Security Practices for Removable Media and Devices

Portable hardware such as removable media are often relied on for storing secondary copies of sensitive data. They include everything from USB and SD cards to CF and external hard drives. Their portability, ease of use, and increasing capacities make them incredibly convenient for transporting files, including documents, software, videos, and even trade secrets.

However, even though they are useful, removable devices can serve as gateways to security problems. They may covertly harbor infected codes that deploy as soon as the device is attached to a computer. While it’s an excellent strategy to avoid using removable media altogether, it's probably better to learn how to safely use them.

Keep reading to learn more about the risks of using removable devices and essential security practices that mitigate the risk of using removable media.

Protect Your Computer with Endpoint Protection Software

Removable media have a long history of acting as entry points for malicious codes and as a popular attack vector to infect computers. Given how easy it is to infect computers with removable devices, you should consider installing endpoint protection software to detect and block malicious code from USB devices.

It is also important to only use removable media that belong to you. If you plan on connecting USB devices from friends and family, perhaps consider enabling read-only settings to block data transfers. You should still be able to read files.

Use Device Control Software to Protect Sensitive Data

You can use device control software to only allow authorized encrypted removable media to connect with your computer. These could be devices that you or your co-workers own.

Device control software can detect and control data transfers from USB's and other removable devices. It can also prevent insider threats and accidental data leakage that may happen because of removable devices.

You can also use this software to prevent the unauthorized transfer of sensitive data from your personal computer to infected USB devices. The software can block unauthorized devices from connecting to various endpoints on your computer. It also ensures that any sensitive data is not copied to untrusted removable devices.

Some device control solutions also come with advanced features such as granular control, transfer limits, and temporary passwords. They may also provide encryption to prevent data theft.

Set up Sandbox Environments to Test Removable Media

If you must use untrusted removable media, consider testing it in a sandbox environment. You can use an isolated virtual machine to set up a sandbox environment that can test third party removal media for malicious codes and malware.

A common social engineering tactic is for attackers to leave USB devices lying out in open, public places. They are relying on people who are curious enough to plug the device into their computer.

Hackers might also run a BadUSB attack on your computer. BadUSB exploits vulnerabilities in USB firmware by reprogramming the device and causing it to act as an interface device. It can run a series of automated keystrokes to install malicious software or deploy ransomware to your network.

If you see a USB device lying around, do not plug it into your computer.

Test it in a safe, isolated sandbox environment if you insist on using the USB device. While this method is not foolproof, it is a more secure option than just plugging an unknown device into your computer.

VirtualBox is a user-friendly software that lets you set up sandbox environments within virtual machines with relative ease.

For more information on creating sandbox environments to safely test USB devices, contact our cybersecurity consultants at Microsys Inc.

Don't Use the Same Flash Drives on Home and Work Computers

It is tempting to use the same flash drives on your home and work computers. However, doing so you run the risk of cross-contaminating your computers. This can be devastating to your employer networks and may also harm your own computer.

Install and Update Antivirus Software

Last but not least is the use of antivirus software. Antivirus software can detect, quarantine, and delete malicious code on USB devices before they have a chance of infecting networks. The antivirus software should work alongside endpoint protection tools and device control software.

The antivirus software should be allowed to update itself automatically. Ideally, the antivirus software should have tools for enforcing authorized removable media and devices. They must also provide alerts when USB devices are connected to endpoints.

Keep all Software on Your Computer Up to Date

Updating all software on your computer is the easiest security measure you can take to protect your computer and devices.

To prevent infected USB devices from exploiting your computer, all installed software should be kept up to date. Don't skip security patches and updates released by software developers. These patches are designed to close security loopholes that can be used to gain access to your computer.

If the software has reached the end of its life and no longer receives security patches from the developers, consider finding an alternative. For example, Windows 8 and 8.1 will reach the end of support in 2023.

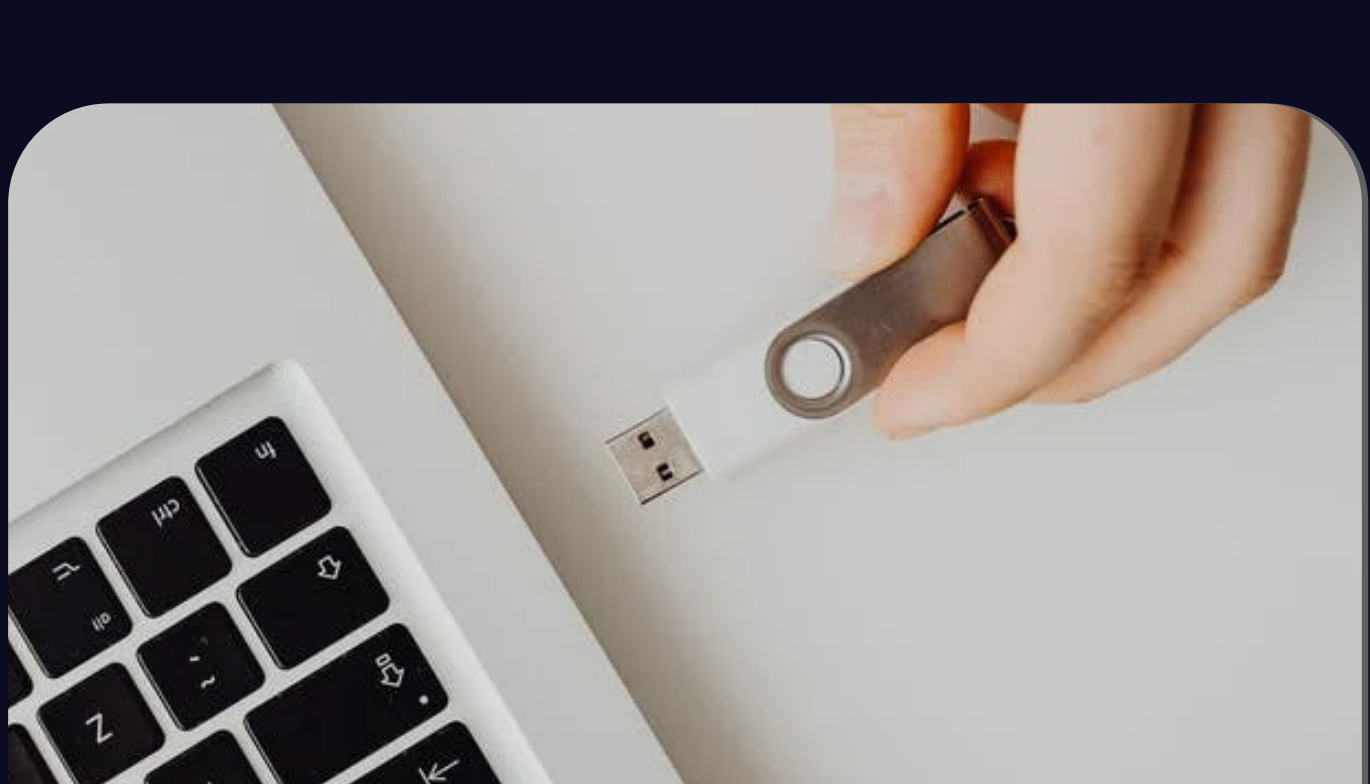
The following types of software should be updated on a priority basis:

Operating system: Most operating systems come with automatic updates but the feature may need to be enabled. Don't disable automatic updates and delay OS updates for a later date because you may forget to manually apply new patches.

Web Browsers: Web browsers are complex pieces of software with all manner of vulnerabilities that hackers can exploit. After all, web browsers are your gateway to the internet. Consider enabling automatic updates on your web browsers.

There's no Avoiding Removable Devices

While you might want to restrict the use of removable devices, doing so may be impractical. This is why it is useful to utilize Endpoint security software to implement a safer approach to removable devices, as discussed earlier.



Wrapping Up

After reading this newsletter, we hope you understand why it is crucial to develop security practices for removable media and devices, especially if you don’t control or trust these devices. To discuss your cybersecurity needs further, or for any other type of help, don't hesitate to get in touch with Microsys Inc.

Get in touch with Microsys Inc.