Cybersecurity Awareness: Simple Tips to Stay Safe Online

With cyber attacks becoming increasingly sophisticated, it's crucial that everyone understands the basics of staying safe online.
This guide provides practical, easy-to-follow advice that anyone can implement to significantly improve their digital security.

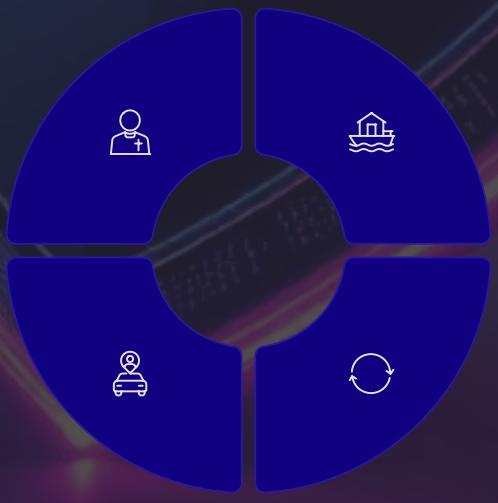
Remember: Cybersecurity is Everyone's Responsibility

Stay Vigilant at Work

Apply security best practices in your professional environment. Your workplace security affects not just you, but your entire organisation.

Help Others

Share your knowledge and assist friends, family, and colleagues in staying safe online. Collective security benefits everyone.



Protect Your Home

Use the same security mindset for personal devices and accounts. Home and work security are interconnected in our digital lives.

Review Regularly

Periodically assess your security habits and update your practices as threats evolve and new protective measures become available.

To find out more or to arrange an awareness or training event please contact us at:
protect@dyfed-powys.police.uk

Heddlu • Police
DYFED-POWYS
Uned Troseddau Economaidd a Seiber
Economic and Cyber Crime Unit (ECCU)

Turn On Multi-Factor Authentication (MFA)



Extra Layer of Protection

MFA requires a second form of verification, such as a code sent to your phone, adding crucial security beyond passwords alone.

Even If Passwords Are Compromised

Your accounts remain protected when attackers only have your password but lack access to your second factor.

Enable on All Accounts

Prioritise email, banking, social media, and work systems. These are the accounts that matter most to your security and privacy.

Use Strong, Unique Passwords

Create Long, Complex Passwords

Consider combining three random words for memorable yet strong passwords.
Including a mix of uppercase, lowercase, numbers, and symbols will also make it stronger.

Never Reuse Passwords

Each account should have its own unique password. If one account is compromised, others remain protected.

Use a Password Manager

Trusted password managers generate, store, and autofill passwords securely, making strong password practices effortless.



Recognise and Report Phishing Attempts

Warning Signs to Watch For

- Urgent or alarming language
- Requests for personal or financial information
- Suspicious links or email addresses

Never Click Unexpected Content

Avoid clicking on attachments or links from unknown senders or unexpected emails, even if they appear to come from familiar sources.

Verify!

Not sure if the message is genuine? Find a trusted method to verify the senders details such as calling them on a number you know is theirs and checking if they sent the message.

Report and Delete

Immediately report phishing emails to your IT team, then delete them to prevent accidental future clicks.



Secure Your Devices and Connections

Lock Your Devices

Use PINs, passwords, or biometric security on all devices. This prevents unauthorised access if your device is lost or stolen.

Avoid Public Wi-Fi for Sensitive Tasks

Don't use public or unsecured Wi-Fi for banking or other sensitive activities. Use VPNs when public Wi-Fi is necessary.

Download from Official Sources

Only download applications from trusted official stores like Google Play or Apple App Store to avoid malicious software.

Keep Your Software Updated

Enable Automatic Updates

Set your devices and applications to update automatically. This ensures you receive critical security patches without delay or manual intervention.

Protection Against Latest Threats

Updates patch security vulnerabilities and protect against the most recent cyber threats and malware variants discovered by security researchers.

Don't Delay Installation

When prompted to install updates, don't postpone them. Delayed updates leave your systems vulnerable to known security flaws.

If in Doubt, Call It Out



Trust Your Instincts

Cyber attacks can be subtle and sophisticated. If something feels suspicious or unusual, don't ignore that feeling seek help from IT professionals or security teams.

Report Incidents Promptly

Quickly report any security incidents or mistakes, such as accidentally clicking a suspicious link. Early reporting can significantly reduce potential harm to you and your organisation.

Knowledge Sharing Protects Everyone

When you share information about threats you've encountered, you help protect colleagues, friends, and family from similar attacks.

Business Continuity Planning for Cyber Attacks

Protect your business, your customers, and your reputation

Why You Need a Plan

- Cyber-attacks can cause downtime, data loss, and financial damage.
- A Business Continuity Plan helps you **recover quickly** and keep operations running.

Key Steps for Your Plan

🔐 1. Identify Critical Assets

- List essential systems (finance, customer data, email, website).
- Decide what must be restored first in an emergency.

💾 2. Backup Data Regularly

- Store backups securely (cloud + offline).
- Test recovery to ensure backups work.

📝 3. Create an Incident Response Checklist

- Who to contact (IT support, bank, regulator - ICO) and their contact details
- Steps to isolate affected systems.
- Communication plan for staff and customers.

👥 4. Assign Roles and Responsibilities

- Nominate a response lead.
- Train staff on what to do if systems are compromised.

🔄 5. Test and Update the Plan

- Run practice scenarios.
- Review and update at least annually.

** Keep a printed copy of your plan somewhere accessible **

Stay Secure, Stay Informed

Cybersecurity is an ongoing journey, not a destination. Threats continuously evolve, and staying informed is crucial for maintaining effective protection.

Trusted Resources

Visit the National Cyber Security Centre (UK) for comprehensive, up-to-date cybersecurity guidance and threat intelligence.

https://www.ncsc.gov.uk

Continuous Learning

Regularly educate yourself about emerging threats, new protective technologies, and evolving best practices in digital security.

Membership with the Cyber Reseilience Centre for Wales can help you keep up to date on the latest threats.

https://wcrcentre.co.uk

Share Knowledge

Help create a more secure digital environment by sharing what you learn with others in your personal and professional networks.

Reminder to Cybersecurity Essentials

Use this reference for quick scanning and to reinforce essential security habits.

Strong Passwords

Unique, complex passwords for every account

Multi-Factor Authentication

Additional verification beyond passwords

Phishing Awareness

Recognise and report suspicious emails

Software Updates

Keep systems patched and current

Device Security

Lock devices and secure connections

Incident Reporting

Call out suspicious activities promptly

Heddlu · Police
DYFED-POWYS
Uned Troseddau Economaidd a Seiber
Economic and Cyber Crime Unit (ECCU)