Celebrated every October, National Cyber Security Awareness Month (NCSAM) – #CyberAware – was created as a collaborative effort between government and industry to ensure that all Americans have the information they need to stay safer and more secure online.

This year marks the 13th annual NCSAM, co-founded and co-led by the U.S. Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA), the nation’s leading nonprofit, public-private partnership focused on cybersecurity education and awareness.

According to a September 2016 survey by HSB, more than one-third of U.S. consumers have experienced a computer virus, hacking incident or other cyber attack in the last year. With cyber crime an ongoing challenge, NCSA and DHS work throughout the year to promote awareness about internet safety and the importance of being a responsible digital citizen. During NCSAM, these actions and efforts come into full focus, creating a moment in time for internet users – in America and across the globe – to reflect on measures we’ve taken to stay safe online and find meaningful ways to improve them.

For this reason, NCSAM 2016 will focus on the various ways individuals can protect themselves while online – whether in the home, at the office or while on the go – work to empower businesses to create a culture of cybersecurity in the workplace, and explore cybersecurity as we enter the age of the Internet of Things. NCSAM strives to instill the idea that by working together to protect the internet, we – and our nation’s economy and critical infrastructure – will be safer and more secure.

Underpinning the month-long initiative to educate consumers and businesses everywhere 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.™ is based on simple, actionable advice that anyone can follow by taking security precautions, thinking about the consequences of their actions online and enjoying the benefits of the internet.
In recognition of how valuable the internet is to our daily lives and the collective effort needed to protect it, the theme for the month, as it has been since 2009, is “Our Shared Responsibility.” Because no individual, business or government entity is solely responsible for securing the internet, everyone must play a role in securing their part of cyberspace, including the devices and networks they use. If everyone does their part – implementing stronger security practices, raising community awareness, educating young people or training employees – our digital society will be safer and more resistant from attacks and more resilient if an attack occurs.
The five weekly themes for NCSAM 2016 will address a variety of internet safety concerns. Easy-to-follow tips, a variety of resources and actionable advice for consumers and businesses will be shared each week.

**WEEK 1: OCTOBER 3-7**

**STOP. THINK. CONNECT.™: The Basic Steps to Online Safety and Security**

Staying safer and more secure online starts with STOP. THINK. CONNECT. – simple, actionable advice anyone can follow.

STOP: make sure security measures are in place. THINK: about the consequences of your actions and behaviors online. CONNECT: and enjoy the Internet.

Week 1 shares user-friendly ways we can protect ourselves and our communities, along with actions to take if impacted by a breach, cybercrime or other online issue.

**WEEK 2: OCTOBER 10-14**

**From the Break Room to the Boardroom: Creating a Culture of Cybersecurity in the Workplace**

Week 2 will focus on creating a culture of cybersecurity in the workplace through efforts like employee education, training and awareness, and by emphasizing risk management, resistance and resilience. Promoting an educated workforce and following best practices – with an emphasis on skill- and career-building for existing personnel and potential new entrants into the cybersecurity workforce – will also be highlighted.

**WEEK 3: OCTOBER 17-21**

**Recognizing and Combating Cybercrime**

While online crime is often associated with hackers stealing personal information for monetary gain, crime on the internet takes many forms. Week 3 will focus on awareness of the different types of online crime, offer steps people can take to better protect themselves, and address how law enforcement and others can collaborate to combat cybercrime. In addition, careers in fighting cybercrime will be spotlighted.

**WEEK 4: OCTOBER 24-28**

**Our Continuously Connected Lives: What’s Your “Apptitude”?**

We are quickly advancing into a world where there is an app for everything. These rapid technological advances, like the Internet of Things, can yield tremendous benefits and cybersecurity is fundamental to realizing their promise. As smart cities, connected healthcare devices, digitized records and smart cars and homes fast become our new reality, creating these cutting-edge technologies in a safe and secure way – along with building a workforce to maintain the infrastructure of our connected world – is essential. Week 4 will examine our future in this connected world and provide strategies for security, safety and privacy.

**WEEK 5: OCTOBER 31**

**Building Resilience in Critical Systems**

The internet underlies nearly every aspect of our daily lives and helps form our critical infrastructure, which keeps crucial systems like electricity, transportation and communications up and running. October 31 will emphasize the importance of critical infrastructure and highlight the role the public can play in keeping it secure. On this last day of October, the transition to Critical Infrastructure Security and Resilience Month in November begins.
STOP. THINK. CONNECT.™ AND NCSAM

our global footprint

- Launched in 2004 by the U.S. Department of Homeland Security and the National Cyber Security Alliance as a broad effort to help all Americans stay safer and more secure online.

- Declared under Presidential Proclamation every year beginning in 2009.

- A global effort, recognized across several countries and regions, including North America, Latin America, Europe, Africa and Australia.

- More than 600 Champions – individuals and organizations that support NCSAM through dedicated initiatives – for NCSAM 2016.

- Supported by NCSA board members, including representatives from ADP; AT&T Services, Inc.; Bank of America; Barclays; BlackBerry Corporation; Cisco; Comcast Corporation; ESET North America; Facebook; Google; Intel Corporation; Logical Operations; Microsoft Corp.; NXP Semiconductors; PayPal; PKWARE; Raytheon; RSA, the Security Division of EMC; Salesforce; SANS Institute; Symantec and Visa Inc.

- Since 2009, the month’s theme has been “Our Shared Responsibility.”

- In 2010, President Obama launched the STOP. THINK. CONNECT. campaign as a national cybersecurity awareness campaign.

- In 2015, NCSAM messages reached an audience of nearly 2 billion people.

Now in its 13th year, NCSAM is recognized across several countries and regions, including North America, Latin America, the European Union, Africa and Australia.

This global commitment to emphasizing safe cybersecurity practices is in large part due to the global reach of STOP. THINK. CONNECT.™, which launched its international program in 2011. The campaign has impacted millions worldwide through collaborative public and private sector efforts, expanding its roster of partners with its simple but increasingly vital message to stay safer and more secure online.

The STOP. THINK. CONNECT.™ directive for all internet users – whether young people surfing the web, consumers shopping online or businesses conducting transactions – is to take safety and security precautions when online and understand the consequences of their actions so everyone can connect and enjoy the internet with a greater peace of mind. The campaign emphasizes basic steps users should take when connected, 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 languages on the way.

In the five years since it began in conjunction with NCSAM, STOP. THINK. CONNECT.™ has signed on nearly 500 organizations – including Fortune 500 companies, small- and medium-sized businesses, colleges and universities, regional banks and a host of others – as official partners of the campaign. STOP. THINK. CONNECT.™ partners adopt the campaign’s messages and use materials to educate their own communities about online safety.
Parent And Teens – Bridging The Digital Disconnect: An August 2016 NCSA study, which was co-sponsored by Microsoft, exposed a “digital disconnect” between 810 parents and 804 teens regarding teens’ online behaviors, experiences and methods for resolving online issues. The study suggests that American teens may have more complicated – and even distressing – online experiences than their parents know, including receiving negative messages about things they had said or done or about their appearance, sexual orientation, gender or race/ethnicity and having concerns about being directed to extremist content. Key findings include that 60 percent of online teens ages 13 to 17 say they have created accounts their parents do not know about, and 39 percent say someone has been mean or cruel to them when they were online or using apps over the past year. Additionally, although a separate survey of parents indicates that they would overwhelmingly want their teens to turn to them first when they face problems online, 40 percent of teens say they would turn to their friends first. Other key findings include:

**Online teens largely experience the online world through their use of smartphones,** and their use of Snapchat (66%) and Instagram (65%) now surpasses their use of Facebook (61%). More than half (52%) of the teens surveyed reported using KiK Messenger.

**Just 13 percent of online teens** say that their parents are “completely aware” of the full extent of their activities online; however, only nine percent say that their online activities should be kept “completely private” from their parents.

The majority of online teens report that they are expected to follow some kind of rules connected to technology use at home, but **28 percent report that their household has no rules** when it comes to their use of internet-connected devices. By comparison, only nine percent of parents of online teens ages 13 to 17 say they have no rules in their household for their children’s use of these technologies.

**About four in ten online teens (39%)** say someone has been mean or cruel to them when they were online or using apps sometime over the past year.
The content of the mean or cruel messages was most often about something the teens said or did (52%) or something about their appearance (45%). About one in four online teens said the messages were about their sexual orientation (27%), their gender (25%) or their race or ethnicity (24%).

Many of the top online safety concerns for teens relate to the privacy and security of their personal information; teens report that they are “very concerned” about someone accessing their accounts without their permission (47%), someone sharing personal information about them online (43%) or someone posting a photo or video of them online that they wanted to remain private (38%).

While not as prominent as various privacy and security-related concerns, worry about exposure to extremist content impacts a sizable minority of online teens. One in four (27%) online teens say they are “very concerned” about being directed to online content about extreme political or religious activities that make them feel uncomfortable.

Forty percent of online teens say that they would turn to friends first when facing serious problems online, while 33 percent cited parents.

Fully 43 percent of online teens say that friends have sought their help because of things that happened online. The majority of online teens (62%) say they have responded by just listening and providing any advice they could.

Even as teens and parents may diverge in a number of areas, they appear to have remarkably consistent priorities when asked about the online safety topics they would most like to learn about. Both parents and teens point to the topic of “preventing identity theft” as the online safety topic they would most like to learn more about.

Key Resources:
Rethink Cyber Safety Rules and the “Tech Talk” with your Teens, Infographic: Keeping up with Generation App.
Microsoft Study: 4 in 10 U.S. Teens Encounter Cruel Treatment Online.
TeenSafe: Find Hidden Apps Your Teen Doesn’t Want You Seeing
**Personal:** It’s virtually impossible to manage our lives and responsibilities without relying on the internet. It is the basic foundation of so much of what we do — from shopping to monitoring health to turning in homework and keeping in touch with friends and family, we are connected 24/7. Here are some startling statistics:

**Seventy two percent of Americans** believe their accounts are secure with only a username and password¹ yet the most common passwords in America are 123456 and 123456789.²

ComScore’s 2015 U.S. Mobile App Report, released last September, revealed that *app use accounts for 54 percent of the time people spend with digital media.*³

**Every two seconds** there is another victim of identity fraud.⁴

Identity fraud was responsible for **$16 billion in losses in 2014.⁵**

**One in five American households** have received notification that their information has been lost in a data breach.⁶

**Sixty-three percent of confirmed data breaches** involved leveraging weak, default or stolen passwords in 2015.⁷

Last year, hackers exposed the personal information of **110 million Americans** — roughly half of the nation’s adults.⁸

In 2015, **21 percent of internet users (18 years and older) had an online account compromised**, such as a social networking account or an email account, and only 23 percent think their accounts are very secure.⁹

**Sixty-two percent of Americans** fear that their smartphone or computer will be hacked.¹⁰

**Theft of personal information and identities** took center stage in 2015, accounting for 53 percent of all data breaches last year.¹¹

In 2015 **some 1,938,383 data records were stolen or lost every day**, 80,766 every hour, 1,346 every minute and 22 every second.¹²

**Key Resources:**

- [Your Digital Spring Cleaning Checklist](#)
- [Get Two Steps Ahead: Protect your Online Accounts with Stronger Authentication Practices](#)
- [The Department of Homeland Security’s STOP. THINK. CONNECT. toolkit](#)

---

¹. 2016 NCSA Strong Authentication Research
¹². Ibid.
**Getting Smart About Apps:** We are quickly advancing into a world where there is an app for everything. While these smart apps make life easier to manage on many levels – from monitoring your thermostat to keeping track of exercise – cybersecurity is fundamental to realizing their benefits.

The amount of time Americans spend on digital media has exploded recently – **growing nearly 50 percent in the past two years**, with more than three-fourths of that growth directly attributable to the mobile app.13

**Seventy-three percent of people** admit to not reading the fine print of contracts, and that includes the fine print of installing an app on devices.14

**Many users ignore the ‘permissions’ on apps**, which can lead to bad software sneaking in undetected.15

**Behind Our Digital Doors – Securing our Connected Homes:** There is a knowledge-confidence gap in many American homes when it comes to cybersecurity, as illustrated in a recent NCSA/ESET study on connected homes. The findings revealed that Americans are leaving their digital doors unsecured despite the fact that one in five American homes received a data breach notification last year. Additionally, 56 percent of those individuals received multiple notifications and 79 percent indicated that they still felt safe in their connected homes – with almost half (49%) showing a remarkably strong sense of confidence. The study also found that more than 40 percent failed to properly secure their wireless routers – the gateway to most digital devices – by not resetting the factory-set default passwords. Other noteworthy findings include:

When asked how confident they are that their home network and the internet-connected devices in the home are secure, **79 percent responded that they felt confidently safe.**
- On a scale of 1-5, **49 percent** percent felt very confident.
- **30 percent** felt confident.

American households need to better secure their digital doors. The wireless router represents a major digital entry point for cyber attacks.

- **Two in five households** – more than 40 percent – did not change the factory set default passwords on their wireless routers.
- **Close to 60 percent** did not (48%) or are not sure (8%) if they changed their router username or password in the last year.
- **60 percent** set up their wireless routers on their own.

---

15. Ibid.
Banks and retail establishments are not the only ones affected by data breaches: **Americans are experiencing breaches at home, too.**

– **One in five American households** have received notification that their information has been lost in a data breach.

– **One in five households** have received notification from a child’s (or children’s) school that their child’s information has been lost in a data breach.

– **In the last 12 months, 54 percent** of those surveyed experienced some kind of negative online security scenario.

– **Among those affected, 44 percent** changed their online behavior as a result.

  – Most common actions were **increased alertness** during internet browsing (63%) and **password change** (56%).

In households across America, **identity theft is the major safety and security concern online:**

– Here’s how internet users responded to “which of the following safety and security concerns do you have about using the internet?”

  – Becoming a victim of ID theft – **58%**
  – Financial information, such as credit card number or banking information, will be stolen – **46%**
  – My social security number will be stolen – **43%**
  – Someone will access my personal information, such as my home address, and my cell phone number will be stolen – **20%**
  – One of my devices will be hacked, and I will no longer be able to use it – **16%**
  – Someone will use information posted about me to commit physical harm, such as knowing I am away for vacation and breaking into my home – **8%**
  – My personal medical information will be stolen – **9%**
  – Someone will post something untrue about me that I cannot fix – **8%**
  – Someone will post an embarrassing or unwanted picture of my kid(s) – **3%**

**Key Resources:**

- [Behind America’s Digital Doors](#)
- [Securing Your Home Network](#)
- [Victim of ID Theft, Fraud or Cybercrime? Here’s What You Can Do](#)
**Small Business:** Data breaches or hacking incidents can shut down small businesses, leading to a lack of trust from consumers, partners and suppliers. As such, small businesses must make plans to protect themselves from cyber threats and help employees stay safe online.

Last year, **43 percent of cyber attacks targeted small businesses.**¹⁷

Since 2014, there’s been **a 55 percent increase in the amount of spear-phishing** campaigns that target employees of a business of any size.¹⁸

Small businesses often underestimate their risk level, with **82 percent of small business owners saying they are not targets for attacks**, because they don’t have anything worth stealing.¹⁹

A single crypto-malware or ransomware attack **costs small and medium-sized companies up to $99,000.**²⁰

**Key Resources:**
- Assess Your Risk,
- 3 Reasons Hackers Love Your Small Business: Infographic,
- So You’ve Had A Data Breach, Now What?

**Shopping:** For many consumers, online shopping has opened the doors to a virtual mall of deals, discounts and convenience. However, as more consumers click to buy, scammers lurk on the sidelines, prepared to take advantage of bad online shopping habits.

**E-commerce sales on Cyber Monday** – the Monday after Thanksgiving – **hit a record $3 billion last year**, making it the biggest online shopping day ever and up 18 percent from 2014.²¹

**One in six online consumers is duped into shopping at rogue sites.**²²

Nineteen percent of consumers **say they would stop shopping at a retailer that had been the victim of a hack**, and 33 percent would stop shopping at that retailer for at least three months.²³

Online shopping can be primetime for phishing. **In the first half of 2014 alone, there were at least 123,741 unique phishing attacks worldwide** – the most in a period since the second half of 2009.²⁴

**Key Resources:**
- Holiday Shopping Goes Mobile: Be Cyber Secure [Infographic],
- STOP. THINK. CONNECT. tips for safe online shopping

---

¹⁸. Ibid.


**Schools:** From grades K-12 to colleges and universities, getting smart about cyber safety is rising to the top of teachers’ lesson plans. Because of the vast amount of personal information stored about students, faculty and employees, educational institutions are fast becoming prime targets for cyber attacks.

727 breaches occurred at educational institutions between 2005 and 2014, resulting in more than 14 million records being made public. These breaches were in higher education as well as trade schools, secondary schools and nonprofit organizations in the education sector. In 2014, 64 percent of millennials say they did not have access to the kind of classes in high school that build awareness or the necessary skills for cyber careers, including computer science.

The threat of cyber attacks to universities is rising. In 2015, breaches at Pennsylvania State University and the University of Virginia were blamed on Chinese hackers. University of Connecticut students’ Social Security numbers and credit card data were stolen. Washington State University and Johns Hopkins University were also targets of attacks.

In 2015, 79 percent of millennials say they have never spoken to a practicing cybersecurity professional or are unsure if they have.

In 2014, 10 percent of reported security breaches involved the education sector.

27. Ibid.
Healthcare: Experts predict that medical data could be the next major area targeted in cyber attacks, as medical information is worth 10 times more than a credit card number on the black market. However, most healthcare organizations remain unprepared to address a cyber threat.

Healthcare data breaches involved more than 112 million records in 2015.

During the first half of 2015, healthcare record data breaches increased sharply. Five of the eight largest healthcare security breaches compromised more than 1 million records during this timeframe.

In the past five years, the average data breach costs a hospital $2.1 million. Nearly 90 percent of healthcare providers were hit by breaches in the past two years.

Most healthcare providers are unprepared to address a cyber threat – with only 53 percent of providers and 66 percent of payers considering themselves ready to defend against an attack.

More than 2.3 million Americans have been victims of medical identity theft.

Sixty-five percent of medical identity theft victims have had to pay an average of $13,500 to resolve the crime.

Medical records, which often contain Social Security numbers, insurance IDs, addresses and medical details, sell for as much as 20 times the price of a stolen credit-card number.

Key Resources:
FTC: Medical Identity Theft,
The Healthcare Industry’s Guide to Keeping Information Safe & Secure When You Are Mobile

38. Ibid.
Cybercrime: Across the globe, cybercrime is on the rise and poses great challenges to keeping all digital citizens safe. From corporations to consumers, anyone who uses the internet is at risk. Crimes such as fraud, identity theft and hacking have resulted in significant costs to large organizations, as well as harm to consumers’ online profile and offline reputation.

In 2014, cybercrime cost Americans $800 million, highlighting a real concern among companies whose technological devices and network systems are widely used.40

Surpassing the annual GDP of most nations, digital crime and intellectual property theft currently costs between $375 billion and $575 billion annually.42

Data breaches on a global scale have increased 15 percent over the past year, costing companies $3.5 million to respond to a data breach.41

The average cost of cybercrime for U.S. retail stores more than doubled from 2013 to an annual average of $8.6 million in 2014.42

Cybercrime and cyber spying cost the U.S. economy $100 billion a year and the global economy $300 billion a year.43

Customer data – email addresses, birth dates, shipping addresses, passwords, etc. – is also valuable. The average sale price for stolen credit card paired with personally identifiable information, such as the card owner’s billing address, was $15 in 2015 – and double the price of the credit card information alone.44

In 2015, hackers stole Social Security numbers and other personal data belonging to 22.1 million people in breaches of the U.S. government’s personnel office.45

Ransomware attacks have surged where victims in the U.S. have paid more than $209 million in ransom payments in the first three months of this year, compared with $25 million in all of 2015.46

Energy companies and electric utilities have experienced a spike in cyberattacks in the last year. Seventy-five percent of companies in the oil, natural gas and electricity sectors have experienced one “successful” cyber attack in the past 12 months.47

Key Resources:
Microsoft Malware Protection Center,
Symantec: Ransomware Do’s and Don’ts,
Federal Trade Commission: Warning Signs of Identity Theft

# A Look at October Events

Note: This is just a sampling of key events from NCSA.

There are many more events posted at [https://staysafeonline.org/about-us/events/](https://staysafeonline.org/about-us/events/)

<table>
<thead>
<tr>
<th>SUNDAY</th>
<th>MONDAY</th>
<th>TUESDAY</th>
<th>WEDNESDAY</th>
<th>THURSDAY</th>
<th>FRIDAY</th>
<th>SATURDAY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SEPT 25</strong></td>
<td><strong>SEP 26</strong></td>
<td><strong>SEP 27</strong></td>
<td><strong>SEP 28</strong></td>
<td><strong>SEP 29</strong></td>
<td><strong>SEPT 30</strong></td>
<td><strong>OCT 1</strong></td>
</tr>
<tr>
<td>Pre-NCSAM Event: Empowering Users to Protect Themselves in Washington, D.C.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>European Cyber Security Month Launch in Brussels</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>OCT 2</strong></th>
<th><strong>OCT 3</strong></th>
<th><strong>OCT 4</strong></th>
<th><strong>OCT 5</strong></th>
<th><strong>OCT 6</strong></th>
<th><strong>OCT 7</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SUNDAY</strong></td>
<td><strong>MONDAY</strong></td>
<td><strong>TUESDAY</strong></td>
<td><strong>WEDNESDAY</strong></td>
<td><strong>THURSDAY</strong></td>
<td><strong>FRIDAY</strong></td>
</tr>
<tr>
<td><strong>OCT 8</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>OCT 9</strong></th>
<th><strong>OCT 10</strong></th>
<th><strong>OCT 11</strong></th>
<th><strong>OCT 12</strong></th>
<th><strong>OCT 13</strong></th>
<th><strong>OCT 14</strong></th>
<th><strong>OCT 15</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SUNDAY</strong></td>
<td><strong>MONDAY</strong></td>
<td><strong>TUESDAY</strong></td>
<td><strong>WEDNESDAY</strong></td>
<td><strong>THURSDAY</strong></td>
<td><strong>FRIDAY</strong></td>
<td><strong>SATURDAY</strong></td>
</tr>
<tr>
<td><strong>OCT 16</strong></td>
<td><strong>OCT 17</strong></td>
<td><strong>OCT 18</strong></td>
<td><strong>OCT 19</strong></td>
<td><strong>OCT 20</strong></td>
<td><strong>OCT 21</strong></td>
<td><strong>OCT 22</strong></td>
</tr>
<tr>
<td>IACP Conference in San Diego, CA</td>
<td>IACP Conference in San Diego, CA</td>
<td>IACP Conference in San Diego, CA</td>
<td>Cybercrime Event with City and County of LA in Los Angeles, CA</td>
<td>Cybersecurity Day at Nova Southeastern University, Fort Lauderdale, FL</td>
<td>The Passcode Cup Cyber Challenge in Washington, D.C.</td>
<td>Third Annual Los Angeles Cyber Security Summit, Los Angeles, CA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>OCT 23</strong></th>
<th><strong>OCT 24</strong></th>
<th><strong>OCT 25</strong></th>
<th><strong>OCT 26</strong></th>
<th><strong>OCT 27</strong></th>
<th><strong>OCT 28</strong></th>
<th><strong>OCT 29</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SUNDAY</strong></td>
<td><strong>MONDAY</strong></td>
<td><strong>TUESDAY</strong></td>
<td><strong>WEDNESDAY</strong></td>
<td><strong>THURSDAY</strong></td>
<td><strong>FRIDAY</strong></td>
<td><strong>SATURDAY</strong></td>
</tr>
<tr>
<td><strong>OCT 30</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>NOV 1</strong></th>
<th><strong>NOV 2</strong></th>
<th><strong>NOV 3</strong></th>
<th><strong>NOV 4</strong></th>
<th><strong>NOV 5</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SUNDAY</strong></td>
<td><strong>MONDAY</strong></td>
<td><strong>TUESDAY</strong></td>
<td><strong>WEDNESDAY</strong></td>
<td><strong>THURSDAY</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SPREAD THE WORD: #CyberAware

topics to explore this October

WEEK 1
+ STOP. THINK. CONNECT.™ – Most Common Consumer Cyber Mistakes
+ Bridging the Parent – Teen Digital Disconnect
+ Take a Fresh Approach to the Parent/Teen “Tech Talk”
+ Why Passwords are Passé: Tips to Secure Your Digital Life
+ Connected Cities: Love Free Public WiFi? So Do Hackers!
+ Beware of Ransomware: Tips to Protect Your Digital Life
+ Public Charging Stations: A Convenience or a Cost?

WEEK 2
+ Why Your Next Job Should be in Cybersecurity
+ The Path to a Career in Cybersecurity
+ Why Hackers Still Love Small Business
+ How to Establish a Culture of Cybersecurity at Your Business
+ Why Cyber Safety Training is the Best Training Your Employees Can Receive

WEEK 3
+ The Internet of Us: Why Protecting our Networks from Cyber Crime Helps Us All
+ What Your Local Police Team is Doing to Fight Cybercrime
+ If Your Health Data Safe? Why Does it Matter?
+ Teaching Your Kids About ID Theft
+ What to do if You’re Stalked Online
+ How Hackers Can Access Your Online Banking Account

WEEK 4
+ Is Your Digital Door Unlocked? The Most Common Vulnerability in the Connected American Home
+ My Car’s Been Hacked! Protecting Yourself and Your Connected Vehicle
+ An App a Day: Tips to Keep Hackers Away
+ Happy Halloween: Time to Clean Out Zombie Apps!

WEEK 5
+ The Critical Importance of Protecting Our 16 Sectors of Critical Infrastructure
+ How a Cyber Attack on Our Critical Infrastructure Would Impact Our Daily Lives
+ November Launches Critical Infrastructure Security and Resilience Month
KEYWORDS IN CYBERSECURITY
a glossary

**Anti-Virus Software:** A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents.

**Black Hat:** A person who attempts to find computer security vulnerabilities and exploit them for personal financial gain or other malicious reasons.

**Chip and Pin:** A system of paying for something using a credit or debit card that has information stored on it on a microchip. You put your PIN number (which is a set of 4 numbers) into a machine with the card to prove who you are, instead of signing.

**Critical Infrastructure:** The systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters.

**Cyberbullying:** The use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.

**Data Breach:** The unauthorized movement or disclosure of sensitive information to an authorized party.

**Encryption:** Converting data into a form that cannot be easily understood by unauthorized people.

**Hack-a-Thon:** An event, typically lasting several days, in which a large number of people meet to engage in collaborative computer programming.

**Hacker:** An unauthorized user who attempts to or gains access to an information system.

**Internet of Things:** The internetworking of physical devices, vehicles, buildings and other items embedded with electronics, software, sensors, actuators and network connectivity that enable these objects to collect and exchange data.

**Internet Service Provider/ISP:** A company that provides internet services, including personal and business access to the internet.

**Malware:** Software that compromises the operation of a system by performing an unauthorized function or process.

**Multi-factor Authentication:** A security tool that uses multiple verification techniques to prove that the person attempting to log onto an account is really them.

**Personally Identifiable Information (PII):** Information that can be used on its own or with other information to identify, contact, or locate a single person or to identify an individual in context.

**Phishing:** A digital form of social engineering to deceive individuals into providing sensitive information.

**Ransomware:** A type of malicious software designed to block access to a computer system until a sum of money is paid.
Spam: The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Spoofing: The forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.

Spyware: Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.

Tokenization: The process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token that has no extrinsic or exploitable meaning or value.

Trolling: Making a deliberately offensive or provocative online posting with the aim of upsetting someone or eliciting an angry response from them.

White Hat: A computer security specialist who breaks into protected systems and networks to test and assess their security.