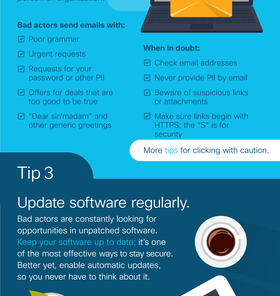
Tips to improve your cyber hygiene

Tip 1

Keep personal information private.

In the wrong hands, personally identifiable information (PII), combined with other personal data (DOB, mother's maiden name), can result in identity theft and cause havoc to your finances and credit. Check out Cisco's approach to PII.



Tip 2

Use caution to avoid bad actors.

Beware of emails from bad actors even if the email seems to be from a trusted person or organization.

Bad actors send emails with:

- ☑ Poor grammar
- ☑ Urgent requests
- ☑ Requests for your password or other PII
- ☑ Offers for deals that are too good to be true
- ☑ "Dear sir/madam" and other generic greetings

When in doubt:

- ☑ Check email addresses
- ☑ Never provide PII by email
- ☑ Beware of suspicious links or attachments
- ☑ Make sure links begin with HTTPS; the "S" is for security

More tips for clicking with caution.

Tip 3

Update software regularly.

Bad actors are constantly looking for opportunities in unpatched software. Keep your software up to date. It's one of the most effective ways to stay secure. Better yet, enable automatic updates, so you never have to think about it.

Tip 4

Create strong passwords and change them often.

We all have dozens of passwords. Any bad actor who guesses just one password can quickly access lots of PII, from your bank data to your home address. Create unique and complex passwords, change them often, and store them safely.

Strong passwords include all of the following:

- ☑ Uppercase and lowercase letters
- ☑ Numbers
- ☑ Symbols
- ☑ 12 or more characters

Tip 5

Use multifactor authentication whenever possible.

Multifactor authentication (MFA), sometimes called two-factor authentication (2FA), strengthens security by requiring additional ways to verify your identity beyond your user ID and password. These added layers guard against phishing, social engineering and password brute force attacks. Additional factors can include a smartphone app and a text to your mobile device.

Tip 6

Be cautious of free Wi-Fi.

Free or public Wi-Fi is particularly vulnerable to hacking. Bad actors can easily capture information, including PII, that you send over the network. Learn more about Wi-Fi attacks and how to protect yourself from them.

When using free Wi-Fi, avoid websites that use and retain your personal data:

- ☑ Online banking
- ☑ School accounts
- ☑ Social media

Tip 7

Don't leave a cyber footprint on a shared or public device.

When using a public computer or any device that is not your own, another user may be able to access your data and accounts.

Before signing off, make sure you:

- ☑ Disable any options to "save password"
- ☑ Log out of your accounts when finished
- ☑ Delete cookies and browsing history

Tip 8

Manage your privacy settings.

Secure your cyber footprint by managing the privacy and security settings on your devices, online services, and applications. That way, you're only sharing information that's actually required, and nothing more.

Tip 9

Regularly audit applications you have installed.

Some mobile apps may have access to more information than you realized. Before downloading a new app, pay close attention to the permissions it requires. Better protect your privacy with this mobile app guide.

Do you really want that app to capture data from any of these?

- ☑ Camera roll
- ☑ Microphone
- ☑ Keystrokes

Tip 10

Secure tomorrow, together.

Share your knowledge to help others become more cyber aware. Good cyber hygiene benefits everyone. Help your family, friends and coworkers stay ahead of the game. To learn more visit trust.cisco.com.