



superhighways

harnessing **technology** for **community** benefit

Cyber security top tips

From Email to AI conference

What we'll be covering:

- ✓ Cyber attacks
- ✓ NCSC's 5 areas to focus on
- ✓ Microsoft 365 security features that can help
- ✓ Resources including interactive online training
- ✓ Other training opportunities



Case study & task:

How is 'Help the Homeless' charity vulnerable to cyber-attacks?

How might a cybercriminal take advantage and attack the charity?





<https://youtu.be/CbETCJ8Yc-U>



Non cyber vulnerabilities

- ✓ Multi use office – PCs / laptops stolen
- ✓ Outreach working – mobile devices lost or stolen
- ✓ Confidential data viewable on office screens

Cyber vulnerabilities

- ✓ Volunteers / trustees using personal devices
- ✓ Regular home & remote working – personal broadband routers, unsecured internet in cafes etc
- ✓ Staff, volunteers, trustees, clients – *maybe* low levels of digital savviness
- ✓ Staff not logging out of the House or Training room PCs
- ✓ Publicly available info via website & social media accounts
- ✓ Phishing – financial fraud (exploiting part time hours of financial manager), route to Local authority / other funders?



Some context about Cyber Attacks

Question:

In the annual DCMS survey 2024, what percentage of charities reported having experienced any kind of cyber security breach or attack in the last 12 months?

32%

20% 32% 56% 76%

7



Why are charities at risk?

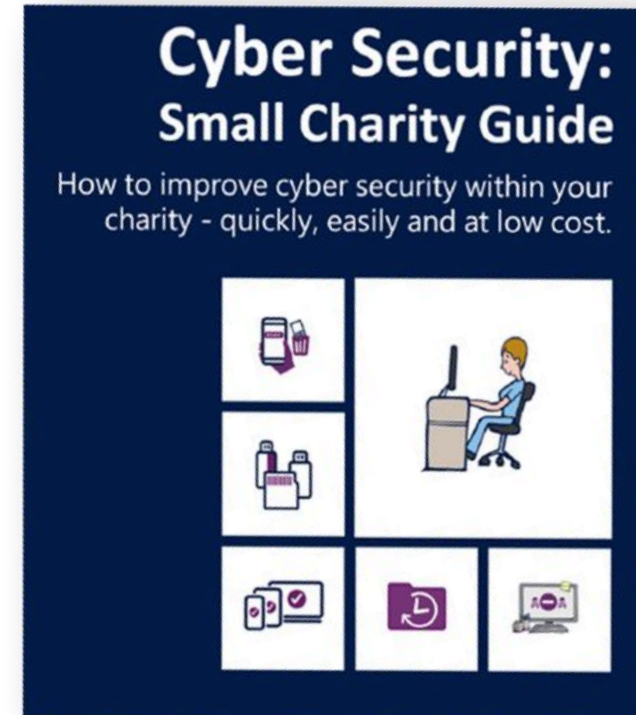
<p>Charities...</p>	<p>Hold funds</p> 	<p>Personal, financial and commercial data of interest or monetary value</p> 	<p>Data is sensitive, valuable and vulnerable to attack</p> 
<p>Impact...</p> <p>Data gets lost</p> 	<p>You have to stop operations</p> 	<p>Financial/Time cost to recover</p> 	<p>Reputation</p> 



What can you do to protect your charity?

The National Cyber Security Centre's 5 quick, simple, free or low cost steps

1. Backing up your data
2. Protecting against malware
3. Keeping your devices secure
4. Creating strong passwords
5. Defending against phishing attacks



[Download the full guide](#)

[Download the infographic](#)



Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.



Identify what needs to be backed up. Normally this will comprise documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases.



Ensure the device containing your backup is not permanently connected to the device holding the original copy, neither physically nor over a local network.



Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.



Switch on PIN/password protection/fingerprint recognition for mobile devices.



Configure devices so that when lost or stolen they can be **tracked, remotely wiped** or **remotely locked**.



Keep your **devices** (and all **installed apps**) **up to date**, using the **'automatically update'** option if available.



When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.



Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your charity from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.



Use antivirus software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.



Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the **'automatically update'** option where available.



Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.



Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.



Ensure staff **don't browse the web** or **check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.



Scan for malware and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).



Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.



Make sure all laptops, MACs and PCs **use encryption products** that require a password to boot. Switch on **password/PIN protection** or **fingerprint recognition** for mobile devices.



Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.



Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).



Do not enforce regular password changes; they only need to be changed when you suspect a compromise.



Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.



Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.



Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.



Most Common Passwords

Is yours here?

select a category below to filter

■ alphanumeric ■ animal ■ fluffy ■ food ■ macho ■ names ■ nerdy ■ rebellious ■ security ■ sports



David McCandless Information is Beautiful
source: 20+ data breaches // [data](#)

MADE WITH VIZsweeT



Creating a Secure Password

- ✓ Choose three random words
 - ✓ carrot printer sparrow
- ✓ Add some punctuation
 - ✓ carrot"printer"sparrow"
- ✓ Add some numbers
 - ✓ 20carrot"printer"sparrow"24
- ✓ You now have a 27-character password that's easy to remember!
- ✓ [Free Password Generator | Create Strong Passwords | Bitwarden](#)



PINs, passwords and biometrics

- Switch on PIN /password protection / fingerprint recognition for all devices
- If using Windows laptops – new installations use the Windows Hello feature, where you choose a PIN specific to that device and with single sign on, signs on to your Office 365 account. But it can't be used to sign on another device. (See [Why a PIN is better than a password](#))



Multi (or Two) Factor Authentication

- ✓ Have you had to sign in to a website or service that requires two factor authentication?
- ✓ Describe the experience.
- ✓ What are the advantages and disadvantages of using two factor authentication?



Why MFA is Important

- ✓ Enhanced Security
 - An extra layer of protection with something you have (phone, authenticator etc.)
- ✓ Protection against Credential Theft
 - 61% of IT breaches involve stolen/compromised credentials
- ✓ Reduction in Unauthorized Access
 - Microsoft say that MFA can protect against over 99% of M365 potential attacks



Key takeaways

1. **Switch on password protection** – where this not enabled by default
2. **Change all default passwords** – to mitigate against ‘open door’ access
3. **Avoid predictable passwords** – have an organisational password policy, implementing NCSC’s 3 random words plus a number and symbol
4. **Use two factor authentication** – where available for the tools you are using
5. **Individual accounts for everyone where possible** – easier to control authorised access Remember to block accounts / change passwords when people leave your organisation



What is Phishing?

- ✓ A scam in which a criminal impersonates a trusted online organisation, sending fake emails to thousands of people to trick them into handing over important sensitive information like account numbers and passwords, or containing links to bad websites.
- ✓ Scammers might try to trick you into sending money, steal your details to sell on, or send you to a dodgy website which could download viruses onto your computer or steal your passwords.



Know the obvious signs of phishing

A phishing attack is a type of cyberattack that tries to trick users into revealing their personal or financial information. Some of the common features of a phishing attack are:

- ✓ - **A fake sender:** The attacker pretends to be someone else, such as a trusted company, a friend, or a government agency. They may use a similar email address, logo, or website to fool the user.
- ✓ - **A sense of urgency:** The attacker creates a false sense of urgency or threat, such as saying that the user's account has been compromised, that they have won a prize, or that they need to update their information immediately.
- ✓ - **A request for information:** The attacker asks the user to click on a link, open an attachment, or provide their personal or financial information. The link may lead to a malicious website that looks legitimate, the attachment may contain malware, or the information may be used for identity theft or fraud.

AI is being used by attackers to effectively personalise phishing emails by analysing and accurately following the tone and style of the sender's email.



Here's two phishing examples

facebook

Hi,

Your Facebook account was recently logged into using a confirmation code and the email address [REDACTED] on April 16, 2022.

Operating system: Windows
Browser: Chrome
IP address: 36.87.22.189
Estimated location: Clearwater, FL

If you did this, you can safely disregard this email.

If you didn't do this, please [secure your account](#) here or by scanning the QR code below.



Thanks,
The Facebook Security Team

OVERDUE INVOICE: New attached Overdue Invoice via Adobe [REDACTED] Coordinator

Source Plain text

From: info <info@[REDACTED]org.uk>
Sent on: Wednesday, December 14, 2022 7:48:14 AM
To: Undisclosed recipients;;
Subject: OVERDUE INVOICE: New attached Overdue Invoice via Adobe [REDACTED] Coordinator
Urgent: High

You have received a new Document Via Adobe

Creating a theory of change for your charity

Sent From: [REDACTED] Coordinator

Document Shared: *INVOICE_Due28736.PDF*

Document Size: [672 KB]

[Download Invoice](#)

NOTE: You may need to download the document for proper and clear view

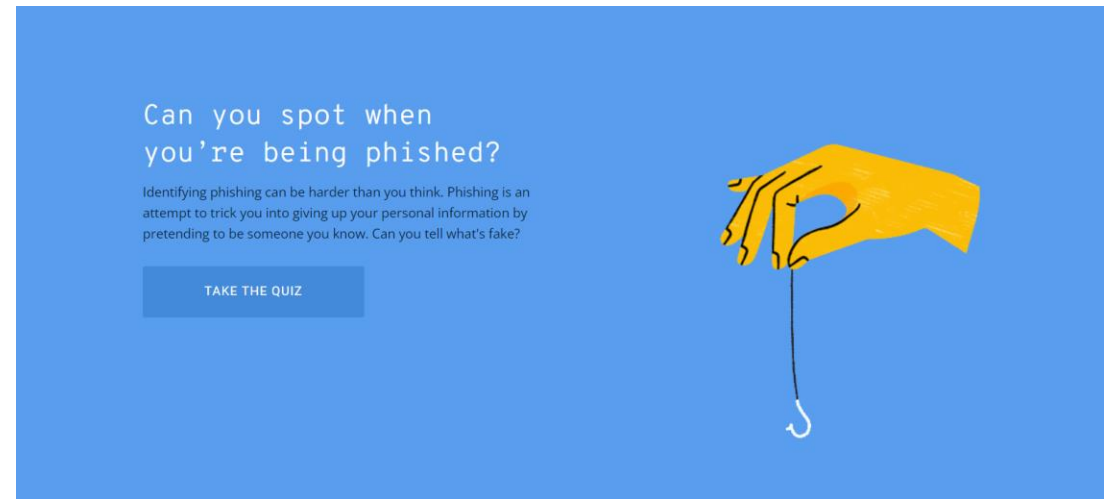


Spotting Phishing Emails

This was put together by a team from Google

[Jigsaw | Phishing Quiz](#)


Let's take the quiz together.



Can you spot when you're being phished?

Identifying phishing can be harder than you think. Phishing is an attempt to trick you into giving up your personal information by pretending to be someone you know. Can you tell what's fake?

TAKE THE QUIZ



Avoiding Spear-Phishing / Check your digital footprint

- ✓ Attackers use publicly available information about your charity and staff to make their phishing messages more convincing, often gleaned from your website and social media accounts
- ✓ What do visitors to your website and social media followers need to know, and what detail is unnecessary (but could be useful for attackers)? What do trustees, staff and volunteers give away about your charity online?
- ✓ See the [CPNI's Digital Footprint Campaign's](#) useful resources including posters and booklets to help you work with staff to minimise online security risks.



Spear-Phishing

Good example of spear-phishing in [Which](#)

4 ways you can avoid being spear-phished

1. Avoid oversharing on social media:
2. Don't give away your data on dodgy websites and on Facebook Surveys
3. Have an up-to-date antivirus installed:
4. Chatting to / winding up scam callers:



Report all attacks

- ✓ Encourage your team to ask for help if they think they might have been a victim of phishing and to raise as soon as possible
- ✓ Take immediate steps if you suspect a successful attack has occurred including scan for malware and change passwords as soon as possible
- ✓ **Avoid a blame culture** – this may discourage people from reporting in future
- ✓ If you believe you have been a victim you should report this through:
 - ✓ Action Fraud
 - ✓ Charity Commission – where there's been a serious incident
 - ✓ Information Commissioners Office – where this has led to a data breach



NCSC's Exercise in a box



✓ <https://exerciseinabox.service.ncsc.gov.uk/>

Identifying and Reporting a Suspected Phishing Email

A short and sharp exercise focussed on phishing, exploring this topic using a combination of interactive activities covering the definition of phishing, the impact, and identifying a phishing email.

🕒 15 - 30 mins

📁 Phishing

Try without registering

Using Passwords

A short and sharp exercise focussed on passwords, exploring this topic using a combination of interactive activities covering the common use of passwords, how attackers find your passwords, and what you can do to limit the risk of your passwords being discovered.

🕒 15 - 30 mins

📁 Passwords

Try without registering

Connecting Securely

A short and sharp exercise focussed on connecting securely to a network when working remotely, exploring this topic using a combination of interactive activities to cover establishing a secure network connection and connecting to a public Wi-Fi network.

🕒 15 - 30 mins

📁 Remote Working

Try without registering

Securing Cloud Productivity Suites

A short and sharp exercise focussed on securing cloud productivity suites, exploring this topic using a combination of interactive activities covering the use of cloud productivity suites and associated security controls you should consider.

🕒 15 - 30 mins

📁 Cloud

Try without registering

What is Malware?

- ✓ Malicious software that is designed to interfere with a computer's normal functioning and that can be used to obtain information and commit cybercrimes.
- ✓ **Ransomware** - a type of malware that makes data or systems unusable until the victim makes a payment



Most common types of Malware

Name	What it does
Adware	Serves unwanted advertisements
Spyware	Collects user activity data without the users acknowledge (to monitor users' activities)
Ransomware	Disable victims access to data until ransom is paid
Fileless Malware	Make changes to files that are native to the Operating System
Trojans	Disguises itself as desirable code (to control the system activities)
Worms	Spreads through a network by replicating itself (to slow down the entire system/network)
Rootkits	Allow the attacker for remote control of victim's device
Keyloggers	Monitor/Record victims' keystrokes
Mobile Malware	Infects on Mobile Devices (similar activities as above)
Bots	Launches abroad flood of attacks (such as Distributed Deny of Services DDoS)



NCSC's 5 tips to protect against malware

1. Use antivirus software on all computers
2. Patch all software and firmware
3. Control access to removable media
4. Switch on your firewall
5. Smartphone guidance



5 tips to keep mobile devices secure

Smartphones, tablets and laptops used outside the safety of the office and home need even more protection than 'desktop' equipment. The NCSC recommends you:

1. Switch on PIN /password protection / fingerprint recognition
2. Configure tracking on your devices
3. Keep devices up to date
4. Don't connect to public Wi-Fi hotspots
5. Replace older devices



NCSC's 4 tips re backups

1. Take regular backups (& check you can restore)
2. Identify what data needs to be backed up
3. Ensure backup devices are NOT permanently connected to your network
4. Consider backing up to the cloud – see <https://www.ncsc.gov.uk/collection/cloud>



How can Microsoft 365 Help?

1. Authentication

- Enforce MFA
- Password controls
- Conditional Access Policies

2. Malware & Phishing

- identify and block suspicious emails, links, and attachments before they reach the users' inbox.
- real-time protection against zero-day exploits, Ransomware & Malware

3. Data Protection

- Data Loss Protection Policies - helps prevent data leaks
- Information protection and encryption help prevent unauthorised access, sharing, or modification of sensitive data.
- Sensitivity labels enable the classification of data

4. Secure Access & Sharing

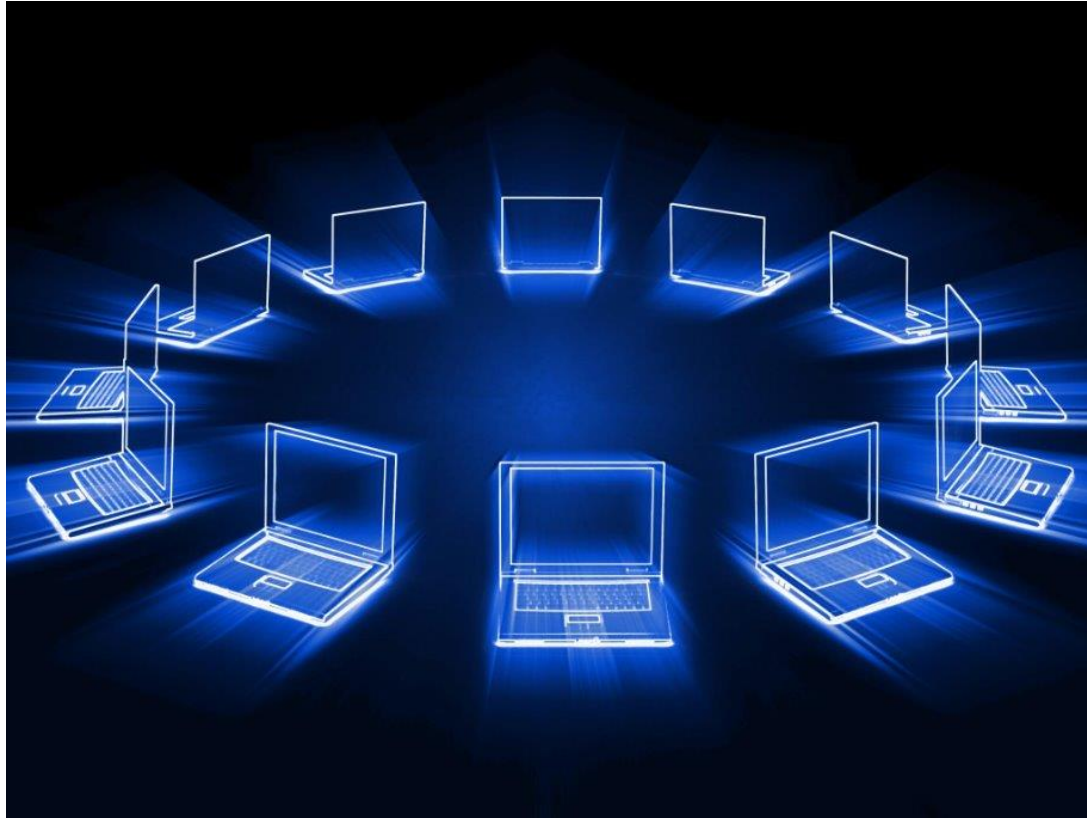
- Secure Sharing of files and collaboration on documents in real-time
- Control who has access to your organization's assets
- Manage and secure devices

5. Monitor & Respond to Threats

- Threat Intelligence - detect and respond to cyber threats in real-time..
- Monitoring tools
- Security and Activity Reports



Windows 10 End of Life: Coming soon to a computer near you!



- ✓ Microsoft will stop supporting Windows 10 on October 14, 2025.
- ✓ If you continue to use Windows 10 after this date, your computer will become more vulnerable to security threats.
- ✓ To stay protected, there is a free upgrade to Windows 11, but you need to check that your computer meets the Windows 11 hardware requirements.



Who is behind cyber attacks?

Online criminals

Are really good at identifying what can be monetised, for example stealing and selling sensitive data, or holding systems and information to ransom.



Foreign governments

Generally interested in accessing really sensitive or valuable information that may give them a strategic or political advantage.

Hackers

Individuals with varying degrees of expertise, often acting in an untargeted way – perhaps to test their own skills or cause disruption for the sake of it.



Political activists

Out to prove a point for political or ideological reasons, perhaps to expose or discredit your organisation's activities.

Terrorists

Interested in spreading propaganda and disruption activities, they generally have less technical capabilities.



Malicious insiders

Use their access to an organisation's data or networks to conduct malicious activity, such as stealing sensitive information to share with competitors.

Honest mistakes

Sometimes staff, with the best of intentions just make a mistake, for example by emailing something sensitive to the wrong email address.



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 malicious 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 smartphones, tablets, laptops or desktop computers that you use can be exploited both remotely and physically, but you can protect them from many common 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 attacker to exploit a device if it is left unlocked, lost or stolen.



Avoid downloading dodgy apps. Only use official app stores (like Google Play or the Apple App Store), which provide some protection from viruses. Don't download apps from unknown vendors and sources.

Use strong passwords

Attackers 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 using 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 attacker 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 two factor authentication (2FA) for important websites like banking and email, if you're given the option. 2FA provides a way of 'double checking' that you really are the person you are claiming to be when you're using online services.

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.



Don't be afraid to challenge policies or processes that make your job difficult. Security that gets in the way of people doing their jobs, doesn't work.



NCSC online training



The image shows a promotional banner for an online training course. On the left, there is a circular logo with 'SU' and the text 'Sponge UK'. The main title 'Cyber Security for small organisations' is written in large, bold, white letters. Below the title is a white button with the text 'START COURSE' and a small downward-pointing chevron icon. The background features a stylized illustration of a woman with dark skin and curly hair, wearing a black top and a gold necklace, looking thoughtfully at a tablet. To the right of the woman, there is a network of icons connected by lines, including a credit card, a USB drive, a shield with a checkmark, a bell, a padlock, and a bug.

SU Sponge UK

Cyber Security for small organisations

START COURSE

[\(See full NCSC Cyber Security for Small Organisations Online Learning offer\)](#)

NCSC's new cyber security training for staff now available

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



<https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available>



Superhighways Cyber Security training

- ✓ Introduction to cyber security basics for everyone (60 min monthly sessions) - 2pm/2nd Tuesday of each Month
 - ✓ Tue 10/12/2024 2 – 3 pm. [Book your space](#)
 - ✓ Tue 14/01/2025 2 – 3 pm. [Book your space](#)
 - ✓ Wed 11/02/2025 2 – 3 pm. [Book your space](#)



Key related policies to check

- ✓ Data protection policy
- ✓ IT Security policy
- ✓ Computer use, email and internet policy







What is this certification?

This is not just to pass or get cyber insurance.

It is a government-backed program to assist the organisation's cyber security protection system hardening to protect themselves against from a common types of cyber attacks.

It also support the clients/end users confident and trust to the organisation in cyber by achieving this certificate.





How is this help to protect?

This help to check the cyber security protection of an organisation/company in the following areas.

Areas	Descriptions
Boundary firewalls and internet gateways	Device(s) between your office network and the internet (blocking harmful or unwanted internet traffic while allowing safe connections)
Secure Configuration	Setting up devices and software to protect against threats
Access Control	Letting the right people/person to see and access the right data/device(s).
Malware Protection	Keeping devices safe from harmful software like virus or spyware, etc,. (Antivirus alone is not enough)
Patch Management	Updating software to fix bugs and keeping it secure from attackers





Certification Levels

There are two levels of certifications;

Cyber Essentials

- This can be done by self-assessment within your organisation or together with your IT service provider.

Cyber Essentials Plus

- You will need to have Cyber Essentials certificate to achieve Plus certificate. Third party will assess your organisations system configurations hardening, according to what has been mentioned in Cyber Essentials. The Plus certificate is issued when passed.

Follow the link for more info of Cyber Essentials: <https://iasme.co.uk/cyber-essentials/>





Certifications

- ✓ Cyber Essentials – an online self assessment verified by a qualified independent assessor
 - ✓ Includes automatic cyber liability insurance for any UK organisation who certifies their whole organisation & have less than £20m annual turnover (terms apply)

Cyber Essentials is priced according to the size of your organisation



0-9 Employees
£320 + VAT

Buy Micro



10-49 Employees
£440 + VAT

Buy Small



50-249 Employees
£500 + VAT

Buy Medium



250+ Employees
£600 + VAT

Buy Large



About Superhighways

Providing tech support to small local charities in London for over 25 years

- ✓ Support
- ✓ [Training](#)
- ✓ Consultancy
- ✓ Digital inclusion
- ✓ [Datawise London](#)
- ✓ [See all services](#)
- ✓ [E-news sign up](#)





Thank you for listening

SUPERHIGHWAYS TECH TEAM

colincregan@superhighways.org.uk

ninehtet@superhighways.org.uk

paulfirby@superhighways.org.uk

@SuperhighwaysUK

#Superhighways

