2017 CHAMPION BACKGROUNDER

National Cyber Security Awareness Month

2017 CHAMPION BACKGROUNDER

CyberAware
National Cyber Security Awareness Month

Launched in 2004 and actively supported annually in October, National Cyber Security Awareness Month (NCSAM) was created as a collaborative effort between government and industry to ensure that all Americans have the information they need to stay safer, more secure and protect their personal information online.

Since its inception under the leadership of the U.S. Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA), NCSAM has grown exponentially, reaching consumers, industry, government, academia and nonprofit organizations nationwide and encouraging all internet users to be #CyberAware.

Each week in October is dedicated to a timely topic of importance to consumers and businesses – bringing widespread attention to critical cybersecurity issues, such as the looming cyber workforce shortage, and the impact of emerging technologies and connected devices on Americans’ security and critical infrastructure.

2017 marks the 14th year of NCSAM!

Today, the month is recognized not only in the U.S. but internationally. This year — and for the first time ever — NCSAM will kick off with a global launch in Washington, D.C. at the Organization of American States on Oct. 3 – livestreamed and translated into multiple languages so digital citizens around the world can join in and be reminded that the internet is a shared resource, and securing it is “Our Shared Global Responsibility.”
Cybersecurity has remained front page news for much of 2017. From global hacks to state-sponsored threats to the influx of concerns around connected cities, homes and devices, cybersecurity and digital privacy is now an issue for everyone and every business.

2017 By The Headlines

“Hotel Guests at Risk After New Data Breach” — AZ Family

“Cyberattack Hits Ukraine Then Spreads Internationally” — The New York Times

“U.S. Hospitals Have Been Hit By The Global Ransomware Attack” — Recode

“Stuffed Toys Leak Details of Half a Million Users” — Vice

“Another Big Malware Attack Ripples Across The World” — CNN

“Data Breach Exposes Millions of Customers Records” — Time Magazine

“School Districts Become Cybercrime Targets” — Government Tech

“Hollywood Hacking Goes Beyond Piracy” — The Vindicator

“Facebook Meme May Reveal More than Musical Tastes” — The New York Times
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 (Canadian), Portuguese (Brazilian), Japanese and Russian — with several more in the works.
The NCSAM Champion program is a way for individuals and organizations to officially show support. Champions represent those dedicated to promoting a safer, more secure and more trusted internet.

**In 2016, 870 Champion organizations** helped spread the word about online safety and security at work, at home and in their local communities.

As a NCSAM Champion you should have received a toolkit that includes a wide variety of resources, such as sample social media content, recommendations for getting involved at work and a press release template, to help promote the month.

**To become a Champion,** [Begin here](#) and pledge to take action in your community.

### Getting Involved in NCSAM 2017

NCSAM 2016 was a breakout year - far exceeding the scope and reach of the month in previous years. From 2015 to 2016, NCSAM’s brand exposure witnessed an incredible jump, increasing total exposure by over 70%.

### 2016 Success

During the months of September, October and November:

- **2016:** Total uses of #CyberAware and #NCSAM: 78,732
- **2016:** Registered Champions: 870 organizations and 432 individuals
- **2015:** Total uses of #CyberAware and #NCSAM: 61,804
- **2015:** Registered Champions: 700 organizations and 283 individuals
- **2014:** Total uses of #NCSAM: 43,000
- **2014:** Registered Champions: 405 organizations

To date, NCSAM 2017 has **MORE THAN 700 CHAMPIONS** that share messaging and support events and activities throughout the month.

NCSAM Champions include:

+ Companies and organizations of all sizes
+ Schools and school districts, colleges and universities
+ Nonprofits
+ Government organizations
+ Individuals
Getting Involved in NCSAM 2017

Overview of 2017 NCSAM Weekly Themes
+ **Week 1:** OCT 2-6: STOP. THINK. CONNECT.TM: Simple Steps to Online Safety
+ **Week 2:** OCT 9-13: Cybersecurity in the Workplace is Everyone’s Business
+ **Week 3:** OCT 16-20: Today’s Predictions for Tomorrow’s Internet
+ **Week 4:** OCT 23-27: The Internet Wants You: Consider A Career in Cybersecurity
+ **Week 5:** OCT 30-31: Building Resilience in Critical Systems

Weekly Support Materials
In order to help you get involved, the NCSA team will provide Champions with a range of assets and collateral that help you to get involved, which drive further engagement around the month.
+ Press release
+ Infographic
+ Memes
+ Sample social media posts
+ Events
+ Research
+ #ChatSTC Twitter chat
+ Collateral email

Ways To Get Involved Throughout The Month

**Circulate or Post Tips and Advice**
+ Post short messages or online safety tips on internal message boards during the month of October.
+ Hang the NCSAM poster around the office about how employees can help to protect personal information and to help create awareness about the month. [Download the poster here.](#)

**Hold Programs and/or Events**
+ Host a lunch & learn at work in October to talk about online safety or one or more of the weekly NCSAM themes.
+ Challenge colleagues to a department-wide competition: explain what cybersecurity means to the organization and the critical role staff play
+ Organize a volunteer day with local schools to teach young people about cybersecurity and online safety using ready-to-use teaching materials and lesson plans. [Find them here.](#)
+ Award certificates of achievement to employees who practice strong cybersecurity. [Use our template.](#)

**Get Involved on Social Media**
+ Share tips and resources on social media using the hashtag #CyberAware
+ Download our social media content (memes, infographics, etc.) to share leading up to and during October
+ Follow NCSA on [Facebook](#) and [Twitter](#)

[Join The #ChatSTC](#)
+ Participate in one (or more!) of the #ChatSTC Twitter chats every Thursday in October at 3 p.m. EDT/noon PDT and Wednesday, Nov. 1 for week 5’s chat.
Week 1: October 2-6

STOP. THINK. CONNECT.™: Simple Steps to Online Safety

Staying safe and secure online is our shared responsibility. Week 1 focuses on easy-to-follow, actionable advice for everyone. It is critical for anyone using the internet to continually learn about and consistently practice good cybersecurity habits. To better protect yourself, you should secure your home networks and mobile devices and take time to learn how to use the internet more safely, securely and responsibly. Week 1 will address the top consumer cyber concerns (identity theft, ransomware and the Internet of Things), provide simple steps to protect against these concerns, and teach you what to do if you fall victim to cybercrime.

#CyberAware Topics to Explore

+ STOP. THINK. CONNECT.™: Most Common Consumer Cyber Mistakes [View resource 1, View resource 2].
+ Beware of Ransomware – Tips to Protect Your Digital Life
+ How to Have the “Tech Talk” with Your Teen [View resource].
+ Are You an Easy Target? 5 Ways Consumers Are Vulnerable to Breaches
+ Kids: The New Victims of ID Theft [View resource].
+ Does Your Family Have a Chief Cybersecurity Officer?
+ Public WiFi and Public Charging Stations – A Convenience or a Cost? [View resource].

NCSA and DHS EVENT: Tuesday, Oct. 3: Global Launch at the Organization of American States in Washington, D.C.

The Organization of American States (OAS) will officially host the global launch of Cyber Security Awareness Month, partnering with NCSA and DHS. The event will focus on online security from an international perspective and how to best work together on cybersecurity issues today and in the future. Topics such as the workforce, IoT and small and medium-sized businesses will be addressed under the “shared global responsibility” umbrella theme. The event will feature strong international participation, with high-level, VIP speakers and attendees representing DHS, other government entities, public and private industry, embassies and more. The event will be livestreamed for widespread, international engagement.

#ChatSTC Twitter Chat: Thursday, Oct. 5, 3:00 p.m. EDT/noon PDT

To see a list of other NCSAM events, click here!
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.

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.

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.

Own your online presence: Set the privacy and security settings on websites to your comfort level for information sharing. It is OK to limit how and with whom you share information.

Need more information? Go to page 22 for the latest research and statistics on top consumer concerns, including identity theft, ransomware and the Internet of Things (IoT).

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

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.

Personal information is like money. Value it.
Week 2: October 9-13

Cybersecurity in the Workplace is Everyone’s Business
Whatever your place of business — whether it’s a large or small organization, healthcare provider, academic institution or government agency – creating a culture of cybersecurity from the break room to the board room is essential and a shared responsibility among all employees.

Every organization needs a plan for employee education, training and awareness that emphasizes risk management, resistance and resilience. Week 2 will showcase how businesses of all types can protect themselves, their employees and their customers against the most common cyber threats. The week will also look at resources to help organizations strengthen their cyber resilience, including the National Institute of Standards and Technology Cybersecurity Framework.

#CyberAware Topics to Explore
+ Your Employees: Are They Your Best Assets or Your Biggest Cybersecurity Risk? View resource.
+ Why Hackers Love Small Business View resource.
+ 5 Cybersecurity Tips That Can Save Your Business
+ How to Establish a Culture of Cybersecurity at Work
+ Why Every Company Should Have a NCSAM Game Plan View resource.
+ Why Cyber Safety Training is the Best Training Your Employees Can Receive

NCSA and DHS EVENT: Tuesday, Oct. 10: Insights on Cybersecurity for Electric Utilities Hosted by NRECA in Arlington, VA
The National Rural Electric Cooperative Association (NRECA) — a membership organization of 900+ consumer-owned electric utilities — will hold a SMB-focused event and workshop on Oct 10. Thought leaders from government and industry will come together for this event, which shines a light on best practices for business and industry.

#ChatSTC Twitter Chat: Thursday, Oct. 12, 3:00 pm. EDT/noon PDT

To see a list of other NCSAM events, click here!

Week 2 #CyberAware Advice for Businesses:
+ Identify your digital “crown jewels”
+ Protect your assets
+ Be able to detect incidents
+ Have a plan for responding
+ Quickly recover normal operations

Among small to mid-sized organizations that experienced a successful ransomware infiltration, 20% reported that they had to cease business operations immediately, and 12% lost revenue. Osterman Research

Time is money: Ransomware demands are not the small business killer, downtime is. 57% of small businesses experienced nine or more hours of downtime, with some organizations down for more than 100 hours because of the infection. Osterman Research

NEED MORE INFORMATION?
To learn more about these recommendations developed by the National Institute of Standards (NIST), visit here. To learn more about the top risks facing businesses, including ransomware and extortion, IoT security threats and insider threats, go to page 25.
Week 3: October 16-20

Today’s Predictions for Tomorrow’s Internet
Take a look into our future through the lens of the connected internet and identify strategies for security, safety and privacy while leveraging the latest technology. With the explosion of digital interconnectivity, it is critical to explore everyone’s role in protecting our cyber ecosystem.

Smart cities, connected healthcare devices, digitized records and smart cars and homes have become our new reality. Week 3 will remind you that your personal data is the fuel that makes smart devices work. While there are tremendous benefits to massive interconnectivity, it is critical to understand how to use cutting-edge technology in safe and secure ways.

#CyberAware Topics to Explore
+ Connected Cars, Fridges and Toys, Oh My! Tips to Shore Up Your Home from Hackers View resource.
+ Artificial Intelligence and Machine Learning: Cybersecurity Friend or Foe?
+ When your Toaster Talks to your Smartphone: The Future of the Internet
+ Top Tips to Keep Hackers Away View resource.
+ My Car’s Been Hacked! Protecting Yourself and Your Connected Vehicle

NCSA and DHS EVENT: Monday, Oct. 16: NCSA and Nasdaq Cybersecurity Summit and Closing Bell Ceremony in New York, NY
From smart cities to autonomous cars to connected coffee makers and healthcare devices, future technologies are booming worldwide. This massive inter-connectivity expands our ability to gain insight about our global societies and who we are. This unprecedented phenomenon also provides countless opportunities for bad actor exploits. Will artificial intelligence, machine learning, standards or even authentication provide the solutions to a safer and more secure connected world? Industry leaders will debate these issues and more at the NCSA and Nasdaq Cybersecurity Summit.

#ChatSTC Twitter Chat: Thursday, Oct. 19, 3:00 p.m. EDT/noon PDT

To see a list of other NCSAM events, click here!

NEW NEWS: Watch for the Microsoft/NSCA’s 2017 “Keeping Up with the Generation App” study.
Learn how to safeguard your IoT devices:
Protecting devices like wearables and smart appliances can be different than securing your computer or smartphone. Research how to keep an IoT device secure before you purchase it, and take steps to safeguard your device over time.

Own your online presence:
Understand what information your devices collect and how it’s managed and stored – and set the privacy and security settings on devices to your comfort level for information sharing.

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.

Research before you buy:
Before adopting a new smart device, do your research to make sure others have had positive experiences from a security and privacy perspective.

Delete when done:
Many of us download apps for specific purposes or have apps that are no longer useful or interesting to us. It’s good security practice to delete apps you no longer use.

Lock down your login:
Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are not enough to protect key accounts like email, banking and social media. Read more.

Need more information? Visit page 24 and 26 to find IoT research on consumers and business.
Week 4: October 23-27

The Internet Wants You: Consider a Career in Cybersecurity

A key risk to our economy and security is the shortage of cybersecurity professionals to protect our extensive networks. Growing the next generation of a skilled cybersecurity workforce — as well as training those already in the workforce — is a starting point to building stronger defenses.

According to a study by the Center for Cyber Safety and Education, there will be a shortage of 1.8 million information security workers by 2022. It is essential that we graduate students entering the workforce to fill the vast number of positions available and use technology safely, securely, ethically and productively. Week 4 will encourage students and professionals to explore cybersecurity as a viable and rewarding profession. Key influencers – such as parents, teachers, guidance counselors and state and local officials – will learn more about this growing field and how to engage youth in pursuing cybersecurity careers.

#CyberAware Topics to Explore

+ Cybersecurity: One of the Fastest Growing Professions with a Huge Skills Gap View resource.
+ Who Me? Why 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

NCSA and DHS EVENT: Tuesday, Oct. 24: Organization of American States– CITI/Cyber Workforce Event in Miami

Florida International University will conduct a training workshop – in partnership with Citibank – targeting students and other groups to learn more about cybersecurity and its many different career options.

#ChatSTC Twitter Chat: Thursday, Oct. 26, 3:00 p.m. EDT/noon PDT

To see a list of other NCSAM events, click here!
Volunteer at school, an afterschool program, boys and girls clubs and community workshops to teach kids about online safety and cybersecurity careers. Check out NCSA’s online safety resources for ideas on what 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.

Inspire students to learn about cybersecurity by mentoring a team in a cyber challenge or hosting events and afterschool 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.

Work with your schools or community-based organizations to create an internship program for hands-on learning.
Week 5: October 30-31

Protecting Critical Infrastructure from Cyber Threats
The systems that support our daily lives – such as electricity, financial institutions and transportation – are increasingly dependent upon the internet. Building resilience in critical infrastructure is crucial to our national security. Week 5 will look at how cybersecurity relates to keeping our traffic lights, running water, phone lines and other critical infrastructure secure.

#CyberAware Topics to Explore
+ The Critical Importance of Protecting Our 16 Sectors of Critical Infrastructure View resource.
+ How a Cyber Attack on Our Critical Infrastructure Would Impact Our Daily Lives

Top #CyberAware Tips:

Lock down your login: Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are not enough to protect key accounts like email, banking and social media. Read more.

Keep a clean machine: Keep all software on internet-connected devices – including PCs, smartphones and tablets – up to date to reduce risk of infection from malware.

When in doubt, throw it out: Cybercriminals often use links in email, social posts and texts to try to steal your personal information. Even if you know the source, if something looks suspicious, delete it.

Safer for me, more secure for all: What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.

#ChatSTC Twitter Chat: Wednesday, Nov. 1, 3:00 p.m. EDT/noon PDT
Host a National Cyber Security Awareness Month Partner Event

Champions are invited to host NCSAM Partner Events and integrate NCSAM branding and themes into their event programming.

**Partner Event Criteria**
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 or Press Materials and/or Announcement

**Social Media**
+ Use #CyberAware

**Online**
+ Post Event Listing on NCSA’s Site
+ Include this link to NCSA’s Site in Event Collateral
+ Visit here for Additional NCSAM Resources and Valuable Information from DHS

**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-founded and co-lead NCSAM
+ October 2017 marks the 14th 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
SANS Security Awareness NCSAM Toolkit

To help you and your organization make the most of this October, SANS Security Awareness has created the NCSAM Planning Toolkit. This kit contains everything you need for a high-impact October, to include a planning matrix on what to do and when, communications templates and resources such as newsletters, posters, tips and other materials.

This kit is designed to work on its own or supplement anything you may already have planned. Simply pick and choose whatever resources or events you want to use. If you have any questions or suggestions on this community resource, please contact SANS Security Awareness at sth-community@sans.org.

Where to Start

Start with the Planning Matrix below, this gives you a high level overview of what you can do each week and when. Each week of October has a specific theme determined by NCSA with SANS Security Awareness materials mapped to each weekly theme.

We have learned the key to a successful security awareness month is effective communication, so make sure you take your communications team out to lunch before October.

+ For OUCH! newsletters, remember you can find more editions and multiple translations in over twenty languages at the OUCH! Archives Site.
# Plan Your National Cyber Security Awareness Month

<table>
<thead>
<tr>
<th>Pre-NCSAM</th>
<th>Resource</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wednesday,</strong></td>
<td><strong>Email Template</strong></td>
<td>Preparing for National Cyber Security Awareness Month (NCSAM)</td>
<td><strong>Optional activities that you can use to replace any of the other ones listed below.</strong></td>
</tr>
<tr>
<td><strong>September 27th</strong></td>
<td><strong>Planning Template</strong></td>
<td>Announcing upcoming activities for NCSAM</td>
<td><strong>Optional activities that you can use to replace any of the other ones listed below.</strong></td>
</tr>
<tr>
<td>** 2017 Security Awareness Report**</td>
<td><strong>2017 Security Awareness Report</strong></td>
<td>Use this report to get the leadership support you need to make your October and overall Awareness Program successful, including getting new staff.</td>
<td><strong>Use this report to get the support you need from leadership, including new staff.</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Week 1</th>
<th>Resource</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monday,</strong></td>
<td><strong>Email Template</strong></td>
<td>STOP. THINK. CONNECT.™: Simple Steps to Online Safety</td>
<td><strong>Staying safe and secure online is our shared responsibility. Here is easy-to-follow, actionable advice for everyone.</strong></td>
</tr>
<tr>
<td><strong>October 2nd</strong></td>
<td><strong>OUCH! Newsletter</strong></td>
<td>Announce activities for that week</td>
<td><strong>You can distribute this newsletter digitally to your staff or print and distribute physical copies.</strong></td>
</tr>
<tr>
<td><strong>Tuesday,</strong></td>
<td><strong>Poster</strong></td>
<td>Four Steps to Staying Secure</td>
<td><strong>You can distribute this poster digitally to your staff, display them on TV or digital monitors or print and distribute physical copies.</strong></td>
</tr>
<tr>
<td><strong>October 3rd</strong></td>
<td><strong>Lunch-n-Learn Presentation / Webcast</strong></td>
<td>Creating a Cyber Secure Home</td>
<td><strong>You can distribute this poster digitally to your staff, display them on TV or digital monitors or print and distribute physical copies.</strong></td>
</tr>
<tr>
<td><strong>Wednesday,</strong></td>
<td><strong>Lunch-n-Learn Presentation / Webcast</strong></td>
<td>Securing Your Kids</td>
<td><strong>These are materials you can use to present your own lunch-n-learn event to staff on how they can secure their kids / family online. This is a great way to generate interest for your environment and engage people throughout your organization.</strong></td>
</tr>
<tr>
<td><strong>October 4th</strong></td>
<td><strong>Video - RSA Workshop on Securing Kids</strong></td>
<td>Top Three Threats Facing Kids</td>
<td><strong>You can link to this site from your own internal portal or distribute the link to this staff via email.</strong></td>
</tr>
</tbody>
</table>
# Plan Your National Cyber Security Awareness Month

<table>
<thead>
<tr>
<th>Week 2</th>
<th>Resource</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday, October 9th</td>
<td>Email template</td>
<td>Announcing upcoming activities for NCSAM</td>
<td>Whatever your place of business, creating a culture of cybersecurity—from the breakroom to the board room—is essential and a shared responsibility among all employees.</td>
</tr>
<tr>
<td>Tuesday, October 10th</td>
<td>OUCH! Newsletter</td>
<td>CEO Fraud</td>
<td>You can distribute this newsletter digitally to your staff or print and distribute physical copies. This newsletter has been modified with the date removed.</td>
</tr>
<tr>
<td>Wednesday, October 11th</td>
<td>Poster</td>
<td>Don’t Get Hooked</td>
<td>You can distribute this poster digitally to your staff, display them on TV or digital monitors or print and distribute physical copies.</td>
</tr>
<tr>
<td>Thursday, October 12th</td>
<td>Guest Speaker</td>
<td>Guest Speaker</td>
<td>Generate excitement and buzz for your event by bringing in a guest speaker, such as someone from the FBI, Secret Service, a vendor, Infragard, your security team or industry recognized experts.</td>
</tr>
<tr>
<td>Friday, October 13th</td>
<td>Online Resource</td>
<td>Tip of the Day Program</td>
<td>Link to the SANS Tip of the Day program so your staff can gain a daily reminder on steps to take to protect themselves at work and at home.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Week 3</th>
<th>Resource</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday, October 16th</td>
<td>Email Template</td>
<td>Announce activities for that week</td>
<td></td>
</tr>
<tr>
<td>Tuesday, October 17th</td>
<td>OUCH! Newsletter</td>
<td>Passphrases</td>
<td>You can distribute this newsletter digitally to your staff or print and distribute physical copies. We selected this topic as strong passwords are one of the most effective means to secure any device.</td>
</tr>
</tbody>
</table>

# Today’s Predictions for Tomorrow’s Internet

With the explosion of digital interconnectivity, it is critical to explore everyone’s role in protecting our cyber ecosystem.
<table>
<thead>
<tr>
<th>Date</th>
<th>Resource</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wednesday, October 18th</td>
<td>Planning Template</td>
<td>Mobile Device Check-up</td>
<td>Setup a booth where employees can bring their mobile devices and ask questions on how to secure them. Also an excellent method to collect metrics.</td>
</tr>
<tr>
<td>Thursday, October 19th</td>
<td>Video of the Month</td>
<td>Malware</td>
<td>Malware, such as ransomware, continues to be one of the biggest challenges most systems and devices face today.</td>
</tr>
<tr>
<td>Friday, October 20th</td>
<td>Poster</td>
<td>You Are a Target</td>
<td>You can distribute this poster digitally to your staff, display them on TV or digital monitors or print and distribute physical copies.</td>
</tr>
<tr>
<td>Week 4</td>
<td></td>
<td>The Internet Wants You: Consider a Career in Cybersecurity</td>
<td>Growing the next generation of a skilled cybersecurity workforce - as well as training those already in the workforce - is a starting point to building stronger defenses.</td>
</tr>
<tr>
<td>Monday, October 23rd</td>
<td>Email Template</td>
<td>Announce activities for that week</td>
<td></td>
</tr>
<tr>
<td>Tuesday, October 24th</td>
<td>Online Assessment</td>
<td>Cybersecurity Aptitude Assessment</td>
<td>Employees / staff can take this free assessment to determine if cybersecurity would be a good career for them.</td>
</tr>
<tr>
<td>Wednesday, October 25th</td>
<td>Cyber Aces</td>
<td>Online Training Platform</td>
<td>Great introductory website for anyone wanting to start a career in cyber security, to include free online training of cybersecurity fundamentals.</td>
</tr>
<tr>
<td>Thursday, October 26th</td>
<td>Holiday Hack Challenge</td>
<td>Hacking Challenge</td>
<td>An annual hacking challenge with multiple levels to test and teach people various hacking / cybersecurity skills.</td>
</tr>
<tr>
<td>Friday, October 27th</td>
<td>Women's and Veteran's Cyber Academy</td>
<td>Cybersecurity programs for Women and Veterans</td>
<td>Programs to enable women and veterans to start a career in cybersecurity.</td>
</tr>
</tbody>
</table>
For General Online Safety Tips and Resources

STOP. THINK. CONNECT.™ // StaySafeOnline

For More Information on NCSAM
StaySafeOnline.org/NCSAM // DHS.gov/NCSAM

Sign up for:

+ NCSA’s email to stay current with the National Cyber Security Alliance (NCSA) and partner news, events and initiatives. You can expect to hear from NCSA on average a few times per month and, in the ramp-up to NCSAM and Data Privacy Day (January 28), more frequently. You can opt out at any time. We do not share our contact lists. Period. Subscribe to NCSA’s Mailing List!

+ NCSA’S #cyberaware monthly family newsletter, to receive the latest news, resources, tips and research geared for parents and young people. Great for your employees to stay up to date and in the know. What they learn transfers from home to work.

Become a STOP. THINK. CONNECT.™ Partner

STOP. THINK. CONNECT.™ is the global online safety education and awareness campaign to help all digital citizens stay safer and more secure online. STOP. THINK. CONNECT.™ is simple, actionable advice that everyone can follow to stay safer and more secure online.

Find Out More and Join The Campaign

+ It’s easy and free to sign up for a license.

+ Partners receive access to a wealth of innovative, educational materials that can be personalized and co-branded.

+ You can also create your own resources using STOP. THINK. CONNECT.™ messaging and branding.
Top Threats Facing Consumers: Studies And Stats

In 2017, the top three cybersecurity consumer concerns were identity theft, ransomware and the Internet of Things. These threats are real and growing – impacting digital citizens across the nation and around the globe.

According to 2016 Microsoft and NCSA research, the #1 concern for both parents and teens was “preventing identity theft.” View source.

According to a 2016 Pew study, 64% of American have personally experienced a major data breach/form of data theft. View source.


According to the FTC, in 2016 13% of the complaints were identity theft-related (surpassed only by debt collection and imposter scams). View source.

According to Javelin Strategy's 2017 Identity Fraud Study, in 2016 six percent of consumers were victims of identity fraud – an increase of more than two million victims (or 16%) from the previous year. View source.

According to the 2017 Unisys Security Index, more Americans are seriously concerned about identity theft (61%) and bankcard fraud (58%) than they are about their own personal safety (39%). View source.
Ransomware:

Ransomware victims have paid more than $25 million in ransoms over the last two years in order to unlock their computer disks and get their data back, according to a 2017 study by researchers at Google, Chainalysis, UC San Diego, and the NYU Tandon School of Engineering. According to a 2016 Kaspersky Lab survey, almost half (43%) of connected consumers today do not know what ransomware is, despite the recent aggressive spread of this type of cyber threat.

Mobile ransomware has risen by over 250% during the first few months of 2017, according to a recent report by Kaspersky Lab. In 2016, Cisco Systems declared ransomware the most profitable type of malware attack in history amid international efforts to stem the global crime wave. Ransomware: Top Threats Facing Consumers: Studies And Stats

According to a 2016 PhishMe study, 93% of phishing emails were infected with ransomware in Q1 of 2016.

In Pew Research’s 2017 “What the Public Knows About Cybersecurity” quiz, only 48% of Americans could correctly define ransomware.
Two minutes is the average time it takes for an IoT device to be hacked, according to Symantec’s 2017 Internet Security Threat Report.

In ESET and NCSA’s 2016 Internet of Stranger Things survey, 40% of respondents were “not confident at all” that IoT devices are safe, secure and able to protect personal information.

The same ESET and NCSA survey found that 50% of consumers indicate that concerns about the cybersecurity of an IoT device have discouraged them from purchasing one.

According to Gartner, 8.4 billion connected things will be in use worldwide in 2017, up 31% from 2016, and will reach 20.4 billion by 2020.

In September 2016 at DEF CON, one of the world’s largest security conferences, 47 vulnerabilities affecting 23 IoT-enabled items (door locks, wheelchairs, thermostats and more) from 21 manufacturers were disclosed.

Default passwords are still the biggest security weakness for IoT devices. Most common password tried by hackers? “Admin” according to Symantec’s 2017 Internet Security Threat Report.

According to Accenture’s 2016 Igniting Growth in Consumer Technology report, 62% of consumers reported that price is the top barrier to purchase of IoT devices, while 47% indicated that they were concerned about privacy and security issues.
Organizations of any size – including healthcare providers, colleges and universities, government agencies and nonprofits – can fall victim to cybercrime, which could result in stolen customer data or intellectual property, and business disruptions. For 2017, the top threats facing businesses are ransomware and extortion, IoT security threats and insider threats. As these cybersecurity threats continue to grow in size and magnitude, companies large and small need to develop a cyber action plan and be aware of the evolving threat landscape.

Ransomware and Extortion:

According to the second annual State of Ransomware study from Malwarebytes and Osterman Research, 20% of small to mid-sized organizations that experienced a successful ransomware infiltration had to cease business operations immediately, and 12% lost revenue. View source.

Time is money: The same Osterman Research study found that 57% of SMBs experienced nine or more hours of downtime, with some organizations down for more than 100 hours because of the infection.

How does ransomware enter an organization? Emails account for 64% of infections in the form of attachments and email links. Websites and web applications account for 16% of infections (Osterman Research).

According to a KPMG Small Business Reputation & The Cyber Risk study, 58% of consumers said that a breach would discourage them from using a business in the future. View source.

According to Symantec’s 2016 Internet Security Threat Index, small businesses are a big target for phishers. In 2015, phishing campaigns targeted small businesses 43% of the time – up from 18% in 2011. View source.

According to the FTC, ransoms can be as much as $30,000 for businesses, and they have skyrocketed in the past year. View source.

For 2017, Cybersecurity Ventures predicts global ransomware damage costs will exceed $5 billion, up from $325 million in 2015. View source.

Carbon Black’s 2017 Ransom Aware survey showed that seven in 10 consumers would consider leaving a business (e.g., their financial institution, healthcare provider) if it were hit by ransomware.

Additionally, only 52% of consumers trust retailers to protect their data. View source.
IoT Security Threats:

According to AT&T's Cybersecurity Insights Report, **85% of enterprises are in the process of or are planning to deploy IoT devices, but only 10% feel confident that they can secure those devices against hackers.** View source.

BI Intelligence estimates that investment in security on IoT devices will account for 30% of the overall cybersecurity market in 2020 because of the urgent market need. View source.

According to Samsung’s recent Open Economy report, there is a “critical” need to secure every IoT device by 2020 and a “very clear danger that technology is running ahead of the game”. The firm said **more than 7.3 billion devices will need to be made secure by their manufacturers in the next three years.** View source.

Symantec established an IoT honeypot in 2015 to track attack attempts against IoT devices; in the 2017 Internet Security Threat Report, they found that the attacks on their honeypot almost doubled from January to December 2016 — from an average of almost 4.6 unique IP addresses/hour in January to more than 8.8/hour in December. View source.

The FTC issued an IoT report in 2015 geared toward businesses, discussing the top security risks in IoT (unauthorized access/use of information, facilitating attacks on other systems, creating risks to personal safety) and urging organizations to build security into devices at the outset and follow the FTC’s guidelines. View source.

The U.S. House of Representatives has called on the FTC to urge device manufacturers to implement security measures. View source.

In “IoT Goes Nuclear,” a recent report, it was shown how IoT hacks could be used to take down all of a city’s traffic lights and/or other critical systems. View source.
Insider Threats to Business:

According to the Ponemon 2016 Cost of Data Breach Study, **insider incidents cost companies $4.3 Million per year** on average. Of those incidents, 65% were caused by employee or contractor negligence, 22% were tied to malicious employees and criminals and almost 10% were caused by outside imposters with stolen credentials. [View source.]

In the 2016 Cyber Security Intelligence Index, IBM found that **60% of all attacks were carried out by insiders.** Of these attacks, three-quarters involved malicious intent, and one-quarter involved inadvertent actors. [View source.]

IBM Security research also found that health care, manufacturing, and financial services are the top three industries under attack, due to their personal data, intellectual property and physical inventory, and massive financial assets, respectively. [View source.]

According to a new SANS survey, **40% of respondents rated malicious insiders as the most damaging threat vector their companies faced.** Furthermore, nearly half (49%) said they were in the process of developing a formal incident response plan with provisions to address insider threat. [View source.]

Harvard Business Review estimated that there may be at least **80 million insider attacks occurring each year in the United States** and noted that the number is likely much higher, as many internal attacks go unreported. [View source.]

According to the 2017 Verizon Data Breach Investigations Report, in **60% of cases of insider and privilege misuse, insiders take data in the hope of turning it into money in the future;** in 17% of cases it is a case of unsanctioned snooping, and 15% of the time it’s to take data to a new employer or start a rival company. [View source.]

Assistant Attorney General for National Security John Carlin called insider threats “one of the most serious threats a company can face.” [View source.]
About the National Cyber Security Alliance:
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 the U.S. Department of Homeland Security (DHS) and NCSA’s Board of Directors, which includes representatives from ADP; Aetna; AT&T Services Inc.; Bank of America; Barclays; CDK Global, LLC; Cisco; Comcast Corporation; ESET North America; Google; Facebook; LifeLock, Inc.; Logical Operations; NXP Semiconductors; RSA, the Security Division of EMC; Symantec Corporation; Intel Corporation; MasterCard; Microsoft Corporation; PayPal; Raytheon; PKWARE; Salesforce; SANS Institute; TeleSign; Visa and Wells Fargo. NCSA’s core efforts include National Cyber Security Awareness Month (October); Data Privacy Day (January 28) and 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. 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.

Media Contacts
Jessica Beffa  Thatcher+Co.  |  720-413-4938  |  ncsa@thatcherandco.com
Barbara Thatcher  Thatcher+Co.  |  408-701-7528  |  ncsa@thatcherandco.com