Scottish Government
Cyber Resilience Unit
Interactive Training Guide

V2.0

Use this toolkit to help get started on training your staff with the following cyber fundamentals:

- Cyber topics to teach your staff
- It includes resources and links to training available
- Awareness raising trusted partners

This interactive guide will provide you with the training essentials on the following topics:

- Password Security
- Phishing
- Social Engineering
- Malware

Note: This guide provides links to authoritative, free sources of advice and guidance that may be useful for meeting basic training needs. This guide is not a replacement for, nor to discourage the developing of quality private sector offerings.

Full list of GCHQ Certified Training courses.

Scottish Government
Riaghaltas na h-Alba
gov.scot

Password Security

Passwords prevent unwanted access to your accounts. It can be difficult to know what makes a password strong. With the increase of online services, coming up with new passwords for every account and trying to remember them can be difficult.

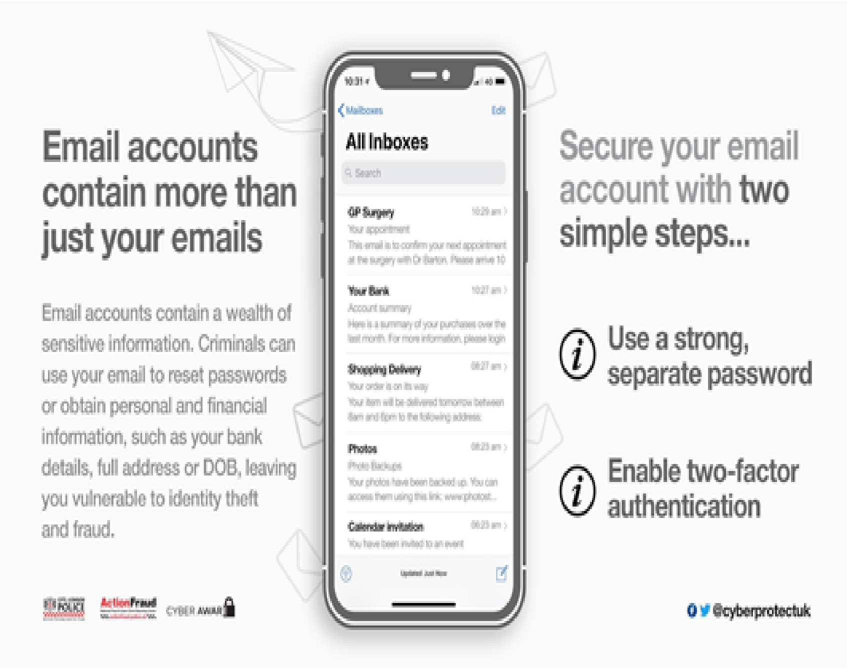
Key Messages: Focus on how to choose a good password, remember them and store them securely – also how to add extra security with Two-Factor Authentication (2FA)

Things to do with your staff:

- Help them learn how to choose a good, strong passphrase. This should be at least three random words. You can do this in small groups or as one-to-one training. Use this article (NCSC – Think Random) to introduce the idea (15 mins)

- Password Managers can be useful for creating and storing passwords. Consider showing your staff how to set up and use a password manager. Some popular password managers are 1Password, Dashlane, LastPass, My1Login. (20 mins) (Find out what the NCSC think of Password Managers here)

- Finally, Two-Factor Authentication is one of the best ways to protect your password. Show staff how they can switch this on for popular accounts (for example their email or social media). This article shows you how to turn it on. (Turn on 2FA) (20 mins)



Email accounts contain more than just your emails

Email accounts contain a wealth of sensitive information. Criminals can use your email to reset passwords or obtain personal and financial information, such as your bank details, full address or DOB, leaving you vulnerable to identity theft and fraud.

Secure your email account with two simple steps...

Use a strong, separate password

Enable two-factor authentication

Other Useful Links / Guidance on Passwords

NCSC – Simplify Your Approach

NCSC - Password Managers

NCSC– Strong Password

Password Video

Phishing

Phishing is when someone pretends to be from a trustworthy source in order to trick you into giving up confidential or important information. Phishing can be carried out via a text message, social media, or by phone, but these days most people use the term 'phishing' to describe attacks that arrive by email.

Key Messages: Understanding how to spot a phishing attack (and 'Spear phishing') - ***Training should be about building confidence*** *and empowering users to make informed decisions. Encourage reporting of cyber incidents.*

Things to do with your staff

- Teach your staff how to spot a phishing attempt. Print out this quiz (Catch The Fish) and use it as a fun activity to help them understand the difference between genuine emails and phishing emails. (15 mins)

- Teach your staff about Spear Phishing. Show them this CPNI Video. Use this Infographic in a training email to staff and print out these posters to raise awareness of spear phishing techniques (Urgency and Authority) (10 mins)

- Consider running a phishing simulation campaign using this guide (CPNI - Designing Phishing simulations)

- An important aim of this campaign is for employees to feel encouraged and supported in reporting suspected spear phishing attempts to their organisation - even if this is after they have clicked. Teach staff how to report a cyber-incident in your organisation. You could pitch this in a way that your staff are working together to try and report 100% of attempts. (This could work alongside your phishing simulation.)

DON'T GET
HACKED!
Use two-factor authentication (2FA) to protect your online accounts.
POLICE
ActionFraud
CYBER AWARE
@cyberprotectuk

Useful Links and Resources about Phishing

CPNI – Don't Take The Bait

Phishing Video - Add this to your social sites / Email to staff

NCSC Guidance for Defending Your Organisations

Social Engineering

Social Engineering is the act of manipulating or tricking people into certain actions including giving up personal or financial information, with approaches usually made by somebody you trust or in authority. (Phishing is a type of Social Engineering Attack).

> *Key Messages: Be aware of what information you are sharing online that could be used in a Social Engineering Attack. Adjust your privacy settings.*

Things to do with your staff

- A digital footprint is the data that's left behind whenever you use a digital service. Show your staff this short video about online identity. Teach staff to understand about their Digital Footprint, use this poster (You are more interesting than you think)

- Carry out an exercise with staff to see what information is shared online about them. Use Part 3 (Website Checklist) to allow you to see what information is online about you, that criminals could potentially use. It will help you to understand and monitor your digital footprint. (20mins)

- Use Mark Zuckerberg Facebook page to understand what information he is sharing about himself which criminals could use to make a convincing social engineering attack. (15 mins) Use this video to show what information companies can get from a simple "like" on a Facebook page.

- Show staff how to manage their digital footprint online and understand what they can do to minimize their vulnerability to security threats.

- Explain to your staff about browser tracking. Show how to use private browsing mode whenever you want to keep your browsing history confidential (for example if you are buying someone a gift). Learn about what it is and how to turn it on.

Useful Links / Resources

CPNI Digital Footprint Campaign

Post / Share this video about computer software service fraud.

CPNI – Social Engineering Video

takefive-stopfraud.org.uk

STOP AND THINK

Your bank or the police will never:

1. Phone and ask you for your PIN or full banking password.
2. Ask you to withdraw money to hand over to them for safe-keeping.
3. Ask you to transfer money out of your account.
4. Send someone to your home to collect cash, PIN, cards or cheque books.

MY MONEY?
MY INFO?
I DON'T
THINK SO
CITY of LONDON POLICE
ActionFraud
@cyberprotectuk

Malware

Malware is short for malicious software, which is created by cyber criminals to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

Key Messages: Always install software and app updates. Back up your most important data to an external hard drive or cloud-based storage.

Things to do with your staff

- Help them learn how to keep all their software up to date. Software and app updates can contain vital security updates to help protect your device. Show staff this video about updates and teach staff how to update their apps and software using this advice. It shows how to update Windows, Mac, Android. For iPhone users, Apple Guide for updating ios Software (20 mins)

- Having a back –up of your data is essential. If your data / information was held to ransom or destroyed, it wouldn't be as big a worry if you have a back up copy. Use this guide to consider what things you should be backing up. More advice about backing up.

- Show staff how to set up Anti Virus software on their own devices. For personal use, there are many internet security software / antivirus suites available. Whichever you choose, make sure it is a reputable brand from a mainstream supplier, and get the best you can afford. Show your staff the different options and how to install them. Remember, they only need to download and use one security software app. Here are a few of the best-known providers. **Norton**, **McAfee**, **Bullguard**, **Sophos**, **AVG**, **Avast**, **Bitdefender** (15mins)

Useful Links/ Resources

Get Safe Online – Software Updates

Get Safe Online – Virus & Spyware

Get Safe Online – Back-Ups

Don't let criminals hold your data hostage!
PAY
LOGIN
Backup your most important data to an external hard drive or cloud-based storage.
POLICE
ActionFraud
CYBER AWARE
@cyberprotectuk
For more information about how to stay safe online, visit Cyberaware.gov.uk

National Cyber Security Centre (NCSC) e–learning

*We would encourage **all staff** to complete this e-learning.*

The National Cyber Security Centre have launched a new resource, 'Top Tips For Staff', to help organisations ensure your staff stay safe online.

‘Top Tips for Staff' is an e-learning video that offers four actionable and practical tips on how to defend yourself at home and at work. It is easy to follow and takes no more than 30 minutes to complete. The training is aimed at staff at any seniority, organisation size or sector and designed for a non-technical audience. This e-learning package can be completed online, or built into your own training platform.

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')

Useful Links/ Resources

Stay Safe Online: Top Tips for Staff

Stay Safe Online: top tips for staff infographic

GCHQ Certified Training

CPNI’s Embedding Security Behaviour Change

Scottish Government
Riaghaltas na h-Alba
gov.scot

Trusted Partners

The National Cyber Security Centre the UK's authority on cyber threat, risk, prevention, awareness, reporting, response and recovery. NCSC continues to develop its advice and support offering.

CPNI has developed a series of security awareness campaigns, designed to provide organisations with a complete range of materials they need. Each campaign set has full guidance on how to run the campaign, and materials such as downloadable posters that can be customised to the organisation, wallets, flyers, videos and checklists

Get Safe Online (GSO) is a UK Government-funded free resource providing practical advice to individuals and businesses on how to protect themselves while on their computers and mobiles device and against fraud, identity theft, viruses and many other problems encountered online.

Take 5, a UK awareness campaign led by FFA UK (part of UK Finance), and delivered with and through a range of partners in the UK payments industry, financial services firms, law enforcement agencies, telecommunication providers, commercial, public and third sector.

You can report cybercrime to Police Scotland as follows:

- Telephone 999 (emergency) or 101 (non-emergency).
- In person at any Police station