PHISH X

SECURITY ON MOBILE DEVICES

Good app is original

The applications also bring updates and improvements, such as new photo filters or features, and can be updated automatically or by entering the official Apple App Store or Google Play store. How about doing it a few times a month? Applications with no initial cost are usually supported by advertisements and / or the sale of personal information to third parties, such as consumer and search profiles.
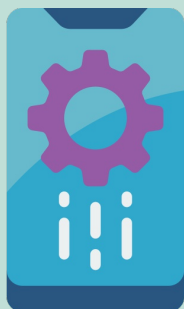
Update often

Your phone must always have the most up-to-date versions of the operating system, such as IOS or Android, in addition to periodic security updates that are released by the device manufacturer a few times a year. While it is more common for older Apple devices to allow recent updates, initiatives by manufacturers on newer models or programs like Android One, which guarantee updates for at least 2 to 3 years, should be prioritized.

Copies, many copies

One of the easiest recommendations is to keep backup copies of your phone data, such as contacts, conversations, photos, and applications. For this you will usually have 3 copies: on the device itself, on your computer and somewhere else, like the cloud.
There are several services from Apple itself (iCloud), Google (Drive) and third parties that allow you to keep the entire photo history of the last trips and the whole family.

phishx.io

PHISHX

SECURITY ON MOBILE DEVICES

Passwords, many passwords

Yes, we can easily access it with biometrics, but we will still need many passwords. In fact, it is recommended to have at least one different password for each access to applications and systems.

To manage these passwords and various places, there are applications on your phone or computer that store and fill them in securely. It is worth it, at least remember that. Look for a Password Manager indication for your device right now.

2 is even safer

How about reducing the risk of incidents, loss of money and keeping your privacy online? Everything is easier when you enable two essential functions in all applications, including financials, social networks, and games: Two-Step Verification and Multiple Factor Authentication.
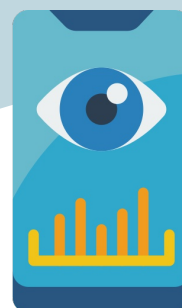
Two-Step Verification ensures that registering a new application will confirm that the person has physical possession of the device, such as the initial configuration of Telegram.

Multiple Factor Authentication ensures that only you will access the application through biometrics, based on your fingerprint or face on devices that allow this functionality. Even WhatsApp already allows this. What are you waiting for?

Your internet protects you

I know it helps to use that Wi-Fi in the cafeteria, it is free and sometimes you just need to inform your data. In addition to being able to chat later about your privacy, your data, even if a simple check-in worth money.

It is always recommended to choose to use the Internet from your device, via the cellular network, when doing something important, such as accessing your bank, purchases or company email. In addition, you can also use an extra layer of protection through your company's or private VPN (private network).

phishx.io