

Smartphones

Here are some steps you can take to safeguard your online activities and minimize the chance you will be affected by Internet fraud.

- ◆ When purchasing a smartphone, learn the features of the device, including the default settings. Turn off features of the device not needed to reduce risk (such as Bluetooth).
- ◆ Depending on the type of phone, the operating system may have native encryption or a third-party application available. Encryption should be enabled to protect your personal data in the case of loss or theft
- ◆ Passcode protect your mobile device. This is the first layer of physical security for the contents of the device. In conjunction with the passcode, enable the screen lock feature so it automatically locks after a period of inactivity. Most phones also have a setting to allow an emergency call without providing the passcode.
- ◆ Do not jailbreak or root your smartphone to remove certain restrictions imposed by the device manufacturer or cellular carrier. Doing this allows nearly unregulated controls of what programs can be installed and how the device can be used. However, this procedure often involves exploiting significant security vulnerabilities and increases the risk of your device being hacked.
- ◆ When you access a WiFi network that is open to the public, your device can be an easy target of criminals. Only use a network you trust.
- ◆ Obtain malware protection for your mobile device. Look for applications that specialize in antivirus or file integrity that help protect your device from malicious applications. Criminals are developing information-stealing malware that target smartphones.
- ◆ Avoid clicking on webpage or application advertisements. Ads are often a source of malicious software.
- ◆ Read the reviews of the application and developer/company who published an application before installing it. Malicious applications do get published in online stores, so only use software you trust.
- ◆ Review and understand the permissions you are giving to applications you download. The permissions should make sense for the type of application you are going to install.
- ◆ Be aware of applications that enable geo-location (GPS). These applications can track your location anywhere. The application can be used for marketing, but can also be used by criminals, raising the risk of assisting a possible stalker and/or burglary.
- ◆ Accept updates to your smartphone's software when prompted by your service or application provider. Remove applications you no longer need.
- ◆ Be sure to have a backup of your contacts and other information on your phone.
- ◆ Be aware of warning signs that may indicate your device is under attack. These include the smartphone battery being warm even when the phone has not been used, the device lights up at unexpected times, unexpected beeps or clicks during conversations, etc. If these happen, be alert and have your cellular carrier check your device.
- ◆ If you decide to sell your device or trade it in, make sure you wipe the device (reset it to factory default) to avoid leaving personal data on the device.

If you have been a victim of an Internet scam or have received an e-mail that you believe was an attempted scan, please file a complaint at <http://www.IC3.gov>.



Want to learn more about information security for your personal banking transactions? Visit firstmidwest.com/safe for the most current resources on a wide array of information security topics.