

Step 5 - Avoid online scams

- ▶ Do not click on links in any unverified emails, texts or other messages (eg. WhatsApp).
- ▶ Verify using a trusted phone number or contact or check via their official website or app.
- ▶ Never be rushed into clicking a link that requests you reset your password, secure your account or requires your personal or banking details.
- ▶ No genuine organisation will phone or message you unexpectedly and ask you to make changes to your device or give them remote access.

Report fraud and cybercrime to Action Fraud
on **0300 123 2040** or **actionfraud.police.uk**

For free cyber security advice and resources
or to arrange a community cyber safety session
email: **CyberProtect@northants.police.uk**



Cyber Safety

**Five simple steps to help keep
you and your family safe online**



Northamptonshire Police

Fighting crime, protecting people

Step 1 - Password security

- ▶ Strong memorable passwords can easily be created by combining three random words. (eg. Trampoline%Sleepy%Dishwasher)
- ▶ Create new passwords for any toys, games, smart devices, etc. connected to the Internet.
- ▶ Never share passwords or on-screen codes with anyone no matter who they claim to be.
- ▶ Consider using a trusted Password Manager if you access multiple website accounts.
- ▶ Always make sure you use a different password for each account or site.

Step 2 - Extra account protection

- ▶ Two-factor authentication (2FA) adds an extra layer of security to your online account.
- ▶ Enable 2FA (via account settings) on each of your important accounts such as email, photo, shopping and social media sites.

Step 3 - Software updates

- ▶ Always keep your device software, apps and other programs up-to-date to fix newly identified security bugs and vulnerabilities.
- ▶ Also enable Automatic Updates on your computer, phone and tablet where available.
- ▶ Do not use devices that cannot be fully updated as this may put your personal data at risk.

Step 4 - Backup important data

- ▶ Make regular copies of all your important documents, messages, contacts, photos and videos on a separate device or system.
- ▶ Ideally use at least one local backup (eg. flash drive, separate hard drive) and a cloud based backup (eg. iCloud, OneDrive, Google Drive).
- ▶ Ensure all of your important documents are included, and that you also disconnect local backup drives to minimise the affect of malware.