Stay safe online

Top tips for staff

Regardless of the size or type of organisation you work for, it's important to understand how to defend yourself from cyber attacks.

The advice summarised to the right is applicable to your working life and your home life.

National Cyber Security Centre
a part of GCHQ

Use strong passwords

Criminals will try the most common passwords (e.g. password1), or use publicly available information to try and access your accounts. If successful, they can use this same password to access your other accounts.

- Create a strong and memorable password for important accounts, such as by combining three random words. Avoid using predictable passwords, such as dates, family and pet names.
- Use a separate password for your work account. If an online account gets compromised, you don't want the criminal to also know your work password.
- If you write your passwords down, store them securely away from your device. Never reveal your password to anyone; your IT team or other provider will be able to reset it if necessary.
- Use 2 step verification (2SV) for important websites like banking and email. 2SV (which is also known as multi-factor authentication or MFA) provides a way of 'double checking' that you really are the person you are claiming to be when you're using online services.

Defend against phishing attacks

Phishing emails appear genuine, but are actually fake. They might try and trick you into revealing sensitive information, or contain links to a scam website or an infected attachment.

- Phishers use publicly available information about you to make their emails appear convincing. Review your privacy settings, and think about what you post.
- Know the techniques that phishers use in emails. This can include urgency or authority cues that pressure you to act.
- Phishers often seek to exploit 'normal' business communications and processes. Make sure you know your organisation's policies and processes to make it easier to spot unusual activity.
- Anybody might click on a phishing email at some point. If you do, tell someone immediately to reduce the potential harm caused.

Secure your devices

The phones, tablets, laptops or desktop computers that you use can be targeted both remotely and physically, but you can protect them from many common cyber attacks.

- Don't ignore software updates - they contain patches that keep your device secure. Your organisation may manage updates, but if you're prompted to install any, make sure you do.
- Always lock your device when you're not using it. Use a PIN, password, or fingerprint/face id. This will make it harder for an criminal to access a device if it is left unlocked, lost or stolen.
- Avoid downloading fake apps. Only use official app stores (like Google Play or the Apple App Store), which provide protection from viruses. Don't download apps from unknown vendors and sources.

If in doubt, call it out

Reporting incidents promptly - usually to your IT team or line manager - can massively reduce the potential harm caused by cyber incidents.

- Cyber attacks can be difficult to spot, so don't hesitate to ask for further guidance or support when something feels suspicious or unusual.
- Report attacks as soon as possible - don't assume that someone else will do it. Even if you've done something (such as clicked on a bad link), always report what's happened.