Our Shared Responsibility
National Cyber Security Awareness Month

NCSAM WEEK 5

OUR SHARED RESPONSIBILITY - WHY ALL USERS ARE TARGETED AND HOW THEY CAN MAKE A POSITIVE DIFFERENCE FOR OVERALL CYBER-SECURITY

A lot of people think that "no one wants to target me or my computer" because they think that they don't have anything important enough to be targeted. This thinking is very wrong and the focus of this much expanded article is to explain why and to explain how they, "the average user", can make a positive difference in combating online criminal activity.

WHY ARE USERS TARGETED?

1. Processing Power - If you have a computer, criminals want access to it. There are a variety of reasons why. A compromised computer can be used to send spam or infect other computers with malware or can become another node on a massive "botnet" of thousands computers and used to target websites and other services. Any and all processing power is useful to cyber-criminals.

2. Bandwidth - If you have bandwidth available or if you have an Internet connection at all, not only will attackers use your computer, but they will also use your bandwidth. If you do not properly secure your home wireless router, someone could be stealing your bandwidth by connecting to it, potentially causing you to have higher service bills if your exceed your transfer limits.

3. Account Access - Any account in a school or business system is a foot in the door and could be used to compromise other systems or even attack other schools or businesses. Once they have access to an account, they can then move to compromise other accounts or elevate the privileges of the account to aid in their attack.

4. Network Access - Accounts are generally used to login to more than just computers - they typically will also allow access to network resources like VPN connections and wireless networking. Attackers will use compromised accounts to gain access to network resources to infect other machines or gain access to servers.

5. Personal and/or financial information - Cyber-criminals collect credit card information, social security numbers, bank account numbers and passwords, driver's license and other state ID cards, medical insurance records and any other information they can use for financial gain. This information is generally collected and sold in large quantities, the newer the information, the better the price for them. The loss of these credentials

can cause you long-term issues, as your credit rating can be affected or your insurance cancelled because of fraudulent claims. Make sure you protect these items and secure them so you will not be a victim.

HOW CAN YOU MAKE CYBER SECURITY "OUR SHARED RESPONSIBILITY"?

1. Protect Your Digital Assets - Making it harder for criminals to obtain your valuable information is the first step toward making a difference.

2. Protect Your Devices and Access Methods - Changing from the default passwords on your wireless routers and other network devices will help prevent attackers from using your resources to attack other users and networks.

3. Keep Your Computers Secure - Make sure you keep current with security updates - set your computer to update automatically. Follow the guidelines concerning passwords and practice safe browsing, emailing and social networking to keep attackers from taking over your accounts or your computer.

4. Report Potential Frauds and Scams - Online frauds and scams can be reported to the **Internet Crime Complaint Center** which is a partnership between the FBI and the National White Collar Crime Center. The center is designed to deal with issues pertaining to identity theft, extortion, and similar crimes, so this is not where you report the latest email about penny stocks or sudden inheritances. The more information the center can obtain from users, the better their chances of stopping future cyber-crime.

We hope that this information has been helpful and informative and that we have managed to raise your awareness of cyber-security!