Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CANADIAN CENTRE FOR CYBER SECURITY

Security tips for peripheral devices

May 2024

ITSAP.70.015

Peripherals are devices that can be connected to and used with a host computer or mobile device to enhance capabilities and improve your user experience. Despite the benefits, these devices can also provide threat actors with another means to compromise your organization's networks, systems, and information.

Peripherals and types of uses

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

To assess the risks introduced by peripherals, your organization should identify the devices currently in use or planned for implementation into one of the following 3 categories:

- 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.

Knowing the types of peripherals and the flow of information can help you choose and prioritize security controls. These security controls can enhance the protection of your

Risks of using peripherals

Threat actors can exploit peripherals in the hopes of gaining access to your networks, systems, and sensitive information. The following 3 examples show how peripherals may be exploited for malicious activity.

Smart cable manipulation

With smart connection cables, such as Lightning and Thunderbolt 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

Direct memory Access (DMA) attacks allow hardware devices to communicate directly with a device's system memory (RAM). 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.

Cat. No. D97-1/70-015-2024E-PDF
ISBN 978-0-660-70986-4

Canada

How to use your peripherals securely

Review the following to help assess the use of peripherals.

Assess peripheral vendors

Your supply chain can impact your security. When purchasing peripherals, be sure to choose a reputable vendor that offers peripherals with integrated security. Use caution when gifted peripherals from unknown parties, for example, a vendor at a conference. Free peripherals may contain malware designed to compromise devices that they are connected to.

Assess the need for each peripheral

You can reduce the risks of peripheral devices by reducing the number of peripherals you use. Assess the security risks posed by each peripheral being used. When possible, only use peripherals that are necessary or improve user experience.

Verify and authenticate peripherals

Before you connect peripherals to networks and devices, verify that the listed device you are choosing is a known and trusted device. Be sure to confirm whether the peripheral is obsolete by checking if it is still supported by vendor, or has reached its end-of -life. You should replace obsolete products to limit vulnerabilities.

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 until they are manually removed. 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 tamper-proof asset label. Labelling will ensure the peripherals can be identified easily and will prevent a threat actor from switching them out with other devices.

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 to consider when using peripherals

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

- Using Bluetooth technology (ITSAP.00.011)
- Internet of Things (IoT) security (ITSAP.00.012)
- Cyber security tips for remote work (ITSAP.10.116)
- Supply chain security for small and medium– sized organizations (ITSAP.00.70)
- Best practices for passphrases and passwords (ITSAP.30.032)
- Obsolete products (ITSAP.00.095)