



SEE
YOURSELF
IN **CYBER**

WAYS TO CREATE A CAMPAIGN

*Key messaging, articles, social media, and more
to promote Cybersecurity Awareness Month 2022*



**CYBERSECURITY
AWARENESS
MONTH 2022**



CYBERSECURITY AWARENESS MONTH 2022

WELCOME

WELCOME TO CYBERSECURITY AWARENESS MONTH 2022

Since 2004, the President of the United States and Congress have declared October to be Cybersecurity Awareness Month, helping individuals protect themselves online as threats to technology and confidential data become more commonplace.

The Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA) lead a collaborative effort between government and industry to raise cybersecurity awareness nationally and internationally. While CISA works to increase cybersecurity throughout the government, its regions and critical infrastructure sectors, NCA works with corporations and the general public to raise awareness of action steps we can take to advance digital security.

SEE
YOURSELF
IN CYBER

This year's campaign theme — "See Yourself in Cyber" — 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 CISA 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. We encourage each of you to engage in this year's efforts by creating your own cyber awareness campaigns and sharing this messaging with your peers.

For individuals and families, we encourage you to See Yourself taking action to stay safe online. That means enabling basic cyber hygiene practices: update your software, think before you click, have good strong passwords or a password keeper, and enable multi-factor authentication (meaning you need "More Than A Password!") on all your sensitive accounts. For those considering joining the cyber community, we encourage you to See Yourself joining the cyber workforce. We'll be talking with leaders from across the country about how we can build a cybersecurity workforce that is bigger, more diverse and dedicated to solving the problems that will help keep the American people safe.

For our partners in industry, we encourage you to See Yourself as part of the solution. That means putting operational collaboration into practice, working together to share information in real-time, and reducing risk and build resilience from the start to protect America's critical infrastructure and the systems that Americans rely on every day.

Throughout October, CISA and NCA will highlight key action steps that everyone should take:

Think Before You Click: Recognize and Report Phishing

Update Your Software

Use Strong Passwords

Enable Multi-Factor Authentication



CYBERSECURITY AWARENESS MONTH 2022

WAYS TO

GET
INVOLVED

WAYS TO GET INVOLVED

There are many ways to get involved in Cybersecurity Awareness Month, including:

1. Join NCA's Champion Program to receive additional resources to support your campaigns: <https://staysafeonline.org/programs/cybersecurity-champion/>.
2. Review the Cybersecurity Awareness Month Public Toolkit. The public toolkit gives you access to free resources you can use all year, including an events calendar, a speaker booking tool, training documents and more.
3. Join the conversation! Using #SeeYourselfInCyber in your social posts will ensure you can view and contribute to the conversation all month long!

HOW YOU CAN PARTICIPATE

Join us at a wide variety of activities and learning opportunities throughout October to learn the cyber basics, as well as advanced cybersecurity issues. We encourage you to explore our website www.cisa.gov/cybersecurity-awareness-month and participate in theme days, including Women in Tech, International Day, and for anyone interested in exploring a career in cybersecurity, Career Day. There will also be a series of webinars including cyber basics, which every user should know.

1. The **CISA Cybersecurity Awareness Month webpage**: www.cisa.gov/cybersecurity-awareness-month
2. CISA on social media:
 - Twitter at **@CISAgov** twitter.com/cisagov
 - LinkedIn at **@Cybersecurity & Infrastructure Security Agency** www.linkedin.com/company/cisagov/
 - Facebook at **@CISA** www.facebook.com/CISA
3. Our partner the **National Cybersecurity Alliance (NCA)** at staysafeonline.org/cybersecurity-awareness-month/





CYBERSECURITY AWARENESS MONTH 2022

TALKING POINTS

TALKING POINTS

The talking points below are available here for easy reference and/or printing.

WHAT IS CYBERSECURITY AWARENESS MONTH

Held every October, Cybersecurity Awareness Month is a collaborative effort between government, industry and the public. It is an effort that reaches from the White House to the individual to raise awareness about cybersecurity and to ensure that everyone has the resources they need to be safe and secure online. As we prepare for the upcoming holidays, October is the ideal time for people to learn about their cyber presence and the role cybersecurity plays in keeping them, their friends and family safe and secure.

COMMONLY USED TERMS:

Let us go over a few of the words we will be using throughout this presentation:

- A **“Threat Actor”** can include a variety of cybercriminals—hackers, social engineers and even shoulder surfers!
- **“Hackers”** use computers and other digital devices to gain unauthorized access to information or damage computer systems. Hackers may have impressive computer skills, but expert knowledge of programming is not always necessary for a successful breach. Any attempt by threat actors or hackers to gain unauthorized access to a digital computer system can constitute a cyber attack.

CYBERCRIME

Cybercrime is defined as any crime committed electronically, such as theft, fraud and even physical threats and endangerment. It is important to know your cyber basics and know how to take action to protect yourself. Being safe on the computer is similar to being safe in your daily offline routine. You would not leave your car unlocked in the middle of a crowded city, so why not apply those same safety principles to your online life?

PHYSICAL CYBER ATTACKS - WHAT ARE THEY?

Cyber attacks do not always have to come from the internet, and malware can hide easily on some of the data storage devices we trust and use daily. Physical cyber attacks use hardware, external storage devices or other physical types of attacks to infect, damage or otherwise compromise digital systems. The attack can hitch a ride on USB storage devices or flash drives, CDs, hard copies of video games and Internet of Things (IoT) devices such as smartphones, smart watches and even signal devices such as key fobs.

WHY SHOULD YOU CARE?

These kinds of attacks are frighteningly versatile, challenging to identify and detect and painfully difficult - sometimes close to impossible - to remove. Always try to keep track of where your storage devices have been, and do not plug “lost-and-found” USB drives into your computer. Keep your personal and workplace data storage and other devices separate to avoid transferring malware from one system to another, just like washing your hands to prevent the flu from spreading!



CYBERSECURITY AWARENESS MONTH 2022

TALKING POINTS

PROTECT YOURSELF ONLINE

There are four easy ways to protect yourself online:

1. **Think Before You Click.** Recognize and report phishing attacks which can infect your machine with malware. Understand what they look like and how to report them.
2. **Update Your Software.** Don't delay – if you see a software update notification, act promptly. Better yet, turn on automatic updates.
3. **Use strong passwords** because it can prevent cyber criminals from gaining access to your accounts.
4. **Enable multi-factor authentication (MFA)** for all important online activities to provide an additional layer of security.

OTHER AVENUES OF ATTACK

Any device that stores information or is connected to the internet can be a way for cyber criminals to gain access to your information systems – or, in some cases, use your devices to attack someone else. Assume that you are vulnerable and take measures to understand and mitigate risk.

PASSWORD TIPS

One of the first lines of defense for keeping your information safe online is the use of a password. Some password tips are as follows:

- **Use different passwords on different accounts.** One of the leading causes of unauthorized access to accounts is the reuse of login credentials (see [National Cyber Awareness System Tips—Choosing and Protecting Passwords](#)).
- **Use the longest password allowed.** The longer and more complicated a password is, the harder it will be for someone to access your accounts. Use 12 characters or more, a short sentence or mix of letters, symbols and numbers to strengthen your passwords.
- **Reset your password every few months.** Reset your passwords regularly, especially when these passwords allow access to confidential accounts, such as banking or medical data. It is vital to reset passwords as it takes most companies an average of six months to notice that a data breach has happened. By the time a data breach is reported, a threat actor could already be using and/or selling your data.
- **Use a password manager.** With just one master password, a password manager can generate and retrieve passwords for every account that you have – encrypting and protecting your online information, including credit card numbers and their three-digit Card Verification Value (CVV) codes, answers to security questions and more.



CYBERSECURITY AWARENESS MONTH 2022

**SAMPLE
EMAIL**

SAMPLE EMAIL

Below is a sample email to announce your organization's participation in the "See Yourself in Cyber" 2022 Cybersecurity Awareness Month campaign. We encourage you to communicate with your organization throughout the month of October to stress the importance of cybersecurity and provide the cyber tools and resources to protect against a potential cyberattack.

Email Subject Line: Protect **[YOUR ORGANIZATION NAME HERE]** and Your Personal Data from Cyber Threats! Join us during Cybersecurity Awareness Month 2022!

DEAR [INSERT NAME],

Welcome to Cybersecurity Awareness Month! **[ORGANIZATION'S NAME]** is pleased to announce our participation in the Cybersecurity and Infrastructure Security Agency's (CISA) annual campaign where together, we can greatly increase our cybersecurity online, at work, and at home by taking a few basic steps.

Take Control of Your Digital Safety!

Throughout the month of October, get to know the basics of cybersecurity at cisa.gov/cybersecurity-awareness-month. This is a great resource for our team as well anyone who could use a little refresher. This site will provide ways to learn and test your knowledge about:

- Recognize and report phishing attacks which can infect your machine with malware
- Update software to ensure the most current protection
- Use long, random and unique passwords
- Enable multi-factor authentication (MFA) for all important online activities to provide an additional layer of security

There will also be live events throughout Cybersecurity Awareness Month if you want to dive into a topic.

We are looking forward to our organization learning more about cyber basics and making us all more secure. Keep an eye out for announcements throughout the month!

[SIGNATURE/NAME]



CYBERSECURITY AWARENESS MONTH 2022

SAMPLE SOCIAL MEDIA POSTS

SAMPLE SOCIAL MEDIA POSTS

Share information on Cybersecurity Awareness Month on your social channels! There are two ways to participate via social media:

1. Post your own using the samples below.
2. Repost our social media posts during Cybersecurity Awareness Month. We will be posting cybersecurity basics, events and theme days throughout October.

TWITTER

Sample Post One

Recommended post date during the first week of October.

We are excited to engage with @CISAgov and @StaySafeOnline for the 19th annual #CybersecurityAwarenessMonth. Follow along on Twitter as CISA and Director Easterly @CISAJen release new #CyberSnacks weekly in October, to help protect organizations and individuals alike.

Sample Post Two

Be proactive, not reactive. You can greatly increase your cybersecurity online, at work and at home by taking a few simple steps. Learn how at: www.cisa.gov/cybersecurity-awareness-month #CybersecurityAwarenessMonth #SeeYourselfInCyber

LINKEDIN

Recommended post date during the first week of October.

We are excited to engage with Cybersecurity and Infrastructure Security Agency and the National Cyber Security Alliance (NCA) for the 19th annual #CybersecurityAwarenessMonth. Follow CISA and [Jen Easterly](#) as they release new #CyberBasics every Monday and Thursday for the month of October, to help protect organizations and individuals. #SeeYourselfInCyber

FACEBOOK

Recommended post date during the first week of October.

We are excited to engage with @CISA and the @staysafeonline for the 19th annual #CybersecurityAwarenessMonth. Follow @CISA as we release new #CyberBasics every week in October, to help protect organizations and individuals. #SeeYourselfInCyber



CYBERSECURITY AWARENESS MONTH 2022

**SAMPLE
NEWSLETTER**

SAMPLE NEWSLETTER

Below is a sample newsletter article to promote your organization's participation in the "See Yourself in Cyber" 2022 Cybersecurity Awareness Month. We encourage you to emphasize the importance of cybersecurity and announce the tools and resources available to protect your organization and individuals from a potential cyber threat.

SEE YOURSELF IN CYBER!

Today we are connected to our smartphones or a computer wherever we go, because of that our world is becoming increasingly dependent on cybersecurity. [INSERT YOUR ORGANIZATION'S NAME] is proud to be a part of the national Cybersecurity Awareness Month to help us all understand the latest ways to protect [INSERT ORGANIZATION NAME], and our friends and families online.

You can greatly increase your cybersecurity online, at work and at home by taking a few simple steps: Enable Multi-Factor Authentication, Use long, random and unique passwords, think before you click: recognize and report phishing, and update your software. Throughout October, we will learn more about these cyber basics through a wide variety of activities and learning opportunities planned for Cybersecurity Awareness Month. The Cybersecurity and Infrastructure Security Agency (CISA) is making it possible for you to learn about cyber basics as well as advanced cybersecurity issues.

At CISA's Cybersecurity Awareness Month website www.cisa.gov/cybersecurity-awareness-month, there is basic information, classes, and even live events happening throughout October. We encourage you to explore the website and participate in theme days including Women in Tech, International Day, and for anyone interested in a career in cybersecurity—Career Day. There will also be a series of webinars including cyber basics such as multi-factor authentication (MFA) and password managers.

In the end, the security we place around our organization is only as strong as you. We encourage you to visit the CISA website, download the Tips Sheets, and share them with your coworkers, family, and friends. After all of this education, you and your organization will be one of the most secure places online.



CYBERSECURITY AWARENESS MONTH 2022

YEAR-ROUND
CYBERSECURITY
RESOURCES

CISA RESOURCES:

- [About CISA](#)
- [CISA Careers](#)
- [CISA Regions](#)
- [Cyber Hygiene Services](#)
- [CISA Shields-Up](#)
- [CISA Central – Cyber Incident Reporting](#)

CYBER PREPAREDNESS RESOURCES

- [Cyber Resource Hub](#)
- [National Cyber Awareness System](#)
- [New Federal Government Cybersecurity Incident and Vulnerability Response Playbooks](#)
- [Communications and Cyber Resiliency Toolkit](#)
- [Cyber Essentials Toolkits](#)
- [CISA Cybersecurity Awareness Program Toolkit](#)
- [StopRansomware.gov](#)
- [Stop Ransomware Guide](#)
- [Cybersecurity Evaluation Tool - Ransomware readiness assessment](#)
- [Cyber Incident Resource Guide for Governors](#)
- [Known Exploited Vulnerabilities Catalog](#)
- [National Cybersecurity Alliance](#)
- [Cyber.org](#)
- [National Cybersecurity Workforce Framework](#)
- [Multi-State Information Sharing and Analysis Center \(MS-ISAC\) SLTT Services](#)

CYBERSECURITY TRAINING COURSES/PROVIDERS

- [Exercises](#)
- [Incident Response Training](#)
- [Industrial Controls System Training from Idaho National Labs-requires registration](#)
- <https://fedvte.usalearning.gov/> - FedVTE-requires account
- [CISA Service Catalog](#)

OTHER RESOURCES:

- [Chemlock CISA](#)



CYBERSECURITY AWARENESS MONTH 2022

CLOSING

CLOSING

Our hope is that this year's campaign will tighten security at home and across communities and businesses alike. We need your help and the help of your peers in protecting the United States, its vast intelligence community and personal and professional assets. This year's campaign shares ways to increase resilience against cyber attacks, provide easy-to-use tools to lock down private data and keep assets secure from criminals, terrorists and foreign entities.

How can we measure success? The campaign was created to help impact every individual in your organization, from its top leadership to general support staff and everyone in between. CISA will be following up in November to measure the effectiveness of the campaign and collect your feedback. Taking the recommended action steps will result in increased cybersecurity for today and the future.

Questions? Email: cyberawareness@cisa.dhs.gov

