Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

SECURITY TIPS FOR PERIPHERAL DEVICES

OCTOBER 2020

ITSAP.70.015

Peripheral devices are devices that you connect to and use with a host computer or mobile device. You can use peripherals to enhance the capabilities of a computer or mobile device and improve your user experience. However, these devices can provide threat actors with another means to compromise your organization's networks, systems, and information.

WHAT ARE PERIPHERALS?

Peripherals include internal and external devices. Internal peripherals are built into a computer or mobile device by the manufacturer (e.g. video and sound cards, internal modems, and hard disk drives). External peripherals are connected either by cable, such as a USB or Thunderbolt cable, or to the host device's port or even wirelessly using Wi-Fi or Bluetooth. Examples of external peripherals include keyboards, cameras, and external hard drives.

To assess the risks introduced by peripherals, your organization should identify the peripherals currently in use or planned for implementation. There are three general categories of peripheral devices:

- An **input peripheral** sends information and instructions to the computer or the mobile device to which it is connected.
- An **output peripheral** receives information and instructions from the computer or the mobile device to which it is connected.
- A **storage peripheral** stores and retains information from a computer or a mobile device.

HOW DO PERIPHERALS PUT ME AT RISK?

Peripherals add convenience and improve your user experience. Threat actors try to exploit peripherals, such as in the example methods below, in the hopes of gaining access to your networks, systems, and sensitive information.

SMART CABLE MANIPULATION

With smart connection cables, such as Lightning and USB-C cables, there are small microcontrollers embedded in the cable. Threat actors can program these microcontrollers, enabling them to attack the device you plug in. There are even commercial cables that contain a wireless hotspot, which can be targeted by threat actors.

FIRMWARE VULNERABILITIES

Threat actors use the device firmware (the software that controls the device hardware) to run rootkits, a type of software that masks itself and hides malware on your device. This type of software enables threat actors to remotely control devices and access things like your network communications or your web cam.

DIRECT MEMORY ACCESS ATTACKS (DMA)

Once a threat actor has compromised device firmware or has physical access to a system, they can carry out DMA attacks to read and overwrite system memory. By overwriting memory, a threat actor can gain control of the system and perform malicious activities.

AWARENESS SERIES

Canada

HOW CAN I USE PERIPHERALS SECURELY?

ASSESS PERIPHERALS

Your supply chain can impact your security. When purchasing peripherals, be sure to choose a reputable vendor that offers peripherals with security integrated. Use caution when gifted peripherals from unknown parties (e.g. a vendor at a conference). These free peripherals may contain malware that is designed to compromise devices that they are plugged into.

VERIFY AND AUTHENTICATE PERIPHERALS

Before you connect peripherals to networks and devices, verify that the listed device you are choosing is the known and trusted device (e.g. the correct printer).

To authenticate and authorize wireless connections, pairing codes and passkeys may be used. Be wary if you receive a pairing or connection request that you haven't initiated. Once connected, devices remain on your list of paired devices. Always remove lost or stolen devices from your paired devices list.

SECURE PHYSICAL DEVICES AND CABLES

Maintain control and custody of your devices, including cables and chargers, to ensure they are not tampered with or switched out for other devices. Label all peripherals with a tamperproof asset label to ensure they can be identified easily and to prevent a threat actor from switching them out with other devices.

Never leave your devices unattended in public places. While it may be second nature to guard your phone or laptop, don't forget to safeguard chargers, cables, and other peripherals.

CHANGE DEFAULT PASSWORDS

Typically, devices come with a default password that is provided by the manufacturer. Be sure to change default passwords, including administrator passwords.

You should use a unique and complex passphrase or password for each peripheral. If using a passphrase, ensure it consists of at least 4 words and is a minimum of 15 characters long.

PATCH AND UPDATE DEVICES

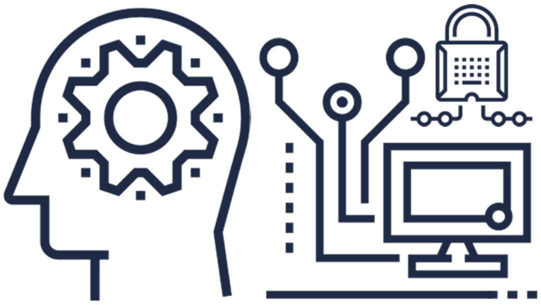
You may know the importance of updating your computer and mobile device operating systems and applications, but don't forget about peripherals. Ensure that you update, debug, and patch firmware regularly to ensure your devices are as secure as possible.

WHAT ELSE SHOULD I CONSIDER?

Before using peripheral devices, assess them against your business and security requirements to determine the associated risks and implement the appropriate safeguards. Your organization should also establish clear policies around the use of peripheral devices.

You can further protect your organization by taking the following actions:

- Be wary when connecting to untrusted peripherals if you're visiting a third-party facility (e.g. HDMI cables, USB dongles). Pay attention to any warnings or permissions requests from these peripherals.
- Log off and shut down devices when not in use.
- Turn off automatic connection capabilities to ensure that your devices do not automatically pair with unknown devices or connect to unsecure networks.
- Connect peripheral devices to a guest network rather than your main internal network.
- Sanitize peripherals to remove sensitive information before disposing of them.
- Train your employees on the acceptable use of peripherals.



LEARN MORE

If you're looking for more cyber security tips on how to protect your devices, your information, and yourself, visit the Cyber Centre website (cyber.gc.ca). To get you started, check out the following publications:

- *ITSAP.00.011 Using Bluetooth Technology*
- *ITSAP.00.012 Internet of Things Security for Small and Medium Organizations*
- *ITSAP.10.116 Cyber Security Tips for Remote Work*
- *ITSAP.00.70 Supply Chain Security for Small and Medium- Sized Organizations*
- *ITSAP.30.032 Best Practices for Passphrases and Passwords*