UNITED STATES CYBER COMMAND

CYBERSECURITY AWARENESS NEWSLETTER

National Cyber Security Awareness Month

Week 1
October 2018

Week 1: October 1-5

Make Your Home a Haven for Online Safety

Cybersecurity should not cease when we leave the workplace. Now more than ever we need to stress the importance instilling online safety and privacy at home.

"Every day, parents and caregivers teach kids basic safety practices – like looking both ways before crossing the street and holding an adult's hand in a crowded place. Easy-to-learn life lessons for online safety and privacy begin with parents leading the way. Learning good cybersecurity practices can also help set a strong foundation for a career in the industry. With family members using the internet to engage in social media, adjust the home thermostat or shop for the latest connected toy, it is vital to make certain that the entire household – including children – learn to use the internet safely and responsibly and that networks and mobile devices are secure. Week 1 will underscore basic cybersecurity essentials the entire family can deploy to protect their homes against cyber threats."

-StaySafeOnline.org

http://fiiisun.com.fi/2018/03/16/thumbs-up-for-online-safety-bill/

Safe Practices/Best Practices

Two critical factors in cybersecurity are to *Prevent* and *Protect*; these factors must be executed in everything that we do in the cyber world. You can initiate the prevention process by limiting the amount of personal information that is publicly available about yourself. This starts by using safe practices when using mobile devices, applications, e-mail, and social networks.

Applying the following safe practices can greatly reduce the potential of threats and increase your cybersecurity posture at home.

Devices

Attackers will work tirelessly to gain control of your devices, compromise your email or messages, or spy on your online activities. We can greatly reduce the risk of compromise by adhering to the following mobile security best practices.

1. *Install reputable antimalware programs from a trusted source*
2. *Keep all device software and applications up to date*
3. *Protect devices and accounts with PINs and strong passwords*
4. *Only download reputable apps, and don't give apps access to data that is not required for the functionality of the application*
5. *Think before you click! Some links and applications could contain viruses or be a part of a phishing attack*
6. *Be mindful of "Free" offers online, they are known for including malware*

Passwords

Always use a strong password! The DoD suggests that passwords be a minimum of 15 characters in length and contain a combination or lowercase letters, uppercase letters, numbers, and special characters. Do not include your name or personal information in your password, and refrain from using simple dictionary words and numerical patterns. Keep in mind that you should not use the same password for different social network sites or on multiple applications.

Additional Government Resources and Useful Links

Cybersecurity Awareness Information**:** https://staysafeonline.org/

How To Check Your Privacy Settings: https://staysafeonline.org/data-privacy-day/check-your-privacy-settings/

Good Computing Practices: http://its.ucsc.edu/security/top10.htmlIdentity

What To Do If You Are a Victim of Cybercrime
https://staysafeonline.org/wp-content/uploads/2017/09/What-To-Do-If-You-Are-a-Victim-of-Cybercrime.pdf

Settings

Modifying your default security settings is one of the first steps in maintaining a secure and safe online persona. Many of the applications we use every day have security settings that are left open, unsecure, and vulnerable by default. It is critical that we manage our privacy and security settings so that little to no information is revealed publicly. Do not allow your profile to be viewed by individuals who you do not know you or to services without your consent. Remember to use the strongest security settings when editing your profile. If you would like to view/change your security settings but are not sure how to do it, please see the "Privacy Settings" link at the footer of this page for suggestions on how to modify your privacy settings.

Posts, Photos and Friends

Watch what you post! Remember that once you post something online, it is posted forever. Make sure you think twice about posting status changes, photos, or comments that you wouldn't want your future employers or certain individuals to see. Remember that many photos that are posted will often have metadata inside the file which could contain location, system/device, and even personal information such as your name. When it comes to social media, everyone who sends you a friend request may not be your friend! Make sure to choose which friends you accept wisely.

https://www.hellotech.com/blog/smart-home-cyberattacks/

If You Become Compromised

The most vigilant cybersecurity professionals can still fall victim to a cyber-attack, malware or online fraud. If you suspect you have become a victim of a cyber-attack below are a few steps that you should immediately execute to protect yourself and prevent any additional compromise.

Disconnect from the Internet immediately, this prevents additional data from being transmitted to the attacker.
Scan Your Device with an up to date antivirus software and remove and threats or malware that has been detected.
Close All Accounts that have been affected by the attack as soon as you are made aware of potential compromise, this can aid in preventing data theft before the attacker has time to access the account.
Look for Signs of Identity Theft and monitor your credit reports.

Please see the "What to do if you're a victim" link at the footer of this page for additional information.

Coming Up Next Week:

CSAM Week 2: October 8-12

Millions of Rewarding Jobs: Education for a Career in Cybersecurity

USCYBERCOM OCIO

The Office of the CIO serves as the IA Subject Matter Experts for the Command. It is our mission to protect the confidentiality, integrity, and availability of Information Systems (IS) and networks throughout USCYBERCOM, while managing a customer-orientated IA organization capable of meeting the needs of all USCYBERCOM customers.

Additional Government Resources and Useful Links

Cybersecurity Awareness Information**:** https://staysafeonline.org/

How To Check Your Privacy Settings: https://staysafeonline.org/data-privacy-day/check-your-privacy-settings/

Good Computing Practices: http://its.ucsc.edu/security/top10.htmlIdentity

What To Do If You Are a Victim of Cybercrime
https://staysafeonline.org/wp-content/uploads/2017/09/What-To-Do-If-You-Are-a-Victim-of-Cybercrime.pdf