Stay secure at work and home with these 11 tips.

The line between our on- and off-line lives is shifting as technologies bring the internet into our workplaces, homes, and everywhere in between. Here are 11 cyber defense best practices for securing your digital systems and data.

1 Set some priorities.

What are your cybersecurity goals? Have you identified which systems and data you will protect? CIS relies on a global community of cyber defense experts to identify, validate, and promote security best practices such as the CIS Controls (formerly the SANS Top 20) and CIS Benchmarks.

- **CIS Controls: Prioritized cybersecurity best practices**
- **CIS Benchmarks: Configuration guidelines for 140+ technologies**

2 Think before you click.

Hover over a link to reveal the destination URL. If it looks different from what you expect, don't click on it. Search instead for the website you need to find or enter the URL directly into your browser's navigation bar.

3 Don't get phished.

If you receive a suspicious email at work, don't open or click on it. Instead, follow up with your IT security department. Suspicious emails will often have a sense of urgency (a sale, emergency, etc.) driving a request for personal data such as banking information or personal details.

- **How to Spot Phishing Messages Like a Pro**

4 Go beyond the password.

Try using a passphrase with letters instead of a simple password. This unique approach can help you remember long strings for added security. Consider the weak password "cheese" compared to the complex passphrases "1l0v3ch33s3" or "m0r3ch33s3pl3as3."

5 Keep it fresh.

Always install the latest updates for your operating system, browser, and any applications installed on your device. Cybercriminals look for outdated, unpatched systems to leverage known vulnerabilities. Don't let yourself (or your organization) become an easy target.

- **Subscribe to advisories**

6 Reflect, then connect.

Before you connect to an unfamiliar Wi-Fi network, think about the risks. What data might be shared over the connection? Using a VPN can help protect you by creating an encrypted, private connection to the internet.

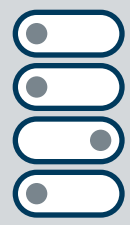
7 Shop smart, shop secure.

Shopping online has become a modern, everyday convenience. Protect sensitive banking data by only shopping on sites you trust. Never save your card information where it could be stolen and used later.

8 Avoid configuration confusion.

Configuration sounds like a big responsibility—and it's an important part of your security program! But it really comes down to the settings for a particular program or machine. You should securely configure workstations, printers, and any network or internet- connected devices in your home or office.

- **Need to be PCI compliant? Check out CIS Benchmarks for operating systems, servers, cloud infrastructure and more.**



9 Don't be the bully.

When conducting business or personal affairs online, remember to be thoughtful and use polite language. Keep in mind that sharing someone's private personal information online, also known as doxxing, is never okay and may get you in legal trouble.

10 Charge with caution.

Don't plug your mobile devices into any outlet you find. Whether it's a work or personal device, you could risk becoming the victim of malware or data theft. If you're worried about running out of battery, bring a back-up power bank.

11 If it matters, use multifactor.

Multifactor authentication relies on more than one of the following to identify you:

- Something you know:
  –a passphrase or swipe pattern
- Something you are:
  –biometrics, fingerprint scanning
- Something you have
  –access to an email account or text code

Use a minimum of two-factor authentication on any important accounts or computers where sensitive data is handled.

CIS® Center for Internet Security®

www.cisecurity.org