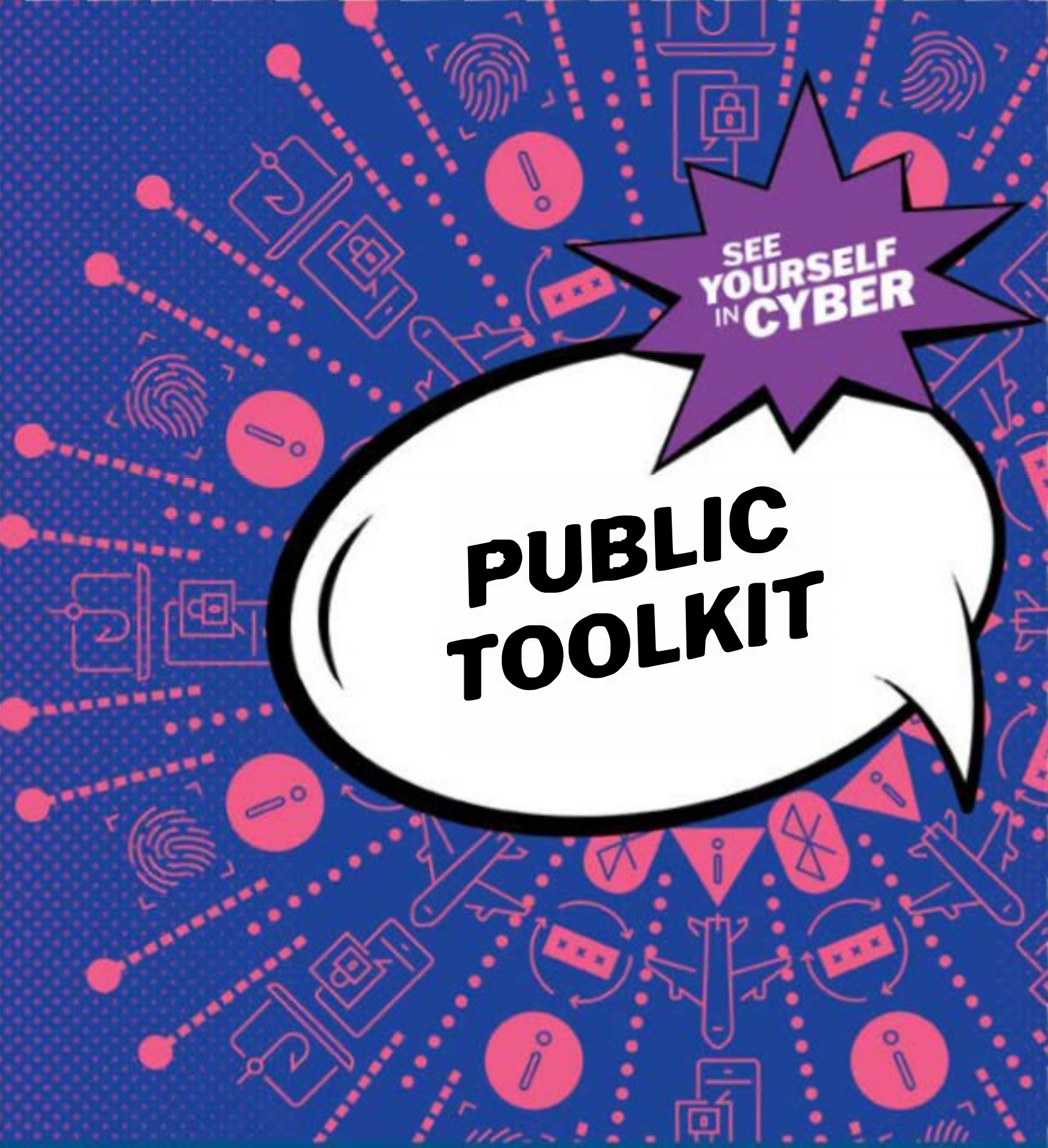


CYBERSECURITY AWARENESS MONTH 2022

CYBERSECURITY AWARENESS MONTH 2022

WELCOME TO CYBERSECURITY AWARENESS MONTH 2022

Since 2004, the President of the United States and Congress have declared October Cybersecurity Awareness Month, helping citizens protect themselves online as our technology, and threats to that technology, become more sophisticated and interwoven in our daily lives.

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: think before you click, update your software, 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.

ABOUT THIS TOOLKIT

The CISA team encourages you to celebrate Cybersecurity Awareness Month with us throughout October. This toolkit will help you provide your organization with the tools and resources to learn the basics of cybersecurity. It contains information about the national campaign in October, as well as resources for getting the word out. You are encouraged to use any resource in this toolkit.

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/

PROMOTING CYBERSECURITY AWARENESS MONTH TO YOUR COMMUNITY

Cybersecurity Awareness Month has an overarching theme that we ask you to use in your own October initiatives. This year, under the theme of "See Yourself in Cyber," the campaign 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. We all have a role to play in cybersecurity.

RESOURCES YOU CAN USE

You do not need to be a cybersecurity expert to help members of your community protect themselves. We are here to guide and support you! This year, Cybersecurity Awareness Month is adding links to year-round cybersecurity resources. Look for them on the Cybersecurity Awareness Month campaign sites like CISA.gov and NCA's Cybersecurity Awareness Month inside this toolkit.

TALKING ABOUT CYBERSECURITY AWARENESS MONTH

The CISA team encourages you to share Cybersecurity Awareness Month with your organization, reflecting the needs of your community. To help you get started, copy and paste (or use as an inspiration) the following samples:

- Email announcing the start of Cybersecurity Awareness Month
- Social media posts (or repost the CISA social media during October)
- Newsletter article to get your organization enthused about the month
- Links to additional cybersecurity resources

TIP SHEET

CYBERSECURITY 101

CYBERSECURITY 101

Cybersecurity is the art of protecting networks, devices, and data from unlawful access or criminal use, and providing confidentiality, integrity, and availability of information. Much of your personal information is stored either on your computer, smartphone, or tablet. Knowing how to protect your information is important, not just for individuals but for organizations, as well. Every time you use the internet, you face choices related to your security. Your security and the security of the nation depends on making responsible online decisions. Making the internet safe and secure requires all of us to take responsibility for our own cybersecurity behavior.

KNOW YOUR CYBER BASICS

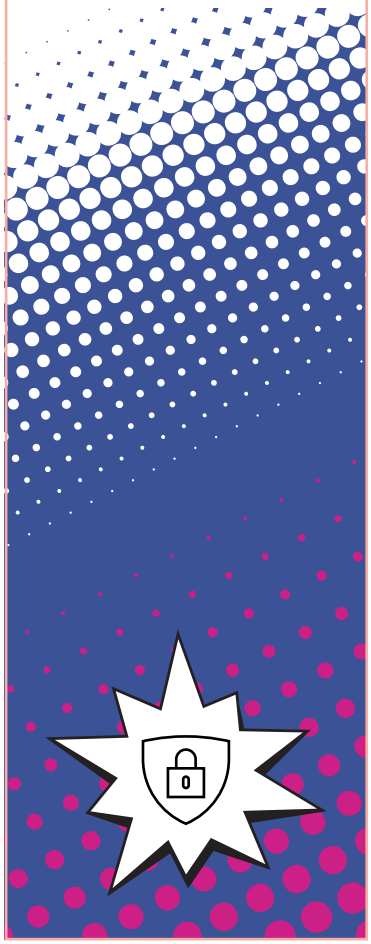
- **Think Before You Click: Recognize and Report Phishing:** If a link looks a little off, think before you click. It could be an attempt to get sensitive information or install malware.
- **Update Your Software:** Don't delay – if you see a software update notification, act promptly. Better yet, turn on automatic updates.
- **Use Strong Passwords:** Use passwords that are long, unique, and randomly generated. Use password managers to generate and remember different, complex passwords for each of your accounts. A password manager will encrypt passwords securing them for you!
- **Enable Multi-Factor Authentication:** You need more than a password to protect your online accounts, and enabling MFA makes you significantly less likely to get hacked.

POTENTIAL THREATS

- **Malware.** A computer can be damaged or the information it contains harmed by malicious code (also known as malware). A malicious program can be a virus, a worm, or a Trojan horse. Hackers, intruders, and attackers are in it to make money off these software flaws.
- **Identity Theft and Scams.** Identity theft and scams are crimes of opportunity, and even those who never use computers can be victims. There are several ways criminals can access your information, including stealing your wallet, overhearing a phone call, looking through your trash, or picking up a receipt that contains your account number.
- **Phishing.** Phishing attacks use emails, texts, and malicious websites that appear to be trusted organizations, such as charity organizations or online stores, to obtain user personal information.

FOLLOW-ON RESOURCES

- Multi-Factor Authentication Guide
- Password and Password Managers Tip Sheet
- Phishing Tip Sheet
- Identity Theft and Internet Scams Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime



CONTINUED ON NEXT PAGE ▸

HOW CRIMINALS LURE YOU IN

Phishing is one of the most common forms of cyber scams that you are likely to experience. The key is that both emails and texts should come from a trusted source. Know what to look for—here are examples of phishing that might be seen in an email to lure you in:

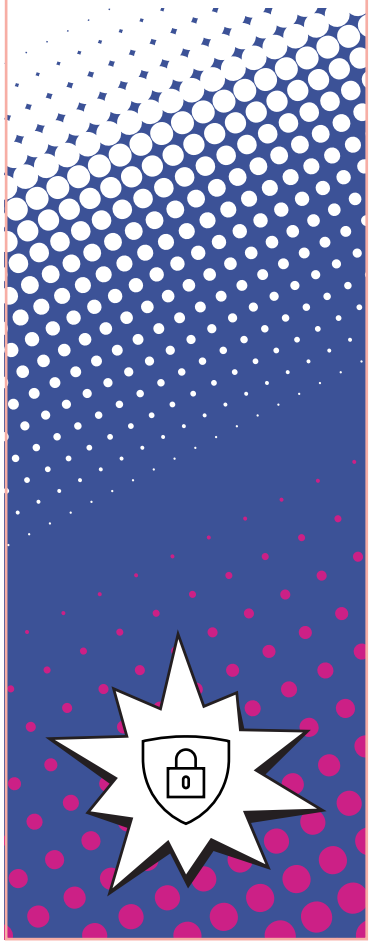
> "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below, and confirm your identity."

> "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

> "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

FOLLOW-ON RESOURCES

- Multi-Factor Authentication Guide
- Password and Password Managers Tip Sheet
- Phishing Tip Sheet
- Identity Theft and Internet Scams Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime



LEARN MORE DURING CYBERSECURITY AWARENESS MONTH

Thank you for your continued support and commitment to Cybersecurity Awareness Month and helping all Americans stay safe and secure online. Please visit www.cisa.gov/cybersecurity-awareness-month to learn more.

TIP SHEET

WHY CYBER SECURITY IS IMPORTANT

AND HOW TO APPROACH IT

WHY CYBERSECURITY IS IMPORTANT AND HOW TO APPROACH IT

Cybersecurity is the art of protecting networks, devices, and data from unlawful access or criminal use. Today, much of your personal information is stored either on your computer, smartphone, tablet, other smart devices or apps like Alexa, smart watches, etc. Knowing how to protect your digital devices is important not just for individuals, but for organizations, as well.

The purpose of cybersecurity is to maintain confidentiality, integrity, and availability of data.

- **Confidentiality**. Ensures the data is accessible by only those who need it—once you post information on the internet, it is there forever.
- **Integrity.** Ensures the data is accurate—corrupt data is of no value to those who need it.
- **Availability**. Ensures the data can be accessed by all those who need it, whenever they need it—fast and reliable connectivity makes computer systems operate more effectively.

Attackers exploit vulnerabilities by using a variety of phishing attacks to compromise the security of networks and devices. To protect your networks, it is vital to become familiar with cyber basics:

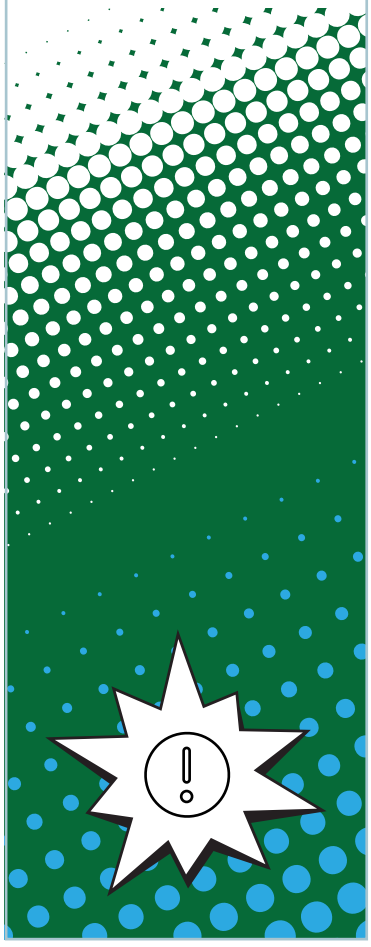
- Attackers can obtain victim identity information by stealing compromised credentials.
- Criminals create new email accounts and hack existing ones to conduct social engineering attacks. A social engineering attack is when an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.
- Phishing emails contain malware and malicious attachments.
- Malware exploits various common vulnerabilities in software and other applications.

KNOW YOUR CYBER BASICS

- **Protect your personal information.** If people have key details from your life, your job title, birth date, and full name, which you may have shared online, they can attempt a phishing attack on you. Cybercriminals can also try to manipulate you into skipping normal security protocols.
- **Be wary of hyperlinks or attachments from suspicious or unknown/ untrusted sources.** Inspect hyperlinks in emails. Hover over links to verify their source. When making a transaction, ensure that URLs begin with “https.” The added “s” indicates encryption is enabled to protect users’ information.

FOLLOW-ON RESOURCES

- Phishing Tip Sheet
- Ransomware Fact Sheet
- Password and Password Managers Tip Sheet
- Multi-Factor Authentication Guide
- Identity Theft and Internet Scams Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime



CONTINUED ON NEXT PAGE ▸

- **Use anti-virus software and keep it up to date.** This is an important protective measure against cybercriminals and malicious threats. It can automatically detect, quarantine, and remove malware. Enable automatic virus updates to ensure maximum protection against the latest threats.
- **Use long, random and unique passwords.** Creating strong passwords is vital to cybersecurity. Use different passwords for different programs and devices. Use long passwords or passphrases to protect your accounts. Always use strong passwords of 12 or more characters.
- **Use a password manager to store your personal passwords for each account.** This tool is commonly used to generate long, random and unique passwords for web applications. Once generated, they are put in a centralized vault, and encrypted with one master password.
- **Strengthen your login protection.** Enable multi-factor authentication (MFA) to ensure that you are the only person who has access to your account. Use it for email, banking, social media, and any other password-protected services. 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.
- **Backup your data.** Routinely backup data on all computers, and make sure that the backup is stored offline. Backup all data including documents, databases, spreadsheets, financial files, human resources files, accounts receivable/payable files, and more.
- **Control physical access.** Prevent access to your backup data by unauthorized individuals. Make sure to use separate user accounts for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.

WHAT TO LOOK FOR

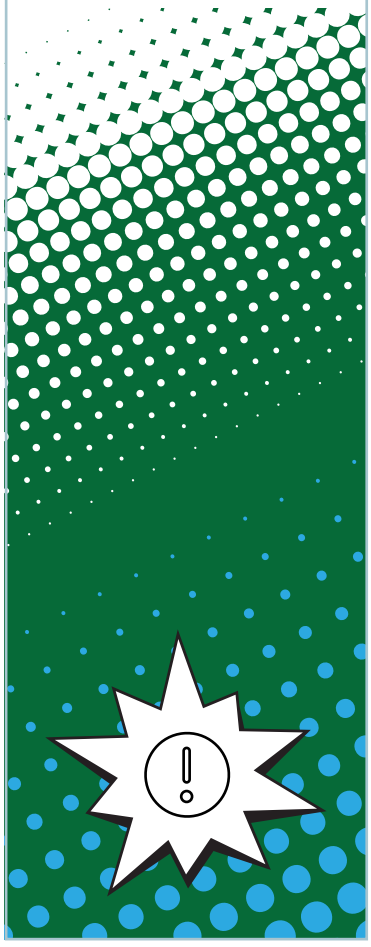
- **Watch for phishing.** Phishing enables cybercriminals to collect your information to make unauthorized purchases or gain access to a secure system. Always check the sender's email address to make sure that it is authentic. Many phishing emails attempt to create a sense of urgency, causing the recipient to fear their account is in jeopardy. If you suspect an email is fraudulent, reach out to the company or person directly on a separate, secure platform.
- **Be aware of risk.** In addition to malware and phishing viruses, the number one security threat is ransomware. Ransomware is a form of malware designed to encrypt files on any device, rendering any file, and the systems that rely on them, unusable.
- **Train your employees regularly on cyber basics.** Employees and emails are the foremost cause of data breaches for small businesses because they are a direct path into your system. Visit the National Initiative for Cybersecurity Careers and Studies (NICCS).

LEARN MORE DURING CYBERSECURITY AWARENESS MONTH

Thank you for your continued support and commitment to Cybersecurity Awareness Month and helping all Americans stay safe and secure online. Please visit www.cisa.gov/cybersecurity-awareness-month to learn more.

FOLLOW-ON RESOURCES

- Phishing Tip Sheet
- Ransomware Fact Sheet
- Password and Password Managers Tip Sheet
- Multi-Factor Authentication Guide
- Identity Theft and Internet Scams Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime



TIP SHEET

PROTECTING YOUR DIGITAL HOME

PROTECTING YOUR DIGITAL HOME

Every year, more of our home devices, including thermostats, outdoor lighting, door locks, coffee makers, and smoke alarms, are connected to the internet to create a"smart home." These advances in technology, commonly referred to as the internet of things (IoT), are convenient and may improve efficiency and safety, however they also pose a new set of security risks.

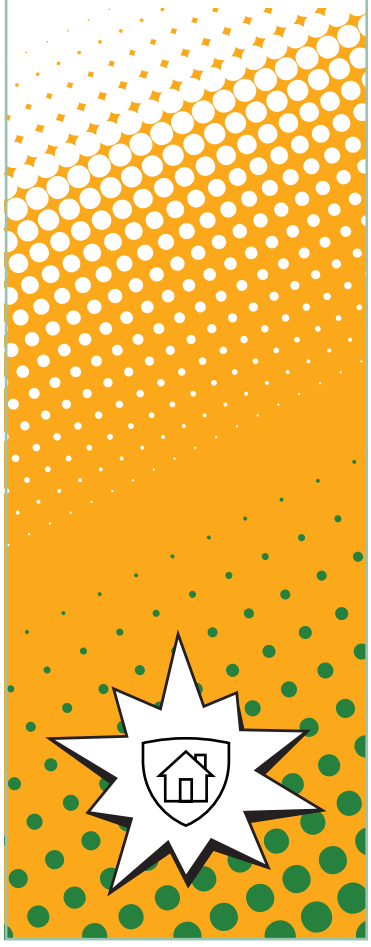
- **Start with your wireless network.** Secure your Wi-Fi network. Your home's wireless router is the primary entrance for cybercriminals to access all your connected devices. Secure Wi-Fi and digital devices by changing the default password and username. Check your internet provider's or router manufacturer's wireless security options. Your internet service provider and router manufacturer may provide information or resources to assist in securing your wireless network.
- **Keep tabs on your apps.** Most connected appliances, toys, and devices are supported by a mobile application. Apps have the ability to gather your personal information while also putting your identity and privacy at risk. Be aware of downloading new, unfamiliar apps or giving default permissions. Check your app permissions and use the "rule of least privilege" to delete apps you no longer need or use.
- **Never click and tell.** Disable location services that allow anyone to see where you are, and where you are not, at any given time. Limit what information you share on social media from home—from personal addresses to where you like to grab coffee. Keep Social Security numbers, account numbers, usernames and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and vacation plans.

KNOW YOUR CYBER BASICS

- **Enable multi-factor authentication (MFA).** to ensure that you are the only person who has access to your account. Use MFA 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 onto hook your key ring.
- **If you connect it, you must protect it.** Whether it is your computer, smartphone, gaming device, or other network devices, the best defense is to stay on top of things by updating to the latest security software, web browser, and operating systems. If you have the option to enable automatic updates to defend against the latest risks, turn it on. And, if you are connecting something to your device, such as a universal serial bus (USB) for an external hard drive, make sure your device's security software scans for viruses and malware. Finally, protect your devices with antivirus software, and be sure to periodically back up any data that cannot be recreated, such as photos or personal documents.

FOLLOW-ON RESOURCES

- Securing Wireless Networks
- Multi-Factor Authentication (MFA) Guide
- Social Media Cybersecurity Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime



TIP SHEET

BE CYBER SECURE AT HOME

BE CYBER SECURE AT HOME

In 2022, CISA reported that, "Every organization in the United States is at risk from cyber threats that can disrupt essential services and potentially result in impacts to public safety." Businesses face significant financial loss when a cyberattack occurs. Cybercriminals often rely on human error—employees failing to install software patches or clicking on malicious links—to gain access to systems. From the top leadership to the newest employee, cybersecurity requires the vigilance of everyone to keep data, customers, and capital safe and secure.

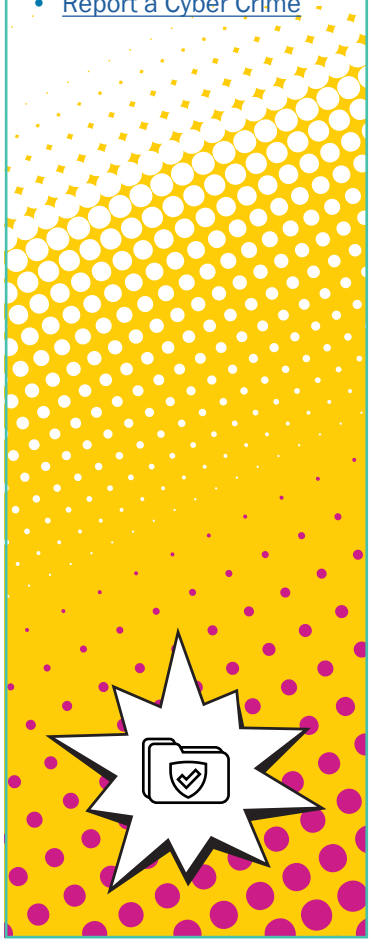
- **Use only approved tools.** Only use organization-approved software and tools for business, including company-provided or approved video conferencing and collaboration tools to initiate and schedule meetings. Unapproved free tools may make your system vulnerable, so check in with your Information Technology (IT) team before using them on your work computer.
- **Secure your meetings.** Take precautions to ensure your virtual meetings are only attended by intended individuals. Plan for what to do if a public meeting is disrupted.
- **Secure your information.** Tailor your security precautions appropriately to the sensitivity of your data. Only share data necessary to accomplish the goals of your meeting.
- **Secure yourself.** Take precautions to avoid unintentionally revealing business and personal information. Ensure home networks are secured.

KNOW YOUR CYBER BASICS

- **Treat business information as personal information.** Business information typically includes a mix of personal and proprietary data. While you may think of trade secrets and company credit accounts, it also includes employee personally identifiable information (PII) through tax forms and payroll accounts. Do not share PII with unknown parties or over unsecured networks.
- **Don't make passwords easy to guess.** As "smart" or data-driven technology evolves, it is important to remember that security measures only work if employees use them correctly. Smart technology runs on data, meaning devices such as smartphones, laptop computers, wireless printers, and other devices are constantly exchanging data to complete tasks. Take proper security precautions and ensure correct configuration to wireless devices in order to prevent data breaches.
- **Stay up to date.** Keep your software updated to the latest version available as per your organization's guidelines. Talk to your organization's IT team about turning on automatic updates, so you don't have to think about it, and set your security software to run regular scans.

FOLLOW-ON RESOURCES

- Telework Essentials Toolkit
- Telework Reference Materials For The At-Home Worker
- Internet of Things Tip Card
- Phishing Tip Sheet
- Social Media Cybersecurity Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime

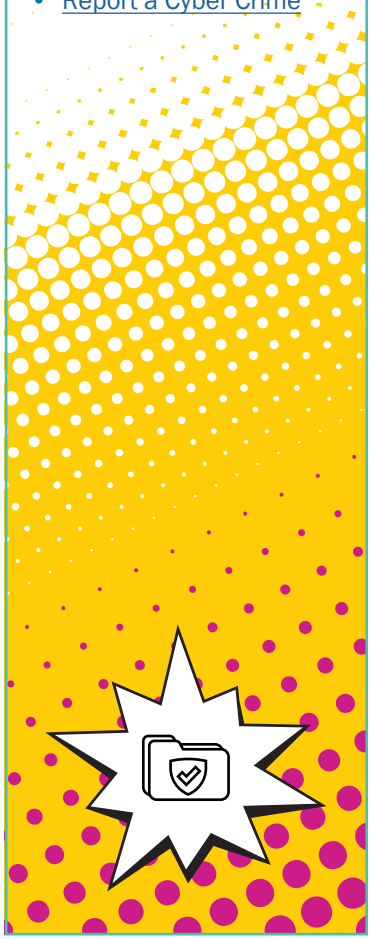


CONTINUED ON NEXT PAGE ▸

- **Follow your company's social media policies.** Employees should avoid oversharing on social media and should not conduct official business, exchange payment, or share PII on social media platforms.
- **Don't trust the sender immediately.** Data breaches can occur even without a cybercriminal hacking into an organization's infrastructure. Many data breaches can be traced back to a single security vulnerability, phishing attempt, or instance of accidental exposure. Be wary of unusual sources, do not click on unknown links, and delete suspicious messages after reporting or forwarding to a supervisor, so that any necessary organizational updates, alerts, or changes can be put into place.

FOLLOW-ON RESOURCES

- Telework Essentials Toolkit
- Telework Reference Matierals For The At-Home Worker
- Internet of Things Tip Card
- Phishing Tip Sheet
- Social Media Cybersecurity Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime



LEARN MORE DURING CYBERSECURITY AWARENESS MONTH

Thank you for your continued support and commitment to Cybersecurity Awareness Month and helping all Americans stay safe and secure online. Please visit www.cisa.gov/cybersecurity-awareness-month to learn more.

TIP SHEET

TAKE IT WITH YOU

CYBERSECURITY WHEN TRAVELING

TAKE CYBERSECURITY WITH YOU WHEN TRAVELING

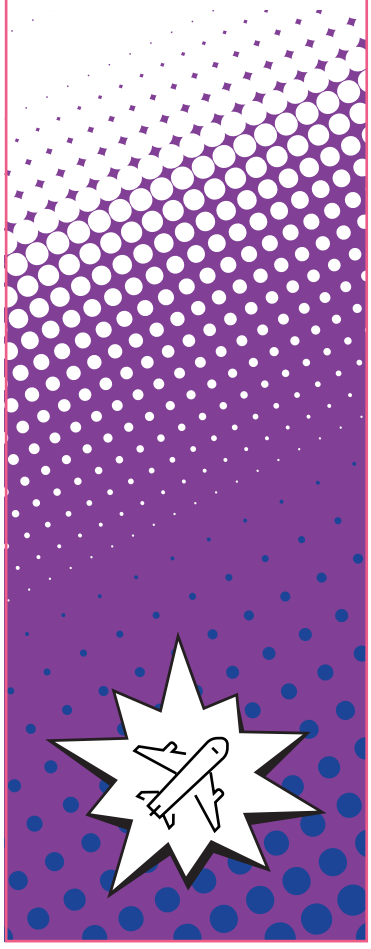
In a world where we are constantly connected, cybersecurity cannot be limited to the home or office. When you are traveling, whether domestically or abroad, it is always important to practice safe online behavior and take proactive steps to secure internet-enabled devices. The more we travel, the more we are at risk for cyberattacks. Whether traveling with personal or business devices, you should always comply with user rules for international travel. Use these tips to connect with confidence while on the go.

KNOW YOUR CYBER BASICS

- **"If You Connect IT, Protect IT."** Whether it is 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.
- **Back up your information.** Back up your contacts, financial data, photos, videos, and other mobile device data to another device or cloud service in case your device is compromised.
- **Enable multi-factor authentication (MFA).** 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.
- **Know who to call for support.** If you experience any system issues, you should know whom to call for IT support. If your device is compromised, you should have a plan on the actions you will take.
- **Never click and tell.** Do not tell the social media world that you are going to be away from your home. Disable geo-tagging and do not post your travel pictures on social media until you return from vacation. Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people do not 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 real 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 are not—at any given time.

FOLLOW-ON RESOURCES

- Social Media Cybersecurity Tip Sheet
- Multi-Factor Authentication Guide
- StaySafeOnline.org
- Report a Cyber Crime

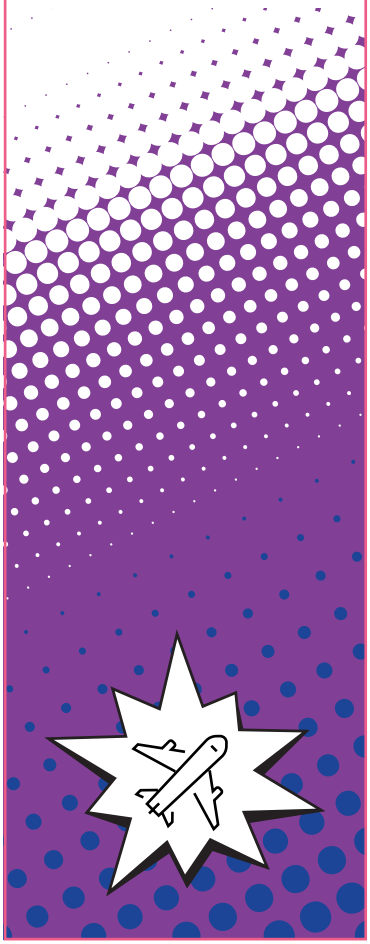


CONTINUED ON NEXT PAGE ▸

- **Stay protected while connected.** Before you connect to any public wireless hotspot—such as at an airport, hotel, or café—turn on your browser's advance security settings and 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.

FOLLOW-ON RESOURCES

- Social Media Cybersecurity Tip Sheet
- Multi-Factor Authentication Guide
- StaySafeOnline.org
- Report a Cyber Crime



LEARN MORE DURING CYBERSECURITY AWARENESS MONTH
Thank you for your continued support and commitment to Cybersecurity Awareness Month and helping all Americans stay safe and secure online. Please visit www.cisa.gov/cybersecurity-awareness-month to learn more.

TIP SHEET

CYBER SECURITY BASICS: MULTI-FACTOR AUTHENTICATION

CYBERSECURITY BASICS FOR MULTI-FACTOR AUTHENTICATION

Have you noticed how security breaches, stolen data, and identity theft are consistently front-page news these days? Perhaps you, or someone you know, are a victim of cybercriminals who stole personal information, banking credentials, or more. As these incidents become more prevalent, you should consider using multi-factor authentication (MFA), also called strong authentication, or two-factor authentication.

This technology may already be familiar to you, as many banking and financial institutions require both a password and one of the following to log in: a call, email, or text containing a code. By applying these principles of verification to more of your personal accounts, such as email, social media, and more, you can better secure your information and identity online.

MFA is defined as a security process that requires more than one method of authentication from independent sources to verify the user's identity. In other words, a person wishing to use the system is given access only after providing two or more pieces of information which uniquely identifies that person.

HOW AND WHEN MFA SHOULD BE USED

There are three categories of credentials: something you either know, have, or are. Here are some examples in each category:

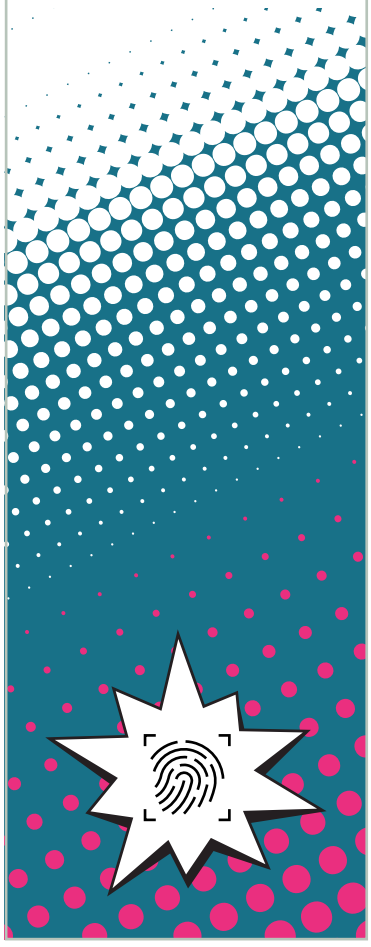
- **Something You Know:** Password/passphrase, pin number.
- **Something You Have:** Security token or software application, verification text, call, email, or smart card.
- **Something You Are:** Fingerprint, facial recognition, voice recognition.

Your credentials must come from at least two different categories for you to gain access. One of the most common methods is to login using your username and password. Then a unique one-time code will be generated and sent to your phone or email, which you would then enter within the allotted amount of time. This unique code is the second factor.

MFA should be used to add an additional layer of security around sites containing sensitive information, or whenever enhanced security is desirable. MFA makes it more difficult for unauthorized people to log in as the account holder. According to the National Institute of Standards and Technology (NIST), MFA should be used whenever possible, especially when it comes to your most sensitive data—like your primary email, financial accounts, and health records. Some organizations will require you to use MFA; with others, it is optional. If you have the option to enable it, you should take the initiative to do so to protect your data and your identity.

FOLLOW-ON RESOURCES

- Password and Password Managers Tip Sheet
- CISA's Multi-Factor Authentication Website
- StaySafeOnline.org
- Report a Cyber Crime



CONTINUED ON NEXT PAGE ▸

TIP SHEET

CYBER SECURITY BASICS:

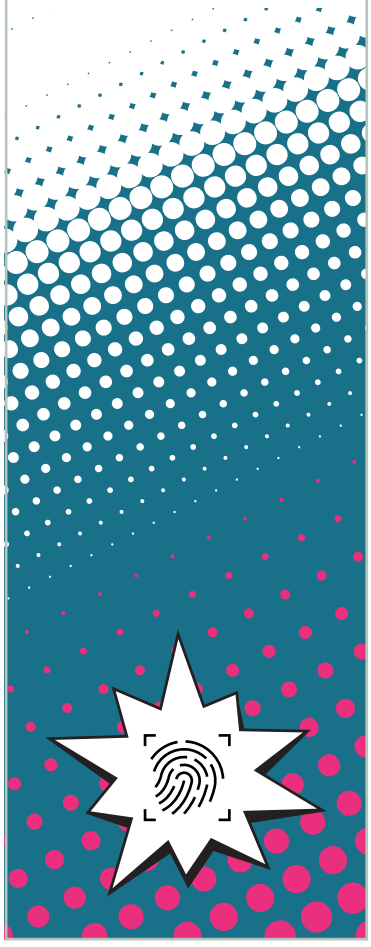
MULTI-FACTOR AUTHENTICATION

KNOW YOUR CYBER BASICS

To learn how to activate MFA on your accounts, visit the Lock Down Your Login Multi-Factor Authentication | CISA page, which gives instructions on how to apply this stronger form of security to many common websites and software products. If any of your accounts are not listed on that resource site, look at your account settings or user profile and check whether MFA is an available option. If you see it there, consider implementing it right away! Usernames and passwords are no longer sufficient to protect accounts with sensitive information. By using multi-factor authentication, you can protect these accounts and reduce the risk of online fraud and identity theft. Consider also activating this feature on your social media accounts!

FOLLOW-ON RESOURCES

- Password and Password Managers Tip Sheet
- CISA's Multi-Factor Authentication Website
- StaySafeOnline.org
- Report a Cyber Crime



LEARN MORE DURING CYBERSECURITY AWARENESS MONTH

Thank you for your continued support and commitment to Cybersecurity Awareness Month and helping all Americans stay safe and secure online. Please visit www.cisa.gov/cybersecurity-awareness-month to learn more.

TIP SHEET

CYBER SECURITY BASICS: PASSWORDS & PASSWORD MANAGEMENT

CYBERSECURITY BASICS FOR PASSWORDS AND PASSWORD MANAGEMENT

Creating long, random and unique password is a critical step to protecting yourself online. Using long passwords is one of the easiest ways to defend yourself from cybercrime. The most secure way to store all your unique passwords is by using a password manager. With just one password, a computer can create and save passwords for every account that you have—protecting your online information, including credit card numbers and their three-digit codes, answers to security questions, and more.

STRONGER PASSWORDS INCREASE SECURITY

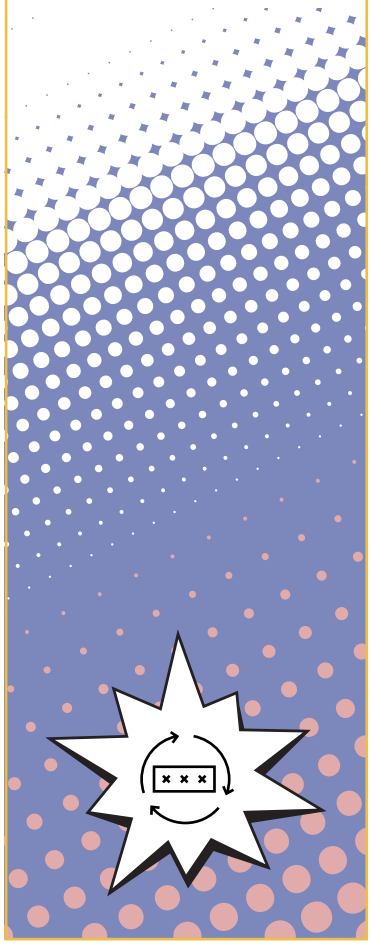
- **Use a long passphrase with 12 or more characters.** Use the longest password or passphrase permissible. For example, you can use a password manager or passphrase such as a news headline or even the title of the last book you read.
- **Don't make passwords easy to guess.** Do not include personal information in your password such as your name or pets' names. This information is often easy to find on social media, making it easier for cybercriminals to hack your accounts.
- **Keep your passwords on the down low.** Do not tell anyone your passwords and watch for attackers trying to trick you into revealing your passwords through email or by phone. Every time you share or reuse a password, it chips away at your security by opening more ways with which it could be misused or stolen.
- **Use unique passwords.** Having different passwords for various accounts helps prevent cyber criminals from gaining access to these accounts and protects you in the event of a breach.

KNOW YOUR CYBER BASICS

- **Strengthen your login protection.** Use 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 password-required service. Enable MFA 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.
- **Fortify your online accounts** by enabling the strongest authentication tools available, such as biometrics (biological measurements—or physical characteristics—that can be used to identify individuals, such as fingerprint mapping, facial recognition, and retinal scans), and/or security keys. Your usernames and passwords are not enough to protect key accounts like email, banking, and social media.

FOLLOW-ON RESOURCES

- CISA's Multi-Factor Authentication Website
- Multi-Factor Authentication Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime



TIP SHEET

CYBER SECURITY BASICS: SOCIAL MEDIA

CYBERSECURITY BASICS FOR SOCIAL MEDIA

Now more than ever, consumers spend an increasing amount of time on the Internet. For every social media account with which you interact, every picture you post, and status you update, you are sharing information about yourself with the world. This information is permanent in cyberspace. It is imperative to be proactive and secure your online safety. Take these steps to connect with confidence and safely navigate the social media world.

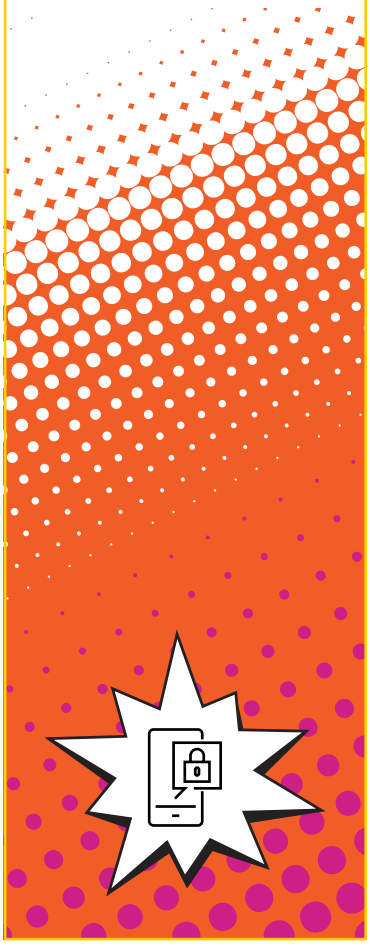
CYBER CRIMINALS AND SOCIAL MEDIA

Cybercriminals use social media to spread malware, malicious links, and malicious advertising. They can also leverage hacked credentials to refine their malware and scamming targets. In addition, they will use the "oversharing" of personal information to target online accounts. It is critical that you practice good cyber hygiene by understanding their tactics and knowing the cyber basics.

- **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 do not realize is that these seemingly random details are all a criminal needs to know to target you, your loved ones, and your physical belongings—online and in the real 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.
- **Connect only with people you trust.** While some social networks might seem safer for connecting because of the limited personal information shared within them, keep your connections to people you know and trust. If communication from a post seems strange or odd, delete it.
- **Speak up if you're being cyberbullied online.** Report any and all instances of cyberbullying you see or experience to the appropriate social platform.
- **Report suspicious or harassing activity.** Work with your social media platform to report and possibly block harassing users. Report an incident if you have been a victim of cybercrime. Local and national authorities are ready to help you.

FOLLOW-ON RESOURCES

- CISA's Multi-Factor Authentication Website
- Phishing Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime



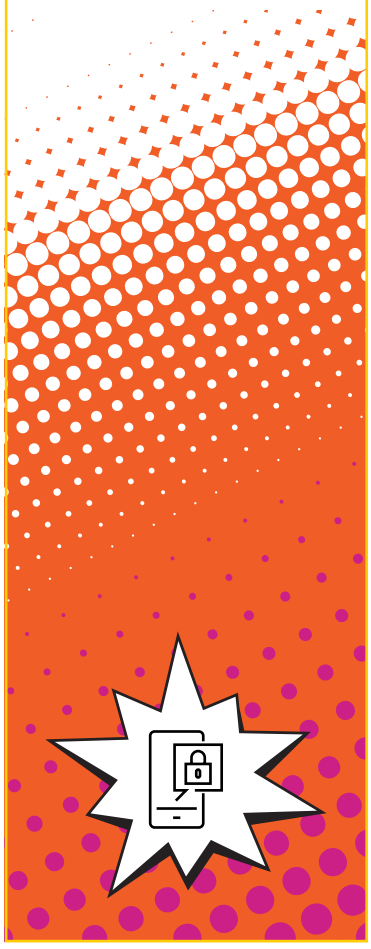
CONTINUED ON NEXT PAGE ▸

KNOW YOUR CYBER BASICS

- **Remember, there is no 'delete' button on the internet.** Share with care, because even if you delete a post or picture from your profile seconds after posting it, chances are someone still saw it, and information is permanent in cyberspace.
- **Update your privacy settings.** Set the privacy and security settings to your comfort level for information sharing. Disable geo-tagging, which allows anyone to see where you are—and where you are not—at any given time.
- **If You Connect IT, Protect IT.** Whether it is your computer, smartphone, game device, or other network device, 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.

FOLLOW-ON RESOURCES

- CISA's Multi-Factor Authentication Website
- Phishing Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime



LEARN MORE DURING CYBERSECURITY AWARENESS MONTH

Thank you for your continued support and commitment to Cybersecurity Awareness Month and helping all Americans stay safe and secure online. Please visit www.cisa.gov/cybersecurity-awareness-month to learn more.

TIP SHEET

CYBER SECURITY BASICS: IDENTITY THEFT & INTERNET SCAMS

CYBERSECURITY BASICS: IDENTITY THEFT AND INTERNET SCAMS

Today's technology allows us to connect around the world, to bank and shop online, and to control our devices from our smartphones. This added convenience brings with it an increased risk of identity theft and internet scams. We can greatly increase our cybersecurity online, at work, and at home by taking a few simple steps.

IDENTITY THEFT

Identity theft happens when someone steals your personal information to commit fraud. The identity thief may use your information to apply for credit, file taxes, or get medical services. These acts can damage your credit status and cost you time and money to restore your good name.

- **Don't reveal personally identifiable information** such as your bank account number, Social Security Number (SSN), or date of birth to unknown sources.
- **Practice safe web surfing** wherever you are by checking for the green lock or padlock icon in your browser bar—this signifies a secure connection.
- **Type website URLs directly into the address bar** instead of clicking on links or copying and pasting from the email.
- **Check with the known sender before clicking on any links.** All emails and messages should be considered suspicious, when in doubt.

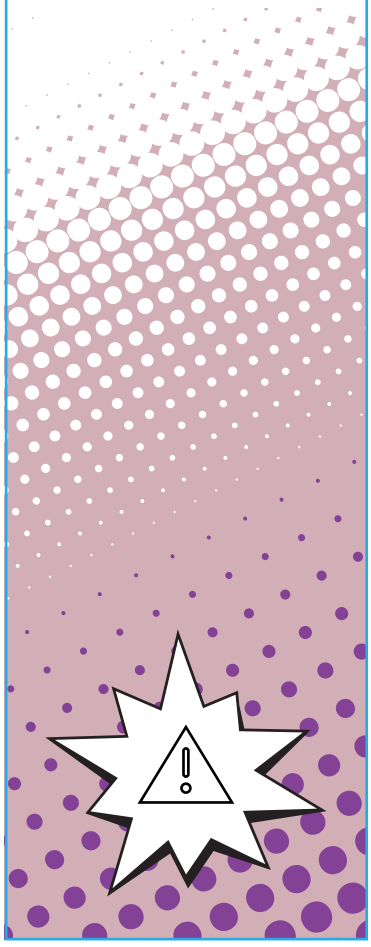
For additional resources to report and recover from identity theft contact the Federal Trade Commission's Identity Theft website: www.identitytheft.gov/#/

COMMON INTERNET SCAMS

- Imposter scams, such as phishing and spoofing, occur when you receive an email or call from a person claiming to be a government official, family member, or friend requesting personal or financial information. For example, an imposter may contact you from the Social Security Administration informing you that your SSN has been suspended, in hopes you will reveal your SSN or pay to have it reactivated.
- Donation scams take the form of emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes. Exercise caution in handling any email involving recent world events, such as COVID-19, or geo-political events. Be wary of social media pleas, texts, or calls.

FOLLOW-ON RESOURCES

- Password and Password Managers Tip Sheet
- CISA's Multi-Factor Authentication Website
- Spoofing and Phishing - FBI
- StaySafeOnline.org
- Report a Cyber Crime



CONTINUED ON NEXT PAGE ▸

TIP SHEET

CYBER SECURITY BASICS: IDENTITY THEFT & INTERNET SCAMS

KNOW YOUR CYBER BASICS

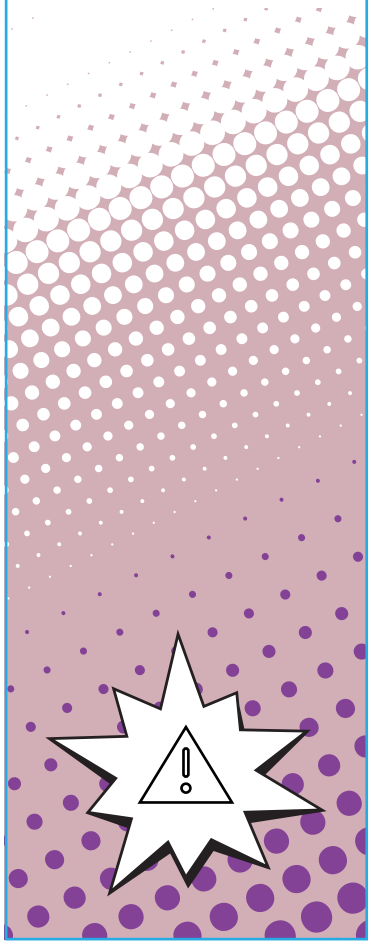
- **Enable multi-factor authentication (MFA).** Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other password-protected service. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring.
- **Shake up your password protocol.** You should consider using the longest password or passphrase permissible. Use long, random and unique passwords for different sites to prevent cyber criminals from gaining access to these accounts and protect you in the event of a breach. Use password managers to generate and remember different passwords for each of your accounts.
- **Stay up to date.** Keep your software updated with the latest version available. Maintain your security settings to keep your information safe by turning on automatic updates so you do not have to think about it, and set your security software to run regular scans.

REPORTING A CYBERCRIME

If you discover that you have become a victim of cybercrime, immediately notify authorities to file a complaint. Keep and record all evidence of the incident and its suspected source. Crime reports will aid investigations and acting immediately can help you recover lost funds or data.

FOLLOW-ON RESOURCES

- Password and Password Managers Tip Sheet
- CISA's Multi-Factor Authentication Website
- Spoofing and Phishing - FBI
- StaySafeOnline.org
- Report a Cyber Crime



LEARN MORE DURING CYBERSECURITY AWARENESS MONTH
Thank you for your continued support and commitment to Cybersecurity Awareness Month and helping all Americans stay safe and secure online. Please visit www.cisa.gov/cybersecurity-awareness-month to learn more.

TIP SHEET

PHISHING ATTACKS

PHISHING

Phishing attacks collect your personal and financial information using email, text, or malicious websites to infect your digital devices with malware. Cybercriminals attempt to lure users to click on a link or open an attachment that infects their computers or mobile phone and makes the user vulnerable to an attack. Think twice because cybersecurity is the collective responsibility of everyone.

Phishing emails or texts may appear to come from a trusted financial institution, e-commerce site, a government agency, or any other service, business, or individual. The email or text may ask for account numbers, passwords, or Social Security Numbers. When users respond or click on a link, attackers take the data to access users' accounts.

HOW CYBERCRIMINALS LURE YOU IN

> "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below, and confirm your identity."

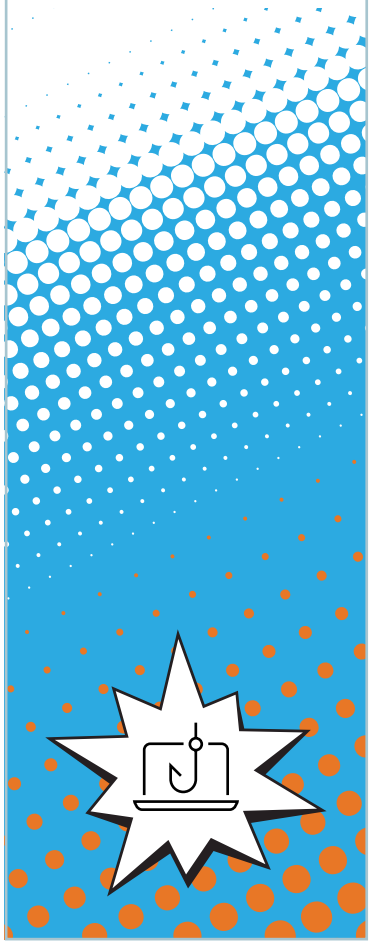
> "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

> "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

- **Play hard to get with strangers.** Links in emails, texts and online posts are often the way cybercriminals compromise your devices. If you are unsure who the message is from—even if the details appear accurate—do not respond, and do not click on any links or attachments—just delete it. Be cautious of generic greetings, as these are often phishing attempts. If you question the message, call the company directly.
- **Think before you act.** Be wary of messages that implore you to act immediately, causing you to fear your account is in jeopardy. If you receive a suspicious message that appears to be from someone you know, reach out to that person directly on a secure platform. If a message is from an organization, but still looks "phishy," reach out to the organization to verify the message.
- **Check hyperlinks.** Avoid clicking on hyperlinks in messages, and hover over links to verify authenticity. Ensure that webpage URLs begin with "https." The "s" indicates encryption is enabled to protect users' information.

FOLLOW-ON RESOURCES

- Password and Password Managers Tip Sheet
- CISA's Multi-Factor Authentication Website
- Identity Theft and Internet Scams Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime



CONTINUED ON NEXT PAGE ▸

- **Once you post on the internet it is there forever.** Keep personal information to yourself. If people have key details from your life like your job title, full name, birthdate and more, they can attempt a direct "spear-phishing" attack on you. Criminals can also use social engineering with these details to try to manipulate you into skipping setting up normal security protocols. In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems.
- **Be alert for suspicious emails.** If you receive an e-mail from a known vendor that seems suspicious, encouraging you to click on a link to your account, **do not click on the link or call the number in the email.** Instead, login directly to your account to verify if there are any issues with your account or call the company using the number listed on their website.

KNOW YOUR CYBER BASICS

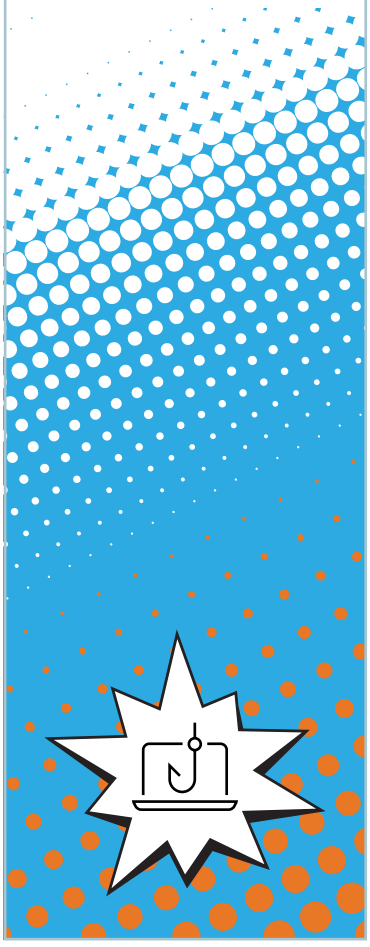
- **Enable multi-factor authentication (MFA).** Enable multi-factor authentication (MFA), meaning use two or more user verification methods to log in to your accounts or devices, to ensure that the only person who can access your account is you. Use it for email, banking, social media, and any other password-protected service. If MFA is an option, enable it on 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.
- **Shake up your password protocol.** Use the longest password or passphrase permissible. Use long, random and unique passwords, which can prevent criminals from gaining access to accounts and protect you in the event of a breach. Use password managers to generate and remember different passwords for each account.
- **Use password managers.** There are password apps to generate and remember different passwords for each account.
- **Install and update antivirus software.** Make sure all your computers, Internet of Things devices, phones, and tablets are equipped with regularly updated antivirus software, email filters, and anti-spyware.

HOW TO REPORT

The Cybersecurity and Infrastructure Security Agency (CISA) Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to CISA.

FOLLOW-ON RESOURCES

- Password and Password Managers Tip Sheet
- CISA's Multi-Factor Authentication Website
- Identity Theft and Internet Scams Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime



LEARN MORE DURING CYBERSECURITY AWARENESS MONTH

Thank you for your continued support and commitment to Cybersecurity Awareness Month and helping all Americans stay safe and secure online. Please visit www.cisa.gov/cybersecurity-awareness-month to learn more.

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:

- Enable multi-factor authentication (MFA) for all important online activities to provide an additional layer of security
- Use long, random and unique passwords
- Think before you click: recognize and report phishing
- Update your software

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.

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 releases 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 YOURORGANIZATION'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: Think Before You Click: Recognize and Report Phishing, Update Your Software: Use Strong Passwords, Enable Multi-Factor Authentication.

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.

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.

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