



Scams Targeting Smartphones and Tablets

From the Office of Minnesota Attorney General Lori Swanson

Studies show the majority of American adults have a smartphone or tablet—and this number is predicted to rise. People use these devices for everything from sending and receiving text messages and emails, to surfing the Internet, listening to music, and downloading “apps.” While these functions can keep people connected, they can also make folks vulnerable to scams.

Scams that target smartphones and tablets take advantage of the connectivity and convenience these devices offer. Here are a few to watch out for:

Email and Text Message Phishing Scams

Phishing scams use deceptive emails and text messages to lure consumers into providing their personal or financial information. To add legitimacy to their phony claims, scam artists often impersonate banks, government agencies, or other organizations. Phishing messages typically ask consumers to provide usernames and passwords, credit and debit card numbers, PINs, or other sensitive information that scam artists can use to commit fraud.

In addition, “clicking” on a link or opening an attachment can install spyware on your device that may send information from your phone to others without your consent or knowledge. While some spyware merely tracks your web surfing habits in hopes of learning your product preferences for marketing purposes, spyware can also be used by fraudsters to steal personal and financial information. Tech-savvy fraudsters also use “key loggers,” system monitors and trojans to capture keystrokes or pictures of your device’s screen in the hope of snagging passwords, account numbers, Social Security numbers, or other sensitive information.

Be wary of any email or text message from someone you don’t know. If you receive a scam phishing message on your device, resist the urge to “click” open the link or phone number to call back. Phishing emails can be reported directly to your email provider, or can be forwarded to the Federal Trade Commission at

spam@uce.gov. You may also report phishing text messages to short code 7726 (which spells “SPAM” on your keypad). Doing so allows service providers to identify the senders of such messages and take steps to limit messages from them going forward.

Look-alike Apps

Cybercriminals are now creating applications—or “apps”—that look and might even function like legitimate apps, but are actually malware designed to steal your personal and financial information, send text messages without your knowledge, or even track your location using your phone’s GPS capabilities. Because it operates in the background of a device’s operating system, malware may go undetected. The criminals that create look-alike malware apps use the information they receive to commit the crimes of theft and identity theft.

You can take steps to ensure the legitimacy of the apps on your smartphone or tablet by only buying or downloading apps from trusted sources. You can also check the Terms of Use or Privacy Policy to learn what information an app will access and how that information will be shared. If you have concerns about an app, delete it from your device and report it to your service provider or the app store from which you purchased it.

High-tech Scams

In a tech support scam, a person receives a call from someone who claims to be a “tech support specialist” with a well-known company. The caller says that your device has been infected by a malicious virus or spyware. He may use scare tactics, claiming that your device will crash or the information on it will be at risk if you don’t immediately fix the problem. The caller says he can correct the problem for a fee if you allow him to remotely install anti-virus software, usually by going to a website to which he sends you. If you let the caller remotely access your device, he may install malware or spyware to steal your personal and financial information.

A similar scam is the “ransomware” scam in which an app or website installs malicious software that causes the app or your device to stop working. You then receive a message telling you that your device has been infected with a virus or malware. The message generally provides a telephone number to call to fix the problem. If you call the number, the scammer will ask you to pay money or download software to repair the problem.

Smartphone and tablet users should be careful about the websites they visit and suspicious calls and text messages. If you have any trouble with your device, contact your service provider directly, using a trusted telephone number, like the one printed on your bill. High-tech scammers often create bogus websites to trick device users into believing they are associated with a service provider—when they are not.

Smartphone and Tablet Security Tips

To prevent a scam targeting your device, consider the following tips:

Set up a password or passcode for your device, and use it.

- Use security software that is appropriate for your operating system and keep it updated.
- Install apps only from trusted sources.
- Customize data encryption, GPS, network connection, and information-sharing settings.
- Be cautious about the information you share and the types of apps you access.
- Contact your cell phone company about remote wiping and tracking. If your device is lost or stolen, these features may provide some protection.
- If your device is lost or stolen, report it.
- Before you upgrade, donate, or recycle your device, make sure you delete all of your personal and financial information.

Additional Resources

You can learn more about device scams and security by talking with your service provider or by exploring the U.S. Department of Homeland Security’s website at www.dhs.gov/stopthinkconnect.

File a complaint with the Federal Trade Commission (FTC) and Federal Communications Commission (FCC). These agencies enforce the laws regarding scam calls and text messages. You may contact the FTC and FCC as follows:

Federal Trade Commission

Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
Toll free helpline: 1-877-382-4357
www.ftccomplaintassistant.gov

Federal Communications Commission

445 12th Street SW
Washington, DC 20554
Toll free: 1-888-225-5322
www.fcc.gov/complaints

For more information on consumer issues, contact the Office of Minnesota Attorney General Lori Swanson as follows:

Office of Minnesota Attorney General Lori Swanson

445 Minnesota Street, Suite 1400
St. Paul, MN 55101
651-296-3353 or 800-657-3787
TTY: 651-297-7206 or 800-366-4812
www.ag.state.mn.us