Keep your apps and software up to date

Patches matter because they fix known flaws in products that attackers can use to compromise your devices

Stay Vigilant. Stay Cyber Aware.

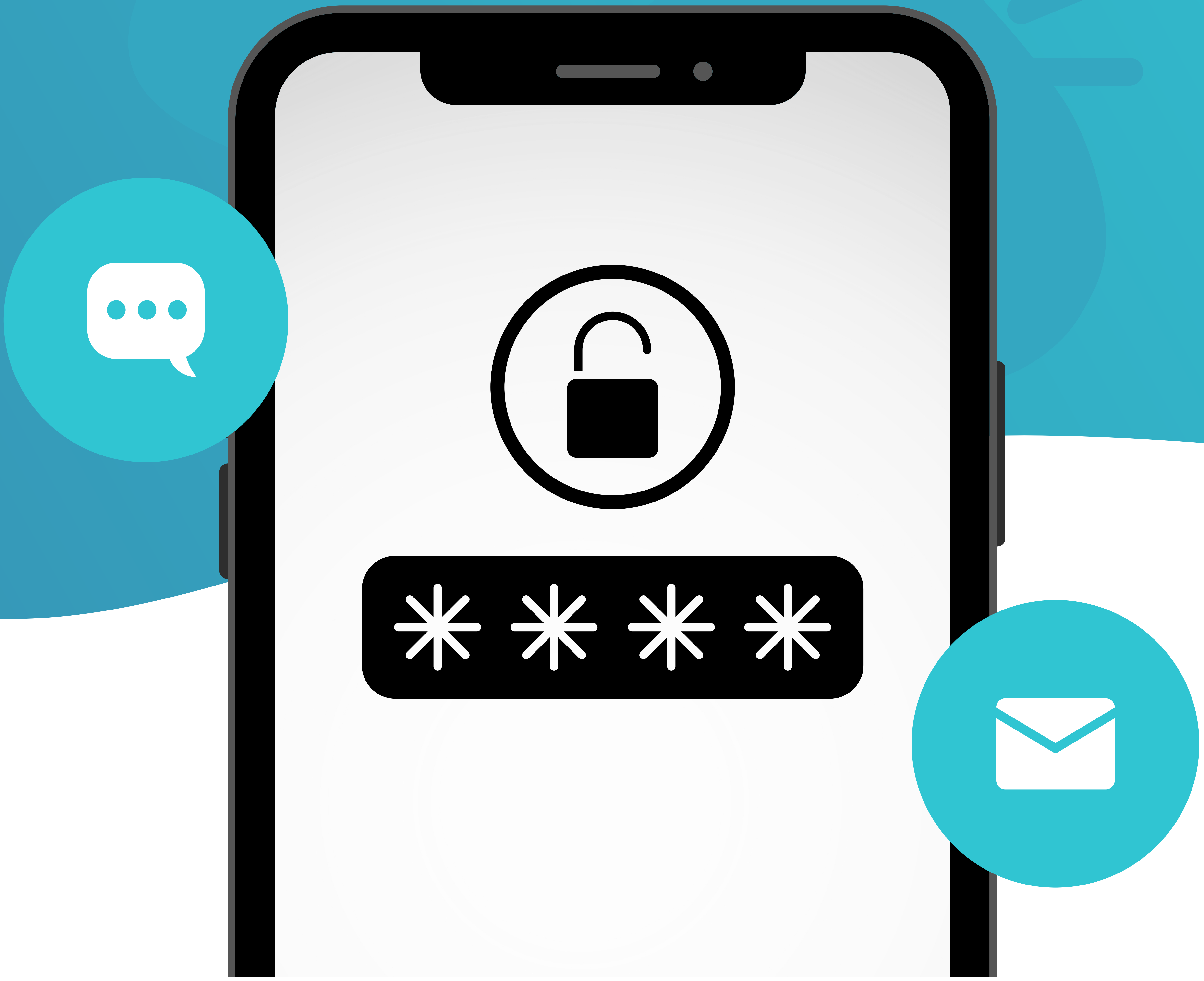
Enable multi-factor authentication (MFA)

MFA helps keep your accounts and devices secure by requiring you to prove your identity multiple times

Stay Vigilant. Stay Cyber Aware.

Enable two-factor authentication (2FA)

2FA helps keep your accounts and devices secure by requiring you to prove your identity more than once



Stay Vigilant. Stay Cyber Aware.

Make sure your home network is secure

Changing the default password on your router and ensuring firmware is updated will help reduce the risk of being hacked

Why use a VPN for extra security?

A Virtual Private Network (VPN) connection disguises your data traffic online and protects it from external access

Stay Vigilant. Stay Cyber Aware.

Don't forget about physical security

Make sure to lock your computer when leaving your desk as well as lock away any paper files which include sensitive information

Stay Vigilant. Stay Cyber Aware.

Are you sharing sensitive information on social media?

Cyber criminals can use the information you post on social media to gain personally identifiable information (PII) about you that can be used against you

Stay Vigilant. Stay Cyber Aware.

Always follow company policies and procedures

Security policies and procedures provide vital guidance that helps us keep our company, colleagues and customers safe from cyber attacks and data loss

Stay Vigilant. Stay Cyber Aware.

Beware of social engineering

Social engineering is an attack vector that relies on human interaction, often involving manipulating people into breaking security procedures to gain access to systems, networks or physical locations

Stay Vigilant. Stay Cyber Aware.

5 telltale signs of a social engineering attack

✓ **The message arrives unexpectedly**

This is a key trait of social engineering, although attackers can also use compromised email accounts to hijack conversations.

✓ **The requested action seems unusual**

Be suspicious if asked to do something you typically wouldn't do (e.g. send money, install something, share customer info, etc).

✓ **The requested action seems risky**

If the action is performed, could it be harmful to the recipient or the business? If so, stop and think.

✓ **An unusual attachment or URL**

Many social engineering scams include a rogue link the user is told to click on or a document/program to download.

✓ **There is a sense of urgency**

Many scams include a heightened sense of urgency, where the scammer wants to communicate a threat of harm.

Stay Vigilant. Stay Cyber Aware.

Don't take the phishing bait!

Phishing emails look like legitimate requests from known entities, often encouraging you to click links, download attachments or provide sensitive information

Remember to think before you click

Stay Vigilant. Stay Cyber Aware.

Phishing awareness tips

✓ Suspicious links in the email

Be cautious if the web address you see when you hover over the link doesn’t seem to match the sender or if the email directs you to a page asking you to log in.

✓ Poor spelling and grammar

Phishing emails and texts can sometimes be littered with spelling and grammatical errors, so look out for these signs.

✓ Request for sensitive information

If asked to share sensitive information that you wouldn't usually share over email, call a known number to verify the request.

✓ Implied urgency or threats

Attackers often rely on a sense of urgency to encourage you to act quickly without giving you time to stop and think.

✓ Suspicious domains

Many malicious emails use a domain that looks similar to the legitimate domains, but with slight differences.

Stay Vigilant. Stay Cyber Aware.

Always use strong, unique and confidential passwords

Your passwords must be unique, private, and easy for you to remember without being easy for an attacker to guess

Stay Vigilant. Stay Cyber Aware.

Password security tips

✓ Don't reuse passwords

If a data breach leaks one of your accounts, the attacker could gain access to other accounts using your reused passwords.

✓ Don't leave passwords in plain sight

Do not leave passwords in an insecure location such as a post-it note, journal, or unencrypted text file.

✓ Don't share your passwords

Never share your passwords or accounts with anyone, not even your coworkers.

✓ Make long and simple passwords

Use a series of unrelated words to create long, simple passwords rather than short and complex ones.

✓ Use multi-factor authentication methods

Leverage the most secure multi-factor authentication method available to you such as an authenticator app.

Stay Vigilant. Stay Cyber Aware.