CYBERSECURITY AWARENESS MONTH

CYBERSECURITY AWARENESS MONTH

2022 PDF GUIDE

A Guide To The 19th Annual Cybersecurity Awareness Month

Presented By NATIONAL CYBERSECURITY ALLIANCE

#BeCyberSmart
#CybersecurityAwarenessMonth

It's easy to stay safe online.

CYBERSECURITY AWARENESS MONTH

TABLE OF CONTENTS

Overview 3

Theme and Messaging 4
Key Behaviors

Your Champion Materials 5

Your Cybersecurity Awareness Month Campaign 10
Social Media
Events and Trainings

Additional Resources 15

Contact Us 16

OVERVIEW

WELCOME TO THE 19TH ANNUAL CYBERSECURITY AWARENESS MONTH!

Each October, the National Cybersecurity Alliance offers you a toolkit featuring messaging and content to equip you with the resources you need to build your own cybersecurity education campaign, whether it's at work, at home, or in your community. Because of the support of our friends and partners, the campaign continues to grow year to year, reaching consumers, small and medium sized businesses, corporations, and families around the world.

The National Cybersecurity Alliance launched Cybersecurity Awareness Month in partnership with the U.S. Department of Homeland Security in 2004. The campaign is a strong collaboration between government and private industry to raise awareness about online security. Since then, the campaign has grown globally, reaching individuals in over 75 countries and territories.

SO THEN, WHAT'S NEW FOR 2022?

Our goal is, and always has been, to empower every individual to protect their personal data from cybercrime and we are proud to continue that goal alongside the Cybersecurity and Infrastructure Security Agency for the 19th year with the overarching theme for 2022: **See Yourself In Cyber**

This year is all about taking action! All month long, we are promoting these four key security behaviors to encourage individuals to take control of their online lives:

1.Enable Multi-Factor Authentication
2.Use Strong Passwords and a Password Manager
3.Update Your Software
4.Recognize and Report Phishing

By focusing on these four habits, we hope more people come to the conclusion that it's easy to stay safe online.

We are excited to share our toolkit to help you educate your employees, customers, families, and friends. Thank you for participating in Cybersecurity Awareness Month!

Lisa Plaggemier

Executive Director

National Cybersecurity Alliance

MESSAGING

This year's theme demonstrates that while cybersecurity may seem like a complex subject, ultimately, it's really all about people . This October will focus on the "people" part of cybersecurity, providing information and resources to help educate partners and the public, and ensure all individuals and organizations make smart decisions whether on the job, at home or at school – now and in the future.

41% of survey respondents in 2021 described cybersecurity as intimidating and frustrating (Oh Behave! The Annual Cybersecurity and Attitudes Behavior Report). While most of the cybersecurity news articles are about massive data breaches and hackers, it can seem overwhelming and feel like you're powerless against it.

With this year's messaging and emphasis on "it's easy to stay safe online", we want to remind everyone that while there are all kinds of ways to keep your data protected, following just four key steps can make a big difference. Cybersecurity doesn't have to be overwhelming. With just a few clicks, you can be on your way to keeping your data safe and secure online.

BRANDING

In 2020, we unveiled a new logo for Cybersecurity Awareness Month. This logo was designed to create a recognizable brand for cybersecurity awareness that could be used year over year, and can easily be incorporated into the marketing or branding of other companies and organizations.

We encourage all Champions to use this logo as they see fit. Download the logos and branding guidelines **here.**

YOUR CHAMPION MATERIALS

Each October, the National Cybersecurity Alliance offers you a toolkit featuring messaging and content to equip you with the resources you need to build your own cybersecurity education campaign, whether it's at work, at home, or in your community. Because of the support of our friends and partners, the campaign continues to grow year to year, reaching consumers, small and medium sized businesses, corporations, and families around the world.

When you sign up to become a champion, you will gain access to the following resources:

- This Cybersecurity Awareness Month 2022 PDF Guide, which includes
    - Details on 2022 messaging and activities
    - Ways to engage with Cybersecurity Awareness Month and the National Cybersecurity Alliance
    - How to host your own Cybersecurity Awareness Month events
- A sample email to promote Cybersecurity Awareness Month to your employees
- A sample press release to announce your participation publicly
- Sample articles related to this year's key messaging
- Downloadable logos and branding guidelines
- Social media graphics for Twitter, Facebook and LinkedIn
- Sample social media posts
- A branded video conference background
- A branded email signature graphic
- Infographics on each of the key messages

Keep reading for ideas on how to use these materials and develop your own activities!

MESSAGING AND CONTENT

To help frame conversations, design resources and drive events, we are focusing on promoting four key behaviors that anyone can adopt to stay safe online.

Instead of using weekly themes, as done in the past, we will highlight each behavior throughout the month of October, to drive home their importance. Though we invite partners to turn them into weekly themes if desired.

Partners are welcome to use these behaviors and resources in their own campaigns, but are also encouraged to promote topics and behaviors most relevant to their organizations. Resources on additional topics can be found on **NCA's website** and **CISA's website.**

Don't forget to use **#BeCyberSmart** when you share tips and resources on social media.

ENABLE MULTI-FACTOR AUTHENTICATION

Nearly half (48%) of US/UK respondents say they have "never heard of MFA." Many people don't realize that multi-factor authentication is an incredibly important tool that goes a long way in keeping accounts secure. In fact, **of those who knew about it (52%)**, most had applied MFA to their online accounts (81%) and were still using it (90%), showing that once MFA is enabled, users will keep using it. This month, we're showing others how easy it is to enable MFA wherever possible.

ADDITIONAL FACTS AND FIGURES

- **Only 26% of companies** use multi-factor authentication. (LastPass)
- **Two-factor authentication** has become more popular over the last two years, with 79% of US/UK respondents saying they used it in 2021, compared to 53% who used it in 2019. (Duo Labs)
- **SMS text messages** are the most common second factor US/UK users choose when logging into two-factor authentication accounts, at 85%. (Duo Labs)

USE STRONG PASSWORDS AND A PASSWORD MANAGER

53% of people rely on their memory to manage passwords. (Ponemon Institute)

As our online lives expand, we've gone from having just a few passwords to today, where we might manage upwards of 100. That's 100 unique passwords to remember, if you're using strong password habits. Password managers can save users a lot of headache and make accounts safer by recommending strong passwords. This October, we're dispelling the misconceptions about password managers and showing others how these tools will keep them safe online.

ADDITIONAL FACTS AND FIGURES

- 43% of adults have shared their password with someone. (Google)
- Only 45% of adults would change a password after a breach. (Google)
- 75% of people said they don't know how to create secure passwords in the first place. (Ponemon Institute)
- 81% of the total number of breaches leveraged stolen or weak passwords. (LastPass)
- 61% of employees use the same passwords for multiple platforms. (LastPass)
- The most commonly used password management strategy was writing them down in a notebook (31%). Remembering passwords was also seen as a popular technique reported by 26% of the participants. (NCA)
- Only 12% of the participants reported using a stand-alone password manager application with another 11% saving their passwords in their browser. (NCA)
- 28% of adults in the US use the same password for all of their online accounts. (Business Insider)
- 65% of Americans don't trust password managers. (Password Manager & YouGov)

UPDATE YOUR SOFTWARE

Nearly a third (31%) of US/UK respondents say they either “sometimes,” “rarely,” or “never” install software updates. (NCA)

One of the easiest ways to keep information secure is to keep software and apps updated. Updates fix general software problems and provide new security patches where criminals might get in. This Cybersecurity Awareness Month, we’re telling others to step away from the “remind me later” button to stay one step ahead of cybercriminals.

ADDITIONAL FACTS AND FIGURES

- 68% of the participants reported installing the latest updates and software as soon as these are available. (NCA)
- Of those who reported installing the latest updates to their devices, 45% had turned on automatic updates. A further 21% noting that they take immediate action when they receive a notification. (NCA)
- Just 20% of Android devices use the latest and safest OS version. (Symantec)

RECOGNIZE AND REPORT PHISHING

Phishing attacks in data breaches increased 11% from 2019 to 2020. It went from 25% to 36% based on analysis of confirmed breaches. (Verizon)

Phishing attacks have become an increasingly common problem for organizations of all sizes and can be very difficult to spot. 30% of small businesses consider phishing attacks to be their top cybersecurity concern. It's important for every individual to stop and think before clicking on a link or attachment in a message and know how to spot the red flags. Cybersecurity Awareness Month 2022 will give individuals the tools they need to recognize a phish and report it to their organization or email provider.

ADDITIONAL FACTS AND FIGURES

- Only 60% of adults could define what "phishing" is. (Google)
- Nearly 3 out of 4 companies experienced a phishing attack in 2020 (Symantecs).
- 72% of respondents reported that they checked to see whether messages were legitimate (i.e. phishing or a scam) compared to 10% who reported not doing so. (NCA)
- Nearly half of the participants (48%) reported phishing emails to the sender (e.g. the real person the cyber criminal tried to impersonate by sending the phishing email). (NCA)
- 42% of the participants said they used the reporting capability on a platform (e.g. Gmail) "very often" or "always". (NCA)

YOUR CYBERSECURITY AWARENESS MONTH CAMPAIGN

This section provides tips on how to get involved in Cybersecurity Awareness Month and develop your own campaign. The goal of Cybersecurity Awareness Month is to promote positive behavior change through simple, empowering messaging. To ensure success this October, keep this goal in mind when creating resources and planning activities.

IN YOUR ORGANIZATION AND COMMUNITY

- Encourage your colleagues and partners to become **2022 Champions** and join the effort to build a safer digital world. Encourage your employees to sign up as Champions too so they can stay up-to-date on resources and activities.
- Send an email to colleagues, employees, customers and/or your school and community about Cybersecurity Awareness Month. Outline how your organization will be involved. Highlight the key behaviors and advice. See the "Sample Employee Email" in your toolkit to get started.
- Incorporate Cybersecurity Awareness Month into a newsletter. Use copy from the "sample employee email" and use information from **staysafeonline.org**
- Do you work with students? Host a poster/video contest where students can create informative online safety resources for their school and community. Display the winning entries and consider awarding prizes!
- Work with leadership to issue an official press release, proclamation, or video announcement to show your organization's support of Cybersecurity Awareness Month. Proclamations should highlight what your company does to practice cybersecurity. See the "Sample Press Release" in your toolkit
- Host a local or virtual event or training for your organization or community. Discuss smart security practices, relevant cybersecurity issues, and allow participants to ask pressing cyber-related questions. Continue reading for more tips on hosting an event.
- Post the Cybersecurity Awareness Month logo on your company's internal or external website.
- Issue a company promotion related to the month, such as a product discount, competition, or giveaways for customers.
- Conduct a mock phishing simulation with employees. Remember to reward positive behavior! Not to punish for mistakes. Consider providing small prizes to those who perform well and are engaged in activities.
- Distribute online safety materials and tip sheets. NCA provides plenty of non-proprietary materials available to download and print from our **library.**

- At the end of the month, send employees an email highlighting your activities, results, and successes. Recap best practices learned throughout the month.
- Remember that cybersecurity education isn't limited to October! Use these ideas to educate your organization and community all year long!

AT HOME

- Share tip sheets and print resources and display them in areas where family members spend time online.
- Hold a family "tech talk" and discuss how each family member can protect their devices, accounts, and personal information.
- Send an email to friends and family informing them that October is Cybersecurity Awareness Month and share helpful tips and resources. Especially with vulnerable groups, such as seniors.

SOCIAL MEDIA

One of the best ways to get involved is to join the conversation online! NCA and CISA highly encourage you to post on online communications channels leading up to and throughout October.

- Post online safety tips and contribute your own advice and resources to social media by using the hashtags #BeCyberSmart and #CybersecurityAwarenessMonth.
- Use our pre-drafted social media posts and graphics leading up to and throughout the month. Feel free to customize them with your own messages and logos
- Replace or incorporate your personal or company profile picture or banner image on social media platforms with the Cybersecurity Awareness Month logo for the duration of October.
- Blog about cybersecurity. Choose a topic that appeals to you and your audience or highlight one of the key behaviors. You can use the sample articles in your toolkit.
- Follow the National Cybersecurity Alliance and Cybersecurity and Infrastructure Security Agency (CISA) on social media to receive the latest online safety news.
  - **National Cybersecurity Alliance**
    - Twitter
    - LinkedIn
    - Facebook
    - Instagram
    - Youtube
    - TikTok
  - **CISA**
    - Twitter
    - LinkedIn
    - Facebook

HOSTING AN EVENT OR TRAINING

Hosting an event or training on online safety is easier than you may think! Below are some ideas to help you get started.

KEEP IT LIGHT

Cybersecurity is a serious issue, but our conversations don't have to be scary. Make sure event content is empowering for your audience. Try to use humor or storytelling to engage learners and get their attention.

SHOW BUY-IN FROM LEADERSHIP

Engage your organizations C-Suite leadership (CEO, CIO, CISO) to emphasize the importance of cybersecurity to the organization and to establish cybersecurity into the corporate culture.

MAKE THE LEARNING EXPERIENCE RELATABLE AND INTERACTIVE

Align your event with what is most important to your organization, but don't be afraid to get creative with the following suggestions.

- Conduct live demonstrations such as how to use a company-issued VPN or how to install a company-approved authenticator app.
- Create a table-top exercise where cross-functional teams act out a scenario and practice their response strategies. **See CISA's tabletop exercise packages.**
- Test your audience's knowledge with a game or poll
- Give the audience time to ask questions
- Make cybersecurity education more relatable for employees by tying the topic to their home or family life, or to their specific department/role in the organization

RECOGNIZE AND REWARD ENGAGEMENT

Give out prizes to participants for performing well on quizzes or asking questions. Even just giving out branded pens, small toys or gift cards can create a fun and engaging event.

DON'T FORGET TO FOLLOW UP

Reach out to your attendees after the event. Thank them for coming and include any slides, information and resources you covered during the event.

ALIGN YOUR EVENT

Below are tips to help you align your event with Cybersecurity Awareness Month and request speakers.

Use the logo in promotional materials, including

- Event invitations
- Signage/backdrops
- Event materials and print-outs

Use the free resources from CISA and NCA as hand-outs or pull copies to use as training content.

- NCA Resource Library
- CISA Resource Hub

List the event on NCA's **community calendar.**

You can submit any public events to our website! Submit the following details to info@staysafeonline.org

- Event title
- Description
- Date and Time
- Location
- Website/registration page

NEED A SPEAKER?

Whether you're looking for a subject matter expert or speaker to present on Cybersecurity Awareness Month to your employees, you can request a speaker from NCA or CISA:

- To request an NCA speaker, complete the speaker request form **here.**
- To request a CISA speaker, fill out and submit a Speaker Request Form **here.** Please submit requests at least two weeks before your event and allow three to five business days for a response to your request.

ADDITIONAL RESOURCES

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

- CISA Cyber Essentials Toolkit - The Cyber Essentials Toolkit is a set of modules designed to break down the CISA Cyber Essentials into bite-sized actions for IT and C-suite leadership to work toward full implementation of each Cyber Essential. Each chapter focuses on recommended actions to build cyber readiness into the six interrelated aspects of an organizational culture of cyber readiness.

- CISA Cyber Hygiene Services - CISA offers several scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors.

- CISA Cybersecurity Training and Exercises - Training is essential to preparing the cybersecurity workforce of tomorrow, and for keeping current cybersecurity workers up-to-date on skills and evolving threats. CISA is committed to providing the nation with access to cybersecurity training and workforce development efforts to develop a more resilient and capable cyber nation.

- FTC Free Publications - Find free publications about scams, privacy, credit, and more from the FTC. You can download and print a few copies, or order in bulk.

- NCA Cybersecurity Education & Career Resources - There is a critical shortage of cybersecurity professionals.NCA has compiled free resources focused on fulfilling the mission of diversifying and filling the gap in the cybersecurity careerforce. For cybersecurity professionals of today and tomorrow.

- NCCOE - The National Cybersecurity Center of Excellence brings together experts from industry, government, and academia to address the real-world needs of securing complex IT systems and protecting the nation's critical infrastructure.

- NICE Cybersecurity Career Awareness Week - Join the National Initiative for Cybersecurity Education (NICE) in promoting awareness & exploration of cybersecurity careers by hosting an event, participating in an event near you, or engaging students with cybersecurity content!

CONTACT US

About the National Cybersecurity Alliance

The National Cybersecurity Alliance is a non-profit organization on a mission to create a more secure, interconnected world.

We advocate for the safe use of all technology and educate everyone on how best to protect ourselves, our families, and our organizations from cybercrime.

We create strong partnerships between governments and corporations to amplify our message and to foster a greater “digital” good.

WEBSITE

staysafeonline.org

CONTACT

info@staysafeonline.org

About the Cybersecurity and Infrastructure Security Agency (CISA)

CISA works with partners to defend against today’s threats and collaborates to build a more secure and resilient infrastructure for the future. We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

WEBSITE

cisa.gov

CONTACT

CyberAwareness@CISA.DHS.gov