



1. Weak password - PASSWORD123 isn't going to cut it. Use a long, strong and unique passphrase instead.
2. Declining MFA makes your accounts easier to access. MFA adds an extra layer of protection.
3. Passwords left lying around can fall into the wrong hands. Keep passwords private.
4. Brad Pitt ❤️ Is that really Brad, or a deepfake romance scam?
5. An urgent request for money, apparently from someone you trust. Always verify unexpected requests another way.
6. Putting off updates is risky, and can leave security gaps open.
7. Updates fix security vulnerabilities, always turn on automatic updates when you can.
8. Oversharing in a selfie. ID cards, documents, screens etc in the background can reveal useful information to cyber criminals.
9. That QR code could be fake. Scammers use them to direct you to malicious websites.
10. Be careful what you share with AI. Never enter sensitive or confidential information.
11. Smart devices? Secure your Wi-Fi with a strong passphrase and consider a guest network.
12. Robo vac or spy vac? Connected devices need protection too. Keep smart devices secure and up to date.

**own
your
online**
cyber smart week