

TOP 10 ONLINE SAFETY RULES

works
for us

Part of Citizens Advice Milton Keynes

Simple explanations to help you stay safe on a computer

1 Use strong passwords

Passwords protect your accounts. Weak or short passwords are easy for attackers to guess or crack.

A strong password should be:

- Long (12-16 characters or more)
- Use letters, numbers and symbols
- Be different for every account

A password manager can safely store passwords so you don't have to remember them all

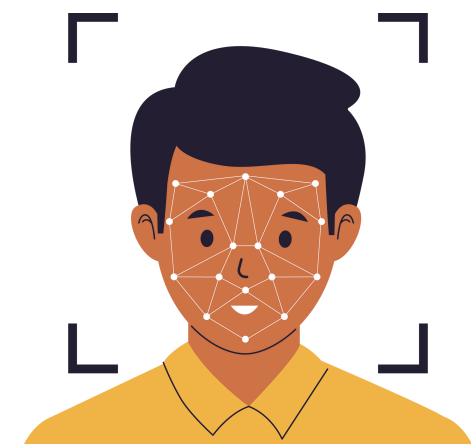


2 Turn on multi-factor authentication (MFA)

MFA adds an extra step when logging in, such as:

- A code sent to your phone
- A fingerprint or face scan

Even if someone steals your password, they still can't log in without this second step.



3 Keep your computer and apps updated

Updates often fix security holes that hackers already know about.

If you delay updates:

- Your device stays vulnerable
- Attacks become easier

Turn on automatic updates so protection happens in the background.



4 Be careful with emails, texts and messages

Many cyberattacks start by tricking people, not breaking computers.

Be cautious if a message:

- Feels urgent or threatening
- Asks for passwords, money, or personal details
- Has strange links or attachments

When unsure, don't click — delete or verify first.



5 Use antivirus or security software

Antivirus software looks for harmful programs like:

- Viruses
- Malware
- Ransomware

Make sure your security software:

- Is always turned on
- Updates automatically to catch new threats

Examples might be Microsoft Defender (Windows Defender)

- Built into Windows: No install needed — it protects your PC right away.
- Decent basic protection against viruses & malware.
- Runs quietly in the background. [Windows Central](#)

Others are available:

Tips Before Installing Third-Party Antivirus

- Only download antivirus software from the official site, not from random pop-ups or links you find online — fake antivirus scams are common. [BSI](#)
- If you install a third-party antivirus, Windows Defender usually turns off automatically to avoid conflicts.



6 Be cautious on public Wi-Fi

Public Wi-Fi is often unsecured, meaning others could spy on your activity.

Avoid:

- Banking
- Shopping
- Entering passwords

If you must use public Wi-Fi, a VPN helps protect your data.



7 Back up important files

Files can be lost due to:

- Accidental deletion
- Computer failure
- Viruses or ransomware

Keep backups:

- On an external hard drive
- Or in secure cloud storage

This way, your files are safe even if something goes wrong.



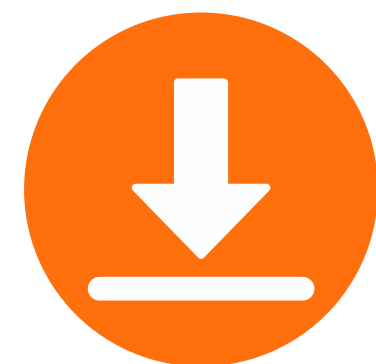
8 Think before you click and download

One unsafe click can install malware without you knowing.

Avoid:

- Unknown links
- Unexpected attachments
- Free software from untrusted websites

If it looks suspicious or too good to be true, don't click.



9 Check app and privacy settings

Many apps ask for access they don't really need.

Regularly check:

- Camera access
- Microphone access
- Location tracking

Only allow permissions that make sense for what the app does.



10 Secure your devices

Simple physical security helps prevent misuse.

Always:

- Use a passcode or screen lock
- Lock your screen when you walk away
- Secure your home Wi-Fi with a strong password
- Cover your webcam when not in use



Key Takeaway

If you remember only three things:

- ✓ Strong passwords + MFA
- ✓ Keep everything updated
- ✓ Stop and think before clicking

These habits protect against most common cyber threats.