IranUnchained Opsec Guide v1
11/5/2023

Use of Anonymous SIM Cards

One of the biggest threats in online activities is the possibility of revealing the true identity behind an anonymous one. Individuals who may take precautions in their online activities often make mistakes in the security of their personal information, leading to the exposure of their true identity and compromising their physical security. One of the most important aspects of information security in this context is the security of the phone number you use.

Security of Internal SIM Cards

According to information obtained from an internal telecommunications company guideline, almost any information you can imagine can be extracted from the mobile phones using internal SIM cards within the country. This ranges from hardware information to geographical location and the ability to throttle internet speed. Therefore, using a physical SIM card for any sensitive activity is associated with risks, and ideally, the device with a SIM card should be completely separate from the device containing sensitive information.

Additionally, refrain from registering in applications using your phone number, as telecommunications companies have the capability to receive links to change passwords and access all associated user accounts.

2FA (Two-Factor Authentication)

For maximum security, enable Two-Factor Authentication (2FA) for all your sensitive user accounts. Use authentication applications like Google Authenticator, rather than using your phone number. SMS messages received on your phone can be read by others, but dedicated Authenticator software stores the second password on your device.

In general, avoid using your SIM card number for any user account, even for backup emails, as the security of your email account, even if strong, can be compromised if it's linked to an insecure phone number.

Using Secure Software

Never use software that operates without a VPN or proxy, as these programs are distributed by intelligence agencies to steal user information. One of the most well-known examples is the "Telegram Gold" app. On the other hand, Signal is one of the safest methods for communication, and Telegram is also a good choice due to its popularity and higher security, as it offers features like Secret Chat and Self-Destruct. However, keep in mind that if the phone

number used for registration is not secure, the account is not safe. For Iranian users, an ideal secure communication method is to create a Telegram account with a virtual number, set a password, and enable Two-Factor Authentication (2FA). Another popular messaging app is WhatsApp, but it is not recommended for sensitive communications due to its structure and lack of respect for personal privacy. Therefore, restrict its use to regular conversations.

The Importance of Separation

As mentioned earlier, since different user accounts can be pathways to other accounts, it's better to use multiple email accounts for different purposes. Do not store information from different accounts, such as passwords, in any of them, and avoid using insecure backups. In this regard, refrain from using a single password for multiple accounts and opt for complex passwords.

Hardware Separation

Keep devices that contain sensitive information separate from your daily devices as much as possible. Mobile phones with SIM cards can be tracked in many ways.

Given this issue, and the fact that purchasing a separate device for sensitive activities is not feasible for most people, a more tangible solution is to create a separate account on personal computers, separate from mobile phones and with no tracking capabilities for SIM card devices.

Paid services for receiving virtual numbers with the ability to purchase using virtual currencies:

Telnum.net
Moremins.com
Virtnum.com