



Cyber Safety

Six simple steps to help you and your family stay safe online

- 1. Password Security**
- 2. Extra Account Protection**
- 3. Password Managers**
- 4. Software updates**
- 5. Backup important data**
- 6. Avoid online scams**

Password Security

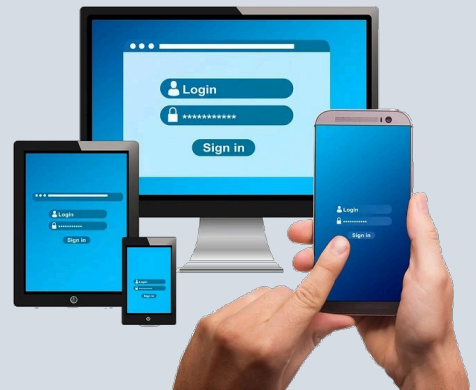
Strong memorable passwords can easily be made by combining three random words. Add numbers and symbols to make it even stronger. (eg.Trampoline%Sleepy*Dishwasher)

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.

Always make sure you use a different password for each account or site.

Avoid using personally relatable names, words or dates in your passwords.



Extra Account Protection

Two factor authentication (2FA) provides an extra layer of security to verify genuine account access.



Enable 2FA (via account settings) on each of your important accounts such as email, cloud storage, shopping and social media sites.

It is advisable to close dormant accounts or any others you do not intend to make use of.

To check to see if any of your online accounts have ever been involved in a data breach click this link and search for your email address: <https://haveibeenpwned.com>

Password Managers

Password managers can create, store and automatically enter passwords for you. They provide a much more secure and convenient alternative to writing passwords down or having to remember and type each password every time you visit an online account.

Password managers can be used on all computers, phones and tablets and some devices even have password management features already built-in.

Password managers can also help protect those family members who might otherwise unknowingly reveal their account passwords to scammers.

Some password managers can notify you about recent website data breaches or leaks and recommend that you change affected passwords.

We recommend that you conduct your own research on what is the right password manager for you and your device.

Ensure you download your password manager from an official app store (Google Play Store, Apple App Store, Amazon Appstore) or the trusted developer's website.

Further guidance on password managers can be found on the NCSC (National Cyber Security Centre) link here:

<https://ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers>



Software updates

Always keep your device software, apps and other programs up-to-date to fix newly identified security bugs and vulnerabilities.



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.

Backup important data

Make regular backup 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) to ensure the integrity of your data.



Ensure all of your important documents are included, and that you also disconnect local backup drives to minimise the effect of malware.

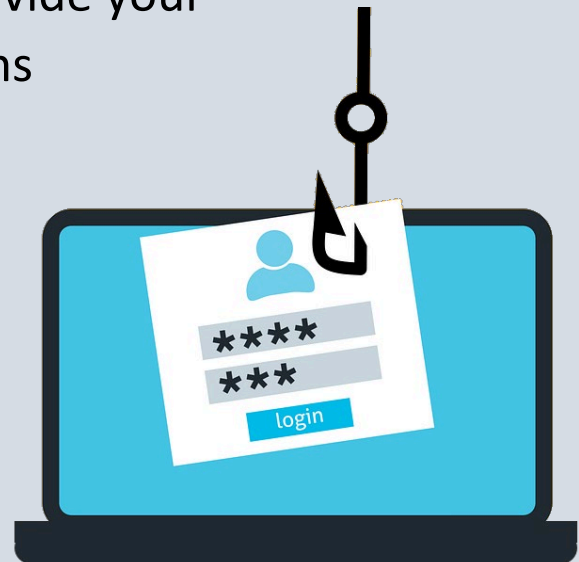
Avoid online scams

Do not click on links in any unverified emails, texts or other messages (eg. WhatsApp).

Never be rushed into clicking links in an unverified email or message, as most of those telling you to reset your password, secure your account or require you to provide your personal or banking details are likely scams

Verify using a trusted phone number or contact or check via the official website or app.

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 via 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