CYBERSECURITY AWARENESS MONTH

SECURE OUR WORLD

Follow these top tips to stay safe online!

USE STRONG PASSWORDS...

Make your passwords:
Long: At least 16 characters
Random: Use upper and lowercase letters, numbers and symbols
Unique: Use a different password for each account

...AND A PASSWORD MANAGER

Password managers can:

- Store all your passwords
- Tell you when you have weak or reused passwords
- Generate strong passwords for you
- Automatically fill logins into sites and apps

TURN ON MULTIFACTOR AUTHENTICATION

It provides **extra security** by confirming your identity when logging into accounts, like entering a code texted to a phone or generated by an authenticator app.

RECOGNIZE AND REPORT PHISHING

Common signs of a phish include:

- Urgent/alarming language
- Requests for personal or financial info
- Poor writing or misspellings
- Incorrect email addresses or links

Spot a phish? Report it to your organization or email provider, then delete it.

UPDATE YOUR SOFTWARE

Software updates ensure your devices are protected against the latest threats. Turn on the **automatic updates** in your device's or app's security settings!

SECURE OUR WORLD

STAY SAFE ONLINE WHEN USING AI

While AI might offer valuable capabilities, always remember to stay proactive and educated about the risks. Here are essential tips to ensure you stay secure while using generative AI.

1. Mind Your Inputs

AI systems learn from user inputs, so refrain from sharing anything you want to keep private, like your workplace's company data or your personal details.

TIP: *Avoid sharing sensitive or confidential information with AI models – if you wouldn't post it on social media, don't share it with AI.*

2. Be Privacy Aware

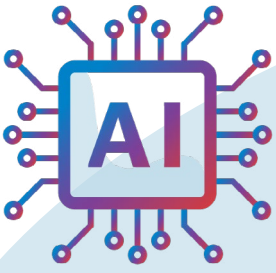
Since AI models often scrape data from the web, what you share publicly online may be copied, in whole or in part, by AI tools.

TIP: *Think about what you share with a wide audience – would you want an AI to have it?*

3. How Hackers Use AI

Cybercriminals may use AI to fool you. Public tools can mimic a person's voice or image (this is sometimes called a "deepfake"). Criminals can make a voice call to mimic a trusted person and steal money or to harass people by posting fake or modified images and videos.

TIP: *Stay updated on cybersecurity best practices. Criminals using AI as a tool makes it more important that everyone protect themselves using the core 4 behaviors: strong passwords, MFA, software updates, and reporting phishing.*



4. AI is a Tool

While AI can assist with tasks, it's important to maintain your expertise and not rely solely on AI-generated content. Prompting isn't the same as creating!

TIP: *Treat AI as a helpful tool rather than a replacement for your skills.*

Remember: Follow the Core 4

As generative AI increases in popularity, adopting the “Core 4” cybersecurity behaviors is paramount for all of us. Use strong, unique passwords (and a password manager!), turn on multifactor authentication for all accounts, keep software updated and watch for phishing.

Use strong passwords

Learn More

Turn on MFA

Learn More

Keep software updated

Learn More

Watch for phishing

Learn More

Taking these steps helps **Secure Our World.**

We can all help one another stay safer online, so share these tips with a family member or friend!

cisa.gov/SecureOurWorld

SECURE OUR WORLD

Install SOFTWARE UPDATES to fix security risks

Update Software Promptly for Safety

When we see an update alert, many of us tend to hit "Remind me later." Think twice before delaying a software update! Keeping software up to date is an easy way to stay safer online. **To make it even more convenient, turn on automatic updates!**

Turn on automatic updates

Look in the device's settings, possibly under Software or Security. Or search the settings for "automatic updates."

Watch for notifications

Not every update can be automatic. Devices—mobile phones, tablets and laptops—will usually notify us that we need to run updates. It's important to install ALL updates, especially for **web browsers and antivirus software.**

Install updates as soon as possible

When notified about software updates, especially critical updates, install them as soon as possible. Online criminals won't wait so we shouldn't either!

Why it's so important to update promptly

If a criminal gets into a device through a security flaw, they will look for personal information and sensitive data to exploit. Technology providers issue software updates to "patch" security weak spots as quickly as possible. **If we don't install them, they can't protect us!**

Software updates can also:

Fix Bugs

Improve Performance

Install Latest Features

Updating software is one way to **Secure Our World.**

We can all help one another
stay safer online, so share these tips with a family member or friend!

cisa.gov/SecureOurWorld

SECURE OUR WORLD

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

OUTSMART online outlaws

Avoid Phishing Scams with Three Simple Tips

Phishing scams are online messages designed to look like they're from a trusted source. We may open what we thought was a safe email, attachment or image only to find ourselves exposed to malware or a scammer looking for our personal data.
The good news is we can take precautions to protect our important data. Learn to recognize the signs and report phishing to protect devices and data.

1 Recognize the common signs

- Urgent or emotionally appealing language
- Requests to send personal or financial information
- Unexpected attachments
- Untrusted shortened URLs
- Email addresses that do not match the supposed sender
- Poor writing/misspellings (less common)

2 Resist and report PHISHING SPAM

Report suspicious messages by using the "report spam" feature. If the message is designed to resemble an organization you trust, report the message by alerting the organization using their contact information found on their webpage.

3 Delete

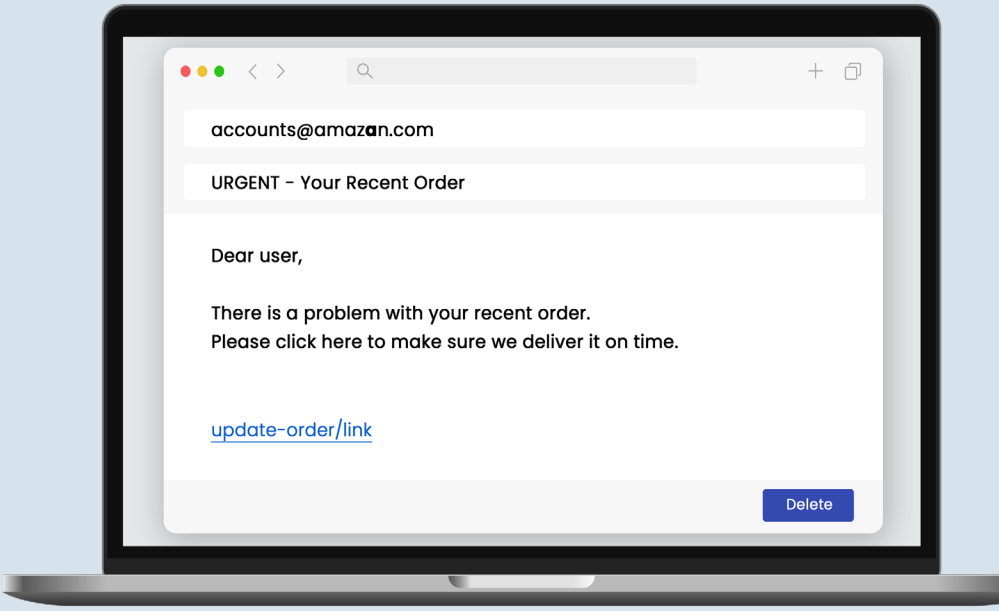
Delete the message. Don't reply or click on any attachment or link, including any "unsubscribe" link. The unsubscribe button could also carry a link used for phishing. **Just delete.**

DELETE

If a message looks suspicious, it's probably phishing.

But even if there's a possibility it could be real, don't click any link, attachment or call any number. Look up another way to contact a company or person directly:

- Go to a company's website to find their contact information
- Call the individual at a known number and confirm whether they sent the message



Avoiding phishing is one way to **Secure Our World.**

We can all help one another stay safer online, so share these tips with a family member or friend!

cisa.gov/SecureOurWorld

REPORTING CYBERCRIME

From identity theft to phishing scams and cyberbullying, the spectrum of cybercrimes is vast and most of us will, unfortunately, encounter it in our digital life. In honor of Cybersecurity Awareness Month, we wanted to help you understand how to navigate these challenges and protect yourself.

General

You can report various forms of cybercrime to the following agencies:
CISA: cisa.gov/report **FBI:** ic3.gov

Hacked Account

Report your hacked account to the respective platform's support team.
Find direct links to popular platforms here:
staysafeonline.org/online-safety-privacy-basics/hacked-accounts/

Ransomware

Contact local law enforcement, including:

- **CISA:** cisa.gov/forms/report
- **FBI:** fbi.gov/contact-us/field-offices
- **U.S. Secret Service:** secretservice.gov/contact/field-offices

Identity Theft

Report identity theft to:
FTC: identitytheft.gov

You can also report to:
ID Theft Resource Center:
idtheftcenter.org or call 888.400.5530

Tax-Related Cybercrime

Report tax-related phishing messages or calls to the IRS via email: phishing@irs.gov

More about tax fraud:
irs.gov/individuals/how-do-you-report-suspected-tax-fraud-activity

Credit Card Fraud

Report credit card fraud to your credit card company or use the FTC's fraud, scam and bad business reporting tool: reportfraud.ftc.gov

Elder Fraud

If you or someone you know has been the victim of elder fraud, contact the U.S. Department of Justice's National Elder Fraud Hotline 833.372.8311

Social Security Fraud

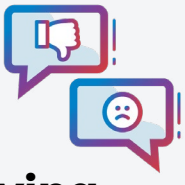
Notify the Social Security Administration if you suspect any fraudulent activities related to your social security number: ssa.gov/fraud or call: 800.269.0271

Business Email Compromise

Report spoofed business-related emails or scams to your organization's IT department and the FBI at: ic3.gov

Online Stalking

If you believe you are being stalked or are a victim of stalkerware, call, chat or text the National Domestic Violence Hotline:
Call: 800.799.7233
Chat: thehotline.org
Text: "Start" to 88788



Cyberbullying

Report cyberbullying to the platform where the bullying occurred or to your child's school.

Report to local law enforcement if there have been threats of violence, stalking or hate crimes at: stopbullying.gov/cyberbullying/how-to-report

Phishing

Report suspicious emails to your email platform and then delete it. Or you can also report to:

- **FTC:** reportfraud.ftc.gov
- **Anti-Phishing Working Group:** reportphishing@apwg.org
- **AARP Fraud Watch Network:** 877.908.3360

Remember: Collect and Keep Evidence

You may be asked to provide evidence when you report certain types of cybercrime. This material can help law enforcement stop and prosecute hackers. All of the following documentation might be considered evidence, but you should keep anything you think could be related to the incident:

- Canceled checks
- Certified or other mail receipts
- Chatroom or newsgroup text
- Credit card receipts
- Envelopes (if you received items via FedEx, UPS or U.S. Mail)
- Log files, if available, with date, time and time zone
- Social media messages
- Money order receipts
- Pamphlets or brochures
- Phone bills
- Copies of emails, preferably electronic copies. If you print the email, include full email header information.
- Copies of web pages, preferably electronic
- Wire receipts

Taking these steps helps **Secure Our World.**

We can all help one another

stay safer online, so share these tips with a family member or friend!

cisa.gov/SecureOurWorld

SECURE OUR WORLD

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

4 EASY WAYS
to stay safe online

Our online world needs to be protected. There are easy things we can do to ensure our information is safe from those wishing to steal it.

Recognize & report phishing

Most successful online intrusions result from a recipient of a "phishing" message accidentally downloading malware or giving their personal information to a spammer. Do not click or engage with these phishing attempts. Instead, recognize them by their use of alarming language or offers that are too good to be true.

Report the phish and delete phishing messages.

Use strong passwords

Simple passwords can be guessed. **Make passwords at least 16 characters long**, random and unique for each account. Use a password manager, a secure program that maintains and creates passwords. This easy-to-use program will store passwords and fill them in automatically on the web.

****

Turn on multifactor authentication (MFA)

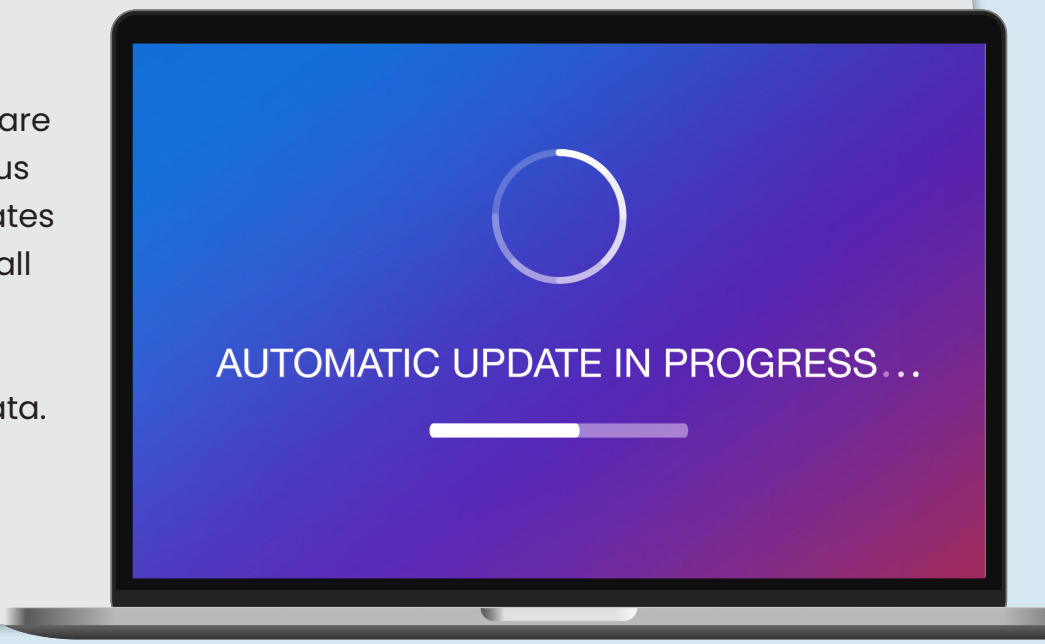
Use MFA on any site that offers it. MFA provides an extra layer of security in addition to a password when logging into accounts and apps, like a face scan or a code sent by text.

Using MFA will make you much less likely to get hacked.

Update software

When devices, apps or software programs (especially antivirus software) notify us that updates are available, we should install them as soon as possible. Updates close security code bugs to better protect our data.

Turn on automatic updates to make it even easier.



Taking these steps helps **Secure Our World.**

We can all help one another stay safer online, so share these tips with a family member or friend!

cisa.gov/SecureOurWorld

SECURE OUR WORLD

Stay **safer** with

MULTIFACTOR AUTHENTICATION (MFA)

How to turn on MFA

MFA provides extra security for our online accounts and apps. This security could be a code sent via text or email or generated by an app, or biometrics like fingerprints and facial recognition. Using MFA confirms our identities when logging into our accounts.

Follow these easy steps on each account

Go to Settings

It may be called Account Settings, Settings & Privacy or similar.

Look for and turn on MFA

It may be called two-factor authentication, two-step verification or similar.

Multifactor Authentication

Confirm

Select how to provide extra login security, such as by entering a code sent via text or email or using facial recognition.

Congratulations!

After setting up MFA, logging in may require completing the MFA security step to prove our identities. It only takes a moment but makes us **significantly safer from malicious hackers!**

Turn on MFA for every online account or app that offers it. Doing so will protect our:

Email | **Banking** | **Social Media** | **Online Purchases** | **Identities**

Using MFA is one way to **Secure Our World.**

We can all help one another stay safer online, so share these tips with a family member or friend!

cisa.gov/SecureOurWorld

SECURE OUR WORLD

Weak PASSWORDS

are the most common way **online criminals** access accounts

Strengthen Passwords with Three Simple Tips

Using strong passwords with the help of a password manager is one of the easiest ways to protect our accounts and keep our information safe.

1 Make them long

At least 16 characters—longer is stronger!

`**********`

2 Make them random

Two ways to do this are:

Use a random string of letters (capitals and lower case), numbers and symbols (the strongest!):

`cXmnZK65rf*&DaaD`

Create a memorable passphrase of 5-7 unrelated words:

`HorsPerpleHatRunBayconShoos`

Get creative with spelling to make it even stronger.

3 Make them unique

Use a different password for each account:

`k8dfh8c@Pfv0gB2`

`LmvF%swVR56s2mW`

`e246gs%mFs#3tv6`

Tip! Use a password manager to remember them.

Let a password manager do the work!

A password manager creates, stores and fills passwords for us automatically. **Then we each only have to remember one strong password**—for the password manager itself. Search trusted sources for "password managers" like Consumer Reports, which offers a selection of highly rated password managers. Read reviews to compare options and find a reputable program for you.

When we choose strong passwords, we make it much harder for someone to steal our:

Data

Money

Identities

Using strong passwords is one way to **Secure Our World.**

We can all help one another stay safer online, so share these tips with a family member or friend!

cisa.gov/SecureOurWorld