



EMPOWERING PEOPLE.



BUILDING SKILLS.



CREATING OPPORTUNITY.



**STAY SAFE ONLINE.
PROTECT YOURSELF.
PROTECT OTHERS.**

This guide provides practical tips to help you stay safe online, protect your personal information and avoid common cyber threats.



CYBER SECURITY & ONLINE SAFETY

Simple steps can protect your personal information, devices and accounts from online threats.



CYBER AWARENESS IS EVERYONE'S RESPONSIBILITY.



1. USE STRONG PASSWORDS

- Use long passwords with a mix of letters, numbers and symbols.
- Avoid using personal information (e.g. name, date of birth).
- Use a different password for each account.
- Consider using a password manager.

Strong passwords protect your accounts.



2. ENABLE TWO-FACTOR AUTHENTICATION (2FA)

- 2FA adds an extra layer of security to your accounts.
- Even if someone gets your password, they still can't access your account.
- Enable 2FA wherever possible.

An extra step makes a big difference.



3. BEWARE OF PHISHING SCAMS

- Be cautious of unexpected emails, texts or messages.
- Don't click on links or download attachments from unknown senders.
- Check the sender's email address carefully.
- Phishing scams try to steal your information.

Think before you click.



4. KEEP YOUR DEVICES AND SOFTWARE UP TO DATE

- Updates fix security flaws and protect against threats.
- Enable automatic updates when possible.
- Keep your antivirus software up to date.

Updates help keep hackers out.



5. USE SECURE WI-FI CONNECTIONS

- Avoid using public Wi-Fi for sensitive activities (e.g. banking).
- If you must, use a VPN for extra protection.
- Always log out of accounts when finished.

Secure connections keep your data safe.



6. PROTECT YOUR PERSONAL INFORMATION

- Only share personal information when necessary.
- Adjust privacy settings on social media.
- Be careful what you post online.
- Your information can be valuable to cyber criminals.

Less information shared, less risk.



7. RECOGNISE COMMON CYBER THREATS

- **Malware:** harmful software that damages or steals data.
- **Ransomware:** locks your files and demands payment.
- **Identity theft:** uses your information to impersonate you.

Awareness is the first defence.



8. BACK UP YOUR DATA REGULARLY

- Back up important files to an external drive or secure cloud storage.
- Backups can help you recover data if your device is lost, stolen or attacked.

Backups today, peace of mind tomorrow.



9. BE MINDFUL OF SOCIAL ENGINEERING

- Scammers may pretend to be someone you trust.
- They may ask for information or access to your accounts.
- Verify requests through another trusted channel.

Verify before you trust.



10. REPORT SUSPICIOUS ACTIVITY

- Report suspicious emails, messages or calls to your organisation or IT team.
- Report scams to Action Fraud: 0300 123 2040 or visit www.actionfraud.police.uk
- Reporting helps protect others.



CYBER SAFETY STARTS WITH YOU.

Stay informed. Stay alert. Stay safe.



NEED SUPPORT?

Drae & Dre Collective CIC can help you build your digital confidence and signpost you to further support.



VISIT OUR WEBSITE

www.draeanddre.com



This guide provides general information and should not be taken as legal advice. It is based on current UK guidance for most adult workers (18+) in Great Britain. Some occupations and workers under 18 may have different legal entitlements. Cyber threats and advice may change over time.



DRAE & DRE
— COLLECTIVE CIC —

EMPOWERING PEOPLE • BUILDING SKILLS • CREATING OPPORTUNITY.