and avoiding browser fingerprinting. No links to personal accounts and contacts. Ideal for Communication Mantra, activating the Emulator only when working on social media.

Cons: Requires a computer to use.

Step1: Use Tutanota to create a free account, dedicated to creating social media accounts and preventing your personal email from becoming a target for advertising and mass surveillance. This approach enables the periodic destruction and recreation of profiles, minimizing exposure to mass surveillance and advertising. Avoid sharing this email with people met on social media, as it serves as a shared email for all Ubinodes activities. Reserve this email solely for social media app credentials and other short-lived purposes, with eventual destruction after a specified duration.

Step 2: It's time to add contacts to your social media apps, allowing their algorithms to suggest your profile to individuals already using these platforms. We provide contact lists in CSV format, requiring conversion to VCF for importation using the freeware csvtovcard. Import all contacts before configuring apps to ensure synchronization with thousands of contacts from the beginning.

08.1 Import in VCF.

Pro: Removes the need to create a Gmail account. Immediate contact importing upon emulator launch.

Con: Requires CSV to VCF conversion.

If there's no pre-installed contact app, refer to step_03.

Note the differing contact usage: Shapr uses GPS positioning, while Twitter and Linkedin rely on contacts.

For LDplayer users, the process for importing multiple VCF files is as follows:

1. Import your VCF files into the emulator, typically stored in /sdcard/Pictures by default.
2. In the contact app, access settings at the right corner, choose import/export, then opt for import from .vcf file.
3. Navigate to the file manager. Click on the three dots at the right corner and choose "Show internal storage" to locate your VCF files' folder.
4. Display files as a list by selecting the icon depicting tiles at the right corner.
5. Click on the first file, hold the leftclick to select multiple files.
6. Once selected, click "open"; the files will be imported into the contact app.
7. After import, remove these files from the emulator's storage to avoid confusion in subsequent imports. Removing files from storage won't delete contacts from the apps.

08.2 Import CSV through Gmail.

If you prefer not to convert to VCF or want to import numerous contacts simultaneously, set up a Burner Gmail account following the provided user manual. Each import allows up to 3000 contacts, capped at a total of 25000 contacts. Ensure your emails are placed in the "Email 1 Value" column using Gmail's template for the import process.

Step 3:

1. Download and install Aurora from https://auroraoss.com/.
2. With Aurora Store, install:
    - A contact app (if LDplayer wasn’t installed).
    - Twitter.
    - Shapr.

- Xing.
- Linkedin (Note: Linkedin often blocks accounts, requesting ID verification; it's owned by Microsoft and part of the Prism program).
- If on a mobile device, install a location spoofing app like Hola Fake GPS.

Create accounts using your Ubinodes' ID. Spoof your location to match your country/state for local connections via apps like Shapr, aiding in networking with potential clients. Similarly, spoofing your location can help find prospective clients or nodes in other countries.

Step 4:

In app settings, enable contact synchronization for all apps.

In Twitter: Settings > Privacy and Safety > Discoverability and contacts.

On Twitter, over time, you'll receive "suggestions" of people to follow. To access these suggestions, click on your profile icon, then navigate to the page displaying the number of people you follow. From there, click on the icon with a plus sign (+) to add people, and you'll be presented with suggestions based on the contacts you've imported. Following these suggestions increases the likelihood of them following you back and becoming aware of Ubinodes. Since there's a daily limit on the number of people you can start following, it's essential to do this regularly to maximize your outreach.

As you're actively following many people to encourage follow-backs, it's important to periodically review the list of accounts you're following. Keep track of those who have followed you back and unfollow those who haven't reciprocated. This helps maintain a balanced ratio between the number of people you follow and those who follow you back. Over time, your following list will consist mostly of users who have followed you back.

After about a month of using the apps and engaging with contacts, it's likely that the algorithms have already suggested relevant connections. At this point, you can export your contacts from Google in CSV format to transfer them to another Node or client.

Once you've exported your contacts, import a new batch of thousands of contacts and resume the process from Step 4, continuing to engage with new connections and building your network.

1. Importing contacts to Google.

While Google is often considered unreliable and unsafe for business, this section provides guidance on managing contacts within Google. Employ a burner Gmail account, as previously discussed in the article, to maintain privacy and security.

09.1 First steps.

1. To cycle your contacts, start by deleting all existing contacts.
2. Afterward, ensure you empty the trash, as the contacts still count towards the limit of 20k. Failure to do so may trigger a notification when attempting to import new contacts.
3. Empty the trash multiple times, as each round deletes only a few thousand contacts, requiring several minutes to complete.
4. Upon importing, contacts are placed under "Labels" and won't display as contacts until manually selected and added.

5. However, they will appear in the contact app on Android and Emulators, allowing their use in social media apps without being added to Google contacts.

09.2 Tips.

- When importing contacts, note that there's a strict limit of 999 contacts per batch. To streamline organization, assign the imported list a label with the same name as the file you're importing. Otherwise, Google may assign its own labels, making it challenging to track which contacts have been used.

1. Creating a marketing strategy.

To create a successful social media strategy, marketers must tailor their approach to meet the needs and desires of their employees. This endeavour demands both time and resources, yet when executed effectively, it fosters a more dedicated client base. Follow these 6 essential steps to ensure client engagement:

1. Establish achievable goals.
2. Research your target audience thoroughly.
3. Identify crucial metrics to track.
4. Create compelling social content.
5. Ensure timely responses on social media.
6. Assess successes and areas for improvement.

The widespread use of social networks has altered how users access news and information. Consequently, adapting marketing strategies to mirror societal changes is crucial. Our primary objective in employing social media is to provide potential clients with a comprehensive understanding of Ubinodes' practices and services.

10.1 Set realistic goals for yourself.

It might appear improbable, but creating a social media strategy that cultivates a committed client community is entirely achievable. Your objectives play a crucial role as they determine the effort and time invested in your campaigns. Begin by addressing modest goals, like initiating a small forum with familiar participants. As engagement in the forum grows, the likelihood of followers or clients forming enduring connections within your network increases significantly.

10.2. Research your target audience.

To effectively reach your target audience, your first step involves identifying the most pertinent social media platform they actively engage with. For instance, if your aim is to engage millennials, platforms like Instagram or TikTok serve as ideal choices due to their substantial millennial user base.

Alternatively, if you're targeting women for your marketing campaign, establishing a presence on Pinterest would be advantageous, given its popularity among female users. Employing demographic data, akin to the aforementioned examples, aids in pinpointing your target audience. Once you've identified the appropriate platform, you can commence gathering pertinent data to support your objectives.

10.3 Decide what the most important metric you need to be aware of.

After collecting data on your target audience and selecting a social media platform to start with, it's crucial to determine which metrics are essential for achieving your goals. Three key metrics that I will prioritize are reach, clicks, and engagement, as I believe these factors drive followers or clients to commit to your network.

In social media terms, reach refers to the number of users who have seen your post. This metric is significant because it provides insight into the extent of your content's reach and effectiveness in reaching your audience.

Clicks are important in social media marketing as they indicate whether your content is resonating positively with your audience. Engagement covers the total number of interactions, such as clicks, likes, or comments, that your content receives. By analyzing these three metrics, you can quickly identify which content is performing well and which needs improvement.

10.4 Create engaging social content.

Your social media content stands as a pivotal element in the success of your marketing strategy. Once you've identified a theme for your content that garners positive reception, consistency becomes key. Maintaining a steady theme allows followers/clients to understand your brand more comprehensively, allowing you to pass your intended message. For instance, using a consistent banner format before your posts helps users get accustomed to it. Changes in format should only be introduced during transitions in viewership to maintain familiarity and engagement.

10.5 Be on time with your social media response.

You foster integrity within your page or channel by maintaining consistent activity through posts and replies. Engaging with your audience demonstrates respect for their time invested in your content. using the data from previous steps helps determine optimal posting times for comments and content to better connect with your audience. Swiftly responding to user inquiries or service requests is crucial. Followers/clients anticipate both promptness and a meaningful response when engaging with you. Timely and meaningful responses ensure your social media strategy operates seamlessly.

10.6 Decide what's working and what can be improved upon.

Over time, you'll identify what works well and where improvements are needed. If your content stagnates, analyse your analytics to discern necessary changes. Mastering this process takes time, so don't fret if your initial ideas don't yield results. Capturing an audience's attention lacks a perfect formula; trial and error is a commonly employed strategy. Seeking peer feedback offers valuable options and ideas for enhancing your social media strategy.

1. Conclusion.

When choosing an Android emulator, Bluestacks and LDplayer function similarly, with Bluestacks often running a bit faster, while LDplayer provides a contacts app and easier GPS spoofing capabilities.

Although the mentioned platforms are crucial, numerous others not included might better suit your company. Therefore, we urge you to define your specific platform needs. Use this article as a foundation to grasp the online profile creation process, but also explore other platforms and their respective audiences.

While the core process for establishing an online business presence remains consistent across platforms, it's the nuanced differences in their offerings that can significantly impact your company's success.

1. Notes.
2. This is done to hide your IP which gives away your location and identity. You can purchase plenty of such services online, a good one would be Protonmail (https://protonvpn.com/about).
3. The non-expiry ability will depend on the country you live in because in countries like EU States or the US you cannot have a non-expiry card if you don't register it. However you can generally register with dummy information. When you register online they ask you for identification details including ID or passport number but you can put dummy (fake) information. Make sure your VPN is connected before going to the website. If your provider doesn't offer online registration nor non-expiry ability, just let the SIM expire and purchase a new one, that's the cost of protecting its privacy.
4. Police, prosecutors etc. Their crimes are "legal" since they've corrupted state institutions. They are the most dangerous sort of criminals, to an individual or to a country. If they've done something illegal, they can cover it up any ways they like. They can intercept and read IMAP, POP3, TLS, SSL. They can spoof your email provider SSL certificate. They can have access to your SMS, emails, meaning a recovery option is often an easy attack possibility for them. That's why you should always use encryption software, encrypt your devices, and buy hardware outside the country you operate.
5. Because if it has been used before with a SIM card under your name you can be identified .Why is that? Every GSM phone has a unique ID called IMEI which cannot be changed. The instant you put a SIM into it, the phone will send to the carrier the IMEI which will be tied to the SIM which is tied to your identity, now the IMEI is tied to your identity forever, it's in the carrier registry which is shared with other carriers and state-sponsored criminals (3), you're burned. Even if you change the SIM, you can be tracked by IMEI.
6. When syncing your contacts, Facebook will allow you to select only 50 contacts. So it's of no use to upload a list of 10,000 contacts to get started with Facebook. However, there is after a very strong network effect, with many second degree contacts who are going to send you friend requests. In no time you'll be friend with enough people to create a room « Ubinodes_xxx – International Marketing » and invite all these friends. The drawback is that since your friend list is built trough requests, you will be trapped in a bubble of similar profiles, same country or same interests. That's of little use for our strategy. So with Facebook be prepared to create new accounts very often.
7. Reddit is asking you to link a Gmail account but it's not sure if it's syncing your contacts as it doesn't seem to be « suggesting » you to anyone.
8. It is difficult to upload photos using an android emulator, it's better to use an android device with scrcpy. When you create an event, the time displayed by the app is often wrong, so include the time in your title. When you create a group, give a descriptive name according to the actual context of your group. For example use "Club Export Burkina Faso" instead of "Ubinodes Burkina Faso".
9. VK is syncing through connecting with your Gmail or Facebook account. It is not looking into your contact app.
10. Facebook has over 2.7 billion users. Since it has the highest amount of advertising, there is a higher chance that your marketing can be lost in the storm. It assists with maintaining a customer base, not creating one. Furthermore, Facebook is "pay-to-play" in terms of marketing.

11. Instagram is great for companies without an advertising budget
12. See this article: https://www.pushbio.io/why-doesnt-my-link-work-on-instagram/
13. Individual Twitter pages can be converted to business pages, but it's recommended to start a fresh page.
14. Individual LinkedIn pages can be converted as well, but the process can be troublesome, and creating a fresh page seems to be a quicker process.
15. Sources.
    - Choosing the platform: https://aofund.org/resource/choosing-right-social-media-platform-your-business/
    - General social media information: https://www.createit.co.nz/blog/creating-engagement-in-an-environment-of-social-media-overload/
    - More social media facts: https://www.socialmediatoday.com/news/the-8-best-social-media-platforms-to-market-your-business-in-2021-infograp/595834/
    - Facebook facts: https://blog.hootsuite.com/facebook-demographics/
    - Instagram statistics: https://blog.hootsuite.com/instagram-statistics/
    - Twitter statistics: https://blog.hootsuite.com/twitter-statistics/
    - LinkedIn statistics: https://blog.hootsuite.com/linkedin-statistics-business/
    - Making Facebook page: https://blog.hootsuite.com/steps-to-create-a-facebook-business-page/
    - Making Instagram business page: https://business.instagram.com/getting-started
    - Making Twitter page: https://business.twitter.com/en/basics/create-a-twitter-business-profile.html
    - Making LinkedIn page: https://www.linkedin.com/help/linkedin/answer/710/create-a-linkedin-page?lang=en

GUIDE · 26 August 2022

Guide to Use Resilio Sync

1.2).

What article is this?

This article offers an in-depth look at Resilio Sync, a file- sharing application utilized within our network. It operates as a peer-to-peer networking tool, enabling users to share files stored on their local devices. The software allows for customizable file permissions, granting peers either read-only access or both read and write privileges to your documents.

Why do we need it?

Resilio plays a pivotal role in Ubinodes' operation, embodying its ethos of decentralization, security, and productivity. Prioritizing security, Resilio employs various network protocols for diverse tasks. Whether you're a client or a node at Ubinodes, expect regular interactions with Resilio. Familiarizing yourself with its features and functionalities is highly recommended for effective daily use.

TL; DR

Resilio Sync is a peer-to-peer networking tool, creating a network of connected devices for resource sharing. Its wide range of functions supports, for instance, a small development team to seamlessly share files during collaborative projects. The user-friendly interface lets you work on your computer, organizing files in folders just as if working solo. Meanwhile, the content of these folders is quietly replicated across all peers, reducing your workload by eliminating the need for manual content sharing and ensuring all team members are consistently up-to-date.

02.3.1 Pros and Cons of Advanced folders versus encrypted

Part 1:

Review

Part 1: Review

1.1 About the Resilio

Resilio, headquartered in San Francisco, California, is a key application Ubinodes employs for decentralized operations. Founded in 2016 by technical experts from BitTorrent, Resilio has become a trusted resource for both individual users and enterprise clients, offering secure and cohesive file transfer solutions across IP networks.

1.2 Application

Resilio Sync excels in rapidly synchronizing data across a network. Modifications to files on Resilio are instantly replicated on all connected devices. Its user interface is straightforward, facilitating secure file sharing without restrictions on size or data usage. This allows Nodes and Clients to exchange files in real-

time, peer-to-peer, bypassing the need for cloud uploads. Using BitTorrent's peer-to-peer technology, Resilio Sync identifies the fastest data transmission routes across devices. It supports file synchronization both locally and over the internet, adhering to the BitTorrent protocol. This capability enables decentralized organizations like Ubinodes to manage their file-based data across various devices, locations, networks, IT infrastructures, and cloud providers, integrating dispersed data and devices. A significant advantage of Resilio Sync is its continuous network availability. Even if a computer is off and a folder is inaccessible, work continuity is maintained, enhancing employee uptime and productivity. Ubinodes prefers Resilio over other cloud services, largely due to the cost-efficiency in maintaining cloud infrastructure.

1.3 Security

Resilio's robust security management features, including SHA- 256 hashing and TCP/UDP forwarding protocols, make it an ideal file-sharing solution for Ubinodes. This aligns well with Ubinodes' emphasis on security, particularly in the face of potential breaches common in borderless and transnational organizations. Ubinodes prioritizes security over convenience, a principle mirrored in Resilio's design. The software consistently places security first, utilizing various network protocols for specific tasks. Resilio Sync, as a key part of our suite of

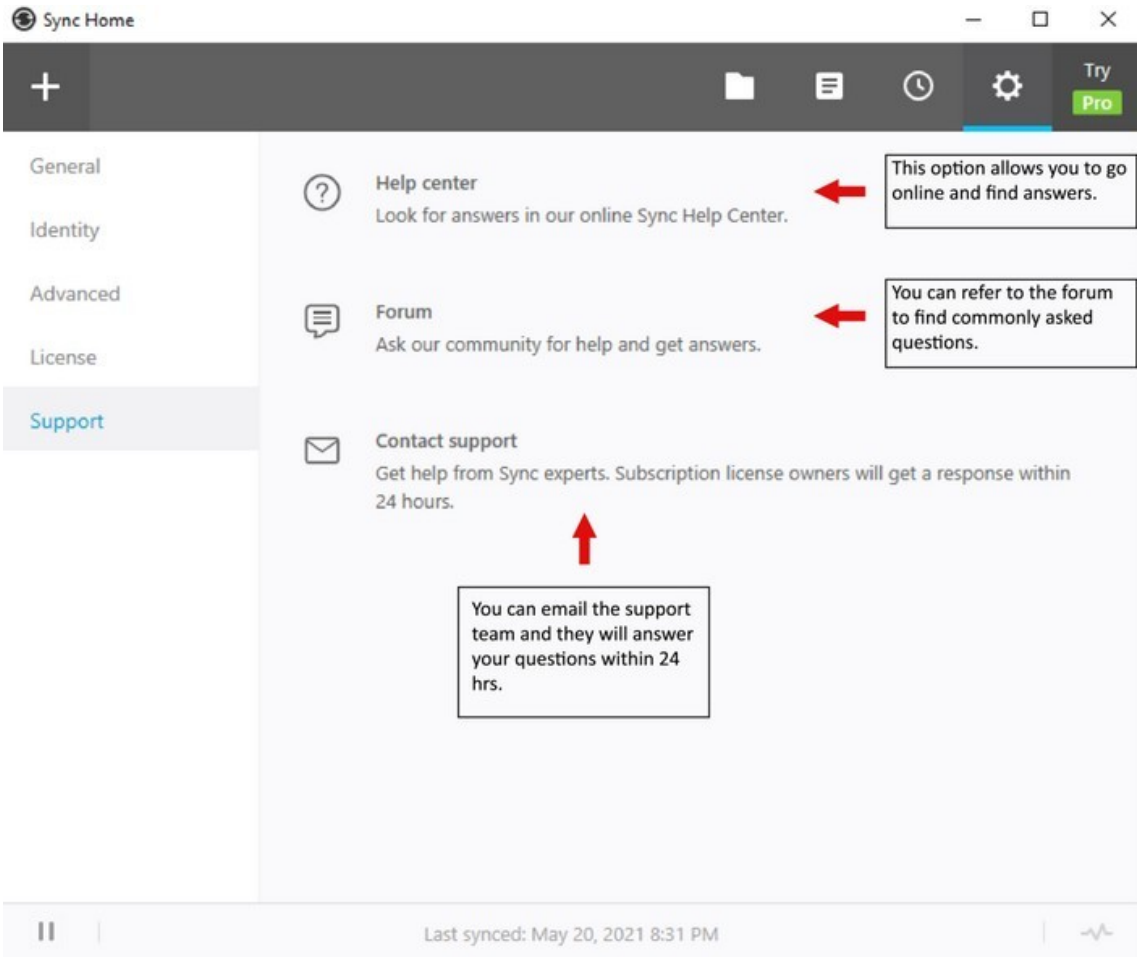
encrypted applications, enables nodes to securely share files with peers and clients remotely. This ensures that project security is maintained and sensitive data is transmitted through secure channels, crucial for the integrity and success of operations at Ubinodes.

1.4 Download

Resilio Sync is available for download on multiple platforms including Windows, Mac, Linux, and FreeBSD. It offers both mobile and desktop app versions, ensuring seamless file synchronization across all your devices. Download the Resilio Sync Home version Resilio must be installed on the C: drive, but the folder you use for syncing can be located anywhere, including removable devices. Additionally, you have the option to upgrade to the Home Pro license directly from the user interface at a later time.

1.5 License

The key differences between a Pro license and a standard license in Resilio Sync are as follows: 1. Folder Types: With the standard Sync Home, users can only create standard folders. In contrast, Sync Home Pro allows for both standard and advanced folders. Standard folders restrict user control over access permissions and sharing capabilities. Advanced folders, available in the Pro version, give users the flexibility to change or revoke access permissions at any time. For example, altering a folder's permission from 'Read Only' to 'Read & Write' doesn't require removing and re-adding the folder; it can be done easily with a single button in Pro, maintaining the existing connection. This feature makes advanced folders more suitable for collaborative work. 2. Device Identity Management: The Pro license offers a streamlined identity management system. Unlike the standard version, where an identity must be created for each device, the Pro version allows users to link all their devices under a single identity. This integration means that any folder added on one device, like a desktop, will automatically be available on all linked devices, such as a mobile phone or laptop. This feature enhances ease of access and synchronization across multiple devices.



01.6 Support

In the user interface of Resilio Sync, you have access to various support channels for assistance and guidance.

This section offers multiple support resources for users. It features a 'Help Center' option, directing users to Resilio's online Sync Help Center for answers to common queries. Additionally, there's a 'Forum' option, where users can interact with other Resilio users, ask questions, and seek assistance. Lastly, the 'Contact Support' option connects users with Sync experts for specialized help.

Part 2: Guide

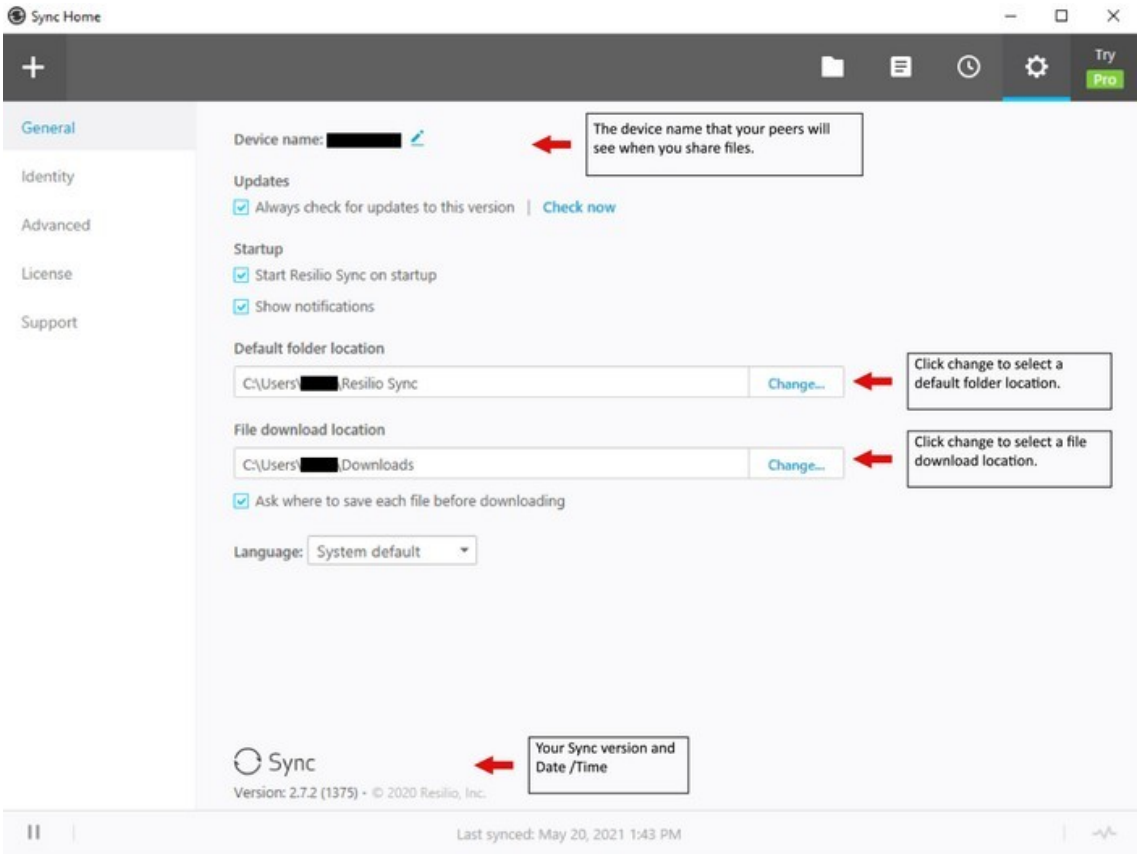
Part 2: Guide

2.1 Preferences

On the homepage of Resilio Sync, you can find the settings button positioned at the top right of the page. Within this section, you will encounter five distinct preference options:

1. General. 2. Identity. 3. Advanced. 4. License. 5. Support.Screenshot: Settings.

Device Name. By default, Resilio Sync automatically assigns your computer's name as the device name, but it's important to customize this for clarity among peers. The device name should be recognizable and relevant to your peers, not just to you. For Ubinodes members, it's expected to change this name to your Ubinodes ID. This helps other nodes and colleagues identify when you are online and avoids simultaneous file access, which can lead to synchronization conflicts and potential data loss. The last file closed could overwrite any work done by teammates. For instance: - Good Name: "Node013_Desktop" (or Android, Macbook, etc.). Including the type of device is useful; it indicates whether you are likely editing a document (as on a computer) or not (as on a mobile device). - Bad Name: Simply "Windows". This doesn't clarify who the user is or the type of device being used.

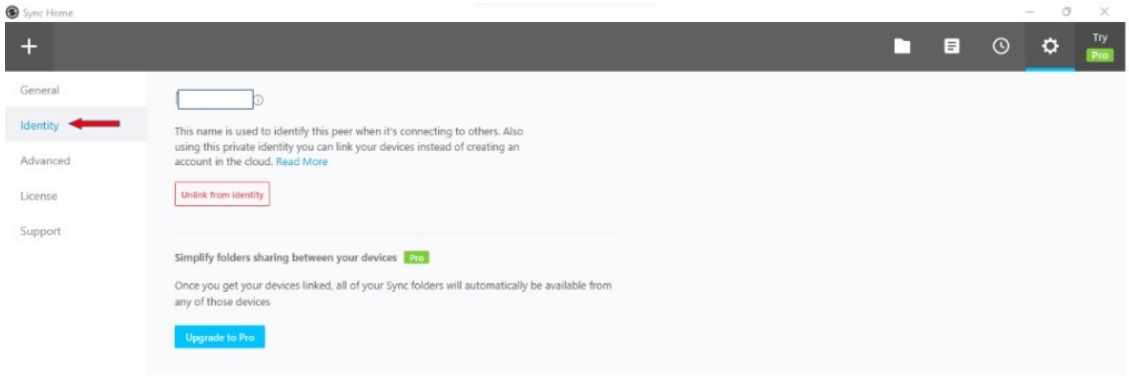


Start Up. Upon updating your device name in Resilio Sync, it's advisable to uncheck the option that says "Start Resilio Sync on startup." This step is particularly important if you're using a USB drive for data storage, separate from the device's operating system. Ensuring that your USB drive is properly mounted before Resilio Sync launches will help maintain data synchronization and prevent potential issues. Default Folder Location. You have the option to select a default folder location for your files in Resilio Sync.

However, it is recommended to keep the option "Ask where to save each file before downloading" checked.

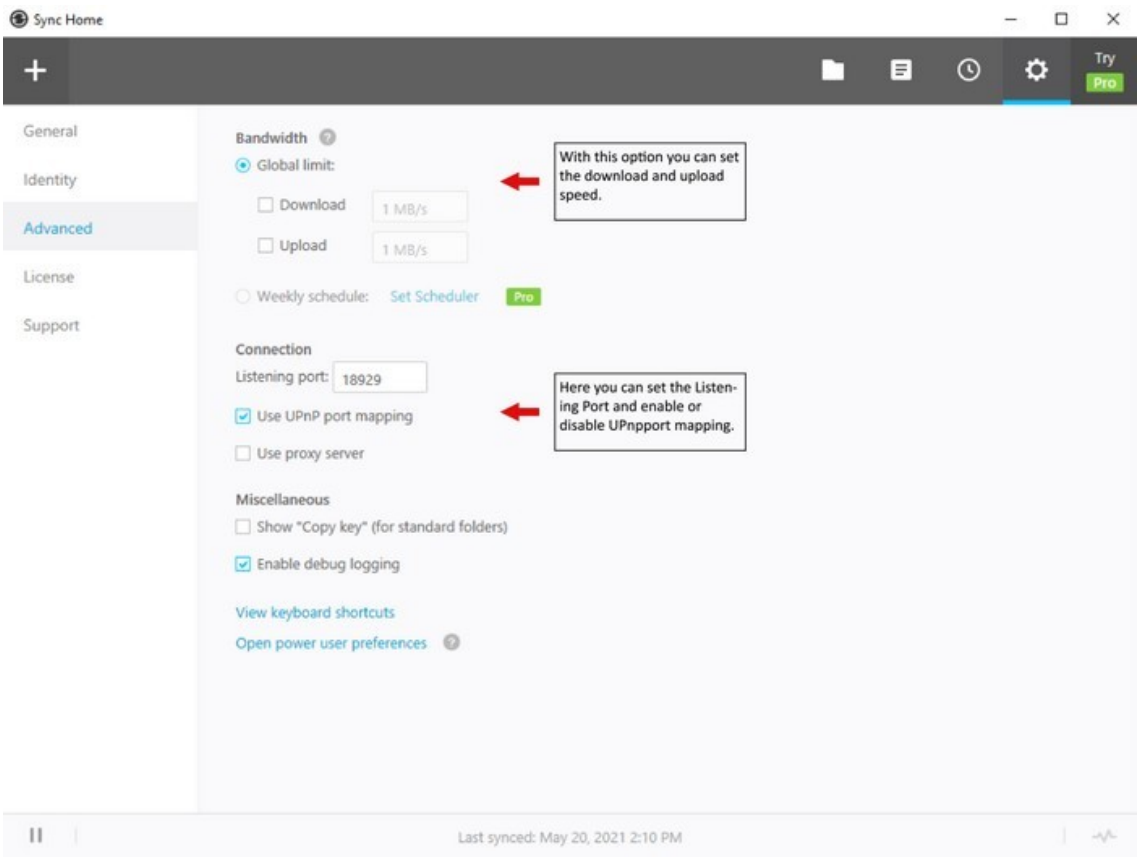
Given the specific way folders are classified in your setup, you'll likely need to assign different locations for each new folder as it's created. This setting ensures you can choose the appropriate destination for each file, maintaining your organization's classification system.

Screenshot: General.



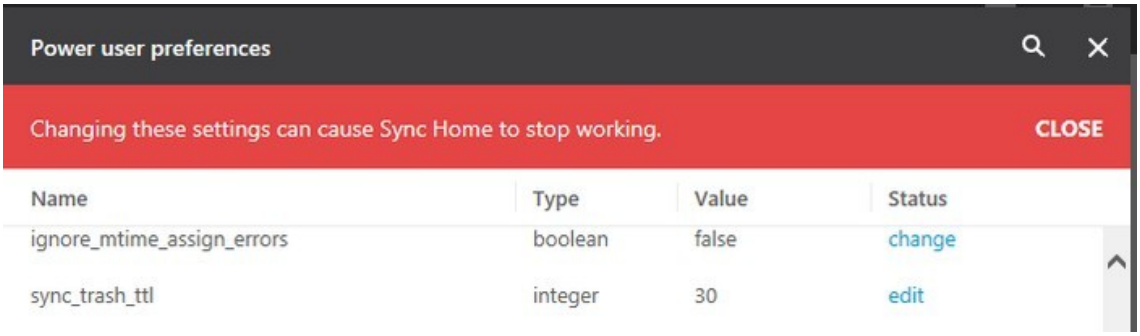
Identity. The identity of your Resilio account is linked to the name you set. This is particularly significant for Pro license holders, as it enables you to unify all your devices under a single license. Once linked, all your folders will be visible in your user interface. This allows you to selectively choose which folders to synchronize on each device, giving you control over the synchronization process on a device-by-device basis.

Screenshot: Identity.



Advanced. Within the Advanced tab in Resilio Sync, users have the ability to adjust settings such as the sync's bandwidth, connection port, and debug logging. However, unless you have specific knowledge or requirements, it's generally not necessary to modify these settings. Resilio is designed to perform efficiently with its default configuration, so most users find that it works well right out of the box.

Screenshot: Advanced.



Trash. In Resilio Sync's Advanced section, navigate to the "Open power user preferences" option at the bottom. Scroll down until you locate the "sync_trash_ttl" setting. Click "edit" and adjust the time from the default 30 days to just 1 day.

This setting controls how long data remains in the ".sync/Archive" sub-folder, essentially Resilio's version of a recycle bin, where deleted files are stored temporarily. By changing this duration from 30 days to 1

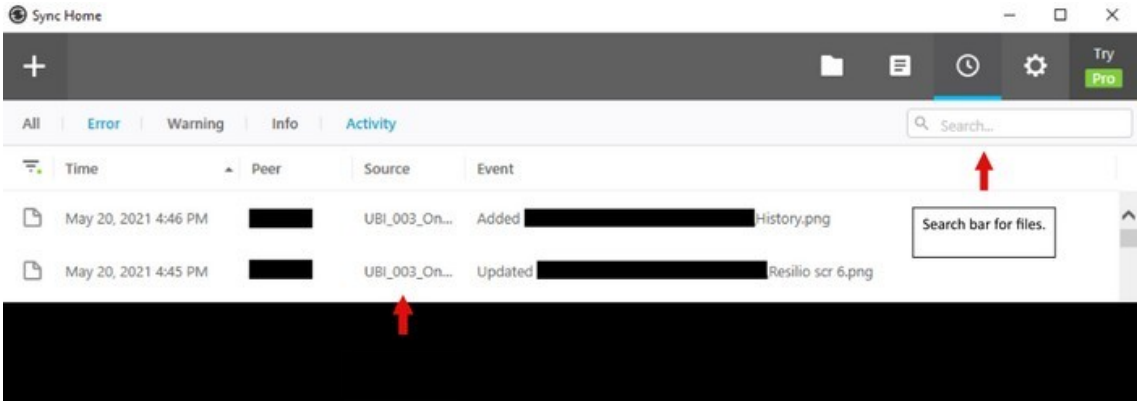
day, you actively reduce your digital footprint, ensuring files in your "sync/Archive" sub-folder are automatically cleared after just one day.

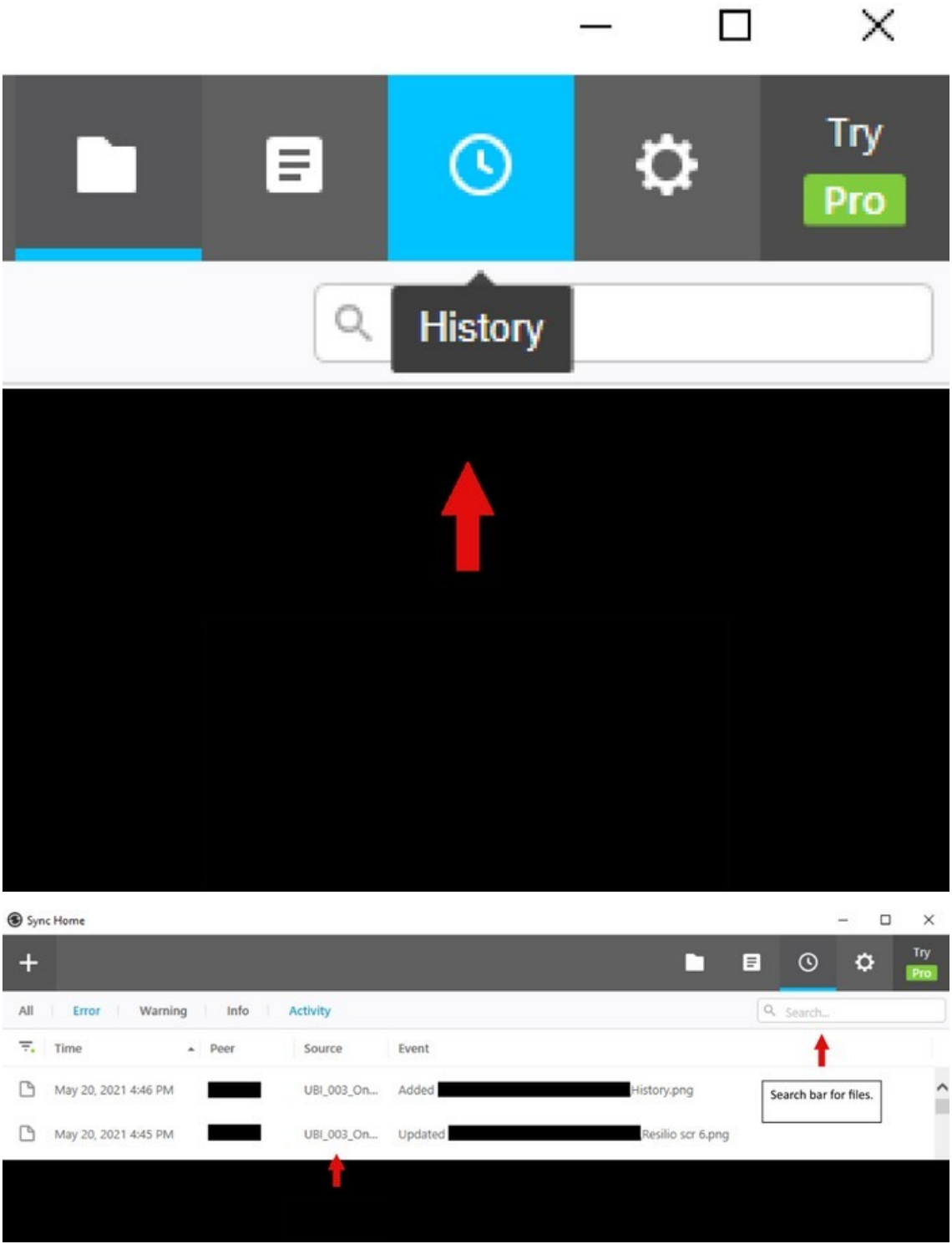
Screenshot: Trash.

History. Users can conveniently search for uploads in Resilio Sync using criteria like errors, warnings, info, and activity. This feature is particularly helpful in ensuring that teammates have received the most recent version of your work or any newly added files, eliminating the need to confirm via messaging apps or email.

When you select a search criterion, the interface displays metadata about previously sent files. Starting from the left, you'll see a timestamp indicating the date and time of the upload. Following this is the peer who shared the file or folder. Next, you'll find the source folder and the event, which includes the file path. If you're looking for a specific file, you can use the search bar located at the top right of the page.

Additionally, at the bottom left of the page, there's an option to pause syncing. This is useful because Resilio





continuously updates, allowing you to see when a file is in the process of syncing.

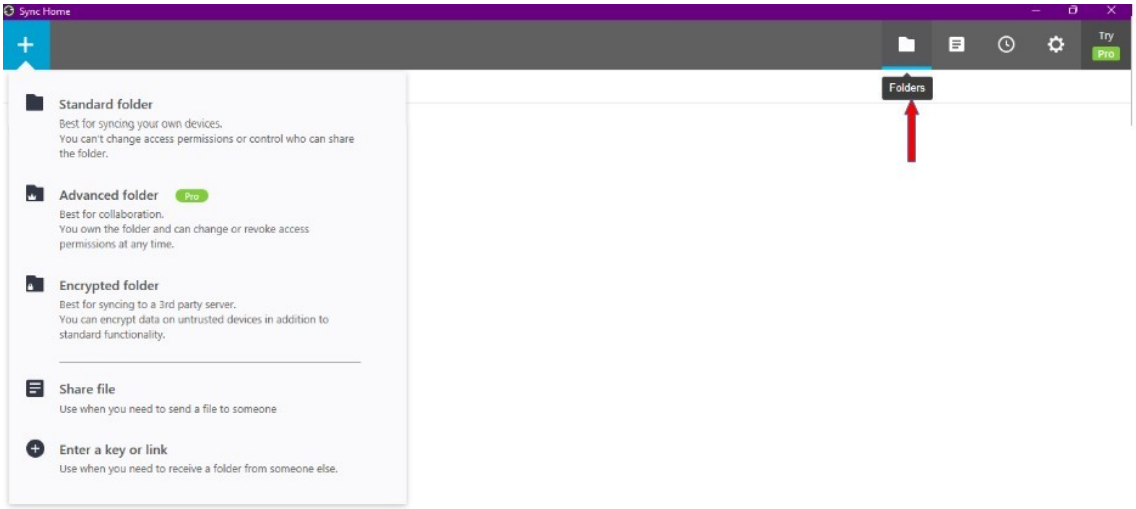
Screenshot: History Tab.

Screenshot: History View.

2.2 Naming Folders

Before adding a folder to Resilio Sync, it must first exist on your computer. Here are the steps to follow: 1. Create the Folder: Firstly, create a new folder on your computer in the location appropriate for the data classification you are using. 2. Name the Folder: Give this folder a name that is meaningful for teamwork. The name should be clear and descriptive to ensure everyone on the team understands its contents and purpose. 3. Add Content and Sync: Once the folder is created and named, you can add the necessary content to it. After this, the folder is ready to be added to Resilio Sync. In Ubinodes, it's important to prefix each folder name with "UBI" unless you are using Resilio for a different purpose. This practice helps to avoid confusion when handling files. For naming conventions, underscores (_) and hyphens (-) are used, particularly because some nodes and clients may be using Linux. Underscores are utilized to connect individual characters that are part of the same information set. Hyphens, on the other hand, are used to separate different information groups. Here's how this works in a folder name: - Numbering: For instance, “UBI_002_Onboarding”. - Confidentiality Level: Such as, “Level_1”. - Purpose: Like, “Node_023”. The complete folder name would be “UBI_002_Onboarding-Level_1- Node023”. The underscore (_) connects characters within a group, while the hyphen (-) separates different information groups. Privacy.

When your Resilio Sync application connects to peers, it retrieves their IP addresses from a server based in Resilio's offices in the United States. During this process, the name of your folder is transmitted in clear text.



Therefore, it's crucial to be mindful of how you name your folders. Inappropriate or sensitive names, such as "recipe for cocaine," should be avoided for security and privacy reasons. It's important to note that while the folder names are transmitted as is, the content within these folders is encrypted before being sent to your peers. This ensures the confidentiality and security of the actual data being shared.

2.3 Adding Folders

Resilio Sync offers secure and straightforward file sharing with no usage or capacity limitations. Its peer-to-peer sharing mechanism ensures instant file transfers, eliminating the need for cloud uploads. The software provides multiple methods for adding folders to your Resilio account, making them accessible from any of your local machines.

To share folders within Resilio, click on the plus icon located in the top left corner of the application. After clicking this icon, you'll be presented with three folder type options: Standard folder, Advanced folder, and Encrypted folder. Each type caters to different sharing and security needs, allowing you to choose the one best suited for your specific requirements.

Screenshot: Folders.

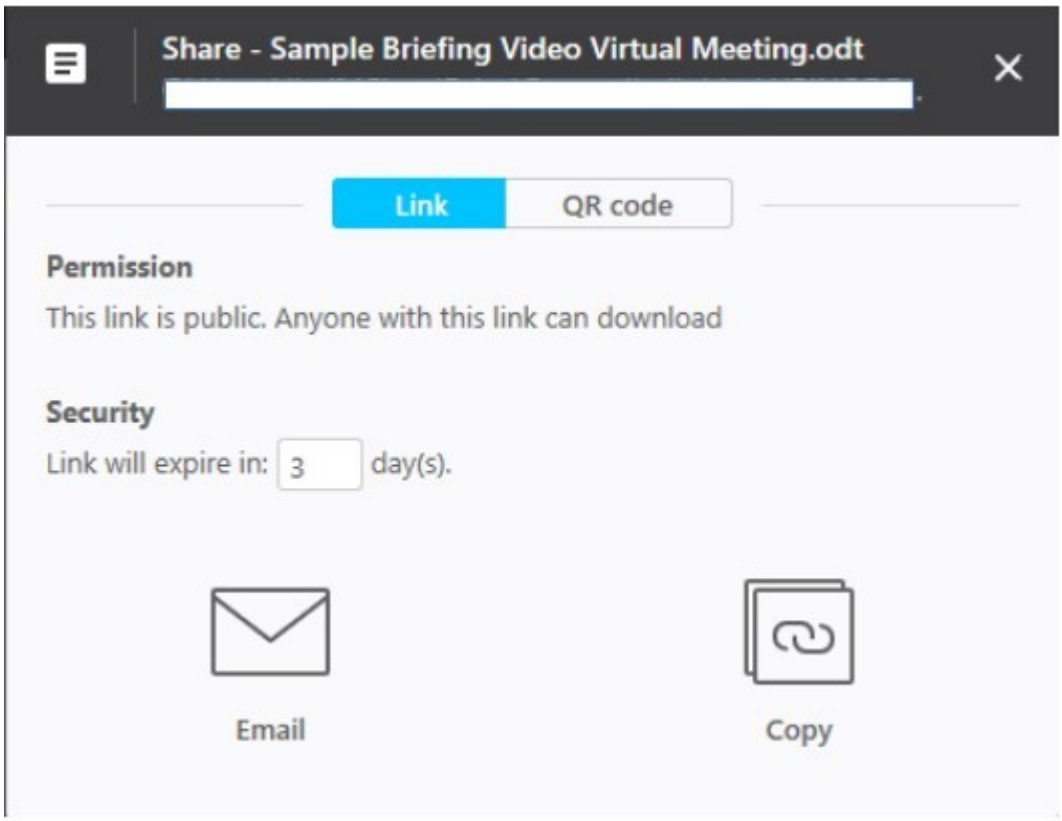
- Standard Folders: Ideal for syncing folders across your personal devices, this option allows users to both grant and manage permissions for a folder. It's a straightforward choice for basic file sharing and synchronization needs.

- Advanced Folders: Suitable for collaborative work involving multiple people. As the owner of an Advanced Folder, you have the flexibility to modify and revoke access permissions whenever necessary. This type of folder is exclusive to the Pro version of Resilio, offering enhanced control for managing collaborative projects.

- Encrypted Folders: Optimal for syncing to third-party servers where data security is a concern. In addition to the standard functionality, this folder type enables you to encrypt data on trusted devices, ensuring that your sensitive information is not transmitted in plain text. This feature is particularly important when the integrity and confidentiality of the data are paramount. Pros and Cons of Advanced folders versus encrypted folders. Advanced folders.

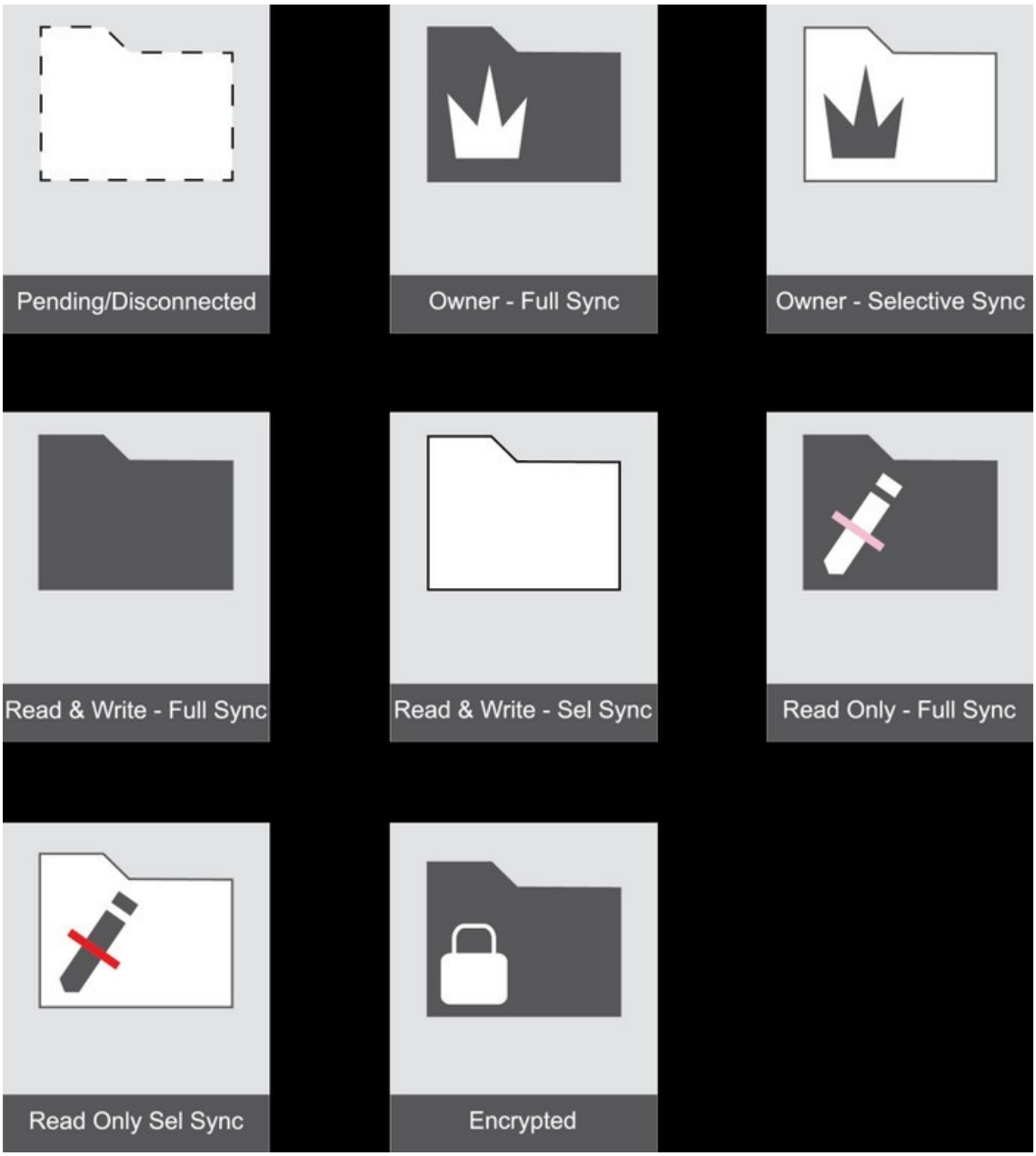
Pro: New peers must be approved, so the notification will help detect MITM attacks. Cons: Can't use encrypted folders to use untrusted servers as relay. To give "owner" rights, the peer must have a paid "pro" license. Encrypted folders. Pro: Can use untrusted server as 24/7 running relay. Anyone with the read key can receive the files; other peers won't get any notification.

2.4 Sharing keys



Screens

hot: Sharing. Nodes and clients in Resilio Sync have the capability to set expiration times for shared links, as illustrated in the figure. After selecting a time frame, nodes can either automatically email the link to their files or manually copy and paste it into a document, such as a Word file, or onto a storage device like a flash drive. It's vital to remember that Resilio Sync does not utilize cloud storage for data transfer. Therefore, all devices intended to use the link must have Resilio Sync installed and actively running. Besides sharing folders via a link, nodes and clients can generate a QR code for scanning by a phone or any QR scanner. Similar to systems like Bitlocker and Wickr, Resilio employs keys for folder sharing. There are distinct keys for Read-Only and Read & Write permissions, allowing precise control over access levels. When sharing a folder with someone outside your account, you can grant them either read-only or read-write access. This system maintains security as any file sharing must be authorized by you. Even if a shared code is distributed online, access remains restricted to those you have explicitly



approved, ensuring that your files remain secure and accessible only to intended recipients.

Folder States.

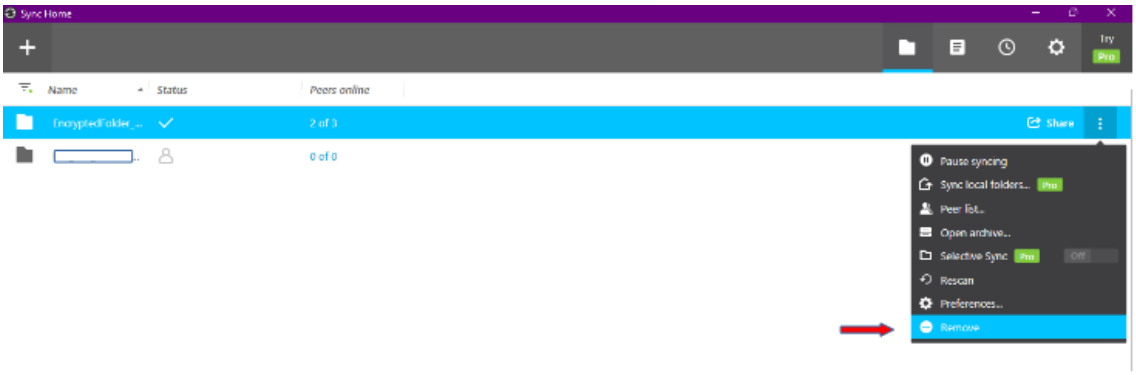
Folder States in Resilio Sync are designed to manage how folders and their contents are accessed and synchronized across devices. Understanding these states is crucial for effective file management: 1. Pending State: This state occurs when a folder requires approval from the owner. If you have already been approved by the owner, this state won't activate. Once approved, the folder connects to the online storage device. If you disconnect a pending folder, it will disconnect from all linked devices. 2. Selective Sync: In this mode, a folder uses minimal hard drive space. Files within a selectively synced folder are replaced by placeholder files. When a placeholder file is double-clicked, Resilio fetches the full file from the source device. This feature is designed to conserve hard drive space. 3. Full Sync: This is when all files

in a folder are fully synchronized across all devices. The process happens automatically and overrides selective sync, ensuring that all devices have the same files in real-time. 4. Read-Only: Folders set to Read-Only prevent users from making changes, removing, or deleting contents. Local settings might allow changes to your local copy of these files, but such modifications prevent updates on the Read-Only file from being received. The crown symbol indicates ownership, and as the owner, you can grant peers access.

5. Encrypted: This state is ideal for backup in untrusted environments, like when adding a folder to a Virtual Private Server (VPS). It helps prevent unauthorized persons from accessing your data. Each folder state in Resilio Sync offers different levels of access and synchronization, allowing you to tailor the functionality to your specific needs and security requirements. Screenshot: Folder State.

2.5 Updating Files in Folders

When updating files on Resilio, especially files created and shared by other nodes or clients, the name of the files should not be changed as it can cause confusion between other nodes and clients connected to the file. If anything must be changed, it should be the date which would usually be the first thing on the name of the file. That way, nodes and clients can be informed if a file is freshly updated or old. Another thing to be careful of when updating files or folders are duplicating. Duplicating files or folders that are synced with other nodes or clients can cause discomposure. It is important to understand that folders are created for specific tasks and once the task in question is completed, folders should be permanently deleted so as to not be recovered. Hence, nodes or clients should never make duplicates or backups. Not only does it confuse other nodes and clients, but, more importantly, it creates security breaches. When working on a shared document, do not save it under a new name, like "xxx updated". This would just add to the confusion. Realise that your fellow workmates are working on other projects and are dealing with dozens of files everyday. Before opening a file, you are expected to ensure that no one else is already on it. Resilio sync doesn’t allow to work simultaneously on a file, so if two people have opened the same file at the same time, the last one to close it will overwrite the previous version meaning that one person will lose its work. You can use chat apps like Wickr or simply see in Resilio if you're the only one online. Through chat apps, you can let others know when you have made changes to a file. Lastly, when working in resilio. It is important to make sure that you are connected with a Relay in order to ensure that your updates are being broadcast to other nodes when they are online. You can find out if you are connected to a relay on resilio by clicking on the "peers online" tab where folders are located. Once there, you can find which relays are online or offline at that moment. Make sure you’re online and connected to a 24/7 ResilioRelay peer to make sure your updates will broadcast to other peers. While working on a file, once you close it, it will synchronize, provided you are connected to the internet.



We have servers called “Resilio Relay” running constantly (24/7). Your file syncs with them, once other peers switch on their PC’s and start Resilio, the file would update from a central server “Resilio Relay” or any other node that is up to date. You get a notification that Resilio is syncing and updating its internal database, this can be found in the hidden .sync folder. In a situation where you force a shutdown of PC, this process may not complete and you’d get a corrupt database error from the app. In a situation where this error occurs, there’s no other option than to recreate the folder from scratch.

2.6 Removing a Folder

To remove a folder from Resilio Sync, follow these steps:

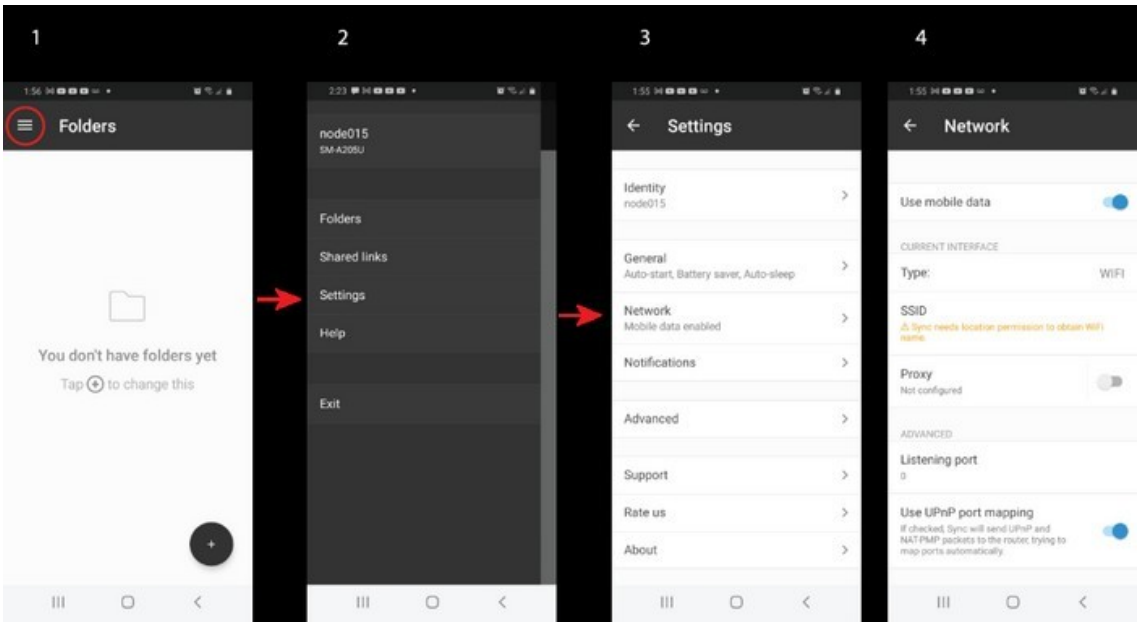
1. Navigate to the folder icon on the navigation bar and left- click it.

2. Find the folder you wish to remove. Once located, hover over the sub-menu icon next to it and left-click to reveal the dropdown menu.

3. Select the "remove" option. This action will delete the folder from Resilio Sync, but it will not affect the folder on your local machine.

It's important to delete obsolete files to ensure that the content of your folders remains intuitive and up-to-date. Regularly managing and removing unnecessary files helps maintain an organized and efficient syncing environment.

Screenshot: Removing.



2.7 Mobile Device

In this guide, we'll explore the Sync settings available on major mobile devices, including Android and iOS. To begin using the mobile version of Resilio Sync, follow these steps:

1. Download the App: Go to the app store on your phone (Google Play Store for Android or Apple App Store for iOS) and download the Resilio Sync app.

2. Create and Link a Test Folder: To familiarize yourself with the mobile application and its various settings, we'll start by creating and linking a test folder.

a. Create a New Folder: Tap the “+” button to create a new folder. You'll then choose the type of folder you want (Standard, Advanced, or Encrypted).

b. Link to a Computer: To link this folder to a computer, use the key provided in the folder's details window. For this demonstration, we're creating a new folder, but you can also link an existing folder using a QR code or a key.

By following these steps, you can effectively set up and manage folders in Resilio Sync on your mobile device, ensuring seamless file synchronization between your phone and other devices.

Screenshot: Mobile Device Folder.

Once you've created a folder in the Resilio Sync app on your mobile device, you can start utilizing its features:

1. Creating and Sharing Sub-Folders: You can create sub- folders within the main folder and share files directly from your phone with peers.

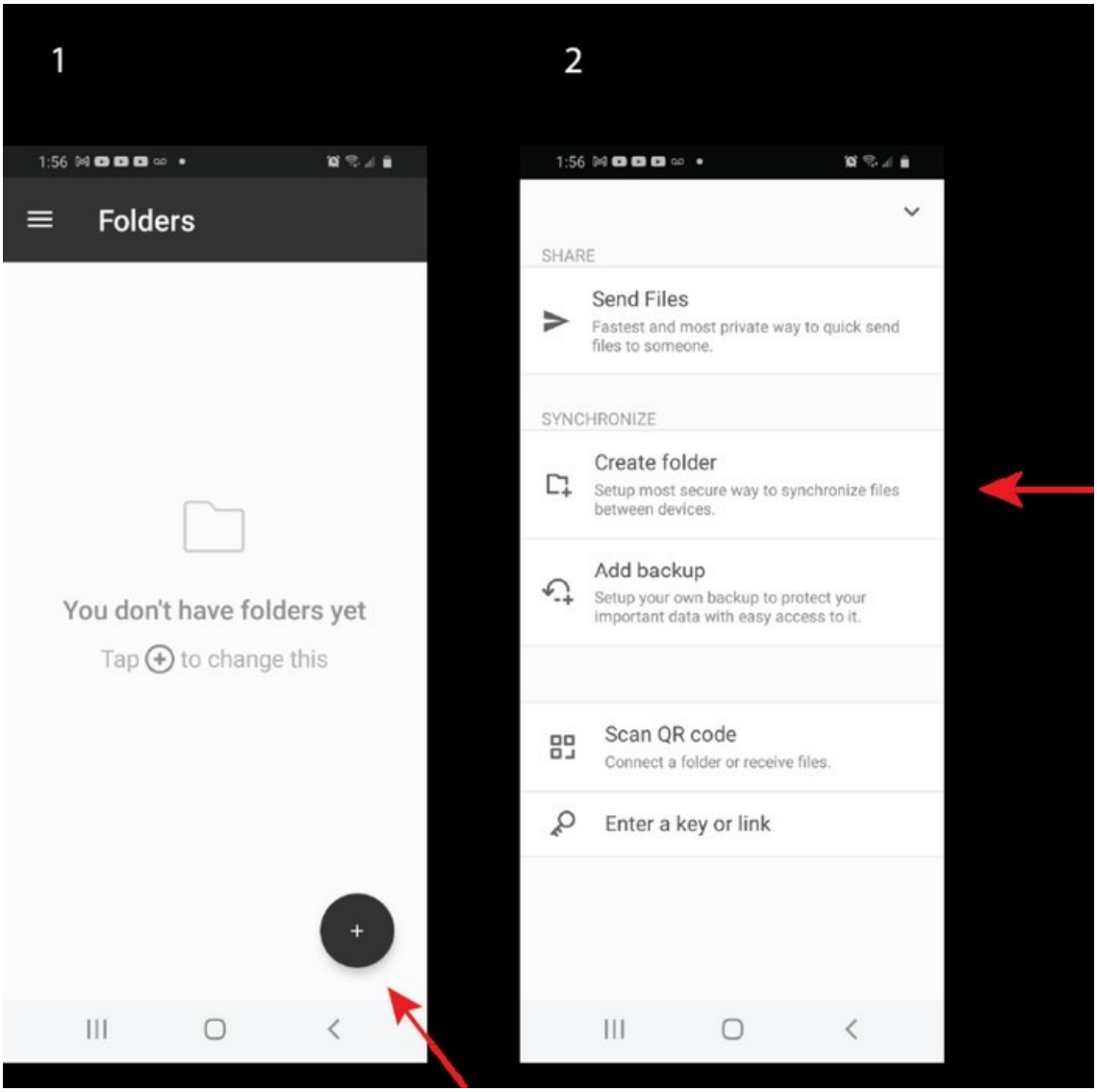
2. Managing Rights and Permissions: The mobile app allows you to manage connected folder rights and permissions, giving you control over who can access and edit the contents.

3. Mobile-Specific Features: The mobile version includes almost all the options available on the desktop version, with the addition of an "Add Backup" feature. This unique mobile function enables you to backup files and folders from your mobile device to a desktop.

4. Sub-Menu Options: The sub-menu offers access to view connected devices, settings, and shared links. Among these, the settings tab is particularly crucial.

5. Settings Tab Functions: - Set Permissions: You can set permissions for folders, determining who can view or edit the contents. - Pause and Disconnect Folders: This function allows you to temporarily halt synchronization or completely disconnect folders as needed. - Network Settings: The settings tab also provides options to tweak the application's network settings. This includes adding hosts, using a relay server, or searching for a Local Area Network (LAN).

These features make the mobile version of Resilio Sync a powerful tool for managing file synchronization and sharing, offering a high degree of flexibility and control, similar to its desktop counterpart.



Screenshot: Mobile Device Settings.

Part 3:

Research

Part 3: Research

3.1 Protocols

Resilio Sync employs a variety of ports and protocols to establish connections between peers, predominantly using TCP and UDP for communications outside the network. The process involves several key steps: 1. Route Learning: Initially, Sync needs to determine the route to the relay servers that facilitate connections between peers and clients. An example of this is Resilio sending a SYN request from a local machine to the service provider's gateway server. 2. Route Information Saving: After determining the path to the relay server, this information is downloaded and stored in the sync.conf file. 3. Listening Port: The listening port used by Sync is indicated in the settings section of the application. This port is subject to the user's firewall settings or port forwarding configurations. For instance, in the given example, the application uses TCP source port 51262 to communicate with the relay server. 4. Network Coordination: Resilio coordinates its networking to identify the most efficient route for data transfer. This ensures instant synchronization and keeps peers informed about the status of files. 5. Security: A critical aspect of Resilio Sync is its commitment to security. It encrypts packets sent over the network/Internet using AES256 PKI-based encryption over TLS 1.2, making it a secure choice for file transfers. 6. Comparative Advantage: When compared to other file-sharing programs like FileZilla and WinSCP, Resilio stands out, particularly in addressing security concerns associated with FTP. Its robust security measures ensure that files and connections are safeguarded against interception by threat actors, maintaining the integrity and confidentiality of data transfers.

```
TCP Packet
-------------------------------------------
###[ Ethernet ]###
  dst       = 15:5d:36:05:o0:84
  src       = 28:77:6e:ce:0a:20
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 52
     id        = 1012
     flags     = DF
     frag      = 0
     ttl       = 128
     proto     = tcp
     chksum    = 0x246e
     src       = 192.168.1.153
     dst       = 45.132.226.156
     \options   \
###[ TCP ]###
        sport     = 51262
        dport     = 5729
        seq       = 4056050198
        ack       = 0
        dataofs   = 8
        reserved  = 0
        flags     = S
        window    = 64240
        chksum    = 0x6744
        urgptr    = 0
        options   = [('MSS', 1460), ('NOP', None), ('WScale', 8), ('NOP', None), ('NOP', None), ('SAckOK', b'')]
```

Screenshot: Protocols.

3.2 Sources

Resilio Sync. (n.d.). Universal file delivery for data intesive envionments: Resilio Connect. Resilio File Sync Software | Unify, Control, and Accelerate Global Enterprise File Workflows. Retrieved from https://www.resilio.com/ Resilio Sync. (n.d.). Universal file delivery for data intesive envionments: Resilio Connect. Learn how to get the most out of Resilio's powerful features. Retrieved from https://www.resilio.com/tech/sync-tutorials-and-howto/

REVIEW · 6 December 2017

WordPress, Tumblr, Steemit, Medium

Introduction.

With the myriad of blogging platforms available today, business owners often face a dilemma in selecting the most suitable platform to promote, engage, and connect with their expanding audience.

Questions such as "Is the interface user-friendly?" and "How many users can I reach with this platform?" as well as concerns regarding data and personal security are common considerations. Additionally, business owners may wonder, "Can I grant admin rights to others, such as my IT team, to post on my behalf?"

To alleviate this stress, we have conducted extensive research on the major blogging platforms. In this article, we will provide detailed reviews of the following platforms:

I. Tumblr, WordPress, Medium, and Steemit, with an in-depth examination of their features.

II. Exploring the process of sharing editor rights on these platforms.

III. Analyzing the pros and cons of each platform.

1. Tumblr is a microblogging site and a social networking site that allows users to post multimedia and various contents to a short form blog.
2. Users can access the website features via the dashboard interface.
3. The dashboard has a live feed of recent posts from other blogs that the user follows.
4. Through the dashboard users are able to comment, like posts that appear on their dashboard and reblog (reposting a blog on your dashboard).
5. With the dashboard, users can upload texts posts, videos, images, link to a blog and quotes.
6. Connectivity to other social media accounts is possible; Facebook and Twitter, whenever there's a post, it will be sent as a status update on Facebook and as a Tweet on Twitter.
7. Users can follow other user's blogs.
8. Bloggers can make their blogs private i.e. only users who have the blogs password can be allowed access.
9. Posts can be scheduled to a particular time or can be delayed, it can also be spread over several hours or days.
10. There are tags to allow users help their audience find posts about certain topics by simply adding tags.
11. For the tech savvy people who want more flexibility, Tumblr allows users to edit their blog's theme, the HTML codes that control the appearance of the blog, users can also use a custom name for their blog.
12. Tumblr is compatible with multiple platforms, iOS, Android and Windows.

1.2-Setting up editors' rights on Tumblr.

To get posting rights, first you create another blog called the group blog where you can invite members.

In order to set up a blog where others can be contributors that can post from separate accounts to your group blog, you have to create a new group blog, then invite new members to join it. Here's how to get you started:

- Log in to the Tumblr Dashboard of your account.
- Select “Create A New Blog” From The Drop-Down List Of Blogs. Fill In The Blog Information. Click “Create blog” Button.

1.3-Give your blog a name and create a password.

- After clicking the "create new blog" tab, enter a title and domain name for the new blog. There’s an option to protect the blog with a password. If you decide to use a password, only people who enter the password will be able to view your blog.

1.4-Invite new members**.**

- In the dashboard of your new blog, select "members" from the menu on the right panel.
- You can invite members to post on the blog through email or by copying and pasting an invite link. Members that are invited will be able to add content to the new blog, but they won't be able to change settings unless you promote them to be admins of the blog.

1.5-Pros:

a.**Simplicity**: Tumblr is good for starting a blog immediately with minimal prep time. You can set up a functioning blog in a few minutes using Tumblr’s readymade customizable themes. This doesn’t require tech or design help.

b.**Cost**: Tumblr is a free platform. They offer premium versions that varies from $9 and $49, premium services give the user the ability to customize the blog as they wish, but the free version is also enough for a great blog.

c.**Community**: By joining Tumblr, you have access to a built in community, making it easy to grow an audience than other blogging platforms. You can gather subscribers, answer questions from readers and re-blog other peoples content all from within the platform.

d.**Self-sustainability:**Tumblr allows you to schedule posts, removing the need for third party apps like Hootsuite and Virtue.

e.**Analytics:**Tumblr gives its users the ability to connect their account to Google Analytics to monitor post effectiveness.

f.**Mobile optimized:**Tumblr is optimized for iOS, Android, and Windows app, meaning your blog is automatically mobile optimized.

g. More tags can be added on Tumblr better than Medium.

1.6-Cons:

a.**Design limitations:**Tumblr’s designs are limited, though Tumblr offers design customization for its themes, Tumblr isn’t for individual’s brands and businesses that have strict brand guidelines or a particular design team.

b.**Functionality limitations:**As mentioned earlier, Tumblr is well-known for its simplicity. Tumblr isn't your best option if you're looking for plugins and widgets.

c.**Users must adapt to its format:**Tumblr has a precise formula that works best on the platform. Light on the copy, more on the imagery and shareable stuff.

d.**Server dependent:**You're mandated by Tumblr server to host your blog, with no option to host using your own website's preferred hosting software. This can be a security concern as well as a technological one. If Tumblr's server goes down or there's a downtime, so does your blog.

e. To read an article on Tumblr, the user has to create a Tumblr account without which the article cannot be read.

2-Wordpress.

1. WordPress is a content management system (CMS) based on PHP and MySQL, it is free and open sourced.
2. For WordPress to function, it has to be installed on a web server on a network host or an internet service host.
3. WordPress features a plugin architecture and uses a template system.
4. WordPress allows users change the look and functionality of the site without changing the site's core code or content with themes.
5. Plugins allow users to extend the functionality and features of a blog or website.
6. WordPress has native applications for WebOS, iOS, Android, BlackBerry and Windows, some of these comes with limited set of options.
7. WordPress has a feature called integrated link management which is the ability to allot multiple categories to posts, search engine friendly, clean permalink structure and supports tagging of posts.
8. WordPress supports Pingback and Trackback standards used for displaying links to other sites that are linked to an article or a post.
9. Posts can be edited in HTML via the visual editor or through plugins that allows a series of customized editing features.

2.1-Setting editors' rights on WP.

WordPress has a user role management system which specifies what a particular user can and cannot do on your site.

To set user roles in the site, you have to be an administrator first, then you can change the role of others by;

i. From the WordPress dashboard go to Users > All users.

ii. Check all the boxes next to the avatars.

iii. Click on the drop down menu Change role to, then select the role you want to assign to the new user.

iv. Click on change.

WordPress has five default user roles:

- Administrator.

- Editor.
- Author.
- Contributor.
- Subscriber.

1.**Administrator:**

- In WordPre.ss, Administrator is the most powerful user role. Users with the administrator role can edit any posts by any users on the site, add new posts and even delete those posts.
- They can install, delete, and edit plugins as well as themes.
- An administrator can add new users to the site, change information about existing users including their passwords as well as delete any user even other administrators.

2.**Editor:**

- Users with the editor role have full control over the content sections of the website. They can add, edit, publish, and delete any posts on a WordPress site including the ones written by others.
- Editors can moderate, edit, and delete comments as well.
- Editors do not have access to alter the settings of the website, install themes and plugins or add new users.

3.**Author:**

- Authors role can write, edit, and publish their own posts. Authors can also delete their own posts, even if they are published.
- Authors cannot create categories when writing posts, though they can choose from previous categories or they can add tags to their posts.
- Authors can view comments even those that are pending review, but they cannot moderate, approve, or delete any comments.
- Authors do not have access to settings, plugins, or themes, so it is kind of a low-risk user role on a site with the only difference being their ability to delete their own posts once they're published.

4.**Contributor:**

- Contributors can add and edit their own posts, but they cannot publish any posts not even posts created by them.
- Contributors have to choose from existing categories because they cannot create new categories but they can add tags to their posts.
- Contributors cannot upload files i.e. they can't add images to articles created by them.
- Contributors cannot approve or delete comments but can only view comments even those awaiting moderation.
- Contributors do not have access to settings, plugins, or themes

5.**Subscriber:**

- Subscribers can only login to your website and update their user profiles. They can change their passwords but they cannot write posts, view comments, or alter any settings on the website.

- Subscribers are useful if you require users to login before they can read a post or leave a comment.

2.2-Pros:

a. WordPress is a Content Management System (CMS) that gives you the ability to update your site without the need for a developer.

b. WordPress is simple to install and operate with no need for learning high level programming language.

c. Websites can be built in a short time depending on the complexity.

d. There are of the shelf plugins and themes not provided by the WordPress core that can add functionality to the site.

e. Due to the open source nature of WordPress, there are various how to tutorial, support forums guides for virtually anything you want to do.

f. WordPress is continuously developed, tested and supported.

2.3-Cons:

a. WordPress is free and open source, its future development or the impact that updates can have on businesses cannot be controlled.

b. It is highly essential that websites be upgraded to the latest versions of WordPress, including its plugins and themes, else problems arise.

c. Since WordPress is open source, it is easy for hackers to find security lapses and plant malicious code.

3-Steemit.

1. Steemit is a social news service which runs a social networking website and blogs on a blockchain database.
2. Steemit produces STEEM dollars and STEEM which are tokens users get for posting, commenting and discovering exciting content.
3. Users can upvote comments and posts, and the authors who's material got upvoted gets a monetary reward in a cryptocurrency token called STEEM.
4. US dollar pegged tokens are called STEEM Dollars.
5. Users are also rewarded for discovering popular content (Curating).
6. Curating is voting post submissions and comments.
7. Steemit uses a reputation system, new accounts start with a reputation of 25.
8. The Steem blockchain has two tokens which are STEEM and STEEM DOLLARS.
9. Steemit also has vested and stored interest called the STEEM POWER, it's strictly for use within the Steem community.

3.1-Pros of Steemit:

I. Steemit is the only social media platform that pays its users for posting and upvoting comments.

II. The community has 200+ members with about 2000 new members signing up everyday.

III. The site is easy to navigate.

IV. Steemits code is open sourced and decentralized.

V. The website is Ad free.

3.2-Cons:

a. The site is in beta phase for now, it is still under construction.

b. There are features still missing.

c. There is no private messaging system.

d. To open an account takes about 7 days.

e. Normal html tags can't be used.

4-Medium

1. Medium is an online publishing platform, a perfect example of social journalism, it has a collection of amateur and professional publications and people, publishers on medium or exclusive blogs.
2. Medium software provides a full What You See Is What You Get (WYSIWYG) user interface when editing online.
3. When an entry is posted it can be recommended and shared by other people, like Twitter, posts can be upvoted like Reddit and content can be assigned a specific theme like Tumblr.
4. Medium has a clap feature which readers can click multiple times to signify if they like an article.
5. Payment to authors is based on how many claps an article receives.
6. Users can create an account using a email address, Facebook, Twitter, or Google account.
7. Posts are sorted by topic rather than writer.

4.1-Pros of Medium:

a.On Medium it is easier to get your blog posts discovered, you can subscribe to authors you enjoy based on a recommendation engine.

b.Authors can easily see all the statistics on views, detailed statistics about their stories, shares, views, complete reads etc.

c.Authors can either publish their stories by themselves or join an organization that publishes articles by a number of authors.

4.2-Cons:

a. Mediums WYSIWYG editor is limited.

b. The commenting system on Medium is ambiguous, each time you click reply, you're redirected to a new page and pressing the back button takes you back to the top of the page and not the comment you left.

c. Medium promotes the company's brand and not the authors brand.

d. Impossible to manage editors' rights. Login is via email and gives owner's rights to anyone.

5-References**:**

- 85ideas.com, E. (2017). The pros & cons of using WordPress for your business. [online] Pragmatic. Available at: https://pragmatic.agency/wordpress-pros-cons/ [Accessed 26 Nov. 2017].
- En.wikipedia.org. (2017). Medium (website). [online] Available at: https://en.wikipedia.org/wiki/Medium_(website) [Accessed 26 Nov. 2017].
- En.wikipedia.org. (2017). Steemit. [online] Available at: https://en.wikipedia.org/wiki/Steemit [Accessed 26 Nov. 2017].
- En.wikipedia.org. (2017). Tumblr. [online] Available at: https://en.wikipedia.org/wiki/Tumblr [Accessed 26 Nov. 2017].
- En.wikipedia.org. (2017). WordPress. [online] Available at: https://en.wikipedia.org/wiki/WordPress [Accessed 26 Nov. 2017].
- Flightpath NYC. (2017). Tumblr for Brands: Pros and Cons of Tumblr Blogging Platform. [online] Available at: https://www.flightpath.com/blog/2016/10/tumblr-for-brands-pros-and-cons-of-tumblr-blogging-platform/ [Accessed 22 Nov. 2017].
- Kessler, S. (2017). HOW TO: Create a Group Tumblr Blog. [online] Mashable. Available at: https://mashable.com/2011/05/01/group-tumblr/#AjZCQZx4emqjh [Accessed 22 Nov. 2017].
- McCullough Web Services. (2017). The Pros and Cons of Using Medium as a Blogging Platform. [online] Available at: https://mccullloughwebservices.com/2017/07/29/using-medium-blogging-platform/ [Accessed 26 Nov. 2017].
- Staff, E. and Staff, A. (2017). Beginner's Guide to WordPress User Roles and Permissions. [online] WPBeginner. Available at: http://www.wpbeginner.com/beginners-guide/wordpress-user-roles-and-permissions/ [Accessed 26 Nov. 2017].
- TwelveSkip. (2017). How To Make Another Blog On The Same Tumblr Account | TWELVESKIP. [online] Available at: http://www.twelveskip.com/tutorials/tumblr/513/how-to-make-another-blog-on-the-same-tumblr-account [Accessed 22 Nov. 2017].

REVIEW · 12 December 2017

Steemit for Business

Our chosen blogging platform is Steemit. We provide feedback, detailing what we perceive as pros and cons, and so forth.

Disclaimer: We are unaffiliated with any of the mentioned companies. This article solely represents our independent findings, and there is no affiliate marketing associated with the provided links for your convenience.

How we write our reviews: For an impartial and comprehensive review, all apps undergo the following testing criteria:

- Real-time usage in actual projects.
- Evaluation by various team members situated in different countries.
- Testing on diverse devices and operating systems.
- A minimum testing period of two weeks, averaging four weeks.
- Peer review by team members precedes submission to the app's publisher for the final review.

This is a guide for:

- Assessing the pros and cons of Employing Steemit as a Business Blogging Platform.
- Establishing a Steemit Account.
- Granting Editor Rights on Steemit.
- Utilizing Markdowns for Post Editing on Steemit.

1. Pros and Cons of Steemit.

1.1 Pros:

- Steemit stands out as the sole social media platform that compensates users for posting and upvoting comments.
- The community boasts over 200 members, witnessing around 2000 new sign-ups daily.
- Navigating the site is user-friendly.
- Steemit's code operates on an open-source and decentralized framework.
- Additionally, the website is ad-free.

1.2 Cons:

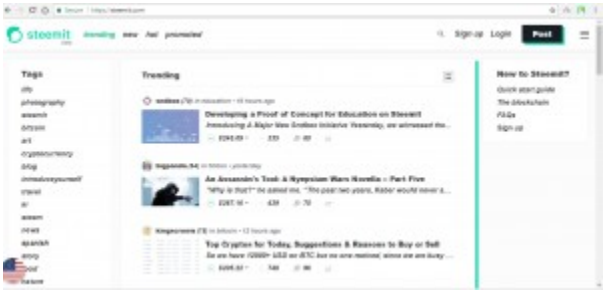
- The site is currently in its beta phase and is under construction.
- Certain features are still unavailable, including a private messaging system.
- The account registration process takes approximately 7 days.
- Additionally, standard HTML tags cannot be utilized.

1. Setting Up An Account.

Step 1: Sign up.

- Enter *https://www.steemit.com/* (https://www.steemit.com/) in your url.

- Click on Sign up.



Step 2: Enter your account name.

- Choose an available account name and proceed by clicking on continue. Caution: Once selected, you won't have the option to change it later.

Step 3: Enter your email.

- Input your email address and proceed by clicking on continue. This email will be utilized for registration and newsletters, excluding password recovery purposes.

Step 4: Country and phone.

- Select your country code from the dropdown menu, then input your phone number and proceed by clicking continue..

- Enter the confirmation code sent and click continue.

Note: It takes Steemit about 7 days (sometimes more) for a Steemit account to be activated.

1. Sharing editing rights:

How to Share Editor Rights on Steemit.

Lost passwords: Emphasizing the criticality of password security is vital, as Steemit does not facilitate password recovery. Once a password is lost or compromised, Steemit is unable to intervene**.**

Posting key: Facilitating editor rights sharing on Steemit is a straightforward process. To post and edit articles for a business or user account, one only needs the username and a posting key. Posting keys serve the purposes of voting and posting on Steemit, distinct from active and owner keys. Team members or editors should be provided with the posting key.

1. Editing Posts using markdowns on Steemit:

Editing posts on Steemit diverges from conventional blogging platforms due to the use of Markdown which is a little different from what users and businesses are used to. Markdown is a lightweight and user-friendly text styling method for the web. It employs a straightforward syntax, incorporating a few non-alphabetic characters for styling, such as (#) or (*). Markdown essentially transforms regular text into styled content.

Here's a compilation of useful hacks for editing on Steemit.

4.1 Headers:

Adding the (#) with a space in the beginning of a word or sentence changes the text to a header.

#H1.

##H2.

###H3.

####H4.

#####H5.

######H6.

4.1.1 Result:

H1.

H2.

H3.

H4.

H5.

H6.

4.2 Emphasis:

Adding the (*) or the (_) at the beginning and end of a text changes the text to either Italics or bold.

- This text will be italic. *

_ This will also be italic. _

This text will be bold.

__ This will also be bold. __

4.2.1 Result:

This text will be italic.

This will also be italic.

This text will be bold.

This will also be bold.

4.3 Lists.

To create lists we can use numbers, (*), (-), (+);

First ordered list item.

Another item.

· · * Unordered sub-list.

Actual numbers don't matter, just that it's a number.

· · 1. Ordered sub-list.

And another item.

- Unordered list can use asterisks.

– Or minuses.

- Or pluses.

4.4 Links.

This are the ways to create links on markdown.

Note: The link must start with https:// not www without which it wouldn't work.

[I'm an inline-style link] (https://www.love4aviation.org)

[I'm an inline-style link with title] (https://www.love4aviation.org "Love4aviation's Homepage")

4.4.1 Result.

I’m an inline-style link.

I’m an inline-style link with title.

5 Images.

Steemit offers a dedicated hosting website named SteemIMG, providing a central location for posting images and gifs. SteemIMG boasts a user-friendly interface and dependable service, facilitating easy picture-taking with a phone and direct upload to Steemit.

Here are several methods for uploading, linking, organizing, and publishing your images on Steemit:

Step 1: Upload the images to SteemIMG.com.

- Right-click on the desired image for upload.
- Choose "Copy Image Address."
- Access https://steemimg.com, then initiate the upload.
- Alternatively, employ drag-and-drop functionality, browse your computer, or add the image URL for SteemIMG.

- Subsequently, paste the copied image URL address.
- Select submit; optionally, choose a category (it’s not compulsory).
- Click upload.

To upload an image on a computer, a live picture, or a mobile phone, follow these steps:

> 1. Visit https://steemimg.com in your browser.

> 2. Either browse the image location on your computer or drag and drop it onto SteemIMG.

> 3. Optionally select a category, then click upload.

> 4. For mobile phones, choose "Start Uploading."

> 5. Decide to take a photo, select from your photo library, or use iCloud Drive.

1. Click on upload.
    - Visit https://steemitimg.com.
    - With your chosen image, navigate to Embed Codes.
    - Select the desired Image URL below the image.
    - Paste the URL in the position where you want it within your article.

If you require assistance or answers to any questions, visit https://www.steemithelp.net/. They cover a range of topics, including Steemit basics, site navigation, posting, curation, and more. Accessing this resource can greatly facilitate your Steemit journey.

1. References.

GitHub. (2017). adam-p/markdown-here. [online] Available at: https://github.com/adam-p/markdown-here/wiki/Markdown-Cheatsheet [Accessed 9 Dec. 2017].

GUIDE · 11 March 2021

WordPress to Twitter

Introduction.

WordPress offers the functionality to directly publish your posts on certain social media platforms once you've linked your website to your social media account. While this feature may seem straightforward and convenient, there's a caveat.

It doesn't work.Result is totally inconsistent.

We use this feature, particularly with Twitter, to keep our stakeholders informed about the various websites we oversee. To access this functionality, follow these steps:

1. Go to WP Admin.
2. Navigate to Settings.
3. Select Sharing.
4. Click on Publicize Settings.
5. Connect your Twitter account. In the following article, you'll find details about all the tests we've conducted.

Top of Form

TL;DR:

Only the Title will show up in your Tweet. So you have to work around this bug.

Step 1:

Creating a post with the URL included solely in the title, leaving the content section blank, and adding a featured image.

Example:

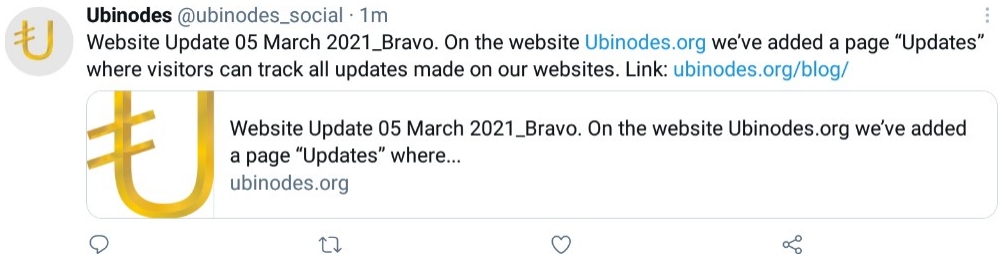
Step 2:

Click on "Publish". Customize the content, but be aware that it may not consistently appear at the top of your Tweet. Sometimes, only the title appears, and it may appear twice.

Step 3:

Please verify on your Twitter account that your post has been published. Occasionally, the content you enter in the title may appear both at the top of the Tweet and in the Tweet link. Then again, the custom message may appear at the top of your Tweet, with the title serving as the content of your tweet, forming a "Head and Tail". Any URL included will be clickable, directing the reader to the corresponding post on your website. Additionally, if you've added a featured image, it may be displayed.

Example:



The title appears twice.

Showing the featured image.

Custom message at the top and featured image. Lucky strike.

Step 4:

Now, it's time to update your post with the correct title and content. Once you click "Update", no automatic posting will occur on Twitter. Therefore, your readers will be directed to a properly published post when they access it.

Example:

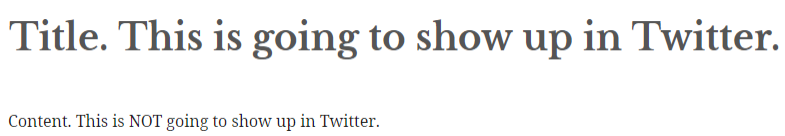
Testing.

We've conducted extensive testing to identify the issues with this feature and explore potential ways to workaround this.

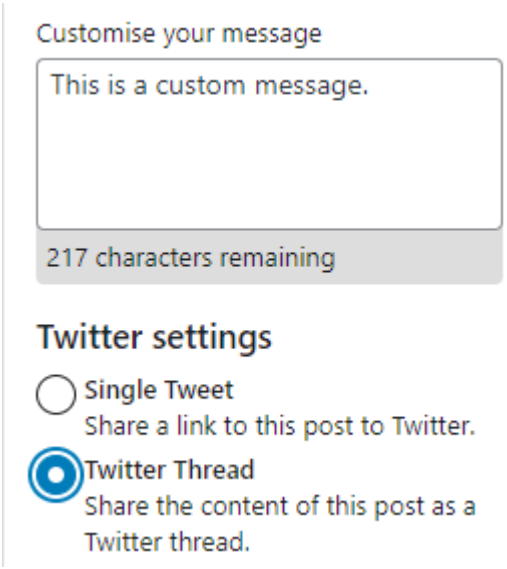
Test 1:

- Testing with one title, one content and one custom message.
- The outcome reveals that the custom message appears at the top of the Tweet while the Title is displayed in the post. However, it's inconsistent as subsequent tests did not display the custom message reliably..

Screenshots:



One Title, One content.



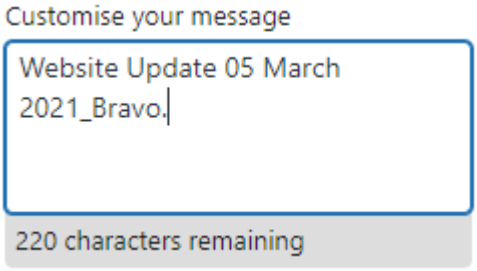
One custom message.

Result. We see the custom message and the Title but not the content.

Test 2:

- Testing with the message all as a title, no content. We added a custom message.
- Result: We see only the tile in the Tweet, both at the top and in the content.

Screenshots:



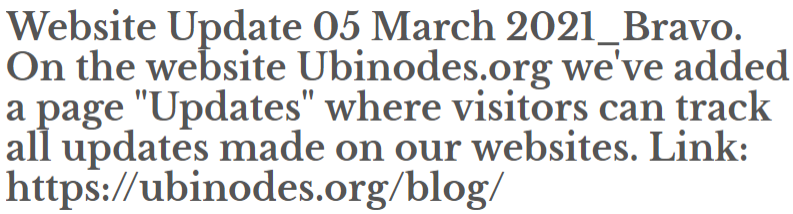
A custom message.

Result. We see only the title.

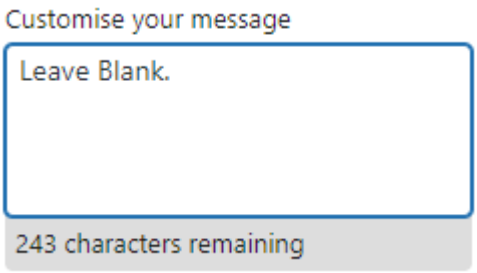
Test 3:

- Testing with the message all as a title and no Custom Message.
- Result: We see the content of the title both a the top of the Tweet and in the content of the Tweet.

Screenshots:



All as a title.



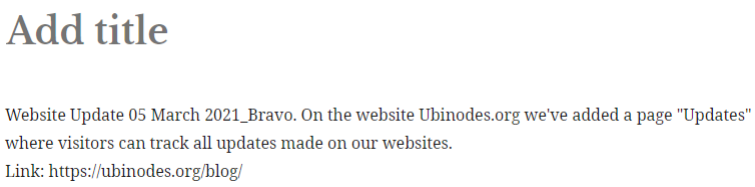
No custom message.

Title in the Tweet, twice.

Test 4:

- Testing with a content only, no title and no custom message.
- Result. Tweet is empty, bot at the top and inside.

Screenshots:



No title, content only.

Result. Tweet is empty.

Test 5:

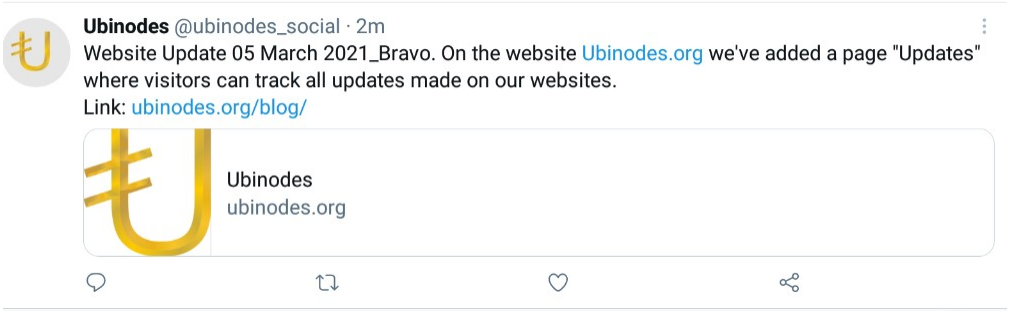
- Testing with no title, one content, and one custom message.

- Result: The custom message appears at the top, the Tweet is empty, but clicking on it directs you to the website's post. This could be the optimal choice if only it were consistent.

-

Screenshots:

No title, One content and One custom message.



The custom message appears at the top and Tweet is empty.

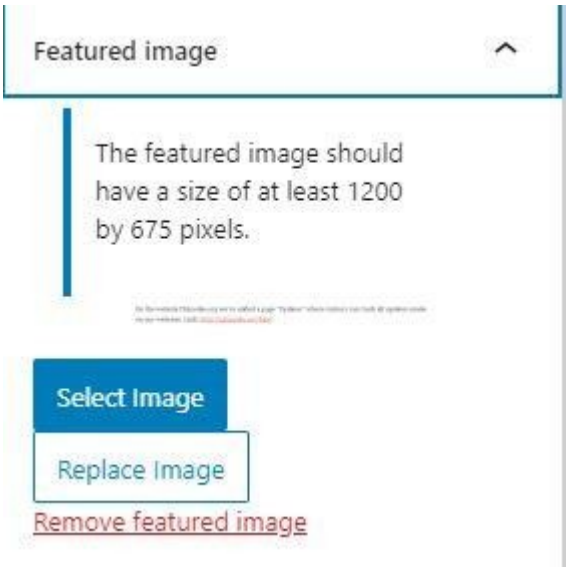
Test 6:

Testing with one title, one content, one custom message, and one featured image yielded varied results. When using a screenshot of the content as the featured image, it did not display. Instead, only the custom content appeared at the top of the Tweet, with the title in the Tweet itself. However, when using another image, such as when posting about Wire in Open Collective, the featured image successfully appeared. Thus, it's possible to utilize a featured image, but not to include text within it.

Screenshots:

Text in the title.

Screenshot of the text used as featured image.



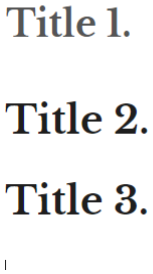
Use a screenshot of the text as featured image.

The screenshot as featured image doesn't show up.

Test 7:

Testing with multiple titles and a custom message yielded the following result: Only Title 1 will appear in the Tweet, both at the top and in the content. The custom message did not display.

Screenshots:



Several titles.

Ubinodes @ubinodes_social · 28s

Title 1.

Title 1.
ubinodes.org

GUIDE · 1 January 2018

WordPress Plugin to Steemit

Using Steemit as our blogging platform, we explored the WordPress plugin for Steemit posting.

This is a guide for:

- Downloaded the WordPress Steem plugin.
- Edited the WordPress Steem plugin.
- Posted on Steemit via the WordPress Steem plugin.
- Discussed pros and cons of using WordPress Steem.

Step 1:

Downloading the WordPress Steem plugin.

Note: To use the WordPress Steem plugin, a WordPress account and a Steemit account are prerequisites; without these, the plugin will not function.

- Enter your WordPress admin link in the browser, input your WordPress username and password.
- In the WordPress dashboard, navigate to Plugin -> Add new. Search for "WordPress Steem" in the search bar, then click download.
- After successful download, select Upload plugin -> Choose file (locate the downloaded file, often in the downloads folder) and click install now.
- Upon successful installation, click activate to enable the plugin.

Step 2:

Editing the WordPress Steem plugin:

- In the WordPress dashboard, select Settings -> Steem. In Steem Settings, adjust the settings to enable direct posting on Steemit from WordPress.
- In the Accounts and Posting key tabs, enter your Steemit username.
- Mark the Default Publish to Steem and Default Update to Steem checkboxes.

- Fill in and check the appropriate boxes that you want and click on Save changes.

Step 3:

Posting on Steemit using the WordPress Steem plugin from WordPress.

- In the WordPress Dashboard, go to Posts -> Add new.
- Input the Article Title and content.
- Fill in the article content, include relevant tags, and click update.

Pros and cons of using WordPress Steem.

Pros:

- Installing and activating the plugin is straightforward.
- Posting on WordPress is equally easy, thanks to its user-friendly visual editor.

Cons:

- As of posting this article, the plugin does not publish on Steemit from WordPress.

REVIEW · 20 January 2018

Tumblr Blog

In reaching its audience, a business must assess the most suitable blogging platform. Love4aviation previously utilized Tumblr alongside other platforms but made a strategic decision in January 2018 to discontinue its use of Tumblr and transition exclusively to Steemit. Here's why:

Introduction.

After thorough consideration, Love4aviation has made the decision to discontinue posting on our Tumblr blog. Let's review the features and drawbacks of Tumblr:

Features and Benefits:

1. Tumblr offers a microblogging and social networking platform where users can post multimedia content to short-form blogs.
2. Access to website features is facilitated through the dashboard interface.
3. The dashboard provides a live feed of recent posts from followed blogs.
4. Users can engage with posts through comments, likes, and reblogs.
5. Various content types can be uploaded through the dashboard, including text, videos, images, links, and quotes.
6. Integration with social media platforms like Facebook and Twitter allows for easy sharing of posts.
7. Users can follow other blogs and make their own blogs private.
8. Posts can be scheduled and tagged for better organization.
9. Advanced users can customize their blog's theme and HTML code.
10. Compatible with multiple platforms, including iOS, Android, and Windows.

Drawbacks:

a. Design limitations restrict customization options, especially for brands and businesses with specific design requirements. b. Functionality limitations, such as the absence of plugins and widgets, may limit customization options. c. Users must adapt to Tumblr's specific format, which emphasizes imagery over text. d. Dependency on Tumblr's servers raises security and reliability concerns. e. Access to articles requires users to create a Tumblr account, which may deter some users and defeat the purpose of easy access to information.

While Tumblr offers many great features for blogging, including the ability to share information with the public, there are drawbacks to consider. As a privately owned company, Tumblr retains the authority to take down articles or close blogs at any time. Additionally, the requirement for users to create an account to access articles may hinder accessibility for some users. Considering these factors, Love4aviation has decided to discontinue its use of Tumblr for sharing information with the general public.

GUIDE · 6 December 2017

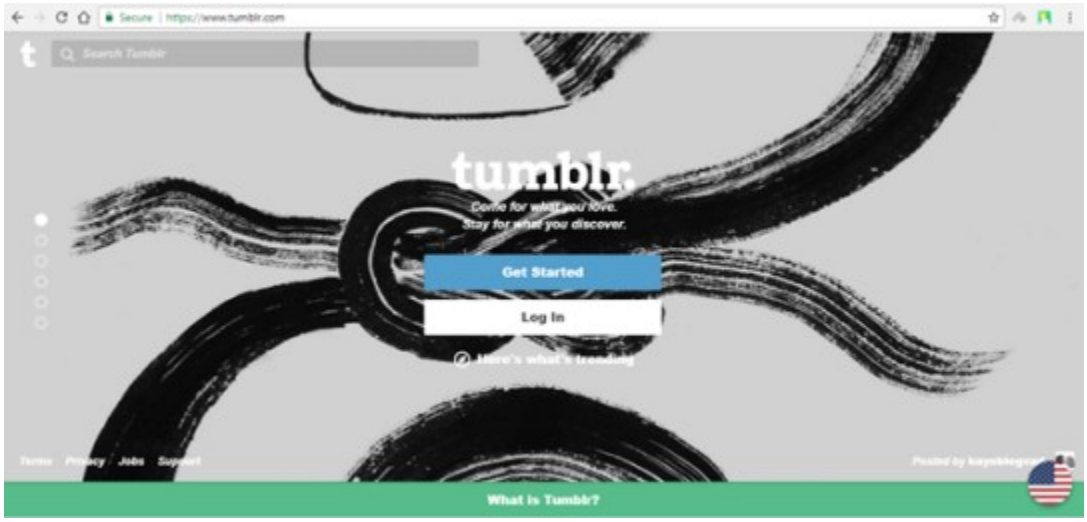
Account on Tumblr

This is a guide for:

- Setting up a Tumblr account.
- Sharing editing rights on Tumblr.
- Pros and cons of using Tumblr as a blogging platform.

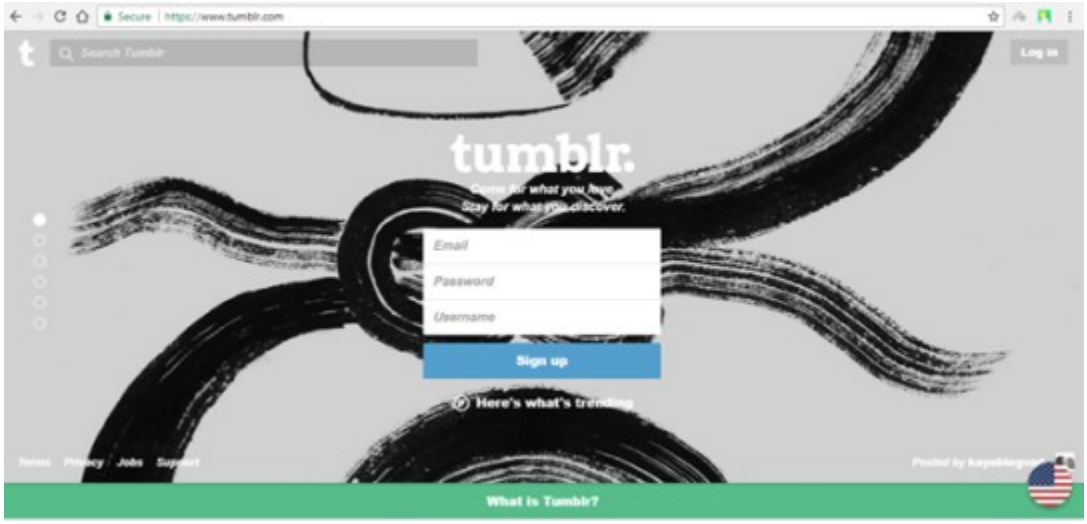
Step 1: Setting up a Tumblr account.

- Enter *https://www.tumblr.com/* (https://www.tumblr.com/) in your url.
- Click on Get Started.



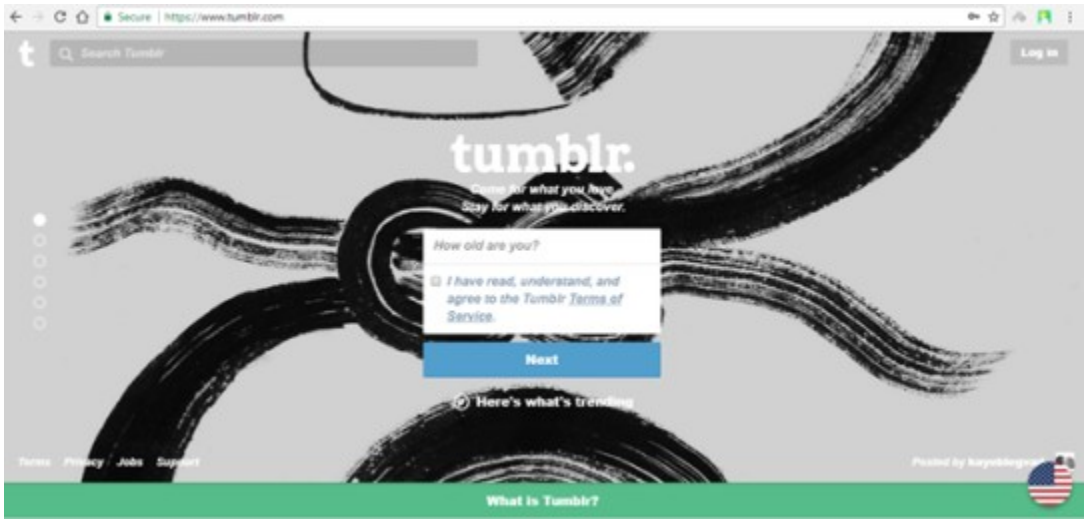
Step 2: Fill In your details

- Enter your email, password and username of choice.



Step 3:

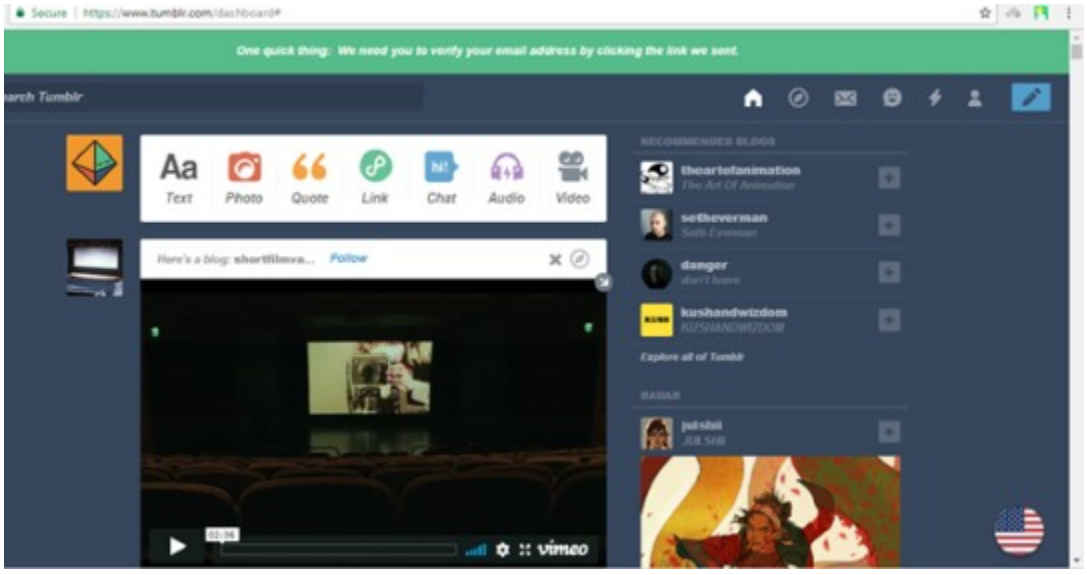
- Enter your age.
- Check the terms and service box, then click next.



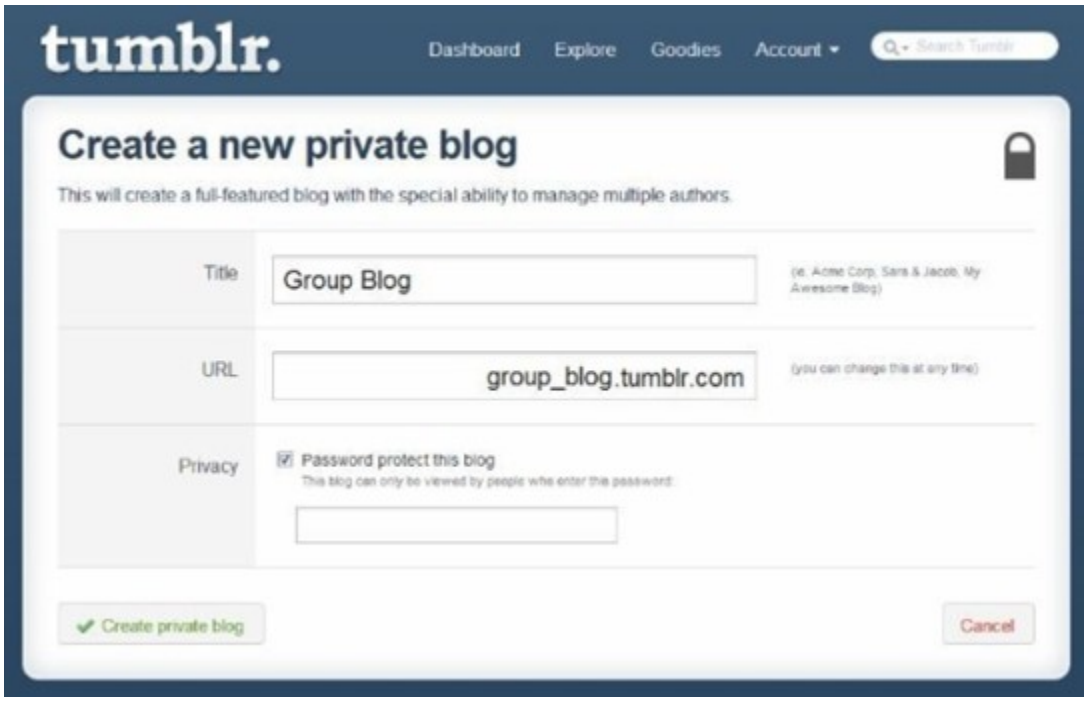
Step 4: Creating Admin on Tumblr.

To set up a company blog where contributors can post from multiple accounts, follow these steps:

1. Log in to the Tumblr Dashboard of your account.
2. Select "Create A New Blog" from the drop-down list of blogs.
3. Fill in the required blog information.
4. Click the "Create blog" button.



Step 5: Give your blog a name and create a password



- After clicking the "create new blog" tab, enter a title and domain name for the new blog. There's an option to protect the blog with a password. If you decide to use a password, only people who enter the password will be able to view your blog.

Step 6: Invite new members.

In the dashboard of your new blog, follow these steps:

5. Select "Members" from the menu on the right panel.
6. You can invite members to post on the blog either through email or by copying and pasting an invite link.
7. Invited members will have the ability to add content to the new blog. However, they won't be able to change settings unless you promote them to be admins of the blog.

Pros:

-**Simplicity:**Tumblr is ideal for quickly starting a blog with minimal preparation. You can set up a functional blog within minutes using Tumblr's ready-made customizable themes, without requiring technical or design assistance.

-**Cost:**Tumblr is a free platform, although premium versions are available ranging from $9 to $49. Premium services offer users the ability to customize their blog extensively, but the free version is sufficient for creating a great blog.

-**Community:**By joining Tumblr, you gain access to a built-in community, simplifying the process of growing an audience compared to other blogging platforms. You can gather subscribers, answer reader questions, and reblog other people's content directly within the platform.

-**Self-sustainability:**Tumblr allows you to schedule posts, eliminating the need for third-party apps such as Hootsuite and Virtue.

-**Analytics:**Tumblr provides users with the ability to connect their account to Google Analytics, allowing them to monitor the effectiveness of their posts.

-**Mobile Optimized:**Tumblr is optimized for iOS, Android, and Windows apps, ensuring that your blog is automatically mobile-optimized for users on various devices.

Cons:

-**Design Limitations:**While Tumblr offers some design customization for its themes, the platform's designs are relatively limited. It may not be suitable for individuals, brands, or businesses with strict brand guidelines or specific design requirements.

-**Functionality Limitations:**Tumblr is known for its simplicity, but it may not be the best option if you require extensive plugins and widgets for your blog.

-**Adaptation to Format:**Tumblr has a specific formula that works best on the platform, emphasizing imagery and shareable content over lengthy text. Users must adhere to this format and adjust their content accordingly to maximize engagement on the platform.

-**Server Dependency:**Tumblr mandates that your blog be hosted on their servers, without the option to use your own preferred hosting software. This can raise concerns regarding security and reliability; if Tumblr's servers experience downtime, your blog will be affected as well.

Sources:

- Flightpath NYC. (2017). Tumblr for Brands: Pros and Cons of Tumblr Blogging Platform. [online] Available at: https://www.flightpath.com/blog/2016/10/tumblr-for-brands-pros-and-cons-of-tumblr-blogging-platform/ [Accessed 22 Nov. 2017].
- Kessler, S. (2017). HOW TO: Create a Group Tumblr Blog. [online] Mashable. Available at: https://mashable.com/2011/05/01/group-tumblr/#AjZCQZx4emqjh [Accessed 22 Nov. 2017].
- TwelveSkip. (2017). How To Make Another Blog On The Same Tumblr Account | TWELVESKIP. [online] Available at: http://www.twelveskip.com/tutorials/tumblr/513/how-to-make-another-blog-on-the-same-tumblr-account [Accessed 22 Nov. 2017].

Part IV

International Business & Affairs

RESEARCH · 21 May 2021

Weaponizing of the US Dollar

Note.

This article is a work in progress and has been published; however, it remains an ongoing meta-study subject to continuous updates. The focus of this article revolves around the potential threats faced by manufacturers intending to export to the US or utilizing the US dollar for their transactions. Follow us on Twitter to stay informed about future updates

What is this?

This is a "Research" article on the Weaponization of the USD and Extra-Jurisdiction.

Why do we need this?

As an international marketing agency like Ubinodes, our priority is to educate our clients about the intricacies of exporting and importing products, particularly in relation to the United States and its interactions involving the USD.

Contents for this Article.

1. Weaponizing of the USD.
2. Prism Program and the Weaponization of the USD.
3. How Companies without U.S. Operation can still face U.S. Law and Regulatory Enforcement.
4. History about the enforcement of Extra-Jurisdiction.
5. Causes.
6. Consequences.
7. Economy.
8. Customs Clearance.
9. Sources.

1. Weaponizing of the USD.

America is leveraging the dollar as a tool to maintain its global economic and geopolitical dominance. With the U.S. accounting for 20 percent of the world's economic output and over half of all global currency reserves and trade conducted in dollars, this influence stems from the Bretton Woods agreement. This agreement, established in 1944, set the framework for commercial and financial relations among the United States, Canada, Western European countries, Australia, and Japan.

The Bretton Woods system marked the first fully negotiated monetary order aimed at governing monetary relations among sovereign states. Key features included the requirement for each country to maintain its external exchange rates within 1 percent by pegging its currency to gold, as well as the IMF's role in addressing temporary balance of payment imbalances and preventing competitive currency devaluations.

However, the system came to an end in 1971, enabling the U.S. to assert control over the global currency supply. The weaponization of the USD is evident in its association with sanctions programs. Legislation such as the International Emergency Economic Powers Act, the Trading With the Enemy Act, and the Patriot Act empower Washington to weaponize payment flows. Coupled with technology and access from SWIFT (Society for Worldwide Interbank Financial Telecommunications), the U.S. can exert unparalleled control over global economic activity (Source 15).

2. Prism Program and the Weaponization of the USD.

The Prism program, operated by the US National Security Agency (NSA), functions as a tool for collecting private electronic data from users of prominent internet services such as Gmail, Facebook, Outlook, and similar platforms.

This program significantly impacts the weaponization of the US dollar by expanding its influence over individuals utilizing these services. Through Prism, the US government gains access to locations beyond its borders, enabling surveillance on entities that might be deemed a threat to the stability of their currency.

3. How Companies without U.S. Operations can still face U.S. Law and Regulatory Enforcement.

America has taken on the role of the global police, assuming the positions of Judge, Jury, and Executioner for international businesses due to the United States' influential position in the world economy. Companies disregarding this global jurisdiction risk exclusion from a vast domestic market or being cut off from dollar payment systems and mainstream banks.

The process appears notably ad hoc. Few cases proceed to court, and settled matters often include gag orders imposed on executives. With minimal oversight, prosecutors have broadened interpretations of what constitutes a link to America warranting prosecution. Even indirect dealings with foreign banks having US branches or using services like Gmail can now lead to potential legal ramifications. For instance, envision China imposing a $5 billion fine on Amazon and imprisoning its executives for conducting business in Africa that didn't breach American law but violated Chinese regulations and was discussed on WeChat.

America has earned the nickname "Judge Dread," akin to the movie featuring Sylvester Stallone, symbolizing its role as the Judge, Jury, and Executioner.

3.1. Example of a Scenario.

Your company's decision to divide specific markets with a main competitor, opting out of entering the U.S. market, can potentially fall under laws prohibiting anti-competitive behaviour. This scenario illustrates how non-US companies might find themselves subject to enforcement actions.

3.2. Another Example of a Scenario.

Your company enters into an agreement to sell products to a distributor in Iran. While your country doesn't restrict trade with Iran, the contract specifies that payments for the products must be made in U.S. dollars. It's worth noting that the US Treasury Department's Office of Foreign Assets Control (OFAC) holds broad authority over commercial and financial dealings with sanctioned countries.

4. History about the enforcement of Extra-Jurisdiction.

Throughout the late 18th and early 19th centuries, the application of U.S. law beyond its borders primarily dealt with torts and piracy. By the early 20th century, this extraterritorial reach gradually extended into environmental and economic regulations, encompassing areas such as antitrust, banking, bankruptcy, securities, taxation, and labour.

From the 1970s onward, the expansion of domestic law's extraterritorial scope intensified, driven by U.S. policy agendas focusing on foreign policy and national security goals. Asserting authority beyond national borders has often led to contentious political clashes with both adversaries and allies, challenging the sovereignty of other nations.

A contemporary example is the ongoing conflict between U.S. and EU laws regarding Iran. In the 21st century, the proliferation of social media technologies and SWIFT's impact has further amplified this extraterritorial influence.

5. Causes.

U.S. dollar transactions serve as a conduit for extending the influence of U.S. law globally. The weaponization of the USD is chiefly propelled by its association with sanction programs. Over half of the world's currency reserves and trade transactions are denominated in dollars. Legislation such as the Patriot Act, Enemy Act, and IEEP Act (International Emergency Economic Powers Act) empowers the United States to weaponize payment flows worldwide. Coupled with access via Swift (referenced earlier), this global messaging system enables the U.S. to maintain control over global economic activities.

6. Consequences.

Using a payment channel via a U.S. bank can subject individuals to prosecution for violating laws concerning American assets. This grants the United States an extraterritorial hold over non-U.S. entities engaged in trade or financing activities with sanctioned entities. Such measures can significantly disrupt and destabilize financial operations, trade, and currency markets, causing disruptions for non-U.S. parties. The extensive power wielded by the U.S. through the dollar is a source of profound concern for many due to its far-reaching capabilities.

7. Economy.

Economic Warfare serves as a key instrument in America's strategic approach to conflicts with other nations. The weaponization of the US dollar plays a dual role, serving both as a tempting incentive and a formidable deterrent. This tactic enables the United States to extend assistance to allies, such as the UN, while adversaries may find themselves excluded from a substantial financial system dominated by the US dollar. The economy becomes a weapon through the swift implementation mentioned in the paragraph on Consequences. An illustrative instance of the US wielding swift as a punitive measure occurred in 2014 when it blocked numerous Russian banks from the SWIFT network amidst deteriorating relations between the two countries. SWIFT functions as an exclusive communication network for financial entities, ensuring the swift and precise exchange of information, particularly in money transfer instructions. The US has effectively harnessed this system to exert influence and control over the global economy.

8. Customs Clearance.

Challenges in customs clearance encompass various factors: unclear logistical planning, navigating border control and distribution laws, understanding diverse market legalities, managing financial risks and currency fluctuations, ensuring market demand, and fostering a diverse workforce. For businesses exporting beyond the U.S., adherence to these customs regulations is vital to avoid facing extraterritorial jurisdiction enforced by the USD. Moreover, secure communication is a crucial strategy while exporting, especially considering the looming threat of USD weaponization. Safeguarding communications from potential access by the United States becomes paramount to avoid legal complications associated with extraterritorial laws. Ubinodes offers numerous reviews on encrypted software and apps, providing insights to shield against potential USD weaponization (Source 13).

9. Sources:

- The Long Arm of American Enforcement: How Companies Without U.S. Operations Can Still Find Themselves Facing U.S. Law and Regulatory Enforcement. *https://www.foley.com/en/insights/publications/2020/06/the-long-arm-of-american-enforcement* (https://www.foley.com/en/insights/publications/2020/06/the-long-arm-of-american-enforcement) Source 01
- The trouble with America's extraterritorial campaign against business. *https://www.economist.com/leaders/2019/01/19/the-trouble-with-americas-extraterritorial-campaign-against-business* (https://www.economist.com/leaders/2019/01/19/the-trouble-with-americas-extraterritorial-campaign-against-business) Source 02
- Extraterritorial U.S. Sanctions. *https://www.swp-berlin.org/10.18449/2019C05/* (https://www.swp-berlin.org/10.18449/2019C05/) Source 03
- How A Weaponized dollar Could Backfire. *https://www.belfercenter.org/publication/how-weaponized-dollar-could-backfire* (https://www.belfercenter.org/publication/how-weaponized-dollar-could-backfire) Source 04
- FIFA, the U.S. Financial System, and U.S. Jurisdiction Over "Foreign" Parties and Events. *https://masspointpllc.com/publications/sanctions-anticorruption-moneylaundering-legal-analysis/amlsanctionsanti-corruption-publications/fifa-the-u-s-dollar-and-financial-system-and-u-s-jurisdiction-over-foreign-parties-and-events/* (https://masspointpllc.com/publications/sanctions-anticorruption-moneylaundering-legal-analysis/amlsanctionsanti-corruption-publications/fifa-the-u-s-dollar-and-financial-system-and-u-s-jurisdiction-over-foreign-parties-and-events/) Source 05
- Weaponizing the Economy. *https://berlinpolicyjournal.com/weaponizing-the-economy/* (https://berlinpolicyjournal.com/weaponizing-the-economy/) Source 06
- SWIFT and the Weaponization of the U.S. Dollar. *https://fee.org/articles/swift-and-the-weaponization-of-the-us-dollar/* (https://fee.org/articles/swift-and-the-weaponization-of-the-us-dollar/) Source 07
- How the U.S. Has Weaponized the Dollar. *https://www.bloombergquint.com/global-economics/how-the-u-s-has-made-a-weapon-of-the-dollar* (https://www.bloombergquint.com/global-economics/how-the-u-s-has-made-a-weapon-of-the-dollar) Source 08
- U.S. Customs Clearance Process. *https://usacustomsclearance.com/process/* (https://usacustomsclearance.com/process/) Source 09

- How the SWIFT System Works. *https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp* (https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp) Source 10
- SWIFT and the Weaponization of the U.S. Dollar. *https://tenthamendmentcenter.com/2018/10/12/swift-and-the-weaponization-of-the-u-s-dollar/* (https://tenthamendmentcenter.com/2018/10/12/swift-and-the-weaponization-of-the-u-s-dollar/) Source 11
- 6 Risks Of Exporting Manufactured Goods — And How To Avoid Them. *https://blog.thomasnet.com/risks-in-exporting-manufactured-goods-and-how-to-avoid-them* (https://blog.thomasnet.com/risks-in-exporting-manufactured-goods-and-how-to-avoid-them) Source 12
- Secure communication. *https://en.wikipedia.org/wiki/Secure_communication* (https://en.wikipedia.org/wiki/Secure_communication) Source 13

RESEARCH · 18 February 2018

ATC's Future in America

Ask a dozen American pilots about the direction ATC reform should take, and you'll likely receive a unanimous response: against privatization! Pilot and aviation lobbyists have effectively vilified any discussion challenging the ATC narrative. Given the complexity of this issue, a second (or third) examination is warranted for a more comprehensive perspective.

Historical perspective.

The U.S. consideration for privatizing air traffic control (ATC) is a longstanding discussion, spanning over three decades, notably prompted by the 1981 ATC strike, exposing organizational fractures within the FAA's ATC.

In the nearly four decades post-strike, a global pursuit for improved aerial traffic management emerged, not confined to the U.S. context it was a global issue. Two decades ago, Canada faced financial constraints hindering ATC infrastructure updates. After careful deliberation, the government opted for a non-profit entity through a contract, encompassing ATC system takeover and infrastructure upgrades. The inherent advantage lay in transparent modernization costs embedded in the contract, benefiting Canadian citizens.

Great Britain's NATS differs in structure as a public-private partnership, reflecting a shared trend of moving away from strictly government-controlled Air Traffic Systems.

Presently, numerous nations, including Germany, Australia, South Africa, and New Zealand (among over 70 others), have chosen to privatize or pseudo-privatize air navigation services. This corporate approach to air traffic management is gaining global momentum, with expectations of the list expanding further.

Diving deeper: the organizational structure of the U.S. system.

Many find confusion in the FAA's organizational structure and how a move towards privatization would impact it. The Air Traffic Organization (ATO), described as the "operational arm of the FAA," represents just one of fourteen headquarters offices within the FAA. While ATO governs all ATC, it constitutes a fraction of the entire FAA, with the remaining segments serving regulatory purposes, unaffected by potential ATC privatization.

Opponents of ATC reform often employ a scare tactic by linking the ATO to the regulatory portion of the FAA, creating a perception of lawlessness. However, this portrayal is inaccurate. Countries that have transitioned to private ATC, like Canada and the UK, maintain separate regulatory agencies—such as the Canadian Aviation Authority (CAA) and the UK Civil Aviation Authority—ensuring compliance with the International Civil Aviation Organization (ICAO). Therefore, there is no basis to assume that a private ATC entity within the FAA would deviate from established regulatory practices.

Compare and contrast.

A common argument asserts that nations with state-owned or private enterprises in air traffic control are considerably smaller or exhibit lower traffic density and counts. While this holds true—Canada shares a similar square mileage but has significantly lower traffic density than the U.S.—Western European nations

like the U.K. and Germany, with extremely dense airspace and high traffic density, are comparably smaller.

My perspective differs. I struggle to accept that traffic density is not proportionate to a nation's population and, consequently, its budget. The U.S.'s larger geographic area or denser population should not impact the proportional budget required for a private contract. In essence, the size difference between the U.S. and other nations, such as Germany or Canada, should not be a deterrent as budgets would adjust accordingly.

Despite concerns about the U.S. NAS being unsuitable for private ATC, Canada, handling 75% of the U.S. traffic count, has efficiently managed and updated its system, challenging the notion that such a transfer is inherently unsafe or unmanageable.

Fear and loathing in…

In my personal observations, even esteemed peers harbor a universal primal fear of disrupting the status quo. Videos from AirVenture emerged, featuring key EAA leaders denouncing the idea as a significant setback for general aviation, even hinting at its potential demise. Ironically, general aviation has been undergoing a gradual decline, with nearly a 10% reduction in total operations since 2009.

This decline appears more pivotal to me than privatizing ATC services since it stems from factors unrelated to air traffic services. If blame were to be assigned within the FAA, it would be to the regulatory aspect, persisting without change. Outdated regulations have impeded general aviation growth for decades, overshadowing concerns about obsolete equipment. People are increasingly unwilling to spend well over $100 per flight hour on aging Cessnas or Pipers.

If the AOPA and EAA genuinely prioritize expanding general aviation access, redirecting efforts towards reducing private flying costs—specifically, deregulating the industry—would be more effective. By doing so, the allure of flying would draw people, as their desire to fly remains strong, akin to DaVinci's time, but the threshold of entry must be more reasonable.

RESEARCH · 27 December 2017

Diamond Aircraft: Ownership Shifts from Europe to Asia

Diamond Aircraft, the manufacturer of the Diamond DM-40, has been acquired by Wanfeng Aviation, a prominent Chinese entity in general aviation. This development follows Wanfeng Aviation's acquisition of a 60% stake in Diamond Canada just a year ago, signaling a significant shift in the general aviation landscape.

Diamond has consistently led technological advancements in the general aviation sector, introducing innovative concepts to an industry that has seen minimal technological evolution over the past five decades. They have pioneered composite design, synthetic vision displays, and diesel engines, bringing a forward-thinking approach to general aviation pilots.

Regarded as a strategic business move, Diamond has lacked the financial resources required to fully support the development initiatives they aspire to achieve. Wanfeng provides the necessary impetus to propel their vision forward, enabling the creation of cutting-edge aircraft for the general aviation sector—a domain currently grappling with a significant technological stagnation. Christian Dries, the departing CEO of Diamond, commented on the December 23rd acquisition, stating, “Diamond is my life’s work. To secure a prosperous long-term future, finding the right partner was essential. Wanfeng, led by Mr. Bin Chen, aligns with my vision for the future of general aviation, investing with a strategic, long-term perspective and possessing the resources to realize this vision. I am confident that Diamond is in capable hands, given our successful year-long partnership in Diamond Canada.”

The acquisition is unsurprising within the aviation community, given China's status as the largest and fastest-growing market globally. Diamond, known for its DA-40 primary training aircraft, is poised to meet the escalating demand in China, where annual aviation growth rates reach 15% in a country housing one-seventh of the world's population. The imperative to secure a rapidly expanding supply of light aircraft aligns with the necessity to meet this burgeoning demand.

The acquisition of general aviation assets is not a recent trend. According to the Rand Corporation, the acquisition spree by Chinese holdings commenced early in the 21st century, notable instances being the purchase of Brantly Helicopter in 2007. Initially, this raised minimal interest as Brantly was largely considered a dormant entity in the aviation domain. However, the acquisition of Teledyne by the Aviation Industry Corporation of China (AVIC) garnered more attention. AVIC, with just under half a million employees and a ranking of 162nd in the Fortune Global 500, presents formidable figures for a corporation existing for just under a decade. The context becomes clearer when recognizing its status as a state-owned holdings corporation.

Ascending the acquisition timeline reveals a systematic takeover of the general aviation industry. Cirrus Aircraft, acquired by AVIC and China Aviation Industry General Aircraft (CAIGA) in 2011, and Tom Hamilton's Glasair Aviation, bought by Zhuhai Hanxing General Aviation Company, Limited, echo this trend. While smaller in scale compared to Teledyne, the purchase of Mooney International Corporation by Henen Meijing Group, a Chinese real estate mogul, stands out due to Mooney's industry icon status and persistent financial struggles.

Chinese acquisitions and mergers in the aviation sector appear closely tied to economic downturns in the U.S. Essentially, general aviation, perceived as a luxury in the West, becomes expendable during overall economic declines. In simpler terms, private aircraft ownership becomes a discretionary expense, often sacrificed when individuals face financial challenges such as meeting mortgage payments. The Rand Corporation identifies that many major purchases by Chinese investors align with the housing crisis and subsequent economic downturn circa 2009. Western investors, constrained by limited capital during that period, hesitated to invest in an industry lacking immediate returns. In contrast, Chinese investors seized the opportunity to acquire struggling industries, with aviation being a particularly attractive market. Given China's economic interests spanning the Pacific Rim, aviation becomes a strategic necessity. By purchasing established American manufacturers and maintaining their operations in the U.S. through Chinese capital, China secures market dominance from a distance, benefiting from Western sales while maintaining exclusive access to the product. Although Diamond will continue selling to Western customers, China now holds exclusive access to the product line and production.

Inevitably, the state of affairs has reached this point. General aviation, burdened by decades of stringent regulation, has impeded progress in aviation technology. Pilots now carry computers instead of their phones aboard space shuttles, yet they navigate airplanes using outdated 'steam gauges' for instrumentation, while their phones could employ software for synthetic vision and pinpoint accuracy. Despite overall effectiveness, aircraft engines lag decades behind their counterparts in the automotive sector. As bureaucratic regulations continue to hinder growth, China remains eager to acquire struggling companies. Of course, there are attached strings to these acquisitions.

Part V

Methodology: How We Work

GUIDE · 29 March 2024

How We Write

1 What is this article about? This article serves as an introduction to the three primary types of articles produced by Ubinodes, detailing the standards for crafting them effectively. Additionally, it provides recommendations for enhancing clarity to cater to online readers.

Why do you need it?

While Ubinodes functions as an international marketing network, one of its core objectives is to stay abreast of developments in the realms of I.T, Business, International Affairs, and more. To achieve this, a consistent effort is required to write and update articles, ensuring that our audience is not misinformed by outdated information.

Maintaining a steady flow of articles not only saves time by preventing the repetition of information to potential clients and candidates but also aligns with our goal of keeping content concise. Recognizing that readers often disengage from articles that do not promptly address their queries, the sections below offer guidance on creating focused and impactful content.

Abstract

While the creation of written works is inherently subjective, embracing standardization contributes to the clarity of our articles. Establishing a consistent format allows readers to navigate seamlessly across various topics. The categorization of articles into three distinct formats ensures the effective sharing of diverse subjects and teachings. The provided formatting and writing suggestions aim to enhance accessibility for readers. Importantly, these guidelines are presented in a general manner, preserving space for individual creativity among our contributors. Through this balance, we strive to deliver informative and engaging content while respecting the unique voice of each creator.

Ubinodes recognizes this trend and tailors its article formatting to align with this shift. Our approach is designed with a focus on the smartphone reader, considering the prevalent behavior of scanning rather than thorough reading in online contexts.

01.2 The Process We Employ

In pursuit of this objective, we have formulated a process grounded in the following principles:

 Articles Should Be Read at a Glance.

Acknowledging the tendency of online readers to scan rather than read in-depth, we adopt a strategy reminiscent of deciphering jumbled words.

We strategically scatter reading clues throughout our content, ensuring comprehension even when readers opt for a cursory glance. This approach accommodates the rapid pace at which individuals consume information online.

 Articles Are Optimized For Thumb-Scrolling.

Given the prevalence of smartphone usage for reading, our articles are crafted with a top-to-bottom flow optimized for thumb-scrolling. This means that information is presented in a progressive depth-of-knowledge manner.

Unlike traditional academic structures (introduction, development, conclusion), we prioritize organizing content based on detail. As readers scroll downward, they encounter information at increasing levels of expertise, enabling them to stop at the point that aligns with their desired level of understanding.

01.3 Publishing Fundamentals

• Streamline Content: Ensure your writing doesn't contain unnecessary filler words that does not add any value. Try to pass information with fewer words without losing the essence of the idea.

• Title Guidelines: Your titles should be engaging enough to capture your reader's attention at first glance. Use important keywords and reinforce it with an action word.

• Go for Conciseness: When writing, use less complex words and your writing should be clear and brief.

• Maintain Consistent Flow: Sustain a cohesive flow throughout the article, allowing readers to follow the narrative seamlessly.

• Formatting Consistency: Compare your formatting with already-published articles on our website for uniformity and adherence to established standards.

01.4 Genres We Cover

To enhance the efficiency of the above-mentioned process, we've classified our articles into three distinct genres: Guide Review Research This classification ensures a structured approach in line with our established writing process.

01.5 Perspectives of Writing Each Genre

Guides: This is created as a manual for users. When writing a guide, you are to write in the perspective of an operator, more like a technician carrying out a specific task.

Review: In this case you're to write in the viewpoint of a user. A review offers honest and first-hand observations and experiences you get when using an app, device, company, markets, industries, countries, etc.

Research: Positioned as an investigative piece, a research article explores the intricacies of using applications, devices, companies, markets, industries, countries, etc., from the standpoint of an expert examining underlying details.

01.6 eBooks

The final article may take the form of an encompassing "all-under-one-roof" piece, integrating elements of a Guide, a Review, and a Research. Each section, however, is distinct within the article. During the writing process, special attention is given to ensuring that the sections are easily scan-readable and thumb-scrollable on a mobile phone. Whether it's the Guide, Review, or Research section, they are written separately, tailored to their specific characteristics.

 Conduct comprehensive research to establish a solid understanding of the subject, ensuring the ability to effectively convey information to others.

 Engage in a testing phase to acquire first-hand experience that resonates with the reader.

 Consider the opportunity to simultaneously develop a Review or a Research article, preventing the waste of valuable knowledge and experience.

 Adhere to our guidelines, ensuring that information is formatted consistently and efficiently for optimal sharing on our platform.

 This preparatory phase varies, ranging from an hour of website reading to several hours of testing to identify optimal approaches.

 Collaboration within a team may be necessary to share opinions and distribute the workload. This can also be practical when connecting computers or devices is essential for testing purposes.

02.1 Guidelines to Follow During Content

Creation. During the content creation phase, consider the following guidelines for an effective article:

 Define Your Audience: Think of your target audience so you can tailor the content appropriately. This may influence points you want to address. The wording should align with the preferences and understanding of your audience.

 Create a TL;DR Summary: Develop a concise summary paragraph to serve as the article's "Too Long; Didn't Read" introduction, providing a quick overview of the main points.

 Maintain Point Consistency: Review the draft, ensuring that each point is roughly the same length. If possible, combine points to maintain a balanced and engaging structure.

 Adhere to Layout and Formatting Guidelines: From the outset, follow the specified guidelines for layout and formatting. This ensures efficient collaboration with others and a cohesive presentation.

02.2 The Publication Process

When preparing for publication, adhere to the following steps to guarantee a high-quality and impactful article:

 Cite All Sources: Include references to all sources used in your article to maintain credibility and transparency.

 Thorough Review: Read through the article multiple times to identify and rectify any oversights. Ensure that no important details are missed during the editing process.

 Seek External Proofreading: Obtain feedback from others to gain a fresh perspective on your final work. However, avoid seeking proofreading too early to prevent fatigue and ensure a comprehensive review toward the end of your work.

 Maintain High Quality through Peer Review: Uphold a high standard of quality by subjecting each article to peer review. This process ensures that the information presented is both factual and relevant, enhancing the overall integrity of your content.

The key lies in imparting knowledge in the simplest manner possible, ensuring accessibility to a diverse audience regardless of age or tech experience. Notably, guides can also be employed for marketing purposes, as exemplified by this very article.

03.1 Key Attributes of this Article

 Technical "On the Field" Use: Given its nature as a "step-by-step" guide, technical explanations are consolidated in end-of-article notes, allowing users (often operators) to complete tasks and later delve into detailed explanations.

 Integral Screenshots: Screenshots are seamlessly integrated with step- by-step actions, enhancing the user's understanding.

 Constructive Opinions: As viewed from an operator's perspective, the guide accommodates constructive opinions, sharing valuable tips and advice without evaluating features or pros and cons.

 It explicitly avoids evaluating features, pros and cons, or delving into technical intricacies.

03.2 Preparation

 Personal Connection and Passion: Drawing from personal experiences and passions aids in selecting a compelling guide topic and facilitates easier writing.

 Collaboration for Detail: Avoid solo work to ensure comprehensive coverage. Collaborate with others to perform actions on different devices, unveiling potential technical glitches and nuances.

 Real-time Testing: Initiate real-time testing by using the product in a live project with diverse participants over a minimum two-week period. This minimizes bias, incorporating different operating systems, team members, and organizational aspects.

 Developer/Manufacturer Interaction: Seek answers to specific questions by reaching out to the developer or manufacturer during the testing phase.

03.3 Creation

 Inclusive Steps: Document every step, regardless of apparent simplicity, to avoid overlooking essential details.

 Challenging Process Documentation: Capture images during testing, focusing on challenging aspects to assist readers in overcoming potential obstacles.

 Informative Tone: Maintain an informative tone throughout the instruction, avoiding condescension.

 Self-Testing or Peer Verification: Conduct thorough testing of the guide, either personally or through peer verification, to ensure its correctness and effectiveness.

04. Review

 Features: Presented in a checklist format, with the option to include a dedicated paragraph for screen shots or photographs.

 Positives and Negatives: An unbiased evaluation, listing pros followed by cons, devoid of personal opinions.

Reviews can also serve marketing purposes, offering observations from the perspective of a distributor or end buyer when assessing industry suppliers, local shops, or client competition.

04.1 Distinctive Features

 User-Centric Raw Description: The review offers a raw, user- centric description, avoiding personal opinions. Strategic Screenshot Placement: Screenshots or photographs providing an overview are placed in a dedicated paragraph to maintain the reading flow. Observation-Based Article: Deeper information is relegated to Notes at the end, adhering to the thumb-scrolling principle. Excessive notes indicate a potential shift to a formal research article. Not a Guide or Research: It does not provide installation instructions or delve into technical details.

04.2 Preparation

Differentiating from a guide, the review demands exploration beyond the immediate subject matter. Researching similar applications and websites is crucial to establish a comparative baseline.

04.3 Content Creation

 Short Paragraph Reviews: Each product receives a concise paragraph review, encompassing all featured aspects.

 Pros and Cons Listing: Include a pros and cons list for each product, catering to readers who prefer a quick overview.

 Affiliation Disclaimer: Emphasize the lack of affiliation with the product and give credit where it's due to maintain transparency and credibility.

05. The Research

A well-executed research article serves as a comprehensive repository of information on the chosen subject, functioning as a "catch-all" document.

Research can also be leveraged for marketing purposes, such as market research. In this scenario, it adopts the perspective of an expert, delving into politics, regulations, history, and more to elucidate the inner workings of the subject.

05.1 Distinctive Features

 Thumb Scrolling Dominance: Emphasizes the thumb-scrolling principle, distinguishing it from guides and reviews.

 Tiered Knowledge Structure:

 General Knowledge (First Tier): Sufficient for shorter articles, requiring basic understanding.

 Advanced Knowledge (Second Tier): Medium-length articles demand a display of topical and subject expertise.

 Expert Knowledge (Third Tier): Specialized articles necessitate total- subject mastery.

 Exclusion of Guide and Review Elements: Does not offer installation instructions or comment on features and pros and cons.

05.2 Preparation

 Comprehensive Topic Exploration: Requires researching all related topics for a holistic view, going beyond mere observation.

 Reader-Centric Approach: Consider the target audience while maintaining clarity for uninformed readers.

 Subject-Specific Understanding: Familiarity with subject-specific terminology is crucial, explained in simple terms for reader comprehension.

05.3 Content Creation

 Information Consolidation: Collate all researched information for a cohesive presentation.

 Flowing Article Draft: Craft a well-structured article that flows seamlessly, facilitating reader engagement.

 Strategic Image Use: Reinforce key points with images, deciding whether to place them in dedicated paragraphs (e.g., screenshots) or integrate them into the content to preserve the reading flow.

Guidelines

06.1 Layout

Font for all text except Footer: Verdana.

• Cover page. (Contains Logo and Title).

• First Page:

◦ What is this article about? (Title, Align Center).

◦ Why do you need it? (Title, Align Center).

◦ Abstract. (Title, Align Center).

• Table of Contents. (Title, Align Center).

◦ Put only H1 in the table of contents.

• Actual Content:

◦ H1. (Align Left, Size 26pt).

▪ H2. (Align Left, Size 18pt).

- **H3. (Align Left, Size 14pt)**

◦ **H4. (Align Left, Size 12pt, bold)**

▪ **Underscore. (Align Left, Size 12pt)**

- **Content. (Justified, Size 12pt)**

• Screenshots (Applicable for Review and Research articles). (Heading 1, Align Left).

• Notes. (Heading 1, Align Left).

• Sources. (Heading 1, Align Left).

• Footer (on all pages, except cover). (Calibri, Align Left, Size 11pt).

06.2 Style

06.2.1 Font, Size. Title: Bold, Size 28pt, alignment centre. Headings: Alignment left. • H1: Size 26pt. • H2: Size 18pt. • H3: Size 14pt. • H4: Bold, Size 12pt. Content: Size 12pt, alignment justified. • Use Bold for hierarchy below Heading 4. Include its punctuation in bold.

06.2.2 Headings & Numerical Consistency. 06.2.2.1 Common style. Set paragraph Style: Always apply the corresponding heading setting first before changing the font and size. That way the PDF reader will display the content of the article in the navigator. Font: Verdana for the entire content except Footer (Calibri). Color: Black for the entire content. Headings: Not bold nor Italic, alignment left. 06.2.2.2 Headings. Heading 1:

06. blabla

• Verdana, 26pt. • Number with two digits (so we include 0 between 1 and 9) followed by a full stop. • Space between the full stop and the sentence. Heading 2:

06.2 blabla

06.2.1 blabla

• Verdana, 14pt. • First number with two digit, identically to its heading 1. • Second number with only one digit. • No full stop at the end. • If you reach more than 9 sub-headers, then this entire paragraph needs to be broken down so as to have a new heading 2 and stay below 9 heading 3. • Space between the full stop and the sentence. Heading 4:

06.2.1.1 blabla

• Verdana, bold, 12pt. • First number with two digit, identically to its heading 1. • Second number with only one digit. • No full stop at the end. • If you reach more than 9 sub-headers, then this entire paragraph needs to be broken down so as to have a new heading 3 and stay below 9 heading 4. • Space between the full stop and the sentence.

06.2.4 Alignments. Centre: • Titles. • Pictures. • Block Quotes and other insertions. Left: • Headings. • Footer. Justified. • Paragraphs.

06.2.5 Body Text. Well-structured paragraphs present all relevant information in a clear and logical flow, eliminating non-essential details where possible. • Style: Normal. • Font: Verdana. • Size: 12pt. 06.2.5.1 Punctuation. Ensure you proofread and edit the document that all punctuations are in place and used according to academic standards. Full stop: In line with our philosophy of writing for smartphone reading and eye-scanning of the content, we deviate from the academic standard in the way that we always put full stop the end of a Heading. Do not use colon at the end of a heading on the pretext that sub-content will follow.

06.2.5.2 Checklists. • Can be bulleted or numbered so as to enhance readability.

06.2.6 Footer. • Format Footer: Untick “Same content on first page” if there is a front page.

• Height: Tick “AutoFit height”. And put 0,10 cm.

• Spacing: Tick “Use dynamic spacing”. And put 1,90 cm.

• Style: Footer. Size 11pt.

• Font: Calibri.

• Align Left.

• High of field 1.5cm.

• Content:

◦ Page x of xx. (Use insert -page number- and -page count-).

◦ Last revised date. Do not change this date if it’s only a cosmetic change (layout). Change it if the actual content was updated. However, in the file name, you must change the date so that when uploading the new file into the website’s Media tab, it won’t interfere with the old file.

◦ Copyright: European Union Public License, version 1.2 (EUPL-1.2).

06.3 Content

06.3.1 Contextualizing Questions. Today, the difficulty is not to access information over the internet but exploit it. So the first page begins by addressing two key questions for the readers. The aim is to help them decide at a glance whether this article is what they were searching for or not.

1. What is this article about?

2. Why do we need it?

06.3.3 Table of contents. A section listing the main paragraphs, aiding readers in quickly grasping the article's content.

Keep it as short and to the point as possible.

Put only H1 in this content.?

06.3.4 Paragraphs. 6.3.4.1 Author's Influence. Our articles present factual information without influencing readers' opinions, encouraging them to draw their own conclusions based on the provided data.

06.3.4.2 Screenshots. • For Reviews and Research articles, in order to maintain reading flow, screenshots are placed in their designated section at the end of the article, before “Notes” and “Sources”.

• In Guides, screenshots are integrated into relevant step-by-step paragraphs.

• In order to facilitate later revisions, first insert a table, then place images and descriptions into rows.

06.3.2 Screenshots. For Reviews and Researches, in order to maintain reading flow, screenshots are added in this specific section, at the end of the article.

06.3.3 Notes. Technical details are placed in notes at the end of the article to streamline paragraphs. Proper referencing, using parentheses, ensures easy access for interested readers. Example: (Note 05).

06.3.4 Sources. Credit to external information sources is given at the end of relevant paragraphs in parentheses. Example: (Source 02).

06.4 Tags

Add tags to articles before posting for easy retrieval.

06.5 Filename

Adhere to our file-naming convention: "Year-Month-Day-Name-of-Article."

This format ensures organizational clarity. The date is the one any change has been made to the file so that in the “Media” tab of the website’s back end, it doesn’t interfere with the previous file.

Note however, that in the content of the document itself, the “last revised” date in the footer is changed only if the actual content has been updated, not if it’s a cosmetic change only (layout) so that readers can know if the content is actually up to date.

If you happen to make several changes the same day, which would imply having identical filenames, then simply use the next day for each update. It is unlikely that the same article will be worked on by another Node the next days without your knowledge, so you can communicate on this topic.

7. WordPress

Featured Images Dimensions: • Featured images should be 700x420. Use Photofiltre for resizing.

Twitter Announcement: After making a post, share a tweet on Ubinode’s timeline using your Twitter account.

Excerpt Writing: Always write a custom excerpt. By default, WordPress may use the initial lines, which might not be descriptive enough for readers.

Dedicated Featured Image: Always use a dedicated featured image. WordPress may default to the first image in the article, which might not accurately represent the content on search engines.

 By adhering to these WordPress tips, you ensure a visually appealing and informative presentation of your articles, enhancing engagement and visibility.

Uploading Article on the WordPress • When uploading articles to the Ubinodes website, adhere to our file- naming convention: "Year-Month-Day-Name-of-Article."

• Ensure the article you’re about to post aligns with our naming structure.

• If this is an updated version, remove the previous one from the media folder.

Creating a ‘how to’ guide (2021a) Creating a ‘How to’ Guide. Available at: https://www.bath.ac.uk/guides/creating-a-how-to-guide (Accessed: 20 November 2023).

Home (2023) Student Academic Success. Available at: https://www.monash.edu/rlo-old/graduate-research-writing/write-the-thesis/ writing-a-literature-review/structure (Accessed: 20 November 2023).

World Leaders in Research-Based User Experience (no date) How people read online: New and old findings, Nielsen Norman Group. Available at: https://www.nngroup.com/articles/how-people-read-online (Accessed: 20 November 2023).

PROTOCOL · 6 April 2021

Protocol for App Reviews

1. Aim.

We have developed a comprehensive protocol for testing applications to ensure transparency and credibility for both our sponsors and readers. Our goal is to maintain consistency across our reviews while providing valuable insights to users.

It's important to note that our reviews are not intended to judge or recommend specific apps. Instead, our focus is on thoroughly examining all features of the application so that end users can make informed decisions based on their specific needs and circumstances.

Our review process encompasses thorough evaluations of the app's security and usability aspects. We will then publish an article detailing our findings. Additionally, we assess the app from a business standpoint, considering factors such as:

- Does the app add value to your organization?
- Does it help in reaching your target audience effectively?
- Is the app user-friendly and easy to adopt, minimizing any potential friction for users?

1. Lists of features.

To facilitate comprehensive reviews and comparisons of various apps, we maintain generic lists for different categories:

-**Communication Apps:**This category includes features such as sending text (email or chat), image sharing, video sharing, VoIP meetings, video conferencing, and file sharing.

-**Website and Blogs.**

-**Operating Systems.**

-**Hardware.**

We systematically review each feature listed, regardless of its apparent relevance, to ensure thoroughness and ease of comparison for our readers. Features are added to the list as needed, without any specific order, enabling us to integrate them seamlessly.

The purpose of the feature list is to prevent the oversight of any essential features. Consequently, some features may appear contradictory, such as those related to privacy versus usability, while others may be deemed irrelevant. However, including all features ensures that readers can make informed decisions by comparing apps side by side.

Top of Form

2. Protocol.

To ensure an unbiased and comprehensive review, all apps undergo the following testing procedures:

-**Real-time Usage:**We utilize the app on real projects to assess its functionality and performance in practical scenarios.

-**Global Testing:**The app is tested by team members located in different countries, including those where internet censorship is prevalent. This allows us to evaluate how the application handles issues related to government restrictions on internet access.

-**Ethical Hacking:**Whenever possible, we include a certified ethical hacker (white hat) in our testing team. This individual examines the code and attempts to intercept communications or gain unauthorized access to the device to identify potential security vulnerabilities.

-**Cross-Platform Testing:**The app is tested on various devices and operating systems. For desktop testing, we use Linux and Windows, and if feasible, macOS. On mobile devices, we test the application on Android and iOS platforms, and if available, AOSP and Linux. We also explore alternative app stores such as APK Pure and F-Droid to determine if the application is accessible outside of mainstream platforms like Google Play or Apple Store.

-**Duration of Testing:**We rigorously test the app for a minimum of two weeks, with an average testing period extending to four weeks. This prolonged assessment ensures a comprehensive understanding of the app's capabilities and performance over time.

-**Peer Review:**Following testing, the article undergoes peer review by other team members. Subsequently, it is sent to the app developers for final review, ensuring accuracy and fairness in our assessment.

3. Milestones, Goals.

To enhance transparency and clarity regarding fund allocation, we've established milestones, referred to as "goals," on the Open Collective platform. These milestones outline the key steps we'll undertake with the funds received. The standard list of milestones is as follows:

1.**Threat Model:**Define a threat model scenario to benchmark the app against.

2.**Specifications Sheet:**Define the needs of end users according to the threat model. Create a specifications sheet with a list of features to be reviewed.

3.**Gather Team:**Based on the threat model scenario, assemble a team of skilled end users in the field to review the app. Ensure representation from different countries to assess the app on an international scale.

4.**Comprehensive Review of the App (Week 1):**Review each feature of the app and draft the article in English.

5.**Comprehensive Review of the App (Week 2):**Continue reviewing each feature of the app and draft the article in English.

6.**Comprehensive Review of the App (Week 3):**Further review each feature of the app and draft the article in English.

7.**Comprehensive Review of the App (Week 4):**Conclude the review of each feature of the app and draft the article in English.

8.**Ethical Hacker:**Hire an Ethical Hacker (also known as a white-hat hacker) to test the vulnerabilities of the app.

9.**Finalize Article:**Based on the report from the ethical hacker, finalize the article and submit it to the app developers for comments. Update the article accordingly.

10.**Translations:**Translate the article into various languages depending on the countries we cover at that time. Example languages include French, Estonian, Spanish, and Portuguese. Share the article with sponsors in all languages.

11.**Publishing:**Share the article with sponsors in all languages under the Copyright European Union Public License, version 1.2 (EUPL-1.2). Three months later, publish the article on our websites.

CHECKLIST · 6 April 2021

Benchmark Features: Communication Apps

To benchmark communication applications systematically, ensuring comprehensive feature coverage across our articles, we formulated a review checklist.

1.1 Code & developers.

- Code: Open source or audited by a trusted third party.
- License: FOSS (Free Open Source Software) or Freemium.
- Liveliness: Actively maintained, with regular app updates.
- Support: Emergency assistance provided by the provider; the team responds to user support requests.
- In-app communication with support team:
- Whitepaper: Detailed whitepaper available explaining the concept.
- Ownership: Identification of the entity responsible for the app's development and maintenance.

-

1.2 Package.

- Platforms: Multiplatform, Windows, Linux, MacOS, Android, iOS, Ubuntu Touch etc.
- App stores: Available from alternative repositories: APKpure, FDroid, Github, team’s website etc. That way user doesn’t have to use a Google or Microsoft account.
- Apk Signature: Signature key provided on website to check that APK downloaded has not be tampered with.
- Digitally signed with Microsoft: So as not to trigger a warning from Windows SmartScreen.
- Push notifications: Uses the standard push notification service provided by the operating system.
- OTA updates: OvertheAir means updates are downloaded automatically by the app.

1.3 Usability.

- Intuitive Adoption: Userfriendly for all, simplifying installation and feature usage.
- Uniform Features: Consistent features across various operating systems like Android, iOS, Windows, and Linux.
- User Administration: Admin capabilities for communication apps and websites/blogs, allowing invitation, removal, moderation, and editor access.

> Desktop Application: Equipped with desktop app support for enhanced productivity and ease of use.

- Synchronicity: Enables offline messaging, eliminating the need for parties to be connected simultaneously, addressing the limitation of peer-to-peer apps like Jami or Briar.
- Content Search: Offline-capable in-app content search engine.
- Contact Search: Search field for locating contacts within the app's contact list.
- QR Code for Contact: Streamlined contact addition through QR code scanning.

- QR Code for Additional Device: Effortless addition of new devices via barcode scanning, eliminating the need for re-entering credentials.
- File Support: Specifies supported file types, including text, images, video, and sound.
- Delivery and Read Receipts: Notifies the sender about message delivery and read status.
- Typing Indicator: Indicates when your contact is typing.
- App Notifications: Displays the number of new messages and allows customizable notification settings for vibration, sound, and deletion.
- Message Notifications: Manage notification preferences for different message types (direct chat, group, forum).
- Trimming: Option to trim older messages based on date or size.
- Export: Encrypts data for secure export to an external device or cloud for device migration.
- Device Synchronization: Ensures messages and contacts are synchronized across devices for seamless chat transitions.
- Night Mode: Enables a dark mode for reduced eye strain.
- Status Indicator: Allows users to indicate availability or choose to hide it.
- Quote: Facilitates quoting and replying to specific messages within a chat.
- Format: Supports text formatting options like bold, italic, and strikethrough.
- Go to Last Message Button: Quick navigation to the latest message in a chat.
- Chat Continuity: Resumes conversations from where they were left off upon returning.
- Contact List: A dedicated list for managing contacts.
- Multi-Account: Supports multiple accounts on a single device.
- Message Segregation: Separates one-on-one, group, and forum messages into distinct spaces.
- Screen Rotation: Automatically rotates the app when the device is rotated, enhancing user experience.

-

-

1.4 Productivity.

- Provides Forums:
- Provides private blog:
- Provides RSS feed:
- File sharing: Ability to share any type of files with contacts
- Own domain name: For emails.
- Can share GPS position:
- Supports bots:
- Voice meetings:
- Video meetings:
- Group invite by link: Ability to invite by giving a link.

- Contact member of a group: Ability to see group members and contact them oneonone.
- IRC like commands: Can obtain lists by using "/" commands.

1.5 Security & Privacy.

- No identifying information: No collection of personal details during purchase and setup (email, phone number, credit card).
- No permission request for device access: Installation does not involve accessing device data, contacts, or media files.
- Resistance to state-sponsored criminals: Guards against legal misconduct by corrupt state entities. Mitigates interception of IMAP, POP3, TLS, SSL, and email provider SSL certificate spoofing. Ensures protection against unauthorized access to SMS and emails.
- Not in a 5 eyes country: App development and server usage are not associated with Australia, Canada, New Zealand, United Kingdom, or United States.
- End-to-end encryption: Ensures cryptographic security for every message and file.
- Encrypted by default: Applies encryption automatically to both direct and group chats, not as an optional feature.
- Zero-Knowledge: Encryption key remains on the user's device, not shared with the server. Data is not stored on a central server after delivery, and no logs are retained.
- Ephemerality: Messages automatically deleted from all recipients' devices after a set time period.
- Data shredding: Deleted files rendered unrecoverable by forensic software (Wickr).
- Chat history: New group members or added devices may or may not have access to older messages based on threat model. Wire restricts access as a security measure.
- Tamper proof: Warns of Man-in-the-Middle attacks or any attempt to tamper with communication, data, or updates.
- Security word: Allows verification of communication integrity through a security word at the beginning of each voice call (Silent Phone, Signal).
- Contact Verification: Enables verification of addressees through device fingerprinting, with a list in the app's settings.
- Auto log off: App logs off after a set delay, distinct from screen lock.
- Password protected: Requires a password or code when launching the app.
- No recovery option: Eliminates recovery via email or SMS to protect against state-sponsored criminals. Recovery options include a code (Tutanota), seed phrase (Session), or none (Wickr Me).
- Data at rest is encrypted: Decryption occurs at app launch, and messages remain inaccessible to third parties, even under legal compulsion (Forensic).
- Anonymous: Sends data through anonymizing networks (Tor, Lokinet) and encrypts metadata (Olvid).
- Plausible deniability: Prevents the creation of identical IDs (same fingerprint) on different devices.
- Prohibits screenshot: Can prevent recipients from taking screenshots.
- Screenshot warning: Sends a notification to the sender if the addressee takes a screenshot (Telegram).

- Lock screen: Allows setting a delay to lock the screen after inactivity.
- Disable keyboard learning: Disables the device's keyboard learning.
- Disable link preview: Option to disable link preview in messages.
- ID revocation: Ability to revoke an ID from a website if devices are compromised (Threema).
- Panic button: Ability to trigger an action to delete data or the account.
- Mobile data in-app deactivation: Ability to deactivate the use of mobile data in app settings.
- Off Grid connection: Possibility to connect directly using Bluetooth or Wifi without internet.
- Decentralization or distribution: Members can communicate even without a central server or host.
- Delete own messages: Ability to delete a message from all devices and recipients' devices.
- Delete groups: Ability to delete a group so it disappears from all members' devices.
- Transparency report or Warrant Canary: Publicly shares any request received by a governmental agency.
- Access and activity logs: Provides information on when and by whom the app has been accessed.
- IP restrictions: Restricts access to pre-approved IP addresses.
- TOR sign up: Ability to create an account using TOR.
- Self-destruct account: Account is deleted after a set period without logging in.

-

-

-

-

1.6 Price and value.

- Cost-Efficiency: Offers affordable plans for large user bases, feasible for a 15-member team with a monthly fee or one-time license fee.
- Anonymous Payment: Accepts payments via anonymous cryptocurrency like Monero.
- Group Size Limitations: Varies across platforms - e.g., Wickr allows 50 members, Threema accommodates 100, Wire supports 250, while Telegram permits thousands in a group.
- File Sharing: Maximum file size for sharing, including videos, varies per platform.

CHECKLIST · 6 April 2021

Benchmark Features: Websites & Blogs

To benchmark websites and blogs systematically and ensure comprehensive coverage of features across our articles, we've devised a checklist of elements to review.

1.1. Code & developers.

- Code: Open source or audited by a trusted third party.
- License: FOSS (Free Open Source Software) or Freemium.
- Liveliness: Actively maintained: App receives regular updates.
- Support: Emergency support provided by the provider. The team responds to user support requests.
- Ownership: Identifying the body responsible for the development and maintenance of the app.

-

1.2. Package.

- Platforms: Available on multiple platforms such as Windows, Linux, MacOS, Android, iOS, Ubuntu Touch, etc.
- App stores: Accessible from alternative repositories like APKpure, F-Droid, Github, the team's website, etc., enabling users to avoid reliance on Google or Microsoft accounts.
- APK Signature: Provision of a signature key on the website to verify the integrity of downloaded APKs.
- Digitally signed with Microsoft: To prevent triggering warnings from Windows SmartScreen.

-

1.3. Usability.

- Intuitive: User-friendly adoption, catering to both technical and non-technical individuals, ensuring ease from installation to utilizing almost all features.
- Consistent Features: Uniformity across all operating systems; features available on one (e.g., Android) mirror those on others (iOS, Windows, Linux).
- User Administration: Not limited to a single admin access (as seen in platforms like Medium) but allows the creation of editor access for the team (similar to WordPress or Steemit).

-

1.4. Productivity.

- Offers Forums.
- Provides Blog.
- Provides RSS feed.
- File hosting: Ability to host any type of files.

- SEO friendly. Content must be accessible to search engines.
- Own domain name: You can use your own domain in the URL.

1.5. Security & Privacy.

- Privacy-Centric Setup: No requirement for personal information (email, phone number, credit card) during purchase or setup.
- No Device Data Access: Does not request access to device data upon installation, preserving user privacy by refraining from scanning contacts or media files.
- Resilience Against State-Sponsored Threats: Protects against state-backed criminals who can manipulate legal systems, intercept communications (IMAP, POP3, TLS, SSL), spoof SSL certificates, access SMS and emails.
- Non-Participation in 5 Eyes Countries: Either in server location or by the app's development team/company, avoids countries like Australia, Canada, New Zealand, United Kingdom, United States.
- Two-Factor Authentication (2FA): Ability to mandate the use of 2FA for every user.
- Access and Activity Logs: Provides records of when and by whom the app was accessed.
- IP Restrictions: Allows restriction of access to pre-approved IP addresses.
- TOR Sign-Up: Capability to register an account using TOR for added anonymity.
- Self-Destructing Accounts: Offers an option to automatically delete accounts after a predetermined period of inactivity.

-

1.6- Price and value.

- Cost-efficiency: Offers a reasonable monthly fee or one-time license cost for a large user base. With a 15-person team, the organization can comfortably manage the monthly expenses.
- Anonymous payment: Supports payment through anonymous cryptocurrency like Monero.

-

CHECKLIST · 6 May 2021

Benchmark Features: Operating Systems

In order to benchmark Operating Systems, not overlook some features and have consistency across our articles, we designed a list of features to review.

1.1 Code & developers:

- Code: Open source or audited by trusted third party.
- License: FOSS (Free Open Source Software), or Freemium.
- Liveliness: Actively maintained: App is regularly updated.
- Support: Emergency support by the provider. The team is answering to support requests from users.

1.2 Package:

- Platforms: Multi-platform, Windows, Linux, MacOS, Android, iOS, Ubuntu Touch etc.
- App stores: Available from alternative repositories: APKpure, F-Droid, Github, team's website etc. That way user doesn't have to use a Google or Microsoft account.
- Apk Signature: Signature key provided on website to check that APK downloaded has not be tampered with.
- Digitally signed with Microsoft: So as not to trigger a warning from Windows SmartScreen.

1.3 Usability:

- Intuitive: Adoption from the team is easy even for non geeks, from installation to using all most features.
- Data persistence (when you shut down your system, data is saved on the media).

1.4 Productivity:

- Silent updates. Updates are downloaded in the background to keep your system up to date and patched.

1.5 Security & Privacy:

- No identifying information: At purchase and set up (email, phone number, credit card).
- Full disk encryption. During installation, the entire media (drive, USB key, SD card) is encrypted.

1.6 Price and value:

- Cost-effectiveness: For large user base, afordable monthly fee or one-off license fee. If you have 15 people in your team, your organisation can reasonably afford the monthly fee.
- Anonymous payment: Can pay using anonymous cryptocurrency (Monero).

CHECKLIST · 7 May 2021

Benchmark Features: Hardware

In order to benchmark hardware, not overlook some features and have consistency across our articles, we designed a list of features to review.

1.1 Code & developers:

- Code: Open source or audited by trusted third party.
- License: FOSS (Free Open Source Software), or Freemium.
- Liveliness: Actively maintained: App is regularly updated.
- Support: Emergency support by the provider. The team is answering to support requests from users.
- Open source firmwares.

1.2 Package:

- Platforms: Multi-platform, Windows, Linux, MacOS, Android, iOS, Ubuntu Touch etc.
- App stores: Available from alternative repositories: APKpure, F-Droid, Github, team's website etc. That way user doesn't have to use a Google or Microsoft account.
- Apk Signature: Signature key provided on website to check that APK downloaded has not be tampered with.
- Digitally signed with Microsoft: So as not to trigger a warning from Windows SmartScreen.

1.3 Usability:

- Intuitive: Adoption from the team is easy even for non geeks, from installation to using all most features.
- Same features: On all types of operating systems: For example features available on the Android is the same as with iOS which is the same as on Windows which is also available on Linux.
- Administration of users: Example for a communication app: Administrator can Invite, remove, block, mute, define moderators. Example for a website or blog: Not just one single admin access that has to be shared (like Medium), but can create editor's access to the team (like WordPress, Steemit).

1.4 Productivity:

- Battery: Easy to remove battery.

1.5 Security & Privacy:

- No identifying information: At purchase and set up (email, phone number, credit card).
- No permission request for device access: Doesn't access device's data at installation. Doesn't scavenge on your contacts and media files.

- Resistance to state-sponsored criminals: Police, prosecutors etc. Their crimes are “legal” since they’ve corrupted state institutions. They are the most dangerous sort of criminals, to an individual or to a country. If they’ve done something illegal, they can cover it up any ways they like. They can intercept and read IMAP, POP3, TLS, SSL. They can spoof your email provider SSL certificate. They can have access to your SMS, emails, meaning a recovery option is often an easy attack possibility for them.
- Not in a 5 eyes country: Whether for the servers used or the team/company developing the app: Australia, Canada, New Zealand, United Kingdom, United States.
- Hard switches for microphone, camera, GPS.
- Easily removable battery.

1.6 Price and value:

- Cost-effectiveness: For large user base, afordable monthly fee or one-off license fee. Example for a communication app: If you have 15 people in your team, your organisation can reasonably afford the monthly fee.
- Anonymous payment: Can pay using anonymous cryptocurrency (Monero).

Colophon

Ubinodes — The Anthology. Selected articles published 2015–2024 and collected in this edition in 2026. Ubinodes is an international marketing network helping businesses reach new markets worldwide. Find us at ubinodes.org.