State of West Virginia
Cyber Security Tip

Monthly Newsletter

West Virginia Office of Information Security Controls and Compliance

Five Security Myths Debunked

Common Cyber Security Myths

While the Internet has given us the ability to find the answer to almost any question, cybersecurity is a realm where a growing variety of threats are perpetrated by a growing number of malicious actors, creating understandable uncertainty about how to protect ourselves while connected . A small sample of the common myths that need to be debunked are examined in this Newsletter.

Myth #1: No one wants to hack me! I don't have anything worth stealing!
What many people are unaware of is that most of the most common and effective cyber threats are Internet-wide Pfishing exploits generated by automated computer robots ("bot nets"), looking for unsavvy users on vulnerable computers and networks to "own," and from which to steal credentials and identity data. Contrary to what many think, the criminals behind the bot net may simply want to use your device or its storage remotely, either as a "zombie" in denial-of-service (DOS) attacks on Web sites, or for storage of contraband data. This can be done without your knowledge, even though you may have unwittingly agreed to allow this to happen by clicking on a link, or opening an infected attachment.

Myth #2: I can tell if my computer has an infection. It will behave strangely and stop working.
Today's threats, like botnets, are designed to evade your detection so they can quietly keep working away in the background, stealing your private information, like credit card details and account logins, and send it off to a criminal. Don't count on visual evidence to clue you in. Make sure your security software is installed and up-to-date. Do NOT postpone, disable, or otherwise prevent your computer from running security scans.

Myth #3: Malware is something I should only worry about for my desktop and laptop computers.
Many people have Internet security software on their home computer, but neglect their mobile device. Some think that their mobile device is immune from threats. The truth is that *any* Internet-connected device, like a smartphone or tablet, can be infected by malware. Additionally, cybercrime is on the rise for mobile devices -- mobile malware increased by 58 percent in 2013.

Myth #4: Incognito mode protects my privacy
Some browsers have an "Incognito" mode that helps protect your privacy -- but mostly from other people using your computer. It does not protect you from everybody and everything on the Internet. Even though you are warned each time you open an Incognito window, many people still think that browsing in Incognito mode means they can't be tracked, that their Internet Service Provider (ISP) can't see what they're browsing, or that they're somehow anonymous to the party on the other end of their connection. Unfortunately, none of the above is true.

Myth #5: This Is a Technology Problem
Cybersecurity is mostly all about people and online behavior. Yes, there are plenty of important technical controls and tools to help protect systems, but if individuals aren't willing to follow basic computer hygiene practices to protecdt themselves, then they will remain insecure and vulnerable to the ever increasing threats and predators, and put themselves and their organizations at unnecessary risk.

Sources and References

- http://www.vipreantivirus.com/newsletters/
- http://www.microsoft.com/security/resources/botnet-whatis.aspx
- http://www.symantec.com/threatreport

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by: