SECURE OUR WORLD

CYBERSECURITY AWARENESS MONTH

2023 Partner Toolkit

#CybersecurityAwarenessMonth
#SecureOurWorld

Presented By

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

NATIONAL CYBERSECURITY ALLIANCE

TABLE OF CONTENTS

WELCOME TO THE 20TH CYBERSECURITY AWARENESS MONTH!

Held every October, Cybersecurity Awareness Month is a collaboration between the government and private industry to empower everyone to protect their personal data from digital forms of crime. This toolkit is dedicated to creating resources and communications for organizations to talk to their employees and customers about staying safe online.

The Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA) work collaboratively throughout the year in support of Cybersecurity Awareness Month and have created this toolkit with a wealth of resources to help you create your own Cybersecurity Awareness Month campaign!

This year marks the 20th Cybersecurity Awareness Month. Like technology, Cybersecurity Awareness Month has grown rapidly. People now celebrate Cybersecurity Awareness Month all over the world! As we become more dependent on technology, it's more important than ever to strengthen and adapt our cybersecurity habits. This toolkit provides several resources to keep you and your community safe.

NEW EVERGREEN THEME!

We are excited to announce the launch of a brand new, enduring theme that will be used year-round and in future Cybersecurity Awareness Months. Secure Our World is a new awareness campaign from CISA that aims to broadly promote cybersecurity tips and best practices year-round for all individuals. Partners can start incorporating this theme into their future campaigns and year-round initiatives for 2023 and beyond.

SECURE OUR WORLD

KEY MESSAGES

CISA and NCA will promote these four key cybersecurity behaviors throughout October. These behaviors are simple and actionable for both individuals and businesses and provide the basis for Cybersecurity Awareness Month resources, events and presentations:

CREATE STRONG PASSWORDS AND USE A PASSWORD MANAGER

TURN ON MULTIFACTOR AUTHENTICATION

RECOGNIZE AND REPORT PHISHING

UPDATE YOUR SOFTWARE

TONE

The Cybersecurity Awareness Month narrative articulates that cybersecurity doesn't have to be scary. It can be easy to adopt secure habits and even provide you some peace of mind that your online life is safe. We do this through the following tone of voice:

- **Positivity** – Scare tactics don't work. Instead of using scary "hackers in hoodies" imagery, talk about the benefits of reducing cyber risks and how strengthening cybersecurity can protect what matters most in our lives.
- **Approachability** – Cybersecurity seems like a complex subject to many, but it's really all about people. Make cybersecurity relatable and share how practicing good cyber hygiene is something that anyone can do.
- **Simplicity** – Avoid jargon and be sure to define acronyms
- **Back to basics** – Even just practicing cyber hygiene basics provides a solid baseline of security.

MATERIALS

Each October, Champions receive 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. Through the support of our partners, the campaign continues to grow year over year, reaching individuals, families, small and medium sized businesses, corporations, and so many others around the world.

Your toolkit includes:

- This Cybersecurity Awareness Month PDF Guide, which includes
  - Details on 2023 messaging and activities
  - Ways to engage with Cybersecurity Awareness Month
  - How to host your own Cybersecurity Awareness Month events
- Email template to promote Cybersecurity Awareness Month to your employees
- Press release template to announce your participation publicly
- Social media graphics
- Sample social media posts
- Branded video conference background
- Branded email signature graphic
- Infographic
- And coming soon!
  - PSAs and videos
  - Translated resources
  - Tip sheets on each of the four key messages

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

USE STRONG PASSWORDS AND A PASSWORD MANAGER

As our online lives expand, the average user has gone from having just a few passwords to now managing upwards of 100. That's 100 unique passwords to remember, if you're using strong password habits. Password managers can save users the trouble of having to remember multiple passwords and make accounts safer by recommending strong, unique passwords and storing them all in one place.

OUR TIPS AND ADVICE

Using an easy-to-guess password is like locking the door but leaving the key in the lock. Weak passwords can quickly be cracked by computer hackers. The good news is that strong passwords are one of the easiest ways to protect your accounts from compromise and reduce the risk of someone stealing sensitive information, data, money, or even your identity.

STRENGTHEN YOUR PASSWORDS WITH THESE TIPS

1. Longer is stronger: Passwords with at least 16 characters are hardest to crack.
2. Hard to guess: Use a random string of mixed-case letters, numbers and symbols. If you need to memorize a password, create a memorable "passphrase" of 5 – 7 unrelated words. Get creative with spelling and/or add numbers or symbols
3. One of a kind: Use a unique password for each account.

Remembering long, unique passwords for every account in our lives is impossible. Rather than write them down or reuse weak passwords, **use a password manager.**

Password managers generate complex and unique passwords for you, store them all in one place and tell you when you have weak, re-used passwords, or compromised passwords. They can also automatically fill credentials into sites and apps using a secure browser plugin. You only need to remember one master password—the one for accessing the password manager itself. (Tip: Create a memorable long "passphrase" as described above and NEVER write your master password down.)

ADDITIONAL FACTS AND FIGURES

- Only 33% of individuals create unique passwords for all accounts (NCA)
- Only 18% of individuals have downloaded a password manager (NCA)

TURN ON MULTIFACTOR AUTHENTICATION

In a recent National Cybersecurity Alliance survey, 57% of respondents said they have heard of multifactor authentication (MFA), but many people don't realize that multifactor authentication is an incredibly important layer of protection in keeping accounts secure. This month, we're showing others how easy it is to turn on MFA whenever possible.

OUR TIPS AND ADVICE

MFA provides extra security by providing a secondary method confirming your identity when logging into accounts. MFA usually requires you to enter a code sent to your phone or email, or one generated by an authenticator app. Push notifications are also common methods of MFA. This added step prevents unauthorized users from gaining access to your accounts, even if your password has been compromised.

FOLLOW THESE STEPS TO TURN ON MFA

- **Open your app or account settings**
  - It may be called Account Settings, Settings & Privacy or similar.
- **Turn on multifactor authentication**
  - It may also be called two-factor authentication, two-step authentication or similar.
- **Confirm**
  - Select an MFA method to use from the options provided. Examples are:
    - Receiving a code by text or email
    - Using an authenticator app: These phone-based apps generate a new code every 30 seconds or so.
    - Biometrics: This uses facial recognition or fingerprints to confirm your identity.

ADDITIONAL FACTS AND FIGURES

- Of those who have heard of MFA, 79% had applied it to their online accounts. (NCA)
- Of that number, 94% said they are still using MFA, showing that once MFA is enabled, users will keep using it. (NCA)

RECOGNIZE AND REPORT PHISHING

Phishing attacks have become an increasingly common problem for organizations of all sizes and can be very difficult to spot. It's important every individual stop and think before clicking on a link or opening an attachment and know how to spot red flags. Cybersecurity Awareness Month 2023 guidance provides the tools needed to recognize and report phishing it to their organization or email provider.

OUR TIPS AND ADVICE

Phishing occurs when criminals try to get you to open harmful links or attachments that could steal personal information or infect devices. Phishing messages or "bait" usually come in the form of an email, text, direct message on social media or phone call. These messages are often designed to look like they come from a trusted person or organization, to get you to respond. The good news is you can avoid the phish hook and keep accounts secure!

FOLLOW THESE TOP TIPS:

1. Recognize - Look for these common signs:

- Urgent or alarming language
- Requests to send personal and financial information
- Poor writing, misspellings, or unusual language
- Incorrect email addresses, domain names, or links (e.g. amazan.com)

2. Report - If you suspect phishing, report the phish to protect yourself and others.

- Know your organization's guidance for reporting phishing. If your organization offers it, you may find options to report via the "report spam" button in your email toolbar or settings.
- For personal email accounts, you may be able to report spam or phishing to your email provider by right-clicking on the message.

3. Delete - Delete the message. Don't reply or click on any attachment or link, including any "unsubscribe" link. Just delete.

ADDITIONAL FACTS AND FIGURES

- 72% of respondents reported that they checked to see whether messages were legitimate (i.e. phishing or a scam) compared to 15% who reported not doing so. (NCA)
- 47% of the participants said they used the reporting capability on a platform (e.g. Gmail, Outlook) "very often" or "always". (NCA)

UPDATE YOUR SOFTWARE

Approximately 2 in 5 survey respondents say they either “sometimes,” “rarely,” or “never” install software updates (NCA). One of the easiest ways to protect accounts and information is to keep software and applications updated. Updates are periodically released to fix software problems and provide security patches for known vulnerabilities. This Cybersecurity Awareness Month, don’t hit the “remind me later” button. Take action to stay one step ahead of cybercriminals.

OUR TIPS AND ADVICE

Keeping software up to date is an easy way improve your digital security. For added convenience, turn on the automatic updates in your device or application security settings! Set it and forget it!

KEEP SOFTWARE UP TO DATE WITH THESE STEPS:

1. Check for notifications

Devices and applications will usually notify you when the latest software updates become available, but it’s important to check periodically as well. Software updates include devices’ operating systems, programs and apps. It’s important to install ALL updates, especially for web browsers and antivirus software, or apps with financial or sensitive information.

2. Install updates as soon as possible

When a software update becomes available, especially critical updates, be sure to install them as soon as possible. Attackers won’t wait, and you shouldn’t either!

3. Turn on automatic updates

With automatic updates, devices will install updates as soon as they become available—Easy! To turn on the automatic updates feature, look in the device settings, usually under Software or Security.

ADDITIONAL FACTS AND FIGURES

- 36% of survey participants reported installing the latest updates and software as soon as they became available. (NCA)
- Of those who reported installing the latest updates to their devices, 62% had turned on automatic updates. (NCA)

BUILDING YOUR 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

- **Emails**: Send an email to colleagues, employees, customers and/or your school about the month. Outline how your organization will be involved. Highlight the key behaviors and advice provided in this toolkit. See the "Sample Employee Email" in this toolkit to get started.

- **Newsletters**: Incorporate Cybersecurity Awareness Month into a newsletter. Use copy from the "sample employee email".

- **Contests**: 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!

- **Info booth**: Set up an information station! Whether it's in your school's student center or a company break room, set up an area to hand out info sheets and talk to people within your organization or school.

- **Promotion**: Work with leadership to issue an official press release, proclamation, or video announcement to show your organization's support. Announcements should highlight what your company does to practice cybersecurity. See the "Sample Press Release" in this toolkit.

- **Event**: Host a local or virtual event or training for your organization. Discuss smart security practices, relevant cybersecurity issues, and allow participants to ask cyber-related questions. Continue reading for more tips on hosting an event or training session.

- **Gamification**: Host a phishing game or competition. Send fake phishing emails to your employees and reward those who catch and report the most phishing attempts.

BUILDING YOUR CAMPAIGN

IN YOUR ORGANIZATION (continued)

- **Branding**: Post the Cybersecurity Awareness Month logo on your company's internal or external website.

- **Incentives**: Issue a company promotion related to the month, such as a product discount, competition, or giveaways for customers.

- **Training**: Conduct a phishing simulation with employees. Remember to reward positive behavior and not to punish for mistakes. Consider providing small prizes to those who perform well and are engaged in activities.

- **Handouts**: Distribute online safety materials and tip sheets. We provide plenty of non-proprietary materials available to download and print from staysafeonline.org.

- **Recap**: At the end of the month, send employees an email highlighting your activities, results, and successes. Recap best practices learned throughout the month.

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 and teens.

- Create a culture of security in your family. Make it clear to all family members that they should feel comfortable sharing if they've clicked on a malicious link, downloaded something they shouldn't have or have fallen for a scam, especially for kids and seniors.

HOSTING AN EVENT OR TRAINING

Hosting an event or training session 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. Generate event content that 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 organization's senior leadership (CEO, CIO, CISO) to emphasize the importance of cybersecurity to the organization and to demonstrate cybersecurity as part of 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. Giving out branded swag, candy, or gift cards can create a fun and engaging event.

- Do you use a security vendor? See if they have free swag they can send over for you to give out to employees!

DON'T FORGET TO FOLLOW UP

Reach out to your attendees after the event. Thank them for coming and include any presentation materials 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 printouts
- Use the free resources from CISA, NCA, and other organizations, listed in the "Additional Resources" page of this guide, as hand-outs or pull copies to use as training content.
- 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 link

REQUEST A CISA SPEAKER

To request a CISA speaker, submit a Speaker Request Form at here. Speaking requests are processed on a rolling basis and we encourage partners to request speakers year-round!

REQUEST A NATIONAL CYBERSECURITY ALLIANCE PRESENTATION

This October, the National Cybersecurity Alliance is offering fun, interactive Cybersecurity Awareness Month presentations to organizations of all sizes. These informative talks will cover the "cyber basics" and enhance your organization's internal training and events for employees.

By participating in these talks, employees will gain valuable knowledge to strengthen their cybersecurity practices and contribute to a safer digital environment.

To schedule a talk, select a preferred time slot through our "request a speaker form."

TEACH OTHERS HOW TO STAY SAFE ONLINE

Even if you don't think of yourself as a teacher, you have something to share with your friends, neighbors, and other people in your community. Consider volunteering at a community center, senior center, school, library or scout troop to teach others about the cyber basics. Here are some tips to help you prepare a "Cyber Basics" talk

- **Patience** - Reach out early to leaders in the community to pitch your presentation. If you want to give a talk during Cybersecurity Awareness Month, consider reaching out six months in advance. Sounds crazy? A lot of librarians, club leaders, and school administrators plan events very early, so you want to consider their schedules and be courteous of their planning.

- **Audience Focus** - Get an understanding of the tech knowledge of your audience! Talk to the community leader that scheduled your presentation to understand how they use technology within the club/organization and how they might use it in their everyday lives.

- **Takeaways** - Create a slide deck or supplemental material that people can take home with them. Have your presentation double as a learning guide after you leave. Give them resources where they can reach out for more help, especially if they have a cybersecurity incident. Make sure they know what help is available to them, and who they should contact, FBI, CISA, etc. Your job is to give them some education, then leave them with resources, tips, and contacts for them to use on their own.

- **Empower and Educate** - Do not use fear, uncertainty, or doubt to get your point across. Focus on simple, empowering, and friendly tips and language. Stay away from jargon and acronyms. Keep your talk informational and informative without being condescending. They want to learn. Provide more in-depth explanations as needed.

- **Feel it out** - Talk to a community leader on what their biggest concerns, fears, or issues are. Don't go on for 20 minutes about cloud security, if what they really need is to understand what a phishing email looks like. Read your audience!

Check out NCA's Volunteer Toolkit and video series for more tips.

JOIN THE CONVERSATION ONLINE

One of the best ways to get involved is to join the conversation online! We highly encourage you to post on social media 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:

#CybersecurityAwarenessMonth

#SecureOurWorld

- 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 CISA and NCA on social media to receive the latest online safety news.

CISA	NCA
Twitter	Twitter
LinkedIn	LinkedIn
Facebook	Facebook
Instagram	Instagram
Youtube	Youtube

Remember that cybersecurity education isn't limited to October! Use these ideas to educate your organization and community all year long!

ADDITIONAL RESOURCES

Below are free resources useful 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 Hygiene Services - CISA offers several scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to identify and notify organizations of occurring or emerging threats.

CISA Cybersecurity Training and Exercises - Training is essential for keeping workers knowledgable on cybersecurity. CISA is committed to providing the nation with access to cybersecurity training and workforce development materials to develop a more resilient and capable cyber nation.

Cyber.org - Cyber.org empowers K-12 educators to teach cyber confidently, resulting in students with the skills and passion needed to succeed in the cyber workforce.

GetCyberSafe Cybersecurity Awareness Month - When cyber attacks like phishing are successful, they can ruin our days, to put it lightly. That's why, this Cyber Security Awareness Month, we're encouraging Canadians to ruin a cyber criminal's day.

ENISA European Cybersecurity Awareness Month - The European Cybersecurity Month (ECSM) is the European Union's annual campaign dedicated to promoting cybersecurity among EU citizens and organisations, and to providing up-to-date online security information through awareness raising and sharing of good practices.

Federal Trade Commission (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 Resources and Guides - The National Cybersecurity Alliance wants to make it easy for everyone to learn more about cybersecurity and staying safe online. Explore articles and other resources you need to raise awareness at home, work, school, or throughout your community.

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

GET IN TOUCH

THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

As America's Cyber Defense Agency and the National Coordinator for critical infrastructure resiliency and security, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.

WEBSITE

cisa.gov/cybersecurity-awareness-month

CONTACT

AwarenessCampaigns@cisa.dhs.gov

CONTACT YOUR CISA REGIONAL OFFICE BY VISITING
www.cisa.gov/about/regions

REPORT A CYBER ISSUE
report@cisa.dhs.gov or (888) 282-0870.

ABOUT THE NATIONAL CYBERSECURITY ALLIANCE (NCA)

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