UBINODES

RESEARCH:

GET RID OF YOUR EMAILS

Research: 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 greatly enhanced global business efficiency by enabling streamlined communication and instant sharing of files and information. However, this convenience comes with significant risks.

For those with malicious intent—such as 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 cyber security 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 new practices, the rise in online communication and the evolving sophistication of hackers amplify the risks for companies.

2. The Financial Cost of Emailing

A security breach through email can result in significant financial losses for businesses, potentially costing millions of dollars in liability and lost revenue. In 2016, the average total cost of a security breach was 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. According to Avatier's timeline of 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 sent 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, making them vulnerable to unethical interception. In today's digital environment, where email plays a crucial role in both business and personal life, it has become outdated in providing the necessary security. For more insights, refer to our article on Data Privacy in the 21st century.

3. 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.

4. 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 use social engineering to 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 get rid of 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. Additionally, creating aliases can further enhance security by providing an extra layer of protection.

5. Use aliases to compartment

Spy services collaborate in sharing data, using email addresses and phone numbers to interconnect profiles. If an individual consistently uses the same email across various platforms, especially with Prism program participants, they may find themselves trapped in an internet bubble. In this bubble, their searches lead to targeted advertisements, guiding them towards specific items or topics.

In the event of a database breach, the compromised email usually appears first on the Darknet before becoming visible on the Clearnet. Hackers then exploit these exposed emails to attempt to gain access to associated mailboxes. By using distinct aliases for each registration and separate emails for various functions, only one email becomes compromised if a database is breached in such a scenario.

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 feasible when utilizing one alias per website.

For general communications, consider creating an alias for each calendar year. Start fresh annually by 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. For budget-friendly guidance, consult our article on Tutanota vs Protonmail.

For users that prioritize security, take a look at 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 that claim encryption, even Swiss-based Threema ensures that server operators lack access to read your messages.

If privacy is important and you need assurances against data sharing with third parties, these apps are the best choice. Download one today and be rest assured that your information is securely encrypted.