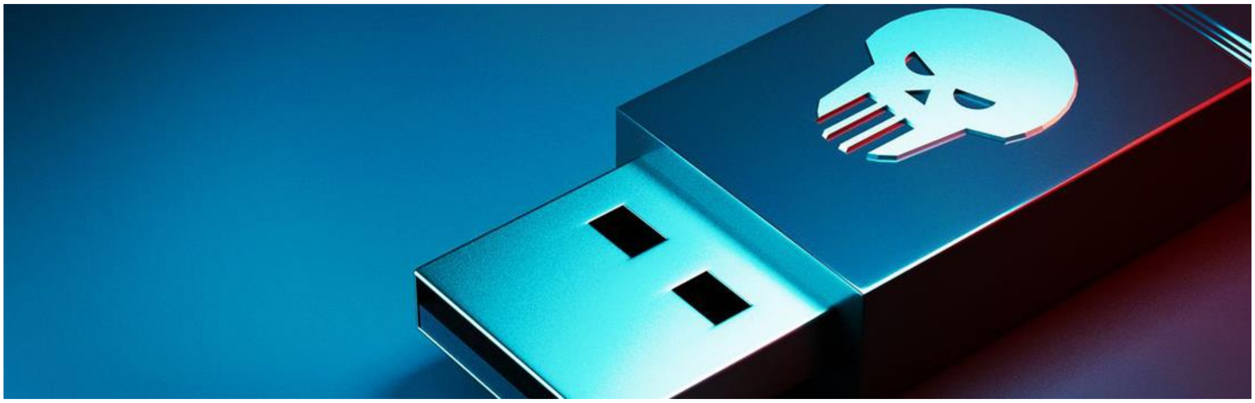
What’s Plugged In?

“Would You Like to Trust This Device?”

Time: 5 minutes (3m25s for reading time + 1m for the quiz? = ~5 minutes)

Points:



Universal serial bus (USB) devices are some of the most frequently used pieces of technology across the globe. Mice, webcams or even phone chargers — just look around you, and there is likely a USB device nearby.

Developed in the 1990s, the USB was made to connect various devices together. One of the most common examples would be plugging a flash drive (a mobile storage device) into a computer’s USB port. The potential for many uses can come with many potential risks, however. Being aware of the risks that USB devices can pose and how you can protect yourself will allow you to take advantage of USBs to the fullest extent.

What are Infected USBs?

When you think of “USB," the first thing that comes to mind may be a flash drive. What about other USB devices like keyboards or webcams? While cybercriminals typically target flash drives, an infected USB device can take on multiple forms.

Infected Flash Drives

Compact in size, flash drives can be commonly found in the office, classroom and day-to-day life. But when a flash drive is infected, it can trick your computer into thinking it’s something that it’s not.

Once an infected flash drive is plugged in, the flash drive can operate like:

- a keyboard, typing like a keyboard on a computer

- a keylogger, saving what's typed on the keyboard (like usernames and passwords)
- a charging cable, overheating/frying equipment
- a camera, recording your webcam or screen

Even though an infected flash drive's content is initially limited to what is pre-loaded onto it, the ability to have a flash drive work like a keyboard can be enough for cybercriminals to create backdoors. A backdoor is a way for cybercriminals to access and steal your information on your computer, tablet or cellphone from anywhere, at any time, without you being aware of it.

Other Infected USB Devices

Flash drives aren't the only susceptible USB device out there though — any USB device can be infected including mice, microphones and printers. While an infected USB device looks normal on the outside, it comes loaded with harmful content capable of infecting your computer, tablet or cellphone.

Like infected flash drives, once an infected USB device is plugged in, it can install viruses, delete content (files on a computer, numbers on cellphone, photos off a tablet), track what's typed on the keyboard (like passwords and payment information) or even create backdoors as mentioned above.

Staying Safe

While all of this information can be concerning, there's good news: by simply avoiding unknown and untrusted USB devices, you can avoid most infected USBs.

A 2016 study revealed that people are very likely to pick up and open an unknown flash drive. After scattering nearly 300 flash drives, researchers found that 98% of the devices were picked up with 45% of them having at least one file opened by users. While it may seem like common sense to avoid plugging in an unknown USB device, cybercriminals know it's not.

Aside from completely avoiding unknown/untrusted USB devices, there are additional options you can employ to ensure the USB devices in your life are uncompromised.

Write Protect Switch

To ensure that your flash drive and computer remain safe, you can purchase a flash drive that includes a write protect switch. When plugging a flash drive into an unknown computer, it is possible for the unknown computer to infect the flash drive. This can lead to subsequent equipment the flash drive is plugged into, like your own computer, to become infected. When enabled, a write protect switch ensures that the flash drive cannot be altered or infected.

Public Isn't Preferred

When using a phone or computer with sensitive information on it, avoid using publicly available USB cables or ports. Charging a company phone on a public charging station or plugging a company flash drive into a hotel's computer is not recommended. Instead, consider using a personal charging device or your own computer to ensure valuable information is not compromised.

Ultimately…

USB devices are extremely versatile and, well, universal! While there are risks to using these devices, following the recommendations above will ensure that your equipment remains safe and uncompromised.

References:

“Don’t Panic, But All USB Devices Have a Massive Security Problem” How-To Geek. Published: 2/12/2017. Accessed: 8/6/2019.

“Digital Signature” TechTarget. Published: 3/2014. Accessed: 8/6/2019.

“Our cure for BadUSB” Kaspersky Daily. Published: 7/8/2016. Accessed: 8/6/2019.

“The facts about BadUSB” NCC Group. Published: 10/8/2014. Accessed: 8/6/2019.

“This thumbdrive hacks computers. “BadUSB” exploit makes devices turn “evil”” arsTECHNICA. Published: 7/31/2014. Accessed: 8/6/2019.

“Users Really Do Plug in USB Drives They Find” University of Illinois at Urbana-Champaign. Published: 8/16/2016. Accessed: 8/6/2019.

“Weaponized USB devices as an attack vector” Kaspersky Daily. Published: 4/17/2019. Accessed: 8/6/2019.

“WHID Injector: How to Bring HID Attacks to the Next Level” Security Affairs. Published: 5/1/2019. Accessed: 8/6/2019.

Quiz Questions

Q1: Infected flash drives were designed to:

A1: Make your life easier- Quite the opposite, actually. Infected flash drives were designed to trick your computer, tablet or cellphone into thinking it is something that it’s not. And by doing so, the infected flash drive is able to harm your computer.

*A2: Trick your computer or phone into thinking it’s something that it’s not- Correct! Infected flash drives were designed to trick your computer, tablet or cellphone into thinking it is something that it’s not. And by doing so, the infected flash drive is able to harm your computer.

A3: Replace regular flash drives- Hopefully not! Infected flash drives were designed to trick your computer, tablet or cellphone into thinking it is something that it’s not. And by doing so, the infected flash drive is able to harm your computer.

Q2: True or False: Infected Flash Drives are the most frequently found Infected USB device.

*A1: True- Correct! While cybercriminals can modify almost any USB device, they typically target flash drives.

A2: False- This is actually True. While cybercriminals can modify almost any USB device, they typically target flash drives.

Q3: The best way to protect yourself from an Infected USB device is:

A1: Plug the device into any available equipment to check if it has any malicious content- This should never be done. As soon as an infected USB device is plugged into equipment, the device is immediately able to compromise equipment. Avoiding unknown and untrusted USB devices is the best way to avoid the dangers of infected USB devices.

A2: Hope for the best- You can do better than that! Avoiding unknown and untrusted USB devices is considered the best way to avoid any dangers of infected USB devices.

*A3: Avoid using unknown and untrusted USB devices- Correct! While this may not always be feasible, using a USB device with a write protect switch and keeping software and operating systems up to date are safe steps to take in addition to avoiding using unknown and untrusted USB devices.