Federal Student Aid

Cybersecurity Awareness Month October 2022

Held every October, Cybersecurity Awareness Month raises awareness about digital security and empowers everyone to protect their personal data from online crime. This year's theme — See Yourself in Cyber — highlights how individuals like you, from everyday technology users to cybersecurity professionals, are the first line of defense to thwarting cybercrime. Below are actionable steps you can take today to stay safe online.

4 Easy Steps to Stay Secure Online

CISA recommends the following steps to improve your online cybersecurity:

1 Watch Out for Phishing

Over 80% of cybersecurity incidents stem from a phishing

attempt. Keep an eye out for typos, poor grammar, and other suspicious characteristics in an email, and don't click any links from unknown sources. Remember to report phishing emails so IT teams and service providers can be on alert and prevent others from becoming victims.

---

2 Update Passwords

Replacing simple, repeated passwords with unique and complex passwords can immediately boost your cybersecurity. Use a password manager to securely store your passwords so you don't have to write down or remember them.

---

3 Enable MFA

The use of multi-factor authentication (MFA) is tremendously effective against account compromises. Review the security settings on your most-used accounts and enable MFA or "Two-Step Factor Authentication" if offered.

---

4 Activate Automatic Updates

Updates are important not only for maintenance, but also for patching vulnerabilities cybercriminals can exploit. Enable automatic updates whenever possible.

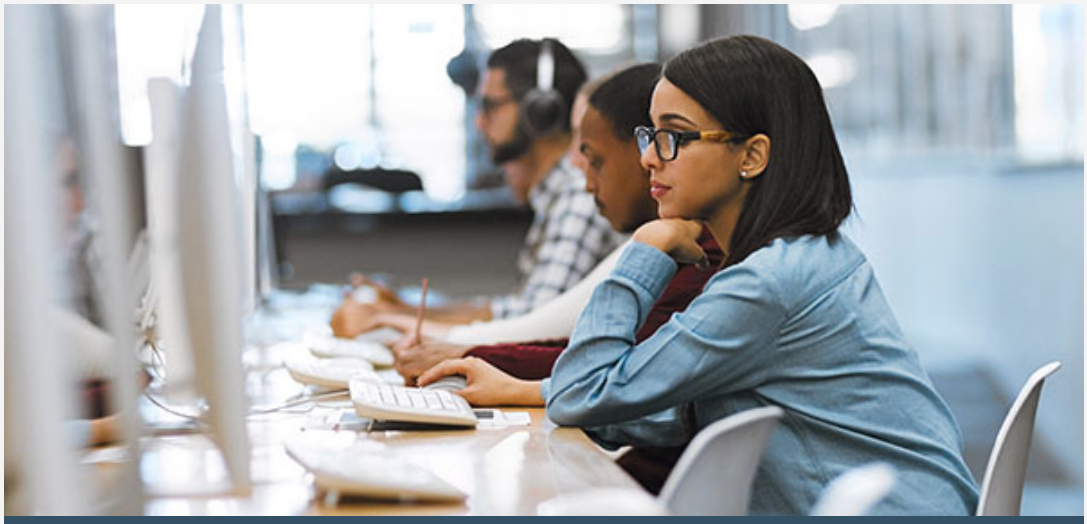
Q: How do password managers keep my credentials safe?

A: Password managers store all your usernames and complex passwords in an encrypted online vault. Password managers can also identify weak or repeated passwords and suggest unique passwords instead. As a bonus, password managers can automatically enter usernames and passwords when you

visit a site and allow you to access login credentials across all your devices.

Lock Hackers Out of Your Home

Securing your home's online security starts with just one device: your router. All online activity flows in and out of this device, so changing the default name (SSID) and password is priority number one. In addition, enable the router's built-in firewall and check that all devices connected to your network have updated software to avoid exploitation of system vulnerabilities.



Preparing for the Worst – Cyber Strategies at Work

Keeping sensitive personal data secure is challenging for educational institutions of all sizes. Here are three steps all schools can take now to protect themselves before an attack happens:

- Create an inventory of all valuable assets and data within your organization.
- Review and list people who have access to important data, systems, and storage locations, and update permissions if needed.
- Create or update your cybersecurity incident response plan, which outlines specific steps to take and people to contact in the event of a breach.