Nine Ways to Stay Safe Online

Cybersecurity practices to protect people, data and critical infrastructure

CYBERSECURITY AWARENESS MONTH

OCTOBER 2025

BUILDING A CYBER STRONG AMERICA

CYBERSECURITY AWARENESS MONTH

OCTOBER 2025

cisa.gov/cybersecurity-awareness-month

What Is Cybersecurity?

Cybersecurity is the protection of computer systems and networks from attacks by malicious actors that could cause unauthorized information disclosure, theft, or damage to hardware, software or data.

Wherever there is technology, there needs to be cybersecurity.

Why Is it Important?

Implementing cybersecurity best practices helps protect intellectual property and other sensitive data, as well as networks and systems that support your operations.

For both government and private entities, developing and implementing tailored cybersecurity plans and processes is key to safeguarding operations and protecting critical infrastructure.

Four Essential Behaviors to Stay Safe Online

- Update software
- Use strong passwords and a password manager
- Turn on multifactor authentication (MFA)
- Recognize and report phishing

Update Software

What should you remember about updates?

- Updates are the easiest way to ensure your devices and apps are protected from the latest threats.
- Updates only protect you if you install them, so:
  - Install them right away.
    (Don't click "remind me later.")
  - Enable automatic updates
    for convenience.

Update Software

Where do you find available updates?

Notifications: Check for notifications on your phone or computer.

Settings: Look in your phone, browser or app settings.

Browser: Check the upper corner of your browser for any alerts.

Use Strong Passwords

What makes a strong password?

Long

- At least 16 characters

Random

- Upper- and lower-case letters
- Numbers
- Special characters
- Spaces
- Consider passphrases (5-7 unrelated words).

Unique

- Different for each account
- NEVER reuse passwords.

Use a Password Manager

Why use a password manager?

- Stores your passwords.
- Alerts you of duplicate passwords.
- Generates strong passwords.
- Fills in your login credentials on websites to make sign-in easy.
- 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 cyberattacks.

Turn on Multifactor Authentication

What is MFA and where should you use it?

Multifactor authentication (MFA) provides an extra layer of security for your accounts by requiring a quick second step to verify your identity when logging in. Use it on every account that offers it, especially:

- Email
- Accounts with financial information
  - Ex: Banks, online stores
- Accounts with personal information
  - Ex: Social media

Turn on Multifactor Authentication

Which MFA methods are best?

Choose the most secure MFA method available. Here are some options, from most to least secure:

Security key: Use a physical security key (such as a YubiKey) to log in. It plugs in or taps your device. It provides the best protection against phishing and is easy to use.

Authenticator app with number matching: An app prompts you to enter a number on your phone. You enter a number shown on the login screen to confirm your identity.

Authenticator app with one-time code: An app generates a new code every 30 seconds.

Biometrics: Uses your fingerprint or face to confirm your identity.

Text or email code: A one-time code is sent to your phone or email. Least secure method.

Recognize and Report Phishing

How can you tell if a message is phishing?

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 or attachment 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

Be aware that AI will make spotting these more challenging—stay diligent.

Recognize and Report Phishing

What should you do if you spot a phish?

DO

- Verify that the communication is real and contact the 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 phishing messages from ever reaching your employees' mailboxes.
- DELETE IT.

DON'T

- Don't click any links you don't trust, even "unsubscribe" (just delete).
- Don't click any attachments you were not expecting or recognize.
- Don't send personal info online or share over the phone.

Level Up Your Defenses

Businesses & governments at all levels can further strengthen their cybersecurity by practicing these behaviors:

- Use logging & monitoring
- Back up data
- Encrypt data

Use Logging & Monitoring

What is logging and monitoring?

- **Logging** is the process of recording activity on your business systems, including who accessed what, when and from where.

- **Monitoring** adds a layer of oversight by reviewing those logs in real time to identify anomalies or unauthorized behavior.

Together, they create a clear picture of normal, baseline behavior. That means you can quickly detect anything suspicious, like unauthorized access or attempted breaches.

Use Logging & Monitoring

How do you start logging and monitoring?

CISA offers free tools that make it simple to collect and review key system logs. Get started here:

- Logging Made Easy
- Malcolm

Back Up Data

Why do you need to back up your data?

A backup is a secure copy of your business's critical data, stored separately from your primary systems.

In the event of a cyber incident, ransomware, system failure or disaster, backups help you restore your data and recover quickly.

Back Up Data

What are the best practices for backing up data?

Follow the 3-2-1 backup rule:

- 3 copies of important files
- 2 different types of storage media (like a hard drive and the cloud)
- 1 copy stored off-site, away from your business location

Encrypt Data

What is encryption?

Encryption keeps your information safe by scrambling sensitive information into unreadable coded language.

The information is only accessible to someone who has the key or code. So, even if criminals gain access to your files, information stays locked and unreadable.

Encrypt Data

What should you encrypt?

Work with your IT team to implement encryption in your organization.

- Encrypt all devices, hard drives, removable media, and laptops with sensitive data and relevant documents for enhanced security.
- Encrypt data both at rest and in transit.
- Back up your data to an external hard drive or a properly vetted cloud service and always encrypt your backups.
- Maintain offline, encrypted backups of data and regularly test your backups.

Report Cyber Incident Information to CISA

What is cyber incident information sharing?

Cyber incident information sharing means reporting suspected or confirmed cyber incidents, system vulnerabilities or suspicious activity to CISA. In return, CISA shares threat intelligence, mitigation tips and technical assistance.

This sharing is **bidirectional**:

- **You share**: Indicators of compromise, attack methods, timelines and system impacts
- **CISA shares:** Alerts, threat bulletins, mitigation advice, protective measures and tools to reduce risk

Additional practices

More ways to increase your cybersecurity:

Report cyber incident information to CISA

Migrate to the .gov domain

Report Cyber Incident Information to CISA

How do you report a cyber incident, or suspected cyber incident?

Use the online form at: cisa.gov/report

Migrate to the .Gov Domain

What is a .gov domain?

Like .com, .org, .edu or .net, .gov is a “top-level” domain—the last part of an internet address like Acme**.com** or StateU**.edu**.

Unlike the other domains, **.gov is reserved exclusively for U.S.-based government organizations**. Only verified federal, state, local, tribal or territorial (SLTT) entities can register for it.

Migrate to the .Gov Domain

Why migrate?

Using a .gov domain builds trust and improves security for public-facing services.

Cybercriminals often create fake websites and email addresses to impersonate government agencies. Migrating your website and email to the .gov domain can help protect your organization and constituents from such scams.

How do you migrate?

Go to get.gov to find out if you’re eligible and get CISA support to migrate.

Additional Resources

- Cybersecurity Awareness Month
- Report a Cyber Issue
- Cross-Sector Cybersecurity Performance Goals
- Cyber Resource Hub
- Cybersecurity Training & Exercises
- CISA YouTube Channel

Get in Touch

Cybersecurity and Infrastructure Security Agency (CISA)

- central@cisa.gov