CDSE pulse VOLUME 1 ISSUE 10
October 2020

THIS MONTH'S FOCUS

NATIONAL CYBERSECURITY AWARENESS MONTH

NATIONAL CYBERSECURITY AWARENESS MONTH

NCSAM is a collaborative effort between Government and industry to provide every American the resources they need to stay safe and secure online while increasing the resilience of the Nation against cyber treats. It was launched in 2004 by the U.S. Department of Homeland Security (DHS) National Cyber Security Division, now called the Cybersecurity and Infrastructure Security Agency (CISA), and the nonprofit National Cyber Security Alliance (NCSA) representing industry. Their shared goal is to expand NCSAM's reach every year and highlight the importance of cybersecurity and staying safe online. This year's theme is "Do Your Part. #BeCyberSmart." It encourages individuals and organizations to own their role in protecting their part of cyberspace while stressing personal accountability and the importance of taking proactive steps to enhance cybersecurity.

This year has been unprecedented for many reasons, including the rise of teleworking due to the COVID-19 pandemic. Increased phishing attacks and identity theft have left individuals compromised due to lack of knowledge, awareness, or vigilance surrounding cyber practices. The Center for Development of Security Excellence (CDSE) aims to focus readers on topics associated with cybersecurity to combat these issues at home and in the office.

DID YOU KNOW?

The U.S. Department of Homeland Security and the National Cyber Security Alliance (NCSA) launched National Cybersecurity Awareness Month (NCSAM) to raise cybersecurity awareness in 2004.

CDSE – Center for Development of Security Excellence

@TheCDSE

Center for Development of Security Excellence

CYBERSECURITY KNOWLEDGE CRITICAL FOR TELEWORKERS DURING PANDEMIC

The COVID-19 pandemic and the resulting social distancing protocols have forced many Americans to work from home. Unfortunately, more people teleworking means more targets for cybersecurity threats. Even the most routine aspects of teleworking such as Virtual Private Networks (VPN), employee email accounts, and virtual meetings are vulnerable to attacks. As NCSAM enters its 17th year, it is important to remember that these vulnerabilities can be secured through vigilance, security procedures, and training.

VPNs are one of the most secure means to access the internet because they create "private tunnels" that encrypt the data that passes through the network. It also masks user identity and promotes online safety and privacy; however, VPNs are still vulnerable to attacks. According to **guidance** published by CISA, organizations are less likely to keep VPNs updated with the latest security updates and patches. Some organizations do not use Multi-Factor Authentication (MFA) for remote access, which grants access only after successfully presenting two or more pieces of evidence. This gap also leaves VPNs open to attacks. CISA offers tips for securing VPNs known as **enterprise VPN solutions**. These tips include updating VPN devices frequently, employing MFAs to increase security, and developing and maintaining enterprise security policies and procedures. A safe internet connection is important, but it is only one aspect of safe teleworking. Another aspect is avoiding interaction with phishing emails.

Phishing occurs when attackers masquerade as trusted entities and try to lure people in with malicious links and suspicious attachments. One of their techniques is to make their fraudulent website or bogus email address look as authentic as possible to trick unsuspecting employees. For instance, google.com is a legitimate website, but go0gle.com is most likely a scam website. Other signs of phishing include emails from unknown senders trying to solicit sensitive or personal information. Some tips to safeguard against phishing include knowing your organization's process for spotting anomalies, being vigilant and aware of sophisticated attacks, paying attention to URLs and domains, and employing MFAs. Phishing attacks were a problem well before the pandemic; however, virtual meetings are a vulnerability that many may not have considered.

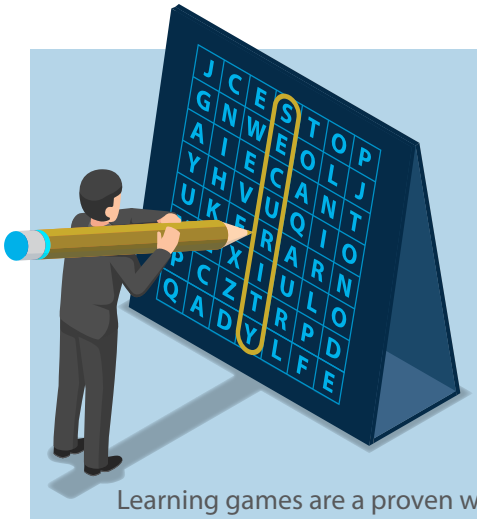
Virtual meetings have become the new norm in 2020. But, government employees were not the only people who adjusted to this new format; so did the cyber threat actors. CDSE recently aired a cybersecurity webinar that included the "dos and don'ts" of virtual meetings. In summary, the "dos" are to prohibit unauthorized software, verify meeting classification, secure meetings, enforce policies, and connect approved devices. The "don'ts" are do not use unauthorized software, do not ignore classification markings, do not open meetings to all, do not overlook or ignore policies, and do not connect unapproved devices.

While the examples presented in this article cover different teleworking security risks, there is one thing they have in common: the employee. According to a 2020 global study conducted by the Ponemon Institute, 62% percent of insider threat incidents were caused by negligence. While cybersecurity and insider threats are different security disciplines, a negligent employee could be the catalyst in a cybersecurity incident. Employees with cybersecurity knowledge are less likely to be negligent. In fact, they are the best line of defense for preventing attacks.

CYBERSECURITY KNOWLEDGE CRITICAL FOR TELEWORKERS DURING PANDEMIC (CONT'D)

Some methods to educate employees include investing in user education, providing frequent refreshers to influence behavior, employing separation of duties, signing acceptable use policies, displaying warning banners, and displaying frequent pop-up reminders. CDSE offers **training, posters, videos, games, and access to policy guidance** to improve and promote organizational and individual cybersecurity awareness.

The number of people teleworking for such an extended period of time was unprecedented before COVID-19, and it is important to remain vigilant and aware during this time of new and increased security vulnerabilities. CISA Director Christopher Krebs expressed the need for vigilance at a virtual cybersecurity conference this September, "We have to make sure that federal agencies that are shifting to a remote work environment or have shifted to a remote environment, that are introducing new risks, that are expanding their attack surface, that we don't take our foot off the gas in terms of the progress we've made." Security professionals need to develop, maintain, and enforce cybersecurity policies, continuously patch and update operating systems, and utilize training to prevent cyberattacks and safeguard the nation.



ENHANCE YOUR CYBERSECURITY KNOWLEDGE WITH SECURITY AWARENESS GAMES

Learning games are a proven way to improve knowledge and retention. Our new cybersecurity games aim to drive awareness with this year's NCSAM theme, "Do Your Part. #BeCyberSmart." Choose from the games below. You can find them under "Cybersecurity" **here** along with other security awareness games.

Word Search: Cyber Terminology
October 5

Crossword Puzzle: #BeCyberSmart
October 12

Jeopardy: "I'll take Cyber"
October 19

CDSE has several Cybersecurity webinars scheduled this month. The first event was the "Know Your CDSE" Cybersecurity Speaker Series on October 1, 2020. If you missed the live event, you can still view the archived Speaker Series under **Cybersecurity**. The Cybersecurity Team has also recorded two NCSAM webcasts with the following release dates:

October 5
Cybersecurity and Telework: Concerns, Challenges, and Practical Solutions Webcast
(Part 1 of two-part series)

October 19
Cybersecurity and Telework: Concerns, Challenges and Practical Solutions Webcast
(Part 2 of two-part series)

...more under "Webinars" on the Cybersecurity catalog page at **https://www.cdse.edu/catalog/cybersecurity.html**

LINKS TO MORE CYBERSECURITY RESOURCES:

NCSAM Webpage
https://www.cisa.gov/national-cyber-security-awareness-month

CISA Cybersecurity Resources
https://www.cisa.gov/cisa-cybersecurity-resources

COVID-19 Exploited by Malicious Cyber Actors
https://us-cert.cisa.gov/ncas/alerts/aa20-099a

National Cyber Security Alliance
https://staysafeonline.org

Federal Trade Commission
https://www.consumer.ftc.gov/files/contact_tracing_scams_infographic-1-508.pdf

CDSE Cybersecurity Toolkit
https://cdse.edu/toolkits/cybersecurity/index.php

NEW PSAS HIGHLIGHT FREE TRAINING, EDUCATION, AND CERTIFICATION

Explore information about security learning opportunities with our new CDSE Public Service Announcements (PSAs). These short PSAs can introduce you to learning paths to help you get to the next level of your career goals.

CDSE:

CDSE OVERVIEW: information on CDSE offerings

EDUCATION:

PROGRAM OVERVIEW: graduate & advanced level security courses

CERTIFICATE PROGRAM: overview of program

UNDERSTANDING ADVERSARIES & THREATS TO THE U.S. AND DOD

STATUTORY, LEGAL, AND REGULATORY BASIS OF DOD SECURITY PROGRAM

Any questions or more information about these PSAs can be directed to **dcsa.ncr.dcsa-cdse.mbx.cdse-communications@mail.mil**

WHAT STUDENTS ARE SAYING

"This is one of the best training courses I have taken. It moves smoothly and has very good information. The format and image of each page make it interesting to participate."
– Student
Cybersecurity Awareness CS130.16

"Great training on a difficult, technical topic."
– Student
Continuous Monitoring CS200.16

PHISHING AWARENESS 101

Phishing is a form of social engineering that fools people into revealing confidential or personal information that can be used illicitly or fraudulently against them. Cybercriminals can also take advantage of information found through social media platforms, location sharing, and in-person conversations. CDSE's phishing prevention poster highlights ways individuals can secure themselves from online fraud and phishing attempts. We invite you to download and share the **poster** within your organization to raise awareness and take our Phishing Awareness **eLearning course**. There's also a Phishing Scams game available through the Federal Trade Commission **here**.

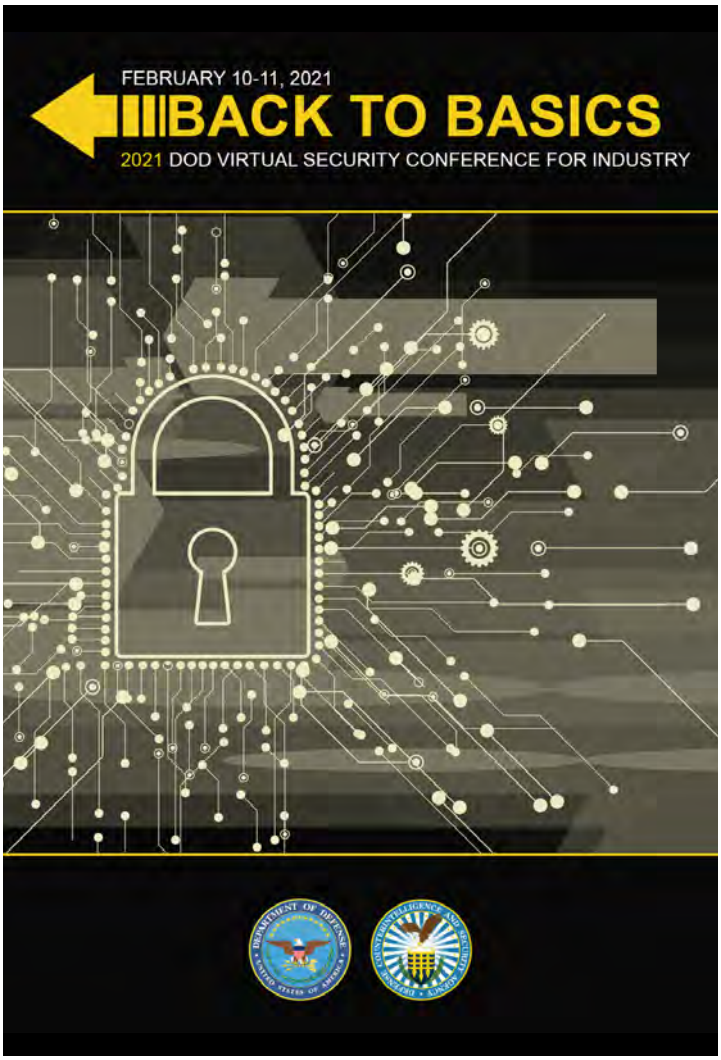
WHAT'S COMING IN NOVEMBER

November is National Critical Infrastructure Security and Resilience Month! This year, the November CDSE Pulse will focus on the Infrastructure Security Month and the resources available to raise awareness and promote actions to protect our nation's critical infrastructure.

In addition, the **"Know Your CDSE: Education" Speaker Series** is scheduled for November 10. The speaker will cover our Education program including requirements, credit recommendations, courses, and certificates. Sign up today to learn how you can broaden your security knowledge and prepare for security leadership positions and responsibilities!

DID YOU MISS THE INSIDER THREAT VIRTUAL SECURITY CONFERENCE?

In case you missed the Virtual Security Conference on September 3, CDSE has made the event resources available to insider threat practitioners, counterintelligence and security professionals from the DoD, federal agencies, private industry, critical infrastructure sectors, and academia. Access the conference presentations in our **webinar archive** under Insider Threat.



UPCOMING WEBINAR: NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER, NOW WHAT?

Thursday, October 22, 2020, 1-2 PM ET

If you are assigned to the NAESOC, make plans to attend this webinar to hear about the current state of NAESOC and FY21 plans. Attendees will also be able to ask questions and get answers in real time from subject matter experts.