TLP:WHITE

Security Tip (ST05-017)

Cybersecurity for Electronic Devices

Original release date: December 19, 2011 | Last revised: June 08, 2017

Why does cybersecurity extend beyond computers?

When you think about cybersecurity, remember that electronics such as smartphones and other Internet-enabled devices may also be vulnerable to attack. Take appropriate precautions to limit your risk.

Actually, the issue is not that cybersecurity extends beyond computers; it is that computers extend beyond traditional laptops and desktops. Many electronic devices are computers—from cell phones and tablets to video games and car navigation systems. While computers provide increased features and functionality, they also introduce new risks. Attackers may be able to take advantage of these technological advancements to target devices previously considered "safe." For example, an attacker may be able to infect your cell phone with a virus, steal your phone or wireless service, or access the data on your device. Not only do these activities have implications for your personal information, but they could also have serious consequences if you store corporate information on the device.

What types of electronics are vulnerable?

Any piece of electronic equipment that uses some kind of computerized component is vulnerable to software imperfections and vulnerabilities. The risks increase if the device is connected to the Internet or a network that an attacker may be able to access. Remember that a wireless connection also introduces these risks. (See Securing Wireless Networks for more information.) The outside connection provides a way for an attacker to send information to or extract information from your device.

How can you protect yourself?

- **Remember physical security** – Having physical access to a device makes it easier for an attacker to extract or corrupt information. Do not leave your device unattended in public or easily accessible areas. (See Protecting Portable Devices: Physical Security.)
- **Keep software up to date** – If the vendor releases updates for the software operating your device, install them as soon as possible. Installing them will prevent attackers from being able to take advantage of known problems or vulnerabilities. (See Understanding Patches.)
- **Use good passwords** – Choose devices that allow you to protect your information with passwords. Select passwords that will be difficult for thieves to guess, and use different passwords for different programs and devices. (See Choosing and Protecting Passwords.) Do not choose options that allow your computer to remember your passwords.
- **Disable remote connectivity** – Some mobile devices are equipped with wireless technologies, such as Bluetooth, that can be used to connect to other devices or computers. You should disable these features when they are not in use. (See Understanding Bluetooth Technology.)

- **Encrypt files** – If you are storing personal or corporate information, see if your device offers the option to encrypt the files. By encrypting files, you ensure that unauthorized people can't view data even if they can physically access it. When you use encryption, it is important to remember your passwords and passphrases; if you forget or lose them, you may lose your data.
- **Be cautious of public Wi-Fi networks** – Before you connect to any public wireless hotspot—like on an airplane or in an airport, hotel, train/bus station or café:
  - Be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate.
  - Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network.
  - Only use sites that begin with “https://” when online shopping or banking. Using your mobile network connection is generally more secure than using a public wireless network.

Authors

US-CERT Publications and Stop.Think.Connect™
