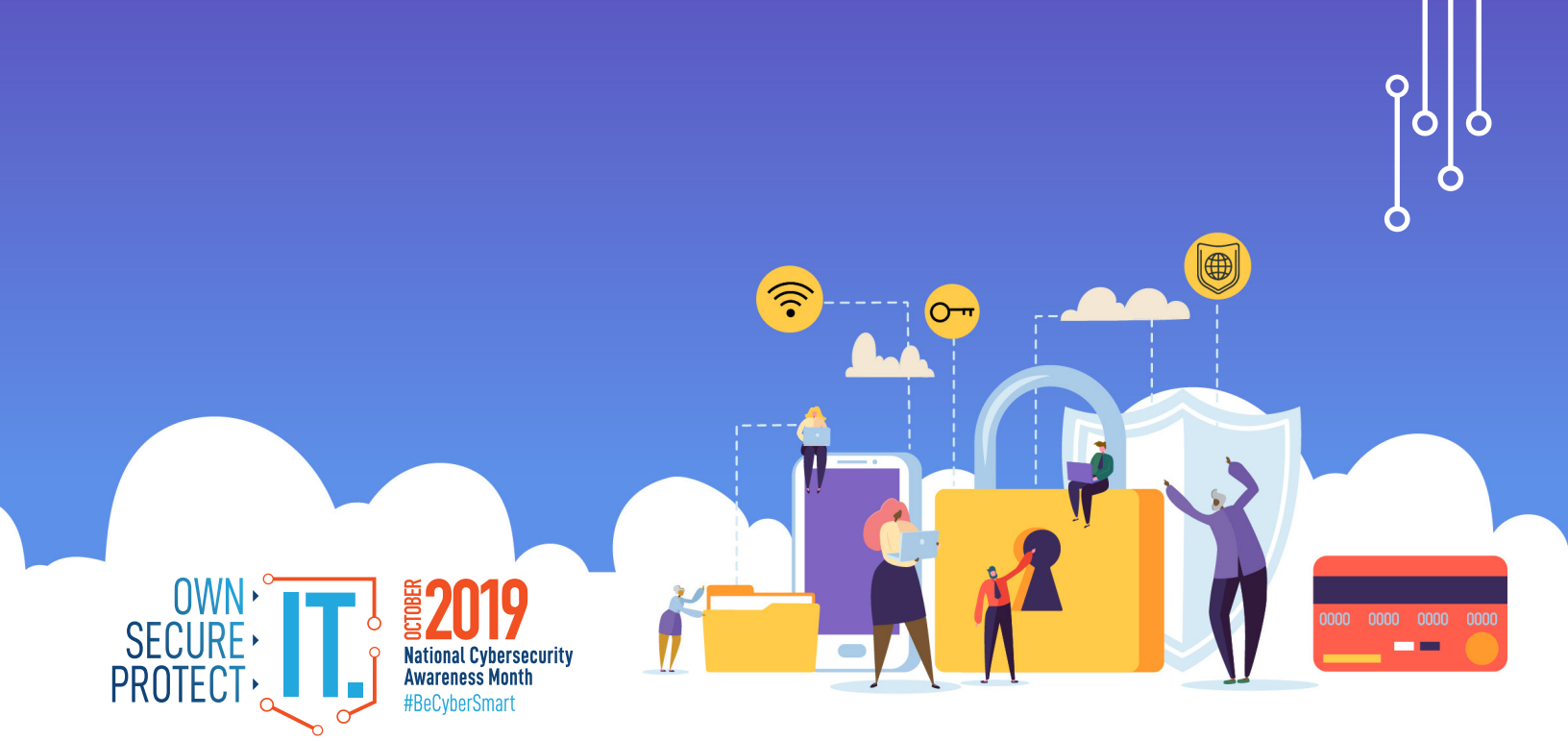


NATIONAL CYBERSECURITY AWARENESS MONTH

2019 TOOLKIT

Key messaging, articles, social media, and more to promote National Cybersecurity Awareness Month 2019

CISA | dhs.gov/ncsam | NATIONAL CYBERSECURITY ALLIANCE | CyberAware

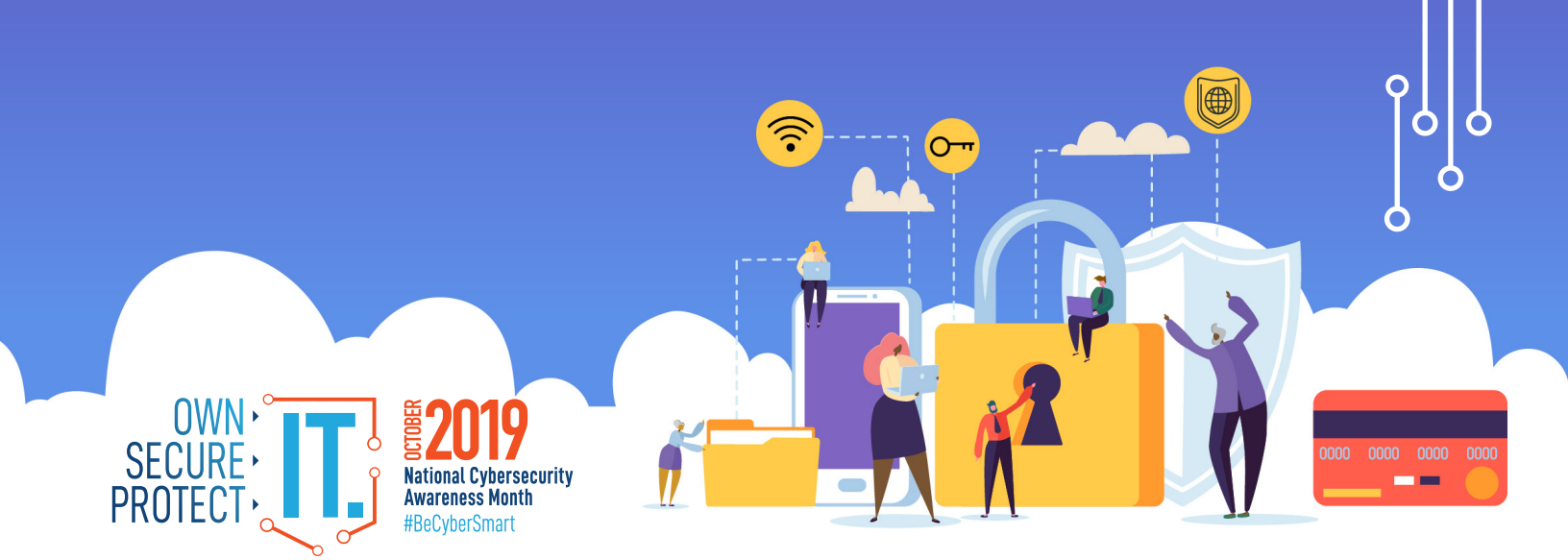
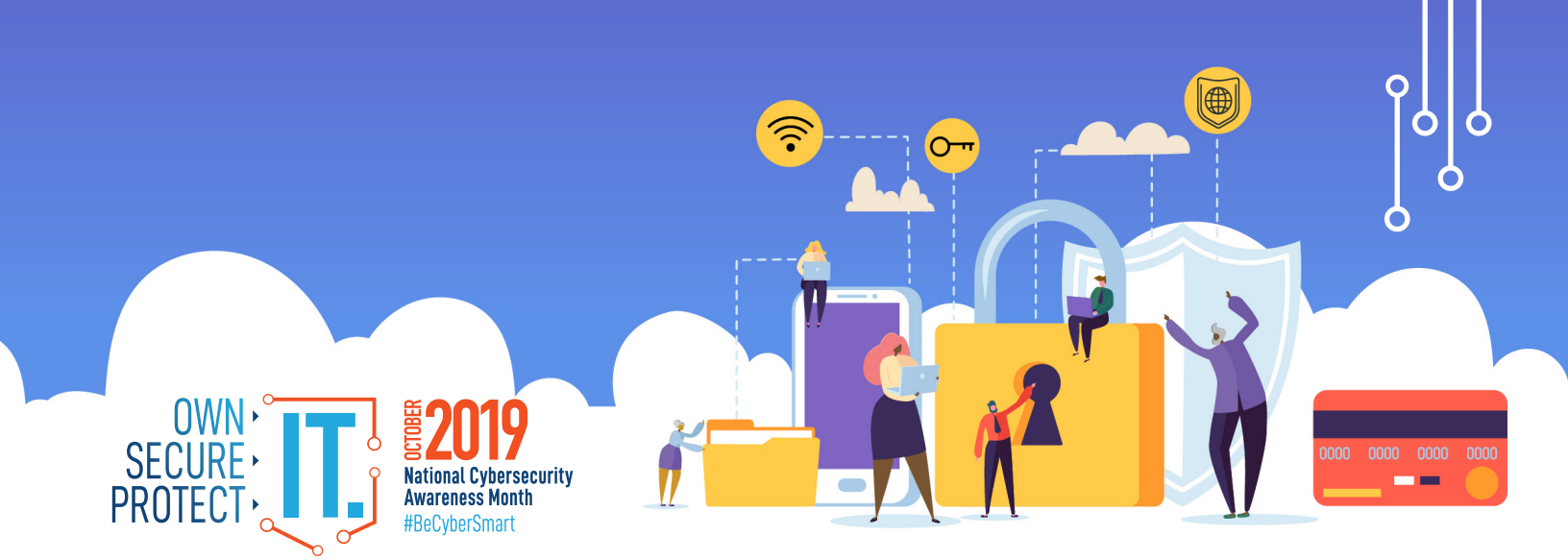


Table Of Contents



Welcome to National Cybersecurity Awareness Month 2019

Held every October, National Cybersecurity Awareness Month (NCSAM) is a collaborative effort between government and industry to ensure every American has the resources they need to stay safe and secure online while increasing the resilience of the Nation against cyber threats.

The Cybersecurity and Infrastructure Security Agency (CISA) and the National Cyber Security Alliance (NCSA) co-lead NCSAM.

Thank you for participating in NCSAM. To assist with your efforts and participation, this document includes a wealth of resources to engage and promote the core theme and critical messages leading up to and throughout October.

Themes and Key Messages for October 2019

This year's overarching theme is "OWN IT. SECURE IT. PROTECT IT." NCSAM will emphasize the role each individual plays in online safety and stress the importance of taking proactive steps to enhance cybersecurity at home and in the workplace. Consider incorporating the theme as you promote and plan your organization's October initiatives.

2019 Overarching Theme

OWN IT. SECURE IT. PROTECT IT.
#BeCyberSmart

NCSAM Key Messages

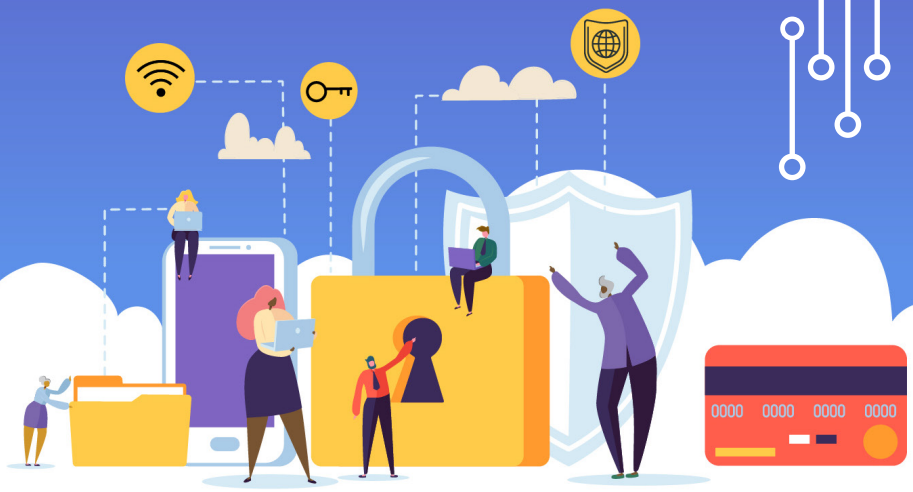
To help frame conversations, design resources, and drive events with internal and external stakeholders, we are breaking down the overarching theme into three components. The key messages below will be featured throughout the month to help drive events, resources, and activities executed by CISA and NCSA. We have included potential topics to help jump start your own NCSAM efforts.

"OWN IT."

Understand your digital profile.
Internet-based devices are present in every aspect of our lives: at home, school, work, and on the go. Constant connection provides opportunities for innovation and modernization, but also presents opportunities for potential cybersecurity threats that can compromise your most important personal information. Understand the devices and applications you use every day to help keep you and your information safe and secure.

OWN IT. SECURE IT. PROTECT IT.

OCTOBER 2019
National Cybersecurity Awareness Month
#BeCyberSmart



Potential Topics:

- Privacy Settings
- Safe Social Media Posting
- Bring Your Own Device (BYOD)
- Internet of Things/Smart Technology
- Don't Let Your Tech Own You

"SECURE IT."

Secure your digital profile.
Cybercriminals are very good at getting personal information from unsuspecting victims, and the methods are getting more sophisticated as technology evolves. Protect against cyber threats by learning about security features available on the equipment and software you use. Apply additional layers of security to your devices – like Multi-Factor Authentication – to better protect your personal information.

Potential Topics:

- Creating Strong Passwords
- Multi-Factor Authentication
- Ecommerce
- Zero Trust
- Protecting Against Phishing

"PROTECT IT."

Maintain your digital profile.
Every click, share, send, and post you make creates a digital trail that can be exploited by cybercriminals. To protect yourself from becoming a cybercrime victim you must understand, secure, and maintain your digital profile. Be familiar with and routinely check privacy settings to help protect your privacy and limit cybercrimes.

Potential Topics:

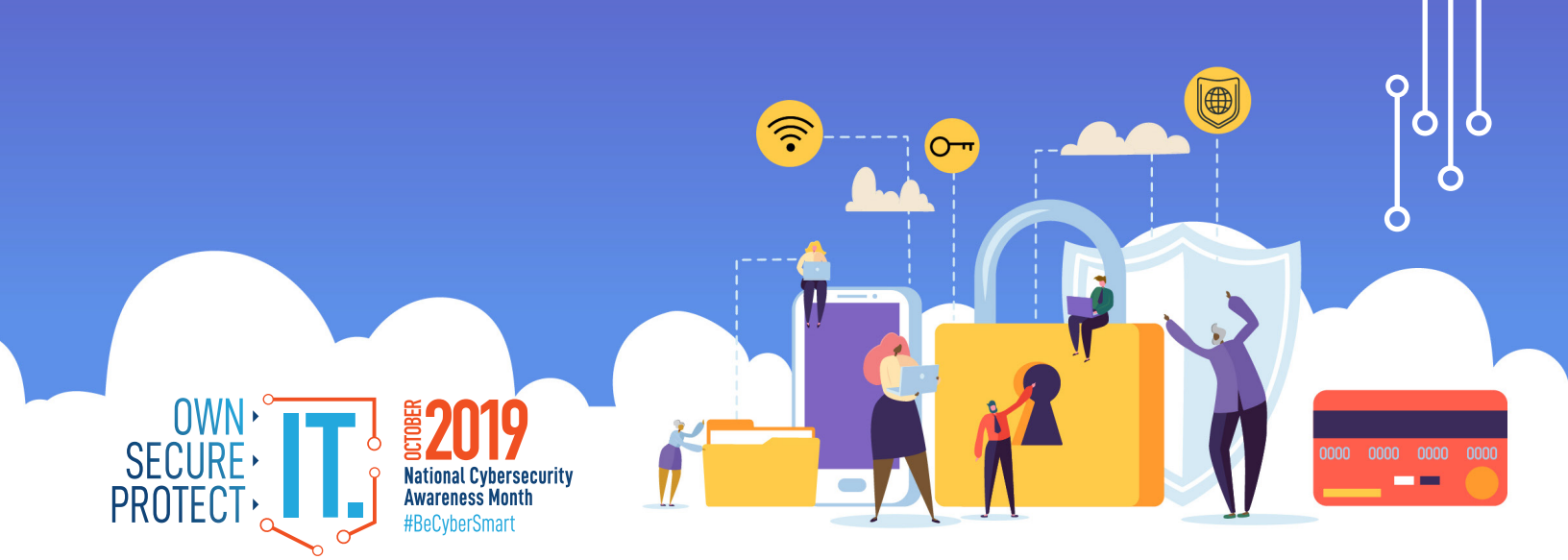
- Researching and Assessing Your Digital Profile
- "Cyber Hygiene"
- Physical Security and Cybersecurity Comparison

How to Engage

This section provides tips on how you can help spread NCSAM cybersecurity messages to reach your intended audiences. The goal of NCSAM 2019 is to promote personal accountability and positive behavior changes when it comes to cybersecurity. To ensure success this October, keep this goal in mind when creating resources, developing activities, and planning events.

Engagement Ideas

- Contribute your voice and resources to social media conversations by using the hashtags #BeCyberSmart and #CyberAware.
- Include messages about the importance of cybersecurity in newsletters, mailings, and websites during October.
- Work with your leadership to issue an official company proclamation to show your company's support of NCSAM and its commitment to OWN IT. SECURE IT. PROTECT IT. Proclamations should highlight what your company does to practice safe cybersecurity.



- Host an event or meeting to discuss local, relevant cybersecurity issues.
- Organize, provide, or promote cybersecurity training and exercise opportunities for your internal and external stakeholders.
- Participate in a local or virtual training or exercise to improve cybersecurity and resilience within your organization.
- Use the Tip Sheets available that offer valuable information on various cybersecurity topics. Whether in the workplace or at home these Tip Sheets have something useful for everyone.
- Become a Friend of the STOP. THINK. CONNECT.™ Campaign by visiting www.dhs.gov/stopthinkconnect.

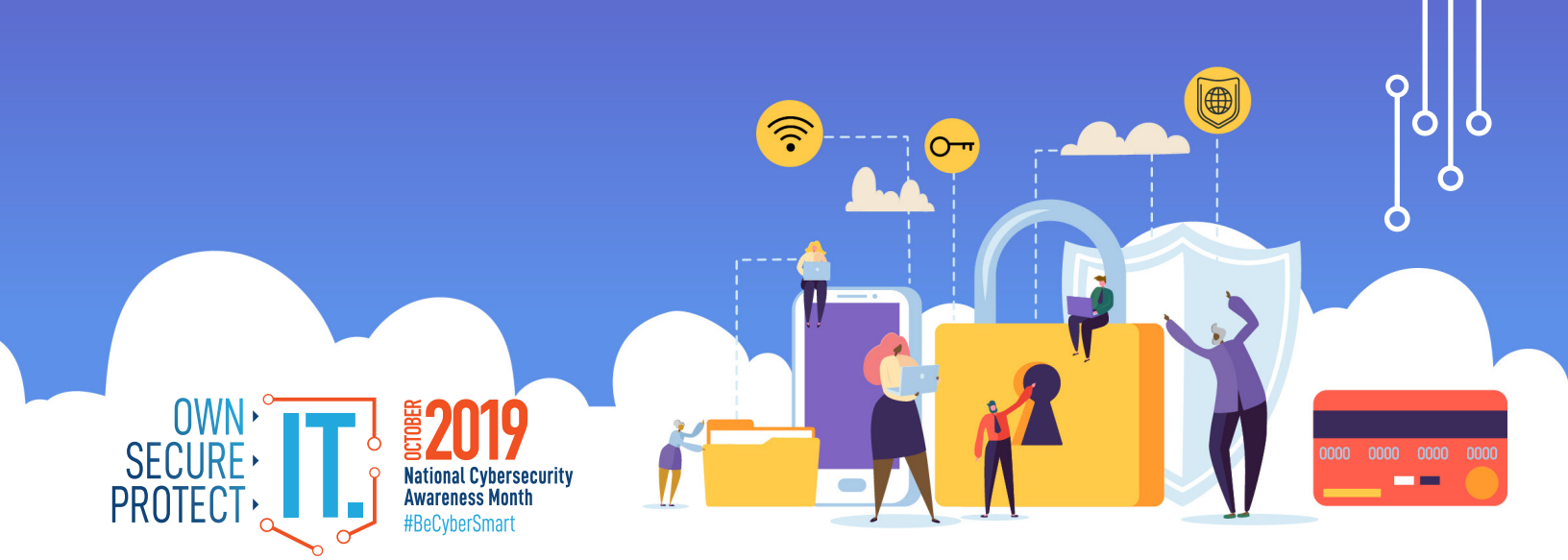
Criteria for Hosting a NCSAM Partner Event

Below are criteria for organizations to use in order to align their events with consistent, harmonized messaging in support of NCSAM 2019 and to be considered a partner event:

- **Use the 2019 NCSAM Logo on Promotional Materials**
  - Event invitations
  - Event signage/backdrops
  - Press materials and/or announcement
- **Social Media**
  - Post about the event (including photos and video clips) on social media using the official NCSAM hashtags #BeCyberSmart and #CyberAware
- **Online**
  - List the event on NCSA's events page. Submit your event details to info@staysafeonline.org including:
    - Event title
    - Event date and time
    - Event location
    - Event website
    - Contact person, including email and/or phone number
    - Any other relevant details
  - Include links to NCSAM pages in event collateral:
    - https://www.dhs.gov/national-cyber-security-awareness-month
    - https://staysafeonline.org/ncsam
- **During the Event**
  - Showcase NCSAM's overarching theme: "Own IT. Secure IT. Protect IT."
  - Align your event's content with the key online safety tips and digital privacy issues outlined in this toolkit

Top Tips to Share during NCSAM

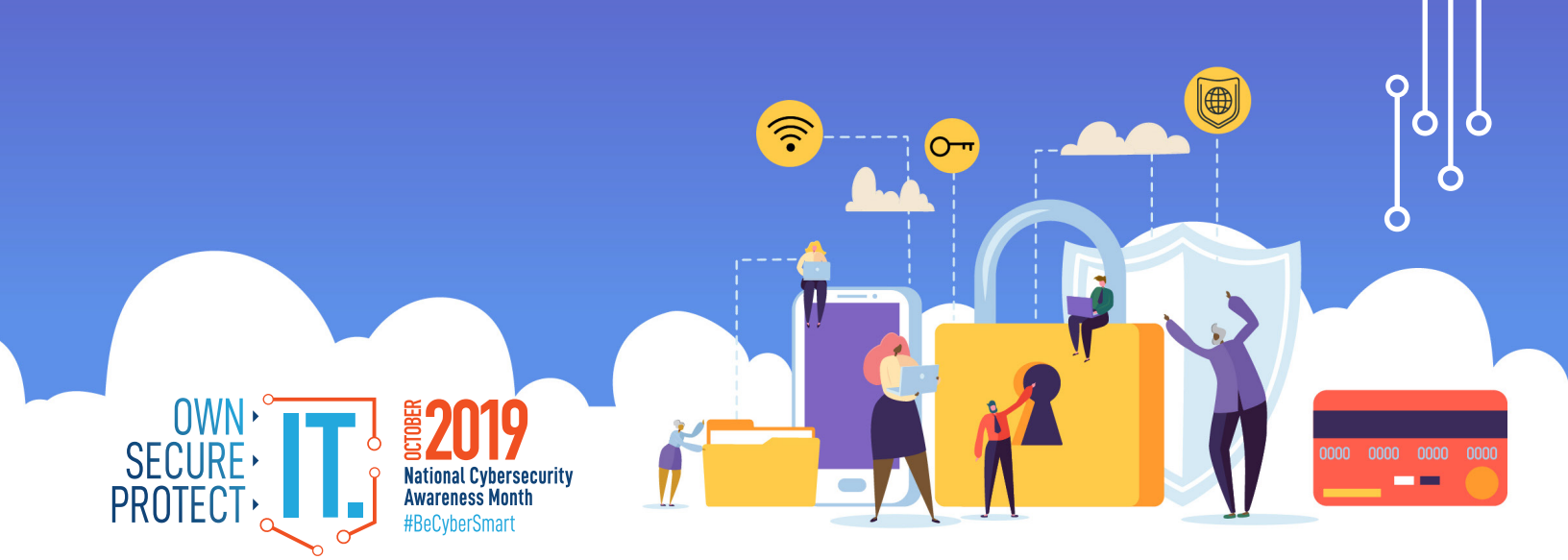
- **Double your login protection.** Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring. Read the Multi-Factor Authentication (MFA) How-to-Guide for more information.



- **Shake up your password protocol.** According to National Institute for Standards and Technology (NIST) guidance, you should consider using the longest password or passphrase permissible. Get creative and customize your standard password for different sites, which can prevent cybercriminals from gaining access to these accounts and protect you in the event of a breach. Use password managers to generate and remember different, complex passwords for each of your accounts. Read the Creating a Password Tip Sheet for more information.
- **If you connect, you must protect.** Whether it's your computer, smartphone, game device, or other network devices, the best defense against viruses and malware is to update to the latest security software, web browser, and operating systems. Sign up for automatic updates, if you can, and protect your devices with anti-virus software. Read the Phishing Tip Sheet for more information.
- **Play hard to get with strangers.** Cybercriminals use phishing tactics, hoping to fool their victims. If you're unsure who an email is from—even if the details appear accurate— or if the email looks "phishy," do not respond and do not click on any links or attachments found in that email. When available use the "junk" or "block" option to no longer receive messages from a particular sender.
- **Never click and tell.** Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don't realize is that these seemingly random details are all criminals need to know to target you, your loved ones, and your physical belongings—online and in the physical world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans. Disable location services that allow anyone to see where you are – and where you aren't – at any given time. Read the Social Media Cybersecurity Tip Sheet for more information.
- **Keep tabs on your apps.** Most connected appliances, toys, and devices are supported by a mobile application. Your mobile device could be filled with suspicious apps running in the background or using default permissions you never realized you approved—gathering your personal information without your knowledge while also putting your identity and privacy at risk. Check your app permissions and use the "rule of least privilege" to delete what you don't need or no longer use. Learn to just say "no" to privilege requests that don't make sense. Only download apps from trusted vendors and sources.
- **Stay protected while connected.** Before you connect to any public wireless hotspot – like at an airport, hotel, or café – be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate. If you do use an unsecured public access point, practice good Internet hygiene by avoiding sensitive activities (e.g., banking) that require passwords or credit cards. Your personal hotspot is often a safer alternative to free Wi-Fi. Only use sites that begin with "https://" when online shopping or banking.

Cybersecurity Resources

Below are useful resources to use both during October and throughout the year. Explore these sites for content to use in blogs, articles, and messaging within your organizations and with external audiences.



- The STOP. THINK. CONNECT.™ Campaign is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Cybersecurity is a shared responsibility. When we all take simple steps to be safer online, it makes using the Internet a more secure experience for everyone. For additional information on STOP. THINK. CONNECT.™, visit https://www.dhs.gov/stopthinkconnect.
- The National Cyber Security Alliance (NCSA) builds strong public/private partnerships to create and implement broad-reaching education and awareness efforts to empower users at home, work, and school with the information they need to keep themselves, their organizations, their systems, and their sensitive information safe and secure online and encourage a culture of cybersecurity. For NCSA recommended events, click: https://staysafeonline.org
- Powered by the U.S. Department of Homeland Security, the "BeCyberSmart" campaign is designed to inspire the younger generation of Americans to take responsibility for their own cyber safety. Learn about cybersecurity basics, common scams, and how to report cybersecurity incidents by visiting the campaign online.
- Looking for information about a particular cybersecurity position or course? The National Initiative for Cybersecurity Careers and Studies (NICCS) tools and resources are available for anyone seeking more information about the cybersecurity field, how to advance a cybersecurity career, and more.

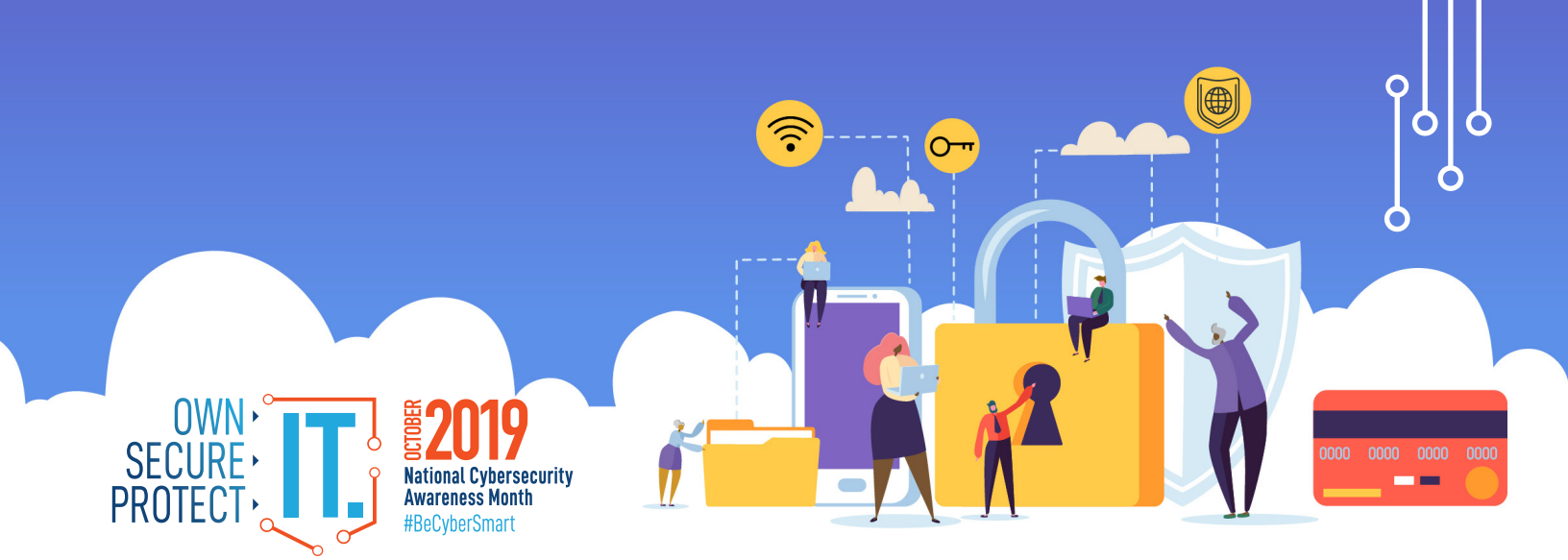
Public Messaging

The official hashtags for NCSAM 2019 are #BeCyberSmart and #CyberAware. Bring visibility to you and your organization's involvement during the month by leveraging these hashtags both before and during October to promote and participate in NCSAM activities and events.

Social Media Communication

Below are sample social media posts to promote NCSAM in your organization. CISA and NCSA highly encourage you to post on your online communication channels leading up to and throughout October.

- Stay connected during National Cybersecurity Awareness Month 2019! Follow @StaySafeOnline and @Cyber to get the latest #BeCyberSmart updates throughout October! #CyberAware
- Prepare to #BeCyberSmart during National Cybersecurity Awareness Month 2019! Check out how you and your organization can get involved throughout October by visiting www.dhs.gov/ncsam #CyberAware
- Want more information on National Cybersecurity Awareness Month 2019? Take a look @StaySafeOnline & @Cyber www.staysafeonline.org & dhs.gov/ncsam #CyberAware
- National Cybersecurity Awareness Month looks at how every employee – from interns to CEOs – has a responsibility for #cybersecurity. #CyberAware
- #DYK there's a free cyber planner available to #smallbiz from @FCC? Find it here: www.fcc.gov/cyberplanner #BeCyberSmart



- Celebrate & #BeCyberSmart with us this National Cybersecurity Awareness Month! We must work together, and all do our part to help build a more secure cyber world. #cybersecurity
- The demand for well-trained cyber pros is at an all-time high. Learn about careers in cyber at https://niccs.us-cert.gov/ #BeCyberSmart #CyberAware
- October is National Cybersecurity Awareness Month! When it comes to #cybersecurity make sure you "OWN IT. SECURE IT. PROTECT IT."! #BeCyberSmart #CyberAware
- How should you approach #cybersecurity? "OWN IT. SECURE IT. PROTECT IT." this October during National Cybersecurity Awareness Month! #BeCyberSmart #CyberAware
- #BeCyberSmart today and every day – join us this October for National Cybersecurity Awareness Month to learn proactive ways to stay safe online. #CyberAware

Sample Communications Calendar

Use the following communications calendar to help plan your awareness and execution efforts leading into and throughout NCSAM. This is intended as a guide only and is not intended to restrict or limit your activities.

August

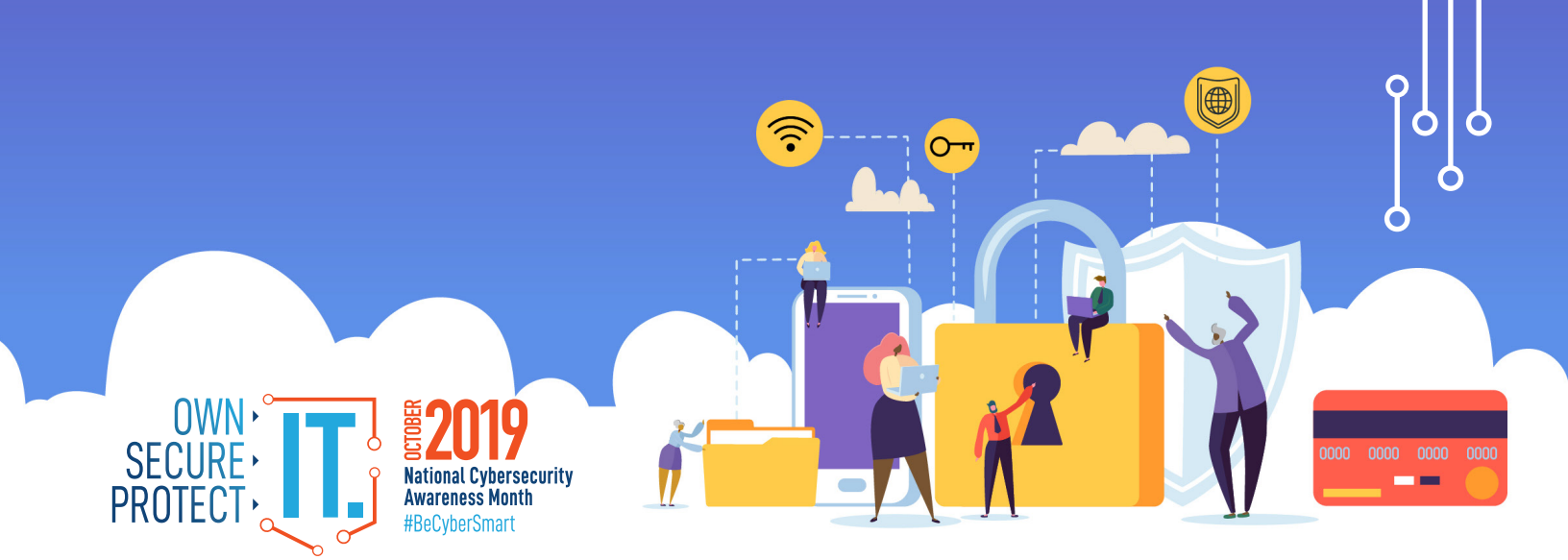
- Begin NCSAM planning between marketing and leadership on October activities and involvement, including potential company communications, news, and research that could be released during the month.
- **Aug. 15:** Attend the NCSA Champion Toolkit Webinar to learn how to use the CISA and NCSA resources - register here.
- **Aug. 19:** Order bulk cybersecurity awareness materials from the FTC to be distributed during October.

September

- **Sept. 4:** Create a digital communications timeline for company and executive social posts, blogs, and emails and other NCSAM promotion throughout the month.
- **Sept. 12:** Issue a press release (to be posted on your website, blog, and social media pages) highlighting your company's involvement in NCSAM.
- **Sept. 17:** Begin two-week countdown to NCSAM on social media channels.
- **Sept. 18:** Send an email to employees announcing your involvement in NCSAM and outlining how your company will get involved leading into and during NCSAM.
- **Sept. 30:** Display NCSAM posters at your business in areas that receive high foot traffic.
- **Sept. 30:** Hold a brown bag lunch for employees to discuss your company's cybersecurity policies and share the NCSAM intro presentation with employees.

October

- **Oct. 1:** Work with your leadership to issue an official company proclamation in support of NCSAM and their commitment to OWN IT. SECURE IT. PROTECT IT.
- **Oct. 1:** Send a customer letter highlighting your business's involvement in NCSAM, and providing helpful "OWN IT. SECURE IT. PROTECT IT." tips for them to #BeCyberSmart.



- **Oct. 1:** Replace or incorporate your company profile picture across social media properties (Twitter, Facebook, LinkedIn, etc.) with the NCSAM logo for duration of October.
- **Oct. 1:** Send/schedule first series of daily or weekly tips to social media and/or employees on how to stay safe online.
- **Oct. 7:** Invite a CISA representative* or a representative from local Federal agencies to speak to your employees about online safety.
- **Oct. 7:** Send/schedule second series of daily or weekly tips to social media and/or employees on how to stay safe online.
- **Oct. 7:** Issue a company news release related to the month (product or offering updates, customer wins, etc.)
- **Oct. 9:** Invite employees to attend "Securing the Supply Chain: Cybersecure My Business™ Webinar" - register here.
- **Oct. 14:** Send/schedule third series of daily or weekly tips to social media and/or employees on how to stay safe online.
- **Oct. 14:** Issue a company news release with research commissioned for the month, when appropriate.
- **Oct. 16:** Conduct a mock phishing simulation with employees.
- **Oct. 21:** Send/schedule fourth series of daily or weekly tips to social media and/or employees on how to stay safe online.
- **Oct. 23:** Host a NCSAM Partner event for employees and/or your local community following the criteria outlined in the toolkit.
- **Oct. 28:** Send/schedule fifth series of daily or weekly tips to social media and/or employees on how to stay safe online.
- **Oct. 29:** Send a final distribution of online safety materials highlighting the importance of being cyber smart all year.
- **Oct. 30/31:** Send employees an email recapping information they've learned throughout the month - consider providing small prizes to those who performed well or were engaged in sponsored activities.

*Please contact us if you need assistance or to request a speaker for your NCSAM events. For more information, please visit https://www.dhs.gov/national-cyber-security-awareness-month. If you would like even more materials (such as posters or additional resources), please email stopthinkconnect@hq.dhs.gov to learn more.