OCTOBER IS CYBERSECURITY MONTH

SEE YOURSELF IN CYBER

alpha TECHNOLOGIES

ARTICLE HIGHLIGHTS

1. THE MANY FACES OF MALWARE
2. BEWARE THE BOTNET
3. MAN IN THE MIDDLE
4. KEEP SOFTWARE & DEVICES UP TO DATE

WEEK 3: RECOGNIZING AND COMBATING CYBERCRIME

Welcome back to our Cybersecurity Awareness Month knowledgebase articles. This week we will be reviewing various types of cyber threats that exist and how to defend yourself against them.

CONTACT US

304-201-7485

salesgroup@alpha-tech.us

www.alpha-tech.us

Hurricane, WV

TO PROTECT & DEFEND THROUGH AWARENESS!

1.) THE MANY FACES OF MALWARE: Malware, or "malicious software", is a broad term that encompasses many different forms of harmful code such as viruses, trojans, adware/spyware, ransomware, etc. Not only can these malicious programs slow down or even crash your devices, but they can also steal sensitive data such as patient/client information or bank account details. To protect yourself from a malware attack, keep your computer and anti-malware software up to date, avoid clicking suspicious email links/attachments/programs, keep your files backed-up, and do not attach unfamiliar devices into your computer, such as an unknown USB drive.

2.) BEWARE THE BOTNET: Did you know that your computer can be turned into a zombie?! It's true, and it is accomplished with something called a botnet. A botnet, short for "robot network", is a collection of computers that have been infected with a certain type of malware and is under the control of the attacker or "bot-herder". Attackers will commonly infect computers across the globe to assemble a fleet big enough to cause substantial damage. When the bot-herder is ready, they can send a command to these computers to have them simultaneously attack a victim. The invasion can range from overloading company servers with denial-of-service attacks to sending spam emails to other victims that could include malware to infect more devices. To avoid being a part of a botnet, always keep your devices and anti-malware solutions up to date, stay aware of suspicious activity on your computer, and always change your default username/password on your device.

3.) MAN IN THE MIDDLE: Anytime you send an email, visit a website, use an application, or even just use your computer while attached to a network, there are communications happening behind the scenes that allow information and data to get from one place to another. This is called network traffic, and while you are unable to see this information flow, someone with the right tools that is on your network could potentially see all the communications you are sending and receiving. This can include usernames, passwords, credit card numbers and other sensitive personal information. To combat this attack, always ensure the websites you are visiting use HTTPS (which can be found in your browsers address bar at the beginning) and use a VPN to connect to a network. These techniques encrypt your data so even if an attacker is monitoring your network, the information they see is illegible and useless to them.

4.) KEEP YOUR SOFTWARE AND DEVICES UP TO DATE: This is something you have likely heard many times in the past, including from these blogs, but there is a reason why it is so important. One of the biggest vulnerabilities that hackers love to exploit are devices that are not kept up to date. Attackers are always scouring the Internet looking for ways to break into a system, and the first place they will start are unpatched devices and software. Like a criminal checking for unlocked car doors, cybercriminals will check for an opening on your software and devices and if they find an "unlocked door", they now have access to your computer, your network, and your data. Developers will release patches to fix security issues, code vulnerabilities, and in a sense, put the lock back on the door. So, I will say it again: ALWAYS keep your devices and software up to date to keep yourself and your information safe.

Tune in next week where we discuss the future of technology and the connected world!