CYBER SECURITY AWARENESS MONTH

WEEK 2: Cyber from the Break Room to the Board Room

Thumbdrives:

A bring-your-own device that we would rather be left at home!

You've seen them; those fun memory stick give-aways that are handed out and won at conferences and workshops. They come in all colors with unique designs, are sometimes branded with company logos, and often have specific data uploaded to them for the programs being presented. But do you know what's really contained on that thumbdrive? Do you know for sure the computers that USB drive has been plugged into were secure and free of viral threats?

USB drives, or thumbdrives, flash drives, and memory sticks, are reusable storage devices that are small enough to carry in your pocket and are able to store many gigabytes of data. That is a lot of information contained in a very small device, and that is one of the biggest problems – their size. These devices are much more likely to be lost or misplaced than a smart phone or laptop. One study noted that British dry cleaners found approximately 9,000 USB drives in pants pockets. Another survey of taxi cabs in London and New York found that over 12,500 handheld devices, including USB drives, are left behind every 6 months.[1] If the USB device is not password protected or its personal or corporate files not encrypted, the device's owner is vulnerable to identity theft and other types of cyber crime.[1]

Several experiments have been conducted to study human response to found USB devices. One study placed 200 USB drives in high-traffic, public areas in large metropolitan locations in the U.S. and found that one in five people will use the found USB device. The devices were used in a manner that could potentially pose a cyber security threat to personal and professional information by opening files, clicking on unfamiliar links, and sending email messages to listed addresses.[2] Even more disturbing was another study that found an increase in people using found USB drives branded with their company logo or a familiar logo.[3] Many of the experiment subjects claimed they only accessed the USB files to find the owner of the device.

In an article published just this year, a study is described where 297 USB drives were randomly dropped on a college campus with some labeled "Confidential" or "Final Exam Answers" or with return address tags so that the people who found them would not access the files or could locate the owners without opening the files. Still, over 45% of those USB drives were picked up and plugged into a computer. Sixty-eight percent of the accessed USB devices were plugged in with no precautions taken. [4, 5]

If loaded with sophisticated malware or virus, hackers can penetrate some of the world's most sensitive networks.[6] For example, the Stuxnet worm, considered the most sophisticated computer virus ever created, infected Iranian nuclear facilities via a booby-trapped USB drive. With a booby-trapped drive, as soon as the device is plugged in, it can take over a keyboard without the user ever realizing anything is taking place.[7] Hackers attempting to break into networks may install malware on thumbdrives to leave in parking lots nearby their intended targets, hoping that a curious user will pick up the thumbdrive, carry it into the office, and insert it into a company computer. This installs the malicious software and allows hackers to access the network.

So, what responsible methods should you employ when using USB drives? [1,8]

- Protect your data and avoid copying Social Security numbers, credit card numbers, and bank information on a USB drive.
- Use secure devices if you must upload personal information. Encrypt it and use a password.
- Keep personal and business USB drives separate.
- Do not plug an unknown USB drive into your computer.
- Use and maintain security software on your computers.
- Keep USB drives in a safe, secure location.

You should consider whether the use of USB drives is in your best interests. For instance, some companies do not allow corporate data to be stored on USB drives. In these cases, employees that work from home are provided with a company computer that is secured and maintained by the company's own IT department. This is the best way to prevent network intrusions and loss of critical information.[9]

> "WE DON'T KNOW WHERE IT'S BEEN OR WHAT DANGERS IT HOLDS, SO IT'S BEST JUST TO LEAVE IT ALONE."

USB drives are convenient and practical when used with best practices; however, so often these best practices and precautions are ignored without a second thought. We should all look at a found USB drive just as we would a hypodermic needle found out on the street. We don't know where it's been or what dangers it holds, so it's best just to leave it alone.[10]

And, definitely remember to leave yours at home!

RESOURCES

1. http://us.norton.com/yoursecurityresource/detail.jsp?aid=usbdrives
2. https://www.comptia.org/about-us/newsroom/press-releases/2015/10/26/find-a-flash-drive-pick-it-up-experiment-shows-how-lack-of-cybersecurity-knowledge-can-impact-organizations
3. http://www.securitymagazine.com/articles/85768-managing-thumb-drive-security-risks
4. http://www.pcmag.com/news/346755/hey-dummy-drop-that-usb-drive
5. http://www.infosecurity-magazine.com/blogs/bhusa-dropped-usb-experiement/
6. http://idt911.com/education/blog/12-security-best-practices-for-usb-drive
7. https://www.opswat.com/blog/usb-security-three-ways-address-usb-risks
8. https://www.us-cert.gov/ncas/tips/ST08-001
9. http://www.nmscorp.com/2014/09/security-risks-imposed-by-the-use-of-usb-drives/
10. https://www.wired.com/2014/07/usb-security/