

Going Mobile: How to be Safer When Using a Smartphone or Tablet

Everywhere you look, people are using smartphones and tablets as portable, hand-held computers. "Unfortunately, cybercriminals are also interested in using or accessing these devices to steal information or commit other crimes," said Michael Benardo, manager of the FDIC's Cyber Fraud and Financial Crimes Section. "That makes it essential for users of mobile devices to take measures to secure them, just as they would a desktop computer."

Here are some basic steps you can take to secure your mobile devices:

Avoid apps that may contain malware. Buy or download from well-known app stores, such as those established by your phone manufacturer or cellular service provider. Consult your financial institution's website to confirm where to download its official app for mobile banking.

Keep your device's operating system and apps updated. Consider opting for automatic updates because doing so will ensure that you have the latest fixes for any security weaknesses the manufacturer discovers. "Cybercriminals try to take advantage of known flaws, so keeping your software up to date will help reduce your vulnerability to foul play," said Robert Brown, a senior ombudsman specialist at the FDIC.

Consider using mobile security software and apps to protect your device. For example, anti-malware software for smartphones and tablets can be purchased from a reputable vendor.

Use a password or other security feature to restrict access in case your device is lost or stolen. Activate the "time out" or "auto lock" feature that secures your mobile device when it is left unused for a certain number of minutes. Set that security feature to start after a relatively brief period of inactivity. Doing so reduces the likelihood that a thief will be able to use your phone or tablet.

Back up data on your smartphone or tablet. This is good to do in case your device is lost, stolen or just stops working one day. Data can easily be backed up to a computer or to a back-up service, which may be offered by your mobile carrier.

Have the ability to remotely remove data from your device if it is lost or stolen. A "remote wipe" protects data from prying eyes. If the device has been backed up, the information can be restored on a replacement device or the original (if you get it back). A number of reputable apps can enable remote wiping.

To learn more about safely using smartphones and tablets, see the Federal Trade Commission's Computer Security Web page at www.consumer.ftc.gov/topics/online-security.