National Cybersecurity Awareness Month

October Marks The 15th Annual National Cybersecurity Awareness Month 3

2018 Week-By-Week Guide 5
Oct. 1-5: Make Your Home A Haven For Online Safety 5
Oct. 8-12: Millions Of Rewarding Jobs: Educating For A Career In Cybersecurity 7
Oct. 15-19: It’s Everyone’s Job To Ensure Online Safety At Work 9
Oct. 22-26: Safeguarding The Nation’s Critical Infrastructure 11

Holding a Partner Event 13

Additional NCSAM Information And Materials 14
October Marks the 15th Annual National Cybersecurity Awareness Month

Since 2004, National Cybersecurity Awareness Month (NCSAM) has represented a collaborative effort between government, nonprofit and industry to ensure that all Americans have the information they need to stay safer and more secure online. Co-led by the National Cyber Security Alliance (NCSA) and U.S. Department of Homeland Security (DHS), NCSAM has grown exponentially – reaching consumers and organizations nationwide and encouraging all internet users to be #CyberAware.

Today, NCSAM is part of the nation’s cultural fabric – sharing space in October alongside Halloween and pumpkin spiced lattes – with industry, schools, government, nonprofits and individuals nationwide participating in the month as Champions to officially show their support.

In 2017, over 1,000 organizations registered as Champions to spread the word about online safety at home, at work and in the community and by hosting NCSAM Partner Events and we appreciate your participation in NCSAM as a 2018 Champion.

As we ramp up toward the fall elections, the 15th annual NCSAM will include a full week dedicated to critical infrastructure – from the power grid to transportation to smart cities and elections. The month will also provide guidance for consumers about how to best protect their digital lifestyles – at home, at work and on the go – and remind everyone that protecting the internet is “Our Shared Responsibility.” In addition, NCSAM 2018 will shine a spotlight on the critical need to build a strong, cybersecure workforce to help ensure families, communities, businesses and the country’s infrastructure are better protected.

“We’ve come a long way in 15 years – there is no longer a line between our online and offline lives. Our homes, societal well-being, economic prosperity and nation’s security all involve the internet. National Cybersecurity Awareness Month reminds us that the internet is a shared resource and responsibility – we are all digital citizens and must take steps to secure ourselves at home, on the job or on the go.”

— Russ Schrader
Executive Director, NCSA

#CyberAware
Our Shared Responsibility

NCSAM’s annual overarching theme is “Our Shared Responsibility” because no individual, business or government entity is solely responsible for securing the internet, and everyone must play a role in protecting their part of cyberspace, including the devices and networks they use.

If everyone does their part – implementing stronger security practices, raising community awareness, educating vulnerable audiences or training employees – our interconnected world will be safer, more resistant from attacks and more resilient if an attack occurs.

STOP | THINK | CONNECT™

Underpinning NCSAM is STOP. THINK. CONNECT™, the global online safety education and awareness campaign co-founded by NCSA and the Anti-Phishing Working Group (APWG) and supported by DHS’ federal engagement.

STOP. THINK. CONNECT™ encourages all internet users – whether young people surfing the web, consumers shopping online or businesses conducting transactions – to take safety and security precautions when connected. Its message is simple: STOP: make sure security measures are in place. THINK: about the consequences of your actions and behaviors online. CONNECT: and enjoy the internet. The campaign also shares basic, actionable steps internet users should take, such as keeping a clean machine, owning your online presence and protecting your personal information. These core messages have been translated into five languages: Spanish, French, Portuguese, Japanese, and Russian.

Week 1: October 1-5
Make Your Home a Haven for Online Safety

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.

Statistics: Connected Homes and Cybersecurity

+ The number of smart homes in North America is expected to hit 73 million by 2021, making up more than 50% of all households.²

+ More than 1 million children — or 1.48% of minors — were victims of identity theft or fraud in 2017. Two-thirds of those affected were age seven or younger.³

+ Both parents and teens are concerned about online security, according to a 2017 NCSA survey. Among their top fears: someone accessing a teen’s account without permission (teens 41% vs. parents 41%); someone sharing a teen’s personal information about them online (teens 39% vs. parents 42%); and having a teen’s photo or video shared that they wanted private (teens 36% vs. parents 34%).⁴

+ Additionally, 34% of teens indicate that they are the most knowledgeable person about cybersecurity in the family – followed by 24% who think dad is, and 18% who think mom is.⁵

#CyberAware Thought Starters:

+ Kids: The New Victims of ID Theft
+ Home, Hacked Home. Tips to Securing Your Connected Household
+ How to Opt in/Opt Out of Smart Home Security and New Devices
+ Tips to Protect Your Family’s Privacy When Buying Connected Toys
+ Smart Fridges, Thermostats and Toys – Oh My!
+ Basic Cyber Safety Begins at Home
+ How to Have the “Tech Talk” with Your Teen
+ Are You an Easy Target? 5 Ways Consumers Are Vulnerable to Breaches
+ Public WiFi and Public Charging Stations: A Convenience or a Cost?

Week 1: #CyberAware Tips to Protecting Yourself and Your Family at Home

**Lock down your login:** Your usernames and passwords are not enough to protect key accounts like email, banking and social media. Strengthen online accounts and use strong authentication tools – like biometrics, security keys or a unique, one-time code through an app on your mobile device – whenever offered. [Read more.]

**Back it up:** Protect your valuable work, music, photos and other digital information by making an electronic copy and storing it safely. If you have a copy of your data and your device falls victim to ransomware or other cyber threats, you will be able to restore the data from a backup.

**Pay attention to the Wi-Fi router in your home:** Use a strong password to protect the device, keep it up to date and name it in a way that won’t let people know it’s in your house.

**Keep a clean machine:** Keep all software on internet-connected devices – including personal computers, smartphones and tablets – current to reduce risk of infection from ransomware and malware.

**Personal information is like money. Value it. Protect it.:** Information about you, such as purchase history or location, has value – just like money. Be thoughtful about who gets that information and how it is collected by apps, websites and all connected devices.

**Share with care:** Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it might affect you or others.

**Simple Ways to Participate in Week One:**
+ Turn on Multi-Factor Authentication to protect your financial, email and social media accounts.
+ Update your software and turn on automatic updates to protect your home network and personal devices.
+ Participate using #CyberAware on social media and include your friends and family in the conversation (head to StaySafeOnline.org to find a wide range of shareable, funny memes, graphics and NSCAM posts).

**Key Resources:**
+ Stay Safe Online: [https://staysafeonline.org/](https://staysafeonline.org/)
+ Identity Theft Resources Center: [https://www.idtheftcenter.org/](https://www.idtheftcenter.org/)
+ Department of Homeland Security, STOP, THINK, CONNECT.™: [https://www.dhs.gov/stopthinkconnect](https://www.dhs.gov/stopthinkconnect)
Week 2: October 8-12

Millions of Rewarding Jobs: Educating for a Career in Cybersecurity

A key risk to our economy and security continues to be the shortage of cybersecurity professionals to safeguard our ever-expanding cyber ecosystem. Raising the next generation of interested and capable cybersecurity professionals is a starting point to building stronger defenses. There are limitless opportunities to educate students of all ages – from high school into higher education and beyond – on the field of cybersecurity as they consider their options. In addition, veterans and individuals who are looking for a new career or re-entering the workforce should explore the multitude of well-paying and rewarding jobs available.

Week 2 will address ways to motivate parents, teachers and counselors to learn more about the cybersecurity field and how to best inspire students and others to seek highly fulfilling cybersecurity careers.

#CyberAware Thought Starters:
+ Veterans Who Are Making A Mark In Cybersecurity
+ It Has Millions Of Job Openings And Pays Well: Why You Should Pursue A Career In Cybersecurity
+ Guiding kids into careers in cybersecurity
+ May the Cyberforce be with you: More Millennials Needed to Fill Cyber Jobs
+ You Don’t Need To Be a Techie to Work in Cybersecurity
+ 5 Universities Developing the Cyber Workforce of the Future
+ How to Become a White Hat Hacker
+ Stand Up to Cybercrime with a Cybersecurity Degree

Statistics: Building the Cybersecurity Workforce

+ Cybersecurity job forecasts have been unable to keep pace with the dramatic rise in cybercrime, which is predicted to cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.⁶

+ The Bureau of Labor Statistics predicts a steep 28% growth rate for cybersecurity positions between 2016 and 2026 — that’s 300% higher than the prediction for all occupations. Moreover, Cybersecurity Ventures predicts there will be 3.5 million cybersecurity job openings by 2021.⁷

+ The median salary for information security analyst was $95,510 in 2017. That’s above the $84,580 average for other computer-related positions and well more than twice the national median salary for all U.S. jobs ($37,690).⁸

+ 40% of millennials internationally say that their parents are a primary source for career advice and 57% of millennials are confident in their parents’ ability to guide them in pursuing a cybersecurity career.⁹

+ From 2013 to 2017, the number of U.S. teachers who talked to their students about cybersecurity careers tripled.¹⁰

⁶ https://cybersecurityventures.com/jobs/

There will be 3.5 million Cybersecurity job openings by 2021.
Week 2: #CyberAware Tips for Parents, Teachers and Industry Professionals

Volunteer at school, an after-school program, Boys & Girls Club, or community workshops to teach kids about online safety and cybersecurity careers.
+ Check out NCSA’s online safety resources for ideas on what topics to cover and materials you can use.

Expose students to opportunities in the field of cybersecurity by hosting an open house at your company to talk about what your cybersecurity department does.

Work with your schools or community-based organizations to create an internship program for hands-on learning.

Inspire students to learn about cybersecurity by mentoring a team in a cyber challenge or hosting events and after-school programs.
+ Check out CyberPatriot, the national youth cyber education program created to inspire students toward careers in cybersecurity or other science, technology, engineering and mathematics (STEM) disciplines.

As a parent, learn about the “educational steps” to a career in cybersecurity and about community organizations that host cyber camps to educate kids about internet safety and security.
+ Visit GenCyber for information on cyber camps held across the country. And check out NCSA’s Parent Primer for Guiding Kids to Careers in Cybersecurity.

Simple Ways to Participate in Week Two:
+ Talk to your kids. For useful tips, download NCSA’s Parent Primer for Guiding Kids to Careers in Cybersecurity.
+ Become a cyber influencer. Share your career story on social media using #CyberAware.
+ Inspire young people by being a mentor in the workplace or at local schools.

Key Resources:
+ Cyber Patriot: https://www.uscyberpatriot.org/
Week 3: October 15-19

It’s Everyone’s Job to Ensure Online Safety at Work

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 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. NCSA’s CyberSecure My Business™ will shed light on how small and medium-sized businesses can protect themselves, their employees and their customers against the most prevalent threats.

Statistics: Small Businesses are Increasingly Targeted by Hackers

+ Small and medium-sized businesses (SMBs) are gaining the attention of hackers. A 2018 Verizon Data Breach Report showed that 58% of cybercrime victims identified as small businesses.¹¹

+ In 2017, cyber attacks cost small and medium-sized businesses an average of $2,235,000 and the percentage of small businesses that have experienced a cyber attack in the past 12 months is up from 55% in 2016 to 61% in 2017.¹²

+ The Better Business Bureau found that more than half of small businesses would be unprofitable within a month if they were to lose permanent access to their essential data.¹³

+ Approximately nine out of ten small businesses report that they have some cybersecurity measures in place, with the most common ones being 1) antivirus protection, 2) firewall protection and 3) employee education.¹⁴

#CyberAware Thought Starters:

+ How the New NIST Small Business Cybersecurity Act will Impact your Company
+ Why Hackers Love Small Business
+ 5 Cybersecurity Tips That Can Save Your Business
+ Your Employees: Are They Your Best Assets or Your Biggest Cybersecurity Risk?
+ How to Establish a Culture of Cybersecurity at Work
+ Why Cyber Safety Training is the Best Training Your Employees Can Receive
+ Who Me? Why You Don’t Need to Be a Techie to Work in Cybersecurity

Week 3: #CyberAware Tips for Employers and Their IT Teams

Identify your digital “crown jewels:” Crown jewels are the data without which your business would have difficulty operating and/or the information that could be a high-value target for cybercriminals.

Protect your assets: Ultimately, your goal is to build a culture of cybersecurity that includes employees knowing how to protect themselves and the business and understanding the cyber risks as your business grows or adds new technologies or functions.

Be able to detect incidents: We have fire alarms in our businesses and homes that alert us to problems. In cybersecurity, the more quickly you know about an incident, the more quickly you can mitigate the impact and get back to normal operations.

Have a plan for responding: Having a recovery plan created before an attack occurs is critical. Make and practice an incident response plan to contain an attack or incident and maintain business operations in the short term.

Quickly recover normal operations: The goal of recovery is to move from the immediate aftermath of a cyber incident to full restoration of normal systems and operations. Like the response step, recovery requires planning. Recovery is not just about fixing the causes and preventing the recurrence of a single incident. It’s about building out your cybersecurity posture across the whole organization (not just the IT person or group), including increasing the focus on planning for potential future events.

Simple Ways to Participate in Week Three:
+ Join NCSAM as an SMB Champion, sign up for the CyberSecure My Business newsletter or sign up as an ongoing STOP.THINK.CONNECT.TM partner.
+ Register for a CyberSecure My Business Event. View a schedule of events here.
+ Stay Up to Date on the Latest Scams but Signing up for Scam Alerts put out by the Federal Trade Commission and Better Business Bureau.

Key Resources:
+ SMB Cybersecurity Awareness Toolkit
+ CyberSecure My Business: https://staysafeonline.org/cybersecure-business/
+ NIST Cybersecurity Framework: https://www.nist.gov/cyberframework
Week 4: October 22-26

Safeguarding the Nation’s Critical Infrastructure

Our day-to-day life depends on the country’s 16 sectors of critical infrastructure, which supply food, water, financial services, public health, communications and power along with other networks and systems. A disruption to this system, which is operated via the internet, can have significant and even catastrophic consequences for our nation.

Week 4 will emphasize the importance of securing our critical infrastructure and highlight the role the public can play in keeping it safe. In addition, it will lead the transition into November’s Critical Infrastructure Security and Resilience Month, which is spearheaded by the U.S. Department of Homeland Security.

Statistics: Critical Infrastructure is at Risk

+ The number of attacks reported to the U.S. Department of Homeland Security’s ICS-CERT cybersecurity response team has gone up almost 400% since 2013 – jumping from 73 to 290 incidents in 2016.15

+ Of the 290 incidents reported to the ICS-CERT cybersecurity response team in 2016:
  - 63 were in the Critical Manufacturing Sector
  - 62 in the Communications Sector
  - 59 in the Energy Sector16

+ The number one risk to critical infrastructure? Spear phishing, which represented 26% of incidents reported to the DHS ICS-CERT.17

#CyberAware Thought Starters:
+ How Hackers are Infiltrating our Election System
+ Going Dark: Challenges to Protecting Our Nation’s Power Grid
+ Cities Under Siege: What to do When Municipalities are Cyber Targets
+ Designing the Secure, Smart Cities of Tomorrow
+ Can One Phishing Attack Bring Down an Entire City?
+ Airplanes and Railroads: When Transportation is Hacked


There has been a 400% rise in reported critical infrastructure attacks from 2013 to 2016.
**Week 4: #CyberAware Tips for Critical Infrastructure Professionals**

**When in doubt, throw it out:** Links in email, tweets, posts and online advertising are often how cybercriminals try to access your information. If it looks suspicious, even if you know the source, it’s best to delete or, if appropriate, mark it as junk.

**Safer for me, more secure for all:** If everyone does their part – implementing stronger security practices, raising community awareness, educating vulnerable audiences or training employees – our interconnected world will be safer, more resistant from attacks and more resilient if an attack occurs.

**Lock down your login:** Your usernames and passwords are not enough to protect key accounts like email, banking and social media. Strengthen online accounts and use strong authentication tools – like biometrics, security keys or a unique, one-time code through an app on your mobile device – whenever offered.

**Keep a clean machine:** Keep all software on internet-connected devices – including personal computers, smartphones and tablets – current to reduce risk of infection from ransomware and malware.

**Simple Ways to Participate in Week Four:**
+ Become a Cyber Influencer on social media and hashtag memes and posts with #CyberAware

**Key Resources:**
+ ICS-CERT: [https://ics-cert.us-cert.gov/](https://ics-cert.us-cert.gov/)
The following shares basic criteria for organizations to use in order to align their events with consistent, harmonized messaging in support of NCSAM.

**Use NCSAM Logo on Promotional Materials**
+ Event Invitations
+ Event Signage/Backdrops
+ Press Materials and/or Announcement

**Online**
+ Post Event Listing on NCSA’s Site [https://staysafeonline.org/ncsam/events](https://staysafeonline.org/ncsam/events)
+ Include Link to NCSA’s Site in Event Collateral [https://staysafeonline.org/ncsam](https://staysafeonline.org/ncsam)
+ Visit [https://www.dhs.gov/ncsam](https://www.dhs.gov/ncsam) for Additional NCSAM Resources and Valuable Information from DHS

**Social Media**
+ Use #CyberAware
+ Promote NCSAM throughout October
+ Sample [social media posts](https://www.dhs.gov/ncsam) and [graphics](https://www.dhs.gov/ncsam) to help you promote your Champion status and NCSAM 2018 on social media

**During Event**
+ Showcase NCSAM’s Core Theme: The internet is a shared resource, and securing it is “Our Shared Responsibility.”
+ Other “Fast Facts”:
  + NCSA and DHS co-lead NCSAM
  + October 2017 marks the 15th NCSAM
  + Address “why” NCSAM is critical

**Support Details/Information**
+ When possible, tie event to the NCSAM Weekly theme/topic
+ Share/distribute STOP. THINK. CONNECT.™ resources
Additional NCSAM Information and Materials

National Cyber Security Awareness Month:
+ https://staysafeonline.org/ncsam

NCSAM Champion Portal:
+ https://staysafeonline.org/ncsam/ncsam-champion/ncsam-champion-signup/

STOP. THINK. CONNECT.™ website:
+ https://stopthinkconnect.org/

About the National Cyber Security Alliance
NCSA is the nation’s leading nonprofit, public-private partnership promoting cybersecurity and privacy education and awareness. NCSA works with a broad array of stakeholders in government, industry and civil society. NCSA’s primary partners are DHS and NCSA’s Board of Directors, which includes representatives from ADP; AT&T Services Inc.; Bank of America; CDK Global, LLC; CertNexus; Cisco; Cofense; Comcast Corporation; ESET North America; Facebook; Google; Intel Corporation; Marriott International; Mastercard; Microsoft Corporation; Mimecast; NXP Semiconductors; Raytheon; Salesforce; Symantec Corporation; Visa and Wells Fargo. NCSA’s core efforts include National Cyber Security Awareness Month (October); Data Privacy Day (Jan. 28); STOP. THINK. CONNECT.™, the global online safety awareness and education campaign co-founded by NCSA and the Anti-Phishing Working Group with federal government leadership from DHS; and CyberSecure My Business™, which offers webinars, web resources and workshops to help businesses be resistant to and resilient from cyberattacks. For more information on NCSA, please visit staysafeonline.org/about-us/overview/.

About the Department of Homeland Security
The Department of Homeland Security has a vital mission: to secure the nation from the many threats we face. This requires the dedication of more than 240,000 employees in jobs that range from aviation and border security to emergency response, from cybersecurity analyst to chemical facility inspector. Our duties are wide-ranging, and our goal is clear - keeping America safe. For more information, visit https://www.dhs.gov/about-dhs.