UBINODES

RESEARCH: SIM, BACKDOORS AND SECURITY.

Research: 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 these companies; this article is based solely 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.

2. 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.

3. How your SIM can also be compromised

1. 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).
2. 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.
3. A cloned SIM can exploit your data plan, escalating your plan costs and using it illicitly for other purposes.
4. The text message SIM concern, exposed in 2013, persists; avoid responding to text messages from users claiming to be your service provider.
5. 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).
6. 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.
7. 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).

4. 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. Cell phones, 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.

5. 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.