

YOUR PHONE IS YOUR LIFE: 10 ESSENTIAL PROTECTIONS

Photos, accounts, banking, messages: everything lives on your phone. These ten measures cover theft, loss, malicious apps, and scams.

01 Lock code + auto-lock

Make sure it can only be used with your code or password, and locks itself when you stop using it.

02 Data encryption

Enable encryption for internal storage and for external memory cards.

03 PIN on the SIM card

Without a PIN, your line can be used in another device to receive your verification codes.

04 Remote tracking and wipe

Software that can locate the device and, if needed, lock it and erase its data remotely.

05 Apps from official stores only

They passed vetting by the company and the community. Outside of them, malware territory.

06 Reviews, downloads, and permissions

Check ratings and download counts before installing. If the permissions are excessive, stop: ask someone with experience.

07 Updates current

An up-to-date operating system and apps close known vulnerabilities.

08 Safe charging

Don't charge just anywhere. On public USB ports use protection and charge-only mode, with no data syncing.

09 Discreet screen

A privacy filter against prying eyes and limited notifications while the device is locked.

10 Backups + cleanup

Back up regularly. Move sensitive content to your computer and delete it from the phone.

>> BONUS: TEXT MESSAGE SCAMS



Smishing

The same phishing tricks arrive by SMS and messaging apps: prizes, "problems with your account," package deliveries. Apply the same protocol: doubt, don't click, verify through the official channel.

IF IT'S LOST OR STOLEN

With items 1-4 enabled, your information stays **protected** even when the device is out of your hands.