TOGETHER

We Improve Our Nation's Cybersecurity

National Cybersecurity Awareness Month 2018

Department of Homeland Security
National Cybersecurity Awareness Month

2018 Toolkit:

key messaging, articles, social media and more to promote National Cybersecurity Awareness Month 2018

dhs.gov/ncsam

#CyberAware

Homeland Security

TOGETHER
We Improve Our Nation's Cybersecurity
National Cybersecurity Awareness Month 2018

Table of Contents

Welcome to National Cybersecurity Awareness Month 2018

This October, National Cybersecurity Awareness Month (NCSAM) commemorates 15 years as an annual initiative to raise awareness about the importance of cybersecurity. NCSAM 2018 is a collaborative effort between government and industry to ensure every American has the resources they need to stay safer and more secure online, while increasing the resilience of the nation during cyber-threats. The U.S. Department of Homeland Security (DHS) is the federal, national lead for NCSAM. DHS also co-leads NCSAM with the National Cyber Security Alliance (NCSA).

NCSAM is a collaborative effort developed by DHS and National Cyber Security Alliance (NCSA)

Thank you for participating in National Cybersecurity Awareness Month. Cybersecurity is our shared responsibility, and we appreciate your efforts throughout the month of October. This document has a wealth of resources to make it easy for you and your organization, regardless of size or industry, to engage and promote NCSAM. Use the table of contents to easily find tips, use social media posts, participate in twitter chats, etc. We also have resources to help you engage many different types of audiences.

Themes and Key Messages for October 2018

This year NCSAM has an overarching theme that we ask our partners to use and promote as you build your October events. DHS also has four key messages that can help you direct resources, drive events, and design activities throughout the month.

2018 Overarching Theme

Cybersecurity is our shared responsibility and we all must work together to improve our Nation's cybersecurity. *Cybersecurity is not just the responsibility of governments, companies, groups, or individuals. Everyone shares the responsibility for cybersecurity – from the average smartphone user to a corporate CEO.*

DHS Key Messages

These key messages are featured throughout the month to help drive events, resources, and activities from DHS.

"Strengthen the Nation's Cybersecurity Ecosystem"

Contribute and commit to strengthening the Nation's Cyber Ecosystem. The cybersecurity ecosystem is made up of distinct but related elements that contribute to the strength of the whole system. Our entire society, from government and law enforcement to the private sector and members of the public, must work cooperatively to improve our network defense. Strengthening the Cybersecurity Ecosystem will help shift the advantage from cyber-attackers to cyber-defenders.

"Tackle it Together"

Cybersecurity is a cross-cutting, cross-sector problem, so we have got to tackle it together. The Nation's increasing dependence on networks and digital systems has brought with it a rise in both the variety, quantity, and sophistication of cyber-threats. The Internet is critical for businesses, the government and individual users, so its security has become a bigger priority. We are all connected in cyberspace and each has a role to play in cybersecurity. Cyber-criminals are inventive, but by ensuring every citizen has the resources and information he or she needs to be a responsible cyber citizen, we will make the Internet more secure for all.

"Build up the Cybersecurity Workforce"

Increase and strengthen the cybersecurity workforce across all sectors. The number of cybersecurity jobs across the nation outpaces the number of people qualified to fill them. The demand for skilled cybersecurity professionals is growing each year. DHS is working with our nation's private industry, academia, non-profit organizations, and governments at all levels to develop and maintain an unrivaled, globally competitive cybersecurity workforce. From young students learning to code, to teachers promoting educational opportunities in science, technology, engineering and math (STEM), and working professionals preparing for certifications, there is a role in cybersecurity for everyone. This October, we challenge you to get involved in learning about your role in building the pipeline of future cybersecurity professionals.

"Secure Critical Infrastructure from Cyber Threats"

Heighten resilience and understand how to best protect critical infrastructure from cyber threats. Our Nation's well-being relies upon secure and resilient critical infrastructure—the assets, systems, and networks that underpin American society. In the past we've trusted in processes, procedures, and specific architectures to keep our critical infrastructure safe. But there is no longer an 'air-gap' between our systems and the Internet to keep cyber-attacks from threatening critical infrastructure. The security of critical systems and infrastructure depends on you and your actions as a cyber-citizen to help keep them safe and resilient.

During the month, NCSA celebrates weekly themes to highlight some of the most important aspects of *Cybersecurity is our Shared Responsibility*. While these themes are more consumer-specific than the DHS Key Messages, each complements the overall messages of NCSAM 2018 by making cybersecurity more personal to the individual. To see the NCSA 2018 themes, please visit: www.staysafeonline.org/ncsam

Please contact us if you need assistance or to request a DHS speaker for your NCSAM events. For more information, please visit https://www.dhs.gov/ncsam. If you would like even more materials (such as posters or additional toolkits) in addition to those included in this packet, please email DHS at stopthinkconnect@hq.dhs.gov to learn more.

How to Engage

In order to have the biggest impact this October, become familiar with the NCSAM 2018 goal of ensuring that everyone knows that they are responsible for cybersecurity, the Internet is a shared resource, and how to prevent online threats to help increase Internet security. This section provides tips for spreading cybersecurity awareness messages that you can share with your internal stakeholders to ensure that NCSAM messages reach your intended audiences.

Congressional members, committees, and staff

- Promote training and exercise opportunities
- Engage state and local officials on current initiatives to improve cybersecurity and resilience
- Include a message about the importance of cybersecurity in newsletters, mailings, and websites during October (graphics and social media images are available as part of this toolkit)
- Write an op-ed in your local paper about the importance of cybersecurity and any of your cybersecurity or STEM-related efforts taking place in your district or state
- Promote interagency and multi-level collaboration on cybersecurity issues

Critical infrastructure owners and operators

- Educate members of your sector about cybersecurity issues and how they relate to the sector's security environment and business operations by hosting an event or symposium
- Include a message about the importance of cybersecurity in newsletters, mailings, and websites
- Highlight your partnership with DHS, other Federal agencies, and the national cybersecurity community to make these vital assets and systems secure and resilient
- Host a town hall to discuss local, relevant cybersecurity issues
- Contribute your voice and resources to social media conversations by using the hashtag #CyberAware and #cybermonth2018

Future Cybersecurity Workforce: students, educators, career changers

- Pursue continuing education by considering a CyberCorps®: Scholarship for Service (SFS) program to study cybersecurity
- Take a cybersecurity class on FedVTE or find a training course on NICCS™
- Consider your continuing education opportunities at a National Centers of Academic Excellence (CAE) institution, which are prestigious programs designated by DHS and NSA
- Talk to students about cybersecurity as a career — teachers can check out our no-cost cybersecurity courses for middle and high school students
- Teachers and educators – check out no-cost, project-based cybersecurity curricula available to you!

Current Cybersecurity Workforce Professionals

- Form your own 'cyber syncs' in your organization – gather your colleagues to discuss the latest and greatest technological advancements, how to best protect your organization from ever-changing cyber-attacks, how to keep your kids safe online, etc.
- Tackle it with IT – ask your organization's IT department to put together a demonstration / presentation emphasizing the importance of staying safe online, consequences of negative online behavior, how your organization can help protect itself against cyber-attacks, etc.
- Tackle it with us! Make sure your organization is a partner of the STOP. THINK. CONNECT.™ Campaign. To learn more about joining, visit https://www.dhs.gov/stopthinkconnect-join-campaign

- Sign up for alerts and get tips on how to safeguard your small business' computers from the United States Computer Emergency Readiness Team (US-CERT)
- Report all suspicious or unusual problems with your computer to your IT department

General public and Federal employees

- Contribute your voice and resources you know about to social media conversations by using the hashtag #CyberAware and #CyberMonth2018
- Participate in a local or virtual training or exercise to improve cybersecurity and resilience
- Become a *Friend* of the STOP. THINK. CONNECT.™ Campaign by visiting www.dhs.gov/stopthinkconnect
- Discuss safe online practices with your fellow employees, neighbors, friends, and family
- Inform your community about the STOP. THINK. CONNECT.™ Campaign and the free resources available
- Blog or post on social networking websites about cybersecurity issues and the STOP. THINK. CONNECT.™ Campaign
- Include a message about the importance of cybersecurity in newsletters, mailings, and websites

Top Tips on Cybersecurity to share during NCSAM

- **Keep a clean machine.** Keeping your internet-connected devices free from malware and infections makes the internet safer for you and more secure for everyone. Regularly scan your personal and office devices for viruses and spyware along with keeping your software up to date. For additional ways to protect your devices please visit: https://www.stopthinkconnect.org/campaigns/keep-a-clean-machine-campaign
- **Avoid oversharing online.** As a young professional, it may be very exciting to share what you do at work with others. Remember your organization's security standards and be careful what you say, especially in public settings. You never know who may be overhearing your conversations. Also, put away your work identification or badge when out in public and when using public transportation. For additional tips to keep safe online visit: https://www.dhs.gov/sites/default/files/publications/Social%20Media%20Guide_3.pdf
- **Protect your password.** Create a password with eight characters or more and a combination of letters, numbers, and symbols, and don't make it easy to guess. Additionally, always opt to enable stronger authentication when available, especially for accounts with sensitive information including your email, medical files, or bank

accounts. For more tips and tricks to protect your password, visit: https://www.dhs.gov/sites/default/files/publications/Best%20Practices%20for%20Creating%20a%20Password.pdf

- **Stay protected while connected.** Before you connect to any public wireless hotspot – like on an airplane or in an airport, hotel, or café – be sure to confirm the name of the network and login procedures with appropriate staff to ensure that the network is legitimate. If devices on your network are compromised for any reason, or if hackers break through an encrypted firewall, someone could be eavesdropping on you—even in your own home on encrypted Wi-Fi. For more useful tips about secure Wi-Fi visit https://www.dhs.gov/be-cyber-smart/cyber-lessons
- **Play hard to get with strangers.** Cyber criminals will often offer a financial reward, threaten you if you don't engage, or claim that someone is in need of help. Don't fall for it! Keep your personal information as private as possible. Cyber criminals can also use social engineering with these details to try to manipulate you into skipping normal security protocols. For more information, please visit: https://www.dhs.gov/be-cyber-smart
- **Report any cybersecurity incident.** Report computer or network vulnerabilities to the National Cybersecurity Communications and Integration Center (NCCIC) at 1-888-282-0870, or at www.us-cert.gov/report. Forward phishing emails or websites to NCCIC at phishing-report@us-cert.gov.
- **Do your part in protecting critical infrastructure.** Our nation's critical infrastructure runs on the Internet. The systems that enable us to live our daily lives—the electrical systems, financial institutions, transportation systems, and more—are all dependent upon a digital ecosystem. As cybersecurity breaches continue to rise in frequency and scale, it is critical for all Americans to understand their role and take steps to protect our critical infrastructure. For more information on how you can help, please visit https://www.us-cert.gov/sites/default/files/publications/Week5TipCard-%20508%20compliant_0_0.pdf.
- **Use the National Initiative for Cybersecurity Careers and Studies (NICCS) website** for resources on all things related to the cybersecurity workforce, from K-12 curricula, to professional development tools, NICCS is a one-stop shop with something for everyone. Visit https://niccs.us-cert.gov for more information today.

Cybersecurity Resources

Below are some useful resources DHS suggests using to enhance your organization's events and promotion of Cybersecurity awareness both during October and throughout the year. Feel free to visit these site or use the text provided below in blogs, articles, and messaging to your organization and external audiences.

- The STOP. THINK. CONNECT.™ Campaign is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Cybersecurity is a shared responsibility. When we all take simple steps to be safer online, it makes using the Internet a more secure experience for everyone. For additional information on STOP. THINK. CONNECT.™, visit https://www.dhs.gov/stopthinkconnect.
- Powered by the U.S. Department of Homeland Security, the "BeCyberSmart" campaign is designed to inspire a younger generation of Americans to take responsibility for their own cyber safety. Learn about cybersecurity basics, common scams, and how to report cybersecurity incidents (as well as getting a first look at the new campaign website!) by visiting the campaign online.
- Looking for specific cybersecurity information? The National Initiative for Cybersecurity Careers and Studies (NICCS) tools and resources are available for anyone seeking to know more about the cybersecurity field, how to advance a cybersecurity career, and more. No matter what your life circumstances are, you can use this roadmap to help direct you to detailed information in specific cybersecurity areas of expertise.
- Increase your knowledge with cybersecurity training. The Federal Virtual Training Environment (FedVTE) is a free online, on-demand cybersecurity training system that is available at no charge for government personnel and Veterans. Managed by DHS, FedVTE contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis. Several courses align with a variety of IT certifications such as Network +, Security +, and Certified Information Systems Security Professional (CISSP). Sign up to take your first class today!
- Want to incorporate cybersecurity lessons into your classroom? The National Integrated Cyber Education Research Center (NICERC) provides hands-on professional development, free cybersecurity curricula to K-12 teachers, and programs and competitions to engage students in science, technology, engineering and math (STEM) disciplines. Teachers are provided lesson plans, teaching tips for facilitating class discussions, quizzes, worksheets, projects, etc. This curriculum can be used in after-school types of programs such as Girl Scouts/Boy Scouts, and Boys & Girls Clubs of America as well.
- The National Initiative for Cybersecurity Education (NICE) mission is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. A robust searchable version of the NICE Cybersecurity Workforce Framework allows you to view cybersecurity Work Roles, necessary tasks, knowledge, skills, and abilities (KSAs), as well as Capability Indicators that show likelihood to succeed in specific cybersecurity Work Roles.

- The DHS Office of Academic Engagement (OAE) works with school administrators, faculty, students, and the academic community on a range of issues. DHS formed the Office of Academic Engagement (OAE) in 2011 to strengthen the Department's relationship with the academic community in three functional areas of engagement, resilience, and outreach. Be sure to check out the OAE Resource Library.
- The DHS, National Protection and Programs Directorate, Office of Infrastructure Protection (IP) leads the coordinated national effort to secure critical infrastructure from all hazards by managing risk and enhancing resilience through collaboration with the critical infrastructure community. For additional information, visit Office of Infrastructure Protection (IP).
- Technology and threats evolve rapidly in today's ever-changing environment. The DHS Science and Technology Directorate (S&T) monitors those threats and capitalizes on technological advancements at a rapid pace, developing solutions and bridging capability gaps at a pace that mirrors the speed of life. S&T's mission is to deliver effective and innovative insight, methods, and solutions for the critical needs of the Homeland Security Enterprise.
- The nation's critical infrastructure provides the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, and the communication systems we rely on to stay in touch with friends and family. There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. PPD-21 identifies 16 critical infrastructure sectors at https://www.dhs.gov/critical-infrastructure-sectors.
- The National Cyber Security Alliance (NCSA) builds strong public/private partnerships to create and implement broad-reaching education and awareness efforts to empower users at home, work and school with the information they need to keep themselves, their organizations, their systems and their sensitive information safe and secure online and encourage a culture of cybersecurity. For NCSA recommended events, click: https://staysafeonline.org/events.

Communication Channels

The official hashtag for NCSAM 2018 is #CyberAware. Bring visibility to you and your organization's involvement during the month by leveraging this hashtag both before and during the month of October to promote and participate in NCSAM activities and events.

Social Media Communication

Below are suggested social media posts to promote NCSAM in your organization. DHS highly encourages you to post on your online communication channels throughout October.

- Stay connected during National Cybersecurity Awareness Month 2018! Follow @STOPTHNKCONNECT and @StaySafeOnline to ensure you are receiving all of the latest #CyberAware updates throughout October 2018!
- Prepare to be #CyberAware during National Cybersecurity Awareness Month 2018! Check out how you and your organization can get involved throughout October by visiting www.dhs.gov/ncsam
- NCSAM looks at how every employee – from interns to CEOs – have a responsibility for cybersecurity. #CyberAware #CyberMonth2018
- Free #cyberplanner available to #smallbiz from @FCC. Find it here: www.fcc.gov/cyberplanner #CyberAware
- Thwarting cyber-attacks at your organization demands constant vigilance and continuous assessment. Use the @DHS Critical Infrastructure Cyber Community (C-Cubed) Voluntary Program to learn how to improve cyber risk management processes. Learn more here: https://www.us-cert.gov/ccubedvp #CyberAware
- Cybersecurity is a cross-cutting, cross-sector problem, so we have got to tackle it together. Help us build a more secure cyber world by celebrating #CyberAware month with us this October! #CyberMonth2018 #Cybersecurity
- The demand for well-trained cyber pros is at an all-time high. Learn about careers in cyber at www.dhs.gov/cyber #CyberAware
- Build your #CyberCareers, take training courses and prepare for cybersecurity certifications with https://niccs.us-cert.gov/training/search and https://fedvte.usalearning.gov #CyberAware
- Tomorrow's cyber defenders are sitting in your classroom today, get them prepared. Learn more about DHS sponsored FREE K-12 cyber curricula here: https://nicerc.org #cybereducation
- Know what you need to succeed—check out the cybersecurity capability indicators, know the skills and knowledge needed to become a well-paid cyber pro! https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework #cyberworkforce

NCSAM 2018 Twitter Chat Schedule

Be sure to participate in the NCSAM 2018 weekly Twitter Chats. DHS and NCSA will discuss a number of topics related to this year's key messages and weekly themes. Follow @Cyber and chime in using #ChatSTC AND #CyberAware in your tweets.

- Oct. 04, 2018 at 3:00 P.M. EDT – Make Your Home a Haven for Online Safety
- Oct. 11, 2018 at 3:00 P.M. EDT – Millions of Rewarding Jobs: Educating for a Career in Cybersecurity
- Oct. 18, 2018 at 3:00 P.M. EDT – It's Everyone's Job to Ensure Online Safety at Work
- Oct. 25, 2018 at 3:00 P.M. EDT – Safeguarding the Nation's Critical Infrastructure

Sample Content

Consider highlighting NCSAM in your organization's communication by including a brief article in your newsletter or a post on your blog. To help get you started, here is an example of what you might want to include.

Option 1: Abbreviated Content

National Cybersecurity Awareness Month 2018

This October, the [Insert Department/Agency name] is joining with the Department of Homeland Security to raise cybersecurity awareness across the nation during National Cybersecurity Awareness Month (NCSAM). The overarching theme for NCSAM is **Cybersecurity is Our Shared Responsibility and We All Must Work Together to Improve our Nation's Cybersecurity.** Cybersecurity is not just the responsibility of governments, companies, groups, or individuals. Everyone shares the responsibility for cybersecurity – from the average smartphone user to a corporate CEO.

- Learn more here: https://www.dhs.gov/ncsam
- Follow and join the conversation using the hashtag #CyberAware

Option 2: Full Page Content

National Cybersecurity Awareness Month 2018

Americans are spending more time online than ever before. As more people use the Internet for online shopping, banking, financial management, and socializing, they also expose themselves to increased cyber risks. Online threats and cyber-attacks threaten the future of our national and economic security. Because cybersecurity is important to our Nation, the [Insert Department/Agency name] is joining with the Department of Homeland Security to raise cybersecurity awareness across the Nation during National Cybersecurity Awareness Month this October.

This year, National Cybersecurity Awareness Month (NCSAM) commemorates 15 years as an annual initiative to raise awareness about the importance of cybersecurity. NCSAM 2018 is a collaborative effort between government and industry to ensure every American has the resources they need to stay safer and more secure online, while increasing the resiliency of the Nation during cyber-threats.

To celebrate National Cybersecurity Awareness Month 2018, [Organization] is [Insert your organization's NCSAM events/efforts]

DHS's efforts this October will promote and emphasize several Key Messages, tied together by one overarching theme for the month: **Cybersecurity is Our Shared Responsibility and We All Must Work Together to Improve our Nation's Cybersecurity**. Cybersecurity is not just the responsibility of governments, companies, groups, or individuals. Everyone shares the responsibility for cybersecurity – from the average smartphone user to a corporate CEO. This October, and every day, follow these simple online safety tips from the DHS STOP. THINK. CONNECT.™ Campaign:

- **Enable stronger authentication.** Always enable stronger authentication for an extra layer of security beyond the password that is available on most major email, social media and financial accounts. Stronger authentication (e.g., multi-factor authentication that can use a one-time code texted to a mobile device) helps verify that a user has authorized access to an online account. For more information about authentication, visit the *Lock Down Your Login Campaign* at www.lockdownyourlogin.org.
- **Make your passwords long & strong.** Use complex passwords with a combination of numbers, symbols, and letters. Use unique passwords for different accounts. Change your passwords regularly, especially if you believe they have been compromised.
- **Keep a clean machine.** Update the security software, operating system, and web browser on all of your Internet-connected devices. Keeping your security software up to date will prevent attackers from taking advantage of known vulnerabilities.
- **When in doubt, throw it out.** Links in email and online posts are often the way cyber criminals compromise your computer. If it looks suspicious (even if you know the source), delete it.
- **Share with care.** Limit the amount of personal information you share online and use privacy settings to avoid sharing information widely.
- **Secure your Wi-Fi network**. Your home's wireless router is the primary entrance for cybercriminals to access all of your connected devices. Secure your Wi-Fi network, and your digital devices, by changing the factory-set default password and username.

Learn more about National Cybersecurity Awareness Month and how to protect yourself from threats online at www.dhs.gov/ncsam.

Frequently Asked Questions

Below are some of the most common questions that are asked about cybersecurity with answers that you can share with your organization to help explain NCSAM-related issues.

Critical infrastructure

- **Q: Where can we learn more about critical infrastructure?**
- **A:** Sign up for the DHS monthly cybersecurity bulletin to learn about the latest cybersecurity events, program updates, tools and resources from DHS and its partners with lots of information about critical infrastructure: https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new
- **Q: Where can I go to learn more about the NIST Cybersecurity Framework?**
- **A:** The NIST Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations in the U.S. can assess and improve their ability to prevent, detect, and respond to cyber-attacks. Visit NIST's website for information on the Cybersecurity Framework: https://www.us-cert.gov/ccubedvp/cybersecurity-framework. The website includes the Cybersecurity Framework V1.1 document, as well as additional resources such as an introduction to the Framework, FAQs, and even Online Learning modules to aid in understanding the Framework.

Cybercrime

- **Q: What is cybercrime?**
- **A:** We don't often consider whether or not the people we interact with online might be breaking the law. But legal wrongdoing is just as prevalent on the internet as it is in the physical world. Cybercrime is any crime, including theft, fraud, and even sometimes murder, which is committed electronically.
- **Q: Why should you care?**
- **A:** We all want a safer world to live in, and it's clear, now more than ever, that computers and other network-enabled devices are part of that world. Being safe on the computer is often very similar to being safe in your daily routine. You wouldn't leave your car unlocked in the middle of a crowded city – so why not apply those same safety principles to your online life?

Ransomware

- **Q: What is ransomware?**
- **A:** It's easy to forget sometimes how valuable the information we store on our computers and devices really is to us. Family photos, financial information, address books, homework assignments – so much of our lives is stored digitally! Ransomware is a type of malware in which the attacker encrypts the victim's data to make it as inaccessible as possible. Then, the hacker demands a ransom to release or unencrypt that information.
- **Q: Why should you care?**
- **A:** The fees extorted by cybercriminals through ransomware can be extreme or prohibitive – not to mention that there's no guarantee that your data will actually be returned to you after you pay! Luckily, there's a simple way to make yourself and your data resistant to ransomware attacks. In addition to keeping your software and antivirus programs up to date, regularly back up your system on the cloud or on an external hard drive. That way, you always have a spare copy of the information that's most important to you.

Physical Cyber Attacks

- **Q: What are physical cyber-attacks?**
- **A:** Cyber-attacks don't always have to come from the internet, and some malware can hide easily on some of the data storage devices we trust and use on a daily basis. Physical cyber-attacks use hardware, external storage devices, or other physical attack vectors to infect, damage, or otherwise compromise digital systems. The attack can hitch a ride on USB storage devices or flash drives, CDs, hard copies of video games, and Internet of Things devices such as smartphones, smart watches, and even signal devices such as key fobs.
- **Q: Why should you care?**
- **A:** These kinds of attacks are frighteningly versatile, very difficult to identify and detect, and painfully difficult – sometimes close to impossible – to remove. Always try to keep track of where your storage devices have been, and don't plug "lost-and-found" USB drives into your computer. Keep your personal and workplace data storage and other devices separate to avoid transferring malware from one system to another – just like washing your hands to prevent the flu from spreading!

Social Engineering

- **Q: What is social engineering?**
- **A:** Sometimes bad actors don't need computers to gain access to your information. Social Engineering is when bad actors gather commonly available information about you and things you care about in order to trick you into revealing information or giving unauthorized access to information systems. Social Engineering attacks

can be quite sophisticated, and are not always easy to recognize. This includes attacks such as Phishing, Swatting, and more.

- **Q: Why should you care?**
- **A:** Social engineering attacks don't require super powered programming skills to be successful. The information you post on social media and other sharing platforms may make you vulnerable to this attack vector, and it may be difficult to tell when you are being targeted.

Phishing

- **Q: What is phishing?**
- **A:** Phishing is a kind of Social Engineering attack in which a bad actor poses as a trusted or reputable source and sends fraudulent digital messages, such as emails, with the intent of manipulating individuals into revealing personal or protected information, or with the intent of gaining unauthorized access to a system through a download or link.
- **Q: Why should you care?**
- **A:** Phishing attacks are some of the most common – and most commonly successful – types of attacks. Learning how to recognize fraudulent messages by paying close attention to detail and never clicking on embedded hyperlinks, as well as remembering to report phishing attempts when you are targeted, are the best ways to defeat this kind of cyber-attack.

Swatting

- **Q: What is swatting?**
- **A:** Think Social Engineering is just for Phishing? Think again. Swatting is an attack centered around *location sharing*. Bad actors use your location to call the police, claiming that the victim has committed a serious crime. Sometimes, the intent behind these attacks are merely pranks – but the consequences are almost always severe.
- **Q: Why should you care?**
- **A:** Unlike many cyber-based attacks, Swatting has clear, physical, and immediate consequences. Imagine police raiding your home on a Swatting bomb threat tip! These attacks can easily result in injury and arrest, and sometimes even death to the victim. Your location is *your* business. Text or call friends the old fashioned way if you want to meet up, share vacation photos only after you've gotten safely home, and remember to turn off location services on your devices when you don't need them.

Cybersecurity Careers

- **Q: What training is available for individuals who want to expand their cybersecurity career?**
- **A:** The Department of Homeland Security has resources for individuals who need or want cybersecurity training to either begin or expand their cybersecurity career and professional skills.
    - The Federal Virtual Training Environment (FedVTE) provides free cybersecurity training to federal, state, local, tribal, and territorial government employees, U.S. active duty military, and Veterans. FedVTE, managed by DHS, contains over 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis. Courses range from beginner to advanced levels.
    - The National Initiative for Cybersecurity Careers & Studies (NICCS) Education and Training Catalog connects the public to more than 3,000 cybersecurity courses offered by organizations across the nation, and more courses are being added every day. With highly customizable search criteria, you can search by proficiency level, specialty area, and/or preferred providers. Additionally, the geospatial search function easily allows you to locate nearby training.

- **Q: Where can I go to learn more about the NICE Cybersecurity Workforce Framework?**
- **A:** The NICE Cybersecurity Workforce Framework provides a blueprint to categorize, organize, and describe cybersecurity work into Categories, Specialty Areas, Work Roles, tasks, and knowledge, skills, and abilities (KSAs).The NICE Workforce Framework provides a common language to talk about cybersecurity roles and jobs. Visit the NICCS website for information and to access additional tools and resources: https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

- **Q: What resources are available for small and midsize businesses (SMBs)?**
- **A:** To help business leaders get started, DHS has provided a list of top resources specially designed to help SMBs recognize and address their cybersecurity risks: https://www.us-cert.gov/ccubedvp/smb.
- **A:** The U.S. Small Business Administration (SBA) provides tools and resources to help SMBs increase cybersecurity resilience. Small Business Development Centers (SBDC) from states such as Michigan (Small Business Big Threat), Kansas, New York, and many others provide in-depth cybersecurity resources such as risk assessments, cybersecurity planning, and trainings for SMBs.

- **Q: Where can I go to learn more about cybersecurity workforce and education?**
- **A:** The National Initiative for Cybersecurity Careers and Studies (NICCS) is a one-stop shop for cybersecurity careers and studies. Visited by nearly 30,000 people monthly, NICCS houses cybersecurity training, formal education, and workforce development related resources. NICCS provides access to information ranging from the NICCS Education and Training Catalog, which connects the public to more than 3,000 cybersecurity courses offered across the nation, to the NICE Cybersecurity Workforce Framework (NICE Framework), which provides a common language to speak about cybersecuirty roles and jobs and helps define professional requirements in cybersecurity.

- **Q: What are some other fields that will lend themselves well to a cybersecurity career?**
- **A:** Veterans who have served and protected the nation are well-positioned to transition into the cybersecurity field. To learn more about training and career transition resources for Veterans, visit https://niccs.us-cert.gov/training/veterans.
- **A:** The cybersecurity field is growing and bringing not only technical jobs to the industry but a number of non-technical jobs as well. From marketing to law and everything in between, consider your existing job and how it may complement the cybersecurity field.
- **A:** Software Developers have a lot of the foundational skill sets recommended to be successful in the cybersecurity career field. With the right organization-provided training, other IT professionals or even non-technical employees can transition into the cybersecurity field.
- **A:** Most STEM fields can lend themselves well to a cybersecurity career due to the nature of critical thinking and communication skills required in STEM positions. Additionally, O*NET shares some necessary skills identified in the field as well: https://www.onetonline.org/link/summary/15-1122.00

- **Q: What exactly is the cybersecurity workforce gap and how big is it?**
- **A:** The cybersecurity workforce gap refers to the large amount of skilled individuals needed to fill open cybersecurity positions to respond to the ever-evolving threat landscape in the cybersecurity field.
    - The cybersecurity workforce gap is expected to reach 1.8 million by 2022, which is a 20% increase from 2015 predictions.[1]

[1] *(ISC)2, Center For Cyber Safety and Education. "2017 Global Information Security Workforce Study." White Paper. July 2017.* https://www.iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf