



1. Create strong and separate passwords

Don't reuse passwords, especially for your most important accounts such as email and banking.



That way if one was to be compromised, the rest of your accounts should be ok. A strong and easy-to-remember password can be created using three random words, e.g.: beachglasskitten.

2. Use Multi-Factor Authentication

Wherever possible, add an additional layer of protection with multi-factor authentication (MFA). Also called two-factor authentication, MFA requires two (or more) methods to verify your log-in attempt is coming from you, before allowing you access to an account.



3. Run updates as soon as possible

Although it can feel like a chore when your PC, Phone, or App wants to run an update, don't delay or ignore this. Updates are often released to patch flaws or vulnerabilities, and therefore will better equip your systems against cyberattacks. For something that can be done in the time it takes to make a coffee, it is a simple way of improving your security.

4. Be smart about what you click

When you receive an email or visit a web page, only click when you are sure what you are viewing is genuine. Always check for signs such as a different sender email or web address, bad grammar, payment requests and demands for you to act urgently. If it looks suspicious, don't trust it – and warn others not to either.



5. Don't overshare

If you use any social media platforms or online forums, it's important to regularly review the information you share and what could be pieced together about your life. You may be making it easy for someone to target you for scams such as identity theft and email phishing. Check privacy settings and consider if there's anything that should be kept off the internet.

6. Be cautious when using public WiFi

The free WiFi you use in that nice coffee shop could make it easy for someone to see and steal the personal information you are sharing over that connection. Only use public WiFi to browse the internet and not for online shopping or logging into your financial accounts. If you need to access personal data, consider using a VPN to do so.

