CDSE pulse
VOLUME 2 ISSUE 10
October 2021

THIS MONTH'S FOCUS

NATIONAL CYBERSECURITY AWARENESS MONTH

NCSAM: A SOLID HISTORY AND A BRIGHT FUTURE

The National Cybersecurity Awareness Month (NCSAM) has grown immensely since its inception 18 years ago. The initiative that started under leadership from the U.S. Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA) now reaches consumers, small and medium-sized businesses, corporations, educational institutions, and people across the nation. This article will look back at the history of NCSAM, why it is important, and how you can contribute as this awareness month continues to build momentum.

NCSAM launched in October 2004 as a broad effort to help all Americans stay safe and secure online. Initially, NCSAM awareness efforts centered on advice like updating your antivirus software. In subsequent years, leading administration officials from DHS, the White House, and other agencies have regularly participated in events across the United States, demonstrating their support of his critical observance. In 2010, the kickoff of NCSAM also included the launch of the **STOP. THINK. CONNECT.** campaign. It is a national public awareness effort that increases the understanding of cyber threats and empowers the American public to be safer and more secure online. It encourages Americans to view Internet safety as a shared responsibility–at home, in the workplace, and in our communities. NCSAM operates similarly to a grassroots campaign with participation from a multitude of industry participants that engage their customers, employees, and the public in awareness. The collaboration of NCSA and DHS on NCSAM is one of the many successful public-private partnerships that are so critical to cybersecurity.

The theme for NCSAM 2021 is "Do Your Part. #BeCyberSmart." The first week of the month spelled out for the public what it means to be cyber smart. "As our lives have become increasingly dependent on technology, virtually all personal and business data is kept on internet-connected platforms, which can become a gold mine for bad actors." The first week also highlighted the best security practices and general cyber hygiene such as creating strong passwords, using multi-factor authentication, backing up your data, and updating your software as great places to start.

CYBERSECURITY AWARENESS MONTH

DID YOU KNOW?

The Internet Crime Complaint Center (IC3), which provides the public with a trustworthy source for information on cybercriminal activity and a way for the public to report when they suspect they are a victim of cyber crime, received a record number of complaints from the American public in 2020: 791,790, with reported losses exceeding $4.1 billion.

CDSE – Center for Development of Security Excellence

@TheCDSE

Center for Development of Security Excellence

NCSAM: A SOLID HISTORY AND A BRIGHT FUTURE (CONT'D)

Week two started on October 11 with "Fight the Phish." Phishing attacks and scams have thrived since the COVID pandemic began in 2020. According to a Verizon 2019 data breach investigations report, phishing attacks account for more than 80 percent of reported security incidents. Week two also stressed the importance of being wary of emails, text messages, or chat boxes that come from a stranger or someone you were not expecting.

Week three will highlight the Cybersecurity Career Awareness Week led by National Initiative for Cybersecurity Education (NICE). This week-long campaign promotes the exploration of cybersecurity careers. Whether its students, veterans, or those seeking a career change, the dynamic field of cybersecurity is rapidly growing and has something for everyone.

Week four is about making security a priority at different levels. For government agencies and businesses, this means building security into products and processes, educating their workforces, and continuously encouraging security best practices/vigilance. For individuals, it is about keeping cybersecurity at the forefront of your mind, as you connect daily.

Everyone, no matter the age or occupation, can participate in NCSAM. For instance, in your private life, you can follow the NCSA and Cybersecurity and Infrastructure Security Agency (CISA) on Twitter, Facebook, YouTube, and LinkedIn to receive the latest online safety news and resources. You can post online safety tips and reminders about NCSAM on your social networks. Be sure to use the hashtag #BeCyberSmart. You can download and share **sample social media** posts leading up to and throughout the month on social media. You could also blog about cybersecurity in October by highlighting one of the NCSAM's calls to action.

Get your community involved by sending an email to colleagues, employees, customers and your school and outline how they can get involved. Host a poster/video contest for students in which participants create informative online safety resources. Work with your leadership to issue an official proclamation to show your organization's support of the month and its commitment to "Do Your Part. #BeCyberSmart." Host a local or virtual event, or training for your organization or community to discuss smart computer practices and relevant cybersecurity issues. Talk to community members about the best security practices for email, social media, and/or online transactions.

Organizations can promote NCSAM using several different avenues: through their social media accounts, newsletters, briefings, town halls, posters, daily or weekly emails/tips/etc. The **NCSA** and **CISA** NCSAM webpages offers messaging, graphics, sample social media posts, videos, tip sheets, and briefings which can be modified for use to raise awareness with your workforce. Providing your workforce with information about cybersecurity training and resources to increase their cybersecurity knowledge will benefit the organization and the individual.

CDSE offers **cybersecurity training and resources** to support DOD and cleared industry personnel. Our products include instructor-led/eLearning courses, videos, posters, shorts, webinars, toolkits, and security awareness games. **The DOD Cyber Exchange** also contains training and resources for the public with some available only to Common Access Card (CAC) holders. Additionally, **CISA** and **NCSA** provide cybersecurity training, guides, reference materials, and other awareness/performance support tools. These training and awareness products are not just for NCSAM and can be promoted throughout the year.

CISA offers **telework guidance** and resources for federal agencies, non-federal organizations, and the at-home worker.

By extending NCSAM's reach, we can expose more people to the best online safety practices. The future of cybersecurity should not be about one organization protecting everyone from cyber threats but instead all organizations and individuals taking steps to operate securely and safely online.

NEW CYBERSECURITY WEBINAR

CDSE recently released a Cybersecurity webcast titled "Cybersecurity and Telework: Concerns, Challenges, and Practical Solutions Part 3 (Collaboration Tools)." Access the new webcast from our **webinar homepage** under Cybersecurity.

ENHANCE YOUR CYBERSECURITY KNOWLEDGE WITH NEW ONLINE GAMES

Learning games are a proven way to raise awareness and improve knowledge. If you're looking for a way to test your cybersecurity knowledge, CDSE will soon release two new security awareness games, Cybersecurity Trivia and 8-Ball II, to help you do just that. You can find them under "Cybersecurity" along with other security awareness games at **https://cdse.edu/resources/games.html**.

NCSAM AND CYBERSECURITY RESOURCES:

PRODUCT	URL
Cybersecurity & Infrastructure Security Agency (CISA)	**https://www.cisa.gov/cybersecurity-awareness-month**
National Cybersecurity Alliance	**https://staysafeonline.org/cybersecurity-awareness-month/**
DOD Cyber Exchange	**https://public.cyber.mil/**
Do's and Don'ts of Network Utilization and Cybersecurity: Defend the DODIN	**https://dl.dod.cyber.mil/wp-content/uploads/covid19/pdf/unclass-cyber_and_networking_dos_and_donts.pdf**
Top Telework Tools	**https://dl.dod.cyber.mil/wp-content/uploads/covid19/pdf/unclass-top_telework_tools-PUBLIC.pdf**
DOD Cyber Exchange Training Catalog for CAC holders (Cybersecurity Awareness Training)	**https://disa.mil/en/NewsandEvents/Training**
CDSE Cybersecurity Training Catalog	**https://www.cdse.edu/Training/Cybersecurity/**
CDSE Cybersecurity Toolkit	**https://www.cdse.edu/Training/Toolkits/Cybersecurity-Toolkit/**

NEW CYBERSECURITY COURSE

CDSE has a new instructor-led cybersecurity course, "Assessing Risk and Applying Security Controls to National Industrial Security Program (NISP) Systems CS301." This course provides students with guidance on applying policies and standards used throughout the U.S. Government to protect information within computer systems, as delineated by the Risk Management Framework (RMF) process. It also provides a comprehensive understanding of contractor requirements under the National Industrial Security Program (NISP). Learn more about the course and register by visiting the course page (**https://www.cdse.edu/Training/Instructor-led/CS301/**).

CDSE pulse
VOLUME 2 ISSUE 10
October 2021

REGISTER FOR SPRING EDUCATION CLASSES

Registration is now open for the spring semester of CDSE Education classes that run from January 10 to May 10, 2022. Classes fill quickly, so please register early to secure your spot in the spring semester.

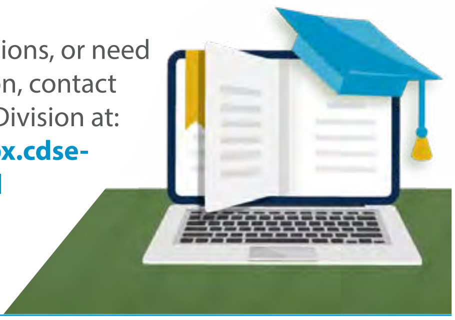
CDSE Education Division offers:

- **Tuition-free, flexible and 100% virtual instructor-led courses**
- **Five Security Education Certificate programs**
- **Highly qualified instructors**
- **Real-world practical assignments**
- **Virtual networking with professionals throughout the security community**

You can learn more about the available classes and register for them by accessing the links here: **https://www.cdse.edu/education/courses.html**.

To register, log into STEPP via: **https://cdse.usalearning.gov/login/index.php**

If you have any questions, or need additional information, contact the CDSE Education Division at: **dss.ncr.dss-cdse.mbx.cdse-education@mail.mil**



THE COUNCIL ON OCCUPATIONAL EDUCATION (COE) TO VIRTUALLY HOLD THE CDSE ACCREDITATION REAFFIRMATION REVIEW

NOVEMBER 29   DECEMBER 3, 2021

CDSE hereby announces it will host a virtual review for accreditation reaffirmation with COE. Persons wishing to make comments should write to: Executive Director, Commission of the Council on Occupational Education, 7840 Roswell Road, Bldg. 300; Suite 325; Atlanta, GA 30350, or submit their comments via the Council website (**www.council.org**). Persons making comments must provide their names and mailing addresses.

★★★★★ WHAT STUDENTS ARE SAYING

Course: Cybersecurity Awareness CS130.16

"The content was engaging and the interactivity was helpful. The information was relevant and the delivery was well done."

"I thought the training was excellent, made me really think, and will apply what I learned professionally and personally."

CDSE WEBSITE MIGRATION

Our website recently migrated to a new web-hosting platform. While our homepage URL (**www.cdse.edu**) is the same, the rest of the website URLs have changed. This may impact your "Favorite" or "Bookmark" pages. We apologize for any inconvenience this causes and thank you for your understanding.