NCSC's cyber security training for staff now available

The NCSC's e-learning package 'Top Tips For Staff' can be completed online, or built into your own training platform.

Sarah Lyons

The NCSC's recent work with small to medium sized enterprises (SMEs), charities, and the legal and accountancy sectors, has highlighted a key issue for those organisations.

There is so much cyber security advice available these days, many people find it hard to know where to start. Some organisations struggle to explain **why** cyber security is something that all staff should care about. Even larger organisations (with dedicated training resources) find it difficult to explain the technical aspects of cyber security in ways that are **relevant** to their staff, so that they can help keep their organisations (and themselves) safe from cyber attack**.**

Equally, many SMEs and charities may not have the resources to put any cyber security policies and training in place at all, leaving staff exposed as their frontline defence against cyber attacks.

For these reasons, the NCSC has produced an e-learning training package: 'Staying Safe Online: Top Tips for Staff'. It's totally free, easy-to-use and takes less than 30 minutes to complete. The training introduces why cyber security is important and how attacks happen, and then covers four key areas:

- defending yourself against phishing
- using strong passwords
- securing your devices
- reporting incidents ('if in doubt, call it out')

The training is primarily aimed at SMEs, charities and the voluntary sector, but can be applied to any organisation, regardless of size or sector. It's been deliberately designed for a non-technical audience (who may have little or no

knowledge of cyber security), with tips that complement any existing policies and procedures.

How to use the 'Top Tips for Staff' training

There are two options for using the e-learning package:

1. The first (and easiest) way is to direct your staff to the Stay Safe Online: Top Tips for Staff or Gadw'n ddiogel ar-lein: Prif awgrymiadau i staff pages which are hosted on the NCSC website. The package is free to use, and includes a short quiz at the end, with links to further reading. No login is required - just click on the link and start learning.

2. The other way is to integrate the package into your own organisation's training platform. You can do this by downloading the zip file from our website, the file you download will depend on your organisations LMS system. There are English and Welsh versions available, which contains the package as a SCORM-compliant file. We have also created an API version as an alternative to help users who have been unable to use SCORM.

    Download SCORM+2004 (English)
    Download SCORM 1.2 (English)
    Download SCORM (Welsh)

Once imported into your own LMS system, you can tweak the package to suit your needs (such as setting a pass rate for the quiz) as the content is covered by the Open Government Licence.

We've also summarised the core messages from the training in the following infographic, which you're also free to download, print, and share. For the best quality, please download the PDF version.

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.

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.

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.
- 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.

However you decide to use the 'Top Tips For Staff' e-learning, we're confident it can help you build cyber defenders amongst your staff, the front-line in protecting your organisation from cyber attacks.

Sarah L
Deputy Director for Economy & Society

WRITTEN BY
Sarah Lyons
Deputy Director, Economy and Society Resilience

PUBLISHED
14 April 2021

WRITTEN FOR
Public sector

Small & medium sized organisations

Large organisations

PART OF BLOG
NCSC publications