PHIN

5 Easy Ways to **Secure Yourself** Against Cyber Attacks

Click on the topic you’d like to explore!

Be cautious when clicking **links**

Use a **firewall** and **anti-virus** software

Use **wifi** carefully

Use **strong passwords** and **multi-factor authentication** (MFA)

Keep **software** up to date

PHIN

Be cautious when clicking links

Phishing emails are a common cyber attack that tricks the recipient into clicking on a malicious link or attachment.

These **links can be disguised** as common websites **or sent from someone disguised** as a person or business you may know and trust.

If you're unsure of the link, manually go to the company's website to confirm whether the link is malicious.

Here's an example:

You receive an email from what appears to be Amazon telling you there's an issue with your order and you need to sign in with the link provided.

In this instance, you should open a separate tab, manually go to www.amazon.com and log in to your account. If there's an issue with your order, it will appear in your account. If not, you'll know you've outsmarted the cyber criminal and should delete that email!

The most frequently impersonated brands include Amazon, Google, Facebook, Whatsapp, Netflix, and Apple.

See other ways

PHIN

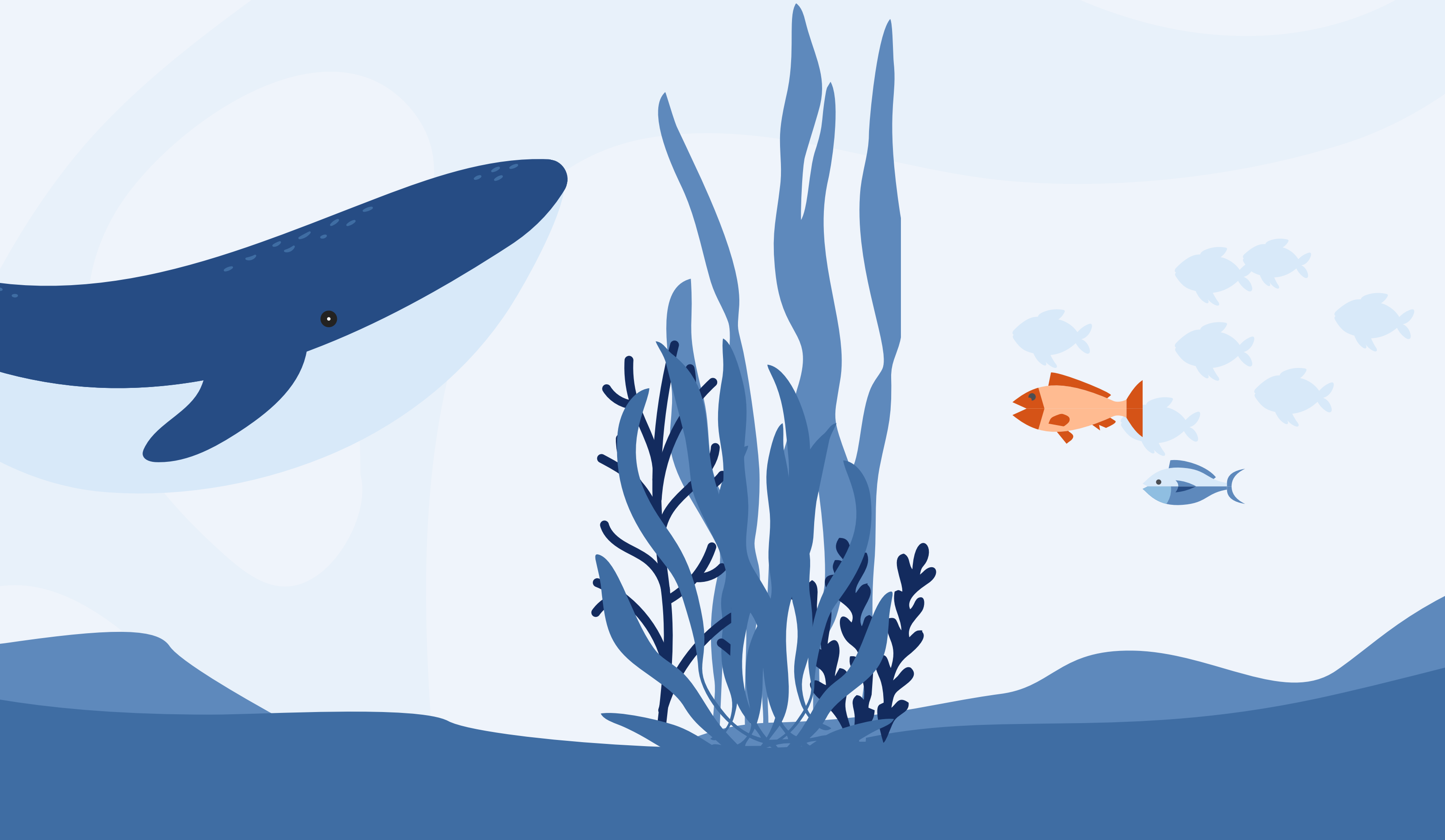
Use a firewall and anti-virus software

A **firewall protects** your computer data **against unauthorized access**.

Anti-virus software detects and removes malicious activity to keep your data secure and your systems working normally.

It is important to have both in place because they each serve a unique and necessary purpose.

See other ways



PHIN

Use strong passwords and multi-factor authentication (MFA)

A strong password includes:

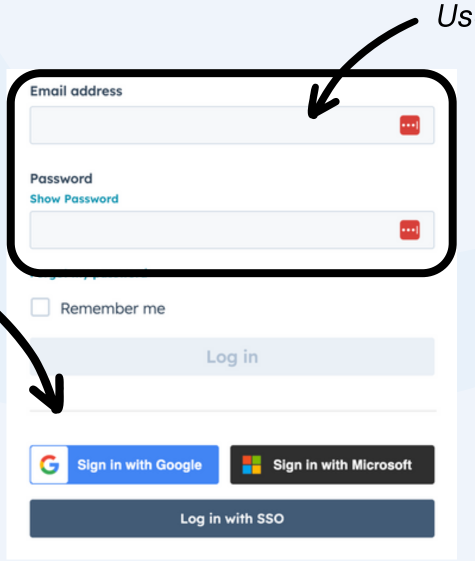
- At *least* 12 characters
- Uppercase and lowercase letters, numbers, and symbols

It should not include names or words found in a dictionary

You should also use different passwords for every account.

Since they can be tricky to remember, we **recommend using a <u>password manager</u>** instead of logging in with Single Sign On (SSO).

Since password managers can come with their own security risks, it's important to double down and **activate 2-factor authentification or MFA**.



Use this

Don't use this

MFA requires you to enter a code from another device in addition to entering your password. This **adds an extra wall of protection** and makes it much more difficult for cybercriminals to access your accounts.

See other ways

Keep your software up to date

Software updates often include security improvements to address any existing vulnerabilities to cyber attacks.

We recommend enabling automatic software updates whenever the option is available. If the updates need to be done manually, you can check the vendors' websites periodically to see when they've released a new update.

It's important to install these updates as soon as they're available.

See other ways

PHIN

Use wifi carefully

Connecting to public wifi can make you an easy target to a cyber attack. Cybercriminals will create wifi with misleading names to make you think they're harmless. Once you connect to them, it will leave you vulnerable to their malicious activity.

Here are some things to consider before connecting to wifi you're unfamiliar with:

1. **Turn off auto-connect and file sharing.** Many devices have a setting that will automatically connect them to nearby wifi or grant the ability to share files.

2. **Use your personal, password-protected hotspot.** This ensures you know who owns the wifi and you control who has access to it.

3. **Use a known network and confirm its authenticity.** Double-check the name and confirm it's a trusted network. Public places often have signs or information on their website with instructions on how to log in.

4. **Avoid accessing sensitive information.** Refrain from logging into banking accounts or other sites with private data.

See other ways