Cyber Security for Home Users

Practical steps to protect yourself, your family and your devices online.

Contents

Strong Passwords

Why this matters

Weak passwords allow criminals to access email, banking and shopping accounts.

Example problem

Many people reuse the same password across multiple websites. If one site suffers a breach attackers try the same password elsewhere.

What you can do

1. Use a password manager
2. Use passwords with 12-16 characters
3. Do not reuse passwords on multiple sites

Multi-Factor Authentication

Why this matters

MFA adds an additional layer of security to accounts.

Example problem

If someone steals your password they still cannot access the account without the second authentication step.

What you can do

1. Enable MFA on email accounts
2. Enable MFA on banking services
3. Use authenticator apps where possible

Email and Phishing Scams

Why this matters

Phishing emails attempt to trick you into revealing passwords or payment details.

Example problem

Many scams pretend to be from delivery companies, banks or government organisations.

What you can do

1. Check the sender address carefully
2. Avoid clicking suspicious links
3. If unsure, visit the official website directly

Software Updates

Why this matters

Updates fix security weaknesses in devices and applications.

Example problem

Many cyber attacks succeed simply because devices are running outdated software.

What you can do

1. Enable automatic updates
2. Update phones, tablets and laptops regularly
3. Replace devices that no longer receive security updates

Backups

Why this matters

Backups protect your files if a device fails or ransomware encrypts your data.

Example problem

Without backups important photos or documents may be permanently lost.

What you can do

1. Back up photos and documents regularly
2. Use cloud backup or external drives
3. Follow the 3-2-1 backup rule

Home Wi-Fi Security

Why this matters

An insecure Wi-Fi network can allow attackers to access devices connected to it.

Example problem

Many routers still use the manufacturer's default administrator password.

What you can do

1. Change the router admin password
2. Use WPA2 or WPA3 encryption
3. Create a guest network for visitors

Social Media Safety

Why this matters

Personal information shared on social media can be used for identity theft or scams.

Example problem

Criminals often gather personal information from public profiles.

What you can do

1. Set your date of birth visibility to Friends Only
2. Avoid sharing location publicly
3. Review privacy settings regularly

Children and Online Safety

Why this matters

Children can be exposed to scams, harmful content and unsafe online interactions.

Example problem

Games and chat platforms sometimes expose children to risks.

What you can do

1. Use parental controls
2. Discuss online safety with children
3. Review privacy settings on apps and games

Signs Your Device May Be Compromised

1. Emails sent from your account that you did not write
2. Unknown login alerts
3. Unexpected bank or payment notifications
4. Browser redirects to strange websites
5. Frequent pop-up warnings or fake antivirus messages

When to Seek Professional Help

If you suspect that a computer, phone or online account has been compromised it may be safer to seek professional assistance.

About Wellis Technology

Wellis Technology provides practical technology guidance and cyber security awareness for businesses, organisations and home users.

www.wellis-technology.co.uk

wellis.technology@gmail.com