SECURING MOBILE DEVICES

LOCK IT UP!

Secure your device with a strong passcode, pattern, or pin, just like you would a computer.

ENABLE REMOTE ACCESS

Most manufacturers offer a service that allows you to connect to your device from your computer in order to locate it, or remotely reset it to factory default.

USE A VPN WHEN ON PUBLIC WIFI

VPNs (Virtual Private Networks) encrypt your connection and are a must-have for mobile security.

INSTALL ANTIVIRUS AND ANTI-MALWARE SOFTWARE

Never forget that mobile devices are just as likely to get infected as computers, if not more so!

KEEP IT CURRENT

The longer you go without updating, the more risk you assume. Enable auto-update to get the latest and greatest versions of software and firmware.

TURN OFF BLUETOOTH

Bluetooth is unsecure and leaves you open to snooping. When not in use, turn it off.

DISABLE AUTO-CONNECT

Cybercriminals set up rogue access points that spoof your previous wi-fi connections, which allows them to seize your personal information. Eliminate this concern by eliminating auto-connect.

VERIFY THE SOURCE

App stores are full of imposters and malicious applications. Double-check the source and read a few reviews before installing.

THINK BEFORE YOU CLICK

Smishing, or phishing via SMS, has been around for a long time. Don't click on any links sent to you randomly by text message.

KEEP IT BACKED UP

In addition to manually backing up, there are a bunch of cloud options available at various price-points. If your device is lost or stops functioning, you'll still have your data!

SAC the security awareness™ COMPANY