UNITED STATES CYBER COMMAND

CYBERSECURITY AWARENESS NEWSLETTER

National Cyber Security Awareness Month

Week 3
October 2018

Week 3: October 15-19

It's Everyone's Job to Ensure Cybersecurity at Work

Creating a culture of cybersecurity in the workplace is a responsibility that we all share. Efforts like employee education, cybersecurity training, and threat awareness and mitigation are necessary to enhance our workplace cybersecurity posture.

"When you are on the job – whether it's at a corporate office, local restaurant, healthcare provider, academic institution or government agency – your organization's online safety and security are a responsibility we all share. And, as the lines between our work and daily lives become increasingly blurred, it is more important than ever to be certain that smart cybersecurity carries over between the two. Week 3 will focus on cybersecurity workforce education, training and awareness while emphasizing risk management, resistance and resilience. Week 3 will also shed light on how businesses can protect themselves, their employees and their customers against the most prevalent threats."

StaySafeOnline.org

Cybersecurity Tips for the Workplace

- Your organization likely has data that attract hackers and malicious actors who would benefit from having, manipulating, selling or destroying that data.
- Passwords should be unique and contain a strong mix of characters. It is also critical make sure that you use different passwords for different accounts.
- Be cautious when clicking links or attachments especially if they are suspicious, if they are not from reputable sources, or if they are unexpected.
- Avoid sensitive browsing in the workplace. Things like banking and shopping should only be done on personal devices and on a trusted network.
- Monitor your accounts/profiles for suspicious activity. If you notice something suspicious or unfamiliar it could mean that your account has been compromised.
- Social engineering can happen in the workplace; be conscientious of people who call or email you in attempts to gain unwarranted and sensitive information.

https://medium.com/webeagle/5-things-you-need-to-include-in-your-employee-cyber-security-policy-8acf3f4dd10d

Additional Government Resources and Useful Links

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

DHS Cyber Security and STEM Training: http://www.dhs.gov/cybersecurity-training-exercises

(*NICE*) The National Initiative for Cybersecurity Education: http://csrc.nist.gov/nice/resources.html

Training Opportunities

Several avenues are available to help train and educate our nation's cyber workforce, from associate's and bachelor's degrees to supplemental education.

- Formal, national cybersecurity education programs, such as the National Initiative for Cybersecurity Education, work to establish an operational, sustainable, and continually improving cybersecurity education program for all Americans.
- The National Centers of Academic Excellence have certified more than 125 institutions nationwide that teach students valuable technical skills and promote research in various disciplines of cybersecurity.
- The National Institute of Standards and Technology (NIST) published the National Cyber security Workforce Framework, which provides a common vocabulary for discussing cyber security work and the associated knowledge, skills and abilities.
- Federal employees, federal contractors and veterans can take advantage of the Federal Virtual Training Environment (FedVTE), available through the National Initiative for Cyber security Education (NICE), a joint effort of the federal government, academia and industry. FedVTE provides a library of training material, including classroom lectures.

https://innovationatwork.ieee.org/securing-internet-things-cyber-attack-critical/bigstock-183364126/

Leaders and Our Shared Responsibility

Leaders in all areas play an important role in the development of our cyber workforce. Today's leaders must be knowledgeable in all aspects of cyber security. They must understand the importance of having a highly trained workforce competent in basic cyber hygiene practices. The importance and necessity of protecting our computers, mobile devices, and networks will continue to increase. To minimize the risk of a cyber-attack everyone, including government, industry partners and the individual user, need to do their part. We must understand the tools used to perform our missions and how to be safe while using them. It is our shared responsibility to be educated on security best practices and to continue to stay abreast of changes to these practices. Our role in keeping information and networks secure should be taken seriously not only at work, but at home.

Coming Up Next Week:

CSAM Week 4: October 23-27

Safeguarding the Nations Critical Infrastructure

USCYBERCOM OCIO

The Office of the CIO serves as the information assurance 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/

DHS Cyber Security and STEM Training: http://www.dhs.gov/cybersecurity-training-exercises

(*NICE*) The National Initiative for Cybersecurity Education: http://csrc.nist.gov/nice/resources.html