CYBERSECURITY
AWARENESS
MONTH

SECURE OUR WORLD

How to Stay Safe Online

SECURE OUR WORLD

October is Cybersecurity Awareness Month

What is Cybersecurity?

- Defined as "the protection of computer systems and networks from attacks by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data..."
- Wherever there is technology, there needs to be cybersecurity.

Why is it Important?

- Implementing cybersecurity best practices is important for individuals as well as organizations of all sizes to protect personal, financial and sensitive information.
- For both government and private entities, developing and implementing tailored cybersecurity plans and processes is key to protecting and maintaining business operations.

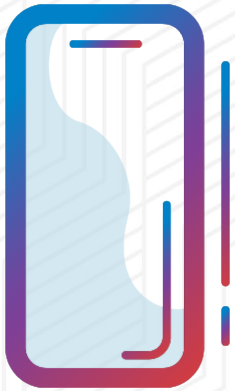
4 Easy Ways to Stay Safe Online

Use Strong Passwords and a Password Manager

Turn on Multifactor Authentication

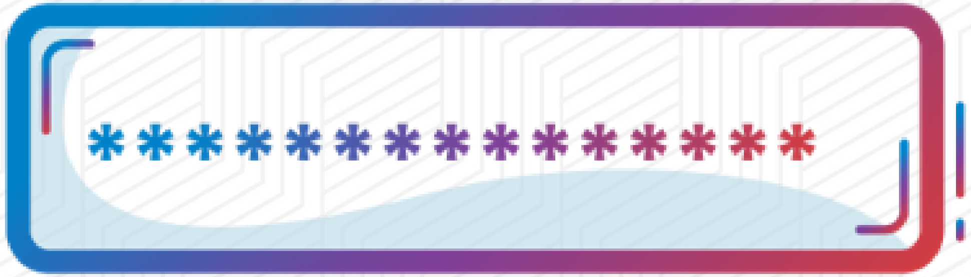
Recognize and Report Phishing Attacks

Update Your Software



Use Strong Passwords

CREATE STRONG PASSWORDS:



- **Long**
  - At least 16 characters
- **Unique**
  - NEVER reuse passwords
- **Random**
  - Upper- and lower-case letters
  - Numbers
  - Special characters
  - Spaces
  - Consider pass-phrases

Use a Password Manager

WHY USE A PASSWORD MANAGER?

- Stores your passwords
- Alerts you of duplicate passwords
- Generates strong new passwords
- Some automatically fill your login credentials into website to make sign-in easy
- It won't fall for a phishing website, even if you do!

Encryption ensures that password managers never "know" what your passwords are, keeping them safe from cyber attacks.

Turn on Multifactor Authentication

WHAT IS IT?

- **A code sent to your phone or email**
- **An authenticator app**
- **A security key**
- **Biometrics**
  - Fingerprint
  - Facial recognition

Turn on Multifactor Authentication

WHERE SHOULD YOU USE IT?

- **Email**
- **Accounts with financial information**
  Ex: Online store
- **Accounts with personal information**
  Ex: Social media

Recognize and Report Phishing

PHISHING RED FLAGS:

- **A tone that’s urgent or makes you scared**
  Ex: "Click this link immediately or your account will be closed"
- **Sender email address doesn’t match the company it’s coming from**
  Ex: Amazon.com vs. Amaz0n.com
- **Unexpected communications such as an email you weren't expecting**
- **Requests to send personal info**
  Legitimate organizations don't ask for personal information through email or an unexpected call.
- **Misspelled words, bad grammar and odd URLs can still be a sign of phishing.**
  Be aware that AI will make spotting these more challenging. Be diligent.

Recognize and Report Phishing

WHAT TO DO IF YOU SPOT A PHISH

Do NOT

- Don't click any links you don’t trust. Delete the email/text.
- Don't click any attachments you were not expecting or recognize.
- Don't send personal info online or share over the phone.

Do

- Verify that the communication is real and contact sender directly through known phone numbers or emails.
- Report it to your IT department or email/phone provider.
- Use email filters
  - Many email services have filters that can help prevent many phishing messages from ever reaching your employees’ mailboxes.
- DELETE IT.

Update Your Software

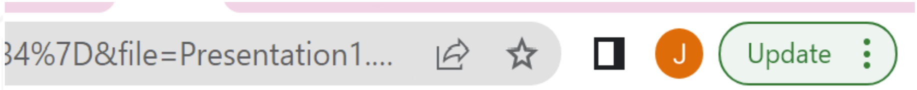
WHY?

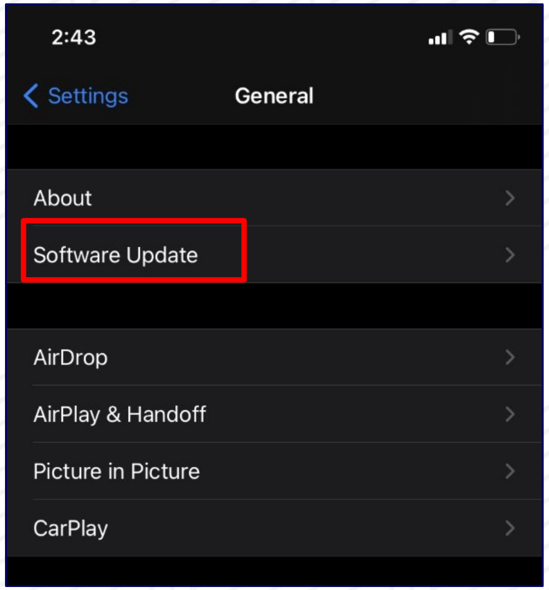
- Updates ensure your devices and apps are protected from the latest threats
- Don't click "remind me later", it could leave you vulnerable to cyber threats
- Automatic updates are the easiest way to stay secure

Update Your Software

WHERE TO FIND AVAILABLE UPDATES

- Check for notifications to your phone or computer
- Look in your phone, browser or app settings
- Check the upper corner of your browser for any alerts





Additional Resources

CISA

- Report a Cyber Issue
- Secure by Design
- Cross-Sector Cybersecurity Performance Goals
- Cyber Resource Hub
- Cybersecurity Training & Exercises
- CISA YouTube Channel

NCA

- Resources and Guides
- Videos and On-Demand Webinars

Get in Touch

CISA

- cisa.gov/cybersecurity-awareness-month
- AwarenessCampaigns@cisa.dhs.gov

NCA

- staysafeonline.org
- info@staysafeonline.org