



superhighways

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

Cyber Security for small charities

ChanceUK team session

What we'll cover today

- ✓ What is a cyber attack
- ✓ Why are you at risk
- ✓ 5 quick, simple, free or low cost steps
- ✓ Other useful sources of information

What is a cyber attack?

Malicious attempts to:

- ✓ Damage
- ✓ Disrupt
- ✓ Or gain unauthorised access

...to computer systems, IT networks or devices (such as laptops, phones and tablets)

Case study & task:

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

How might a cyber criminal take advantage and attack the charity?



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



Cyber vulnerabilities

- ✓ Volunteers / trustees using personal devices
- ✓ Regular home & remote working – personal broadband routers, unsecured internet in cafes etc
- ✓ Staff, volunteers, trustees, clients – 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?

Non cyber vulnerabilities

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

Some context about Cyber Attacks

Question:

In the annual DCMS survey 2022, what percentage of charities (n=424) reported having a cyber security breach in the last 12 months?

26% 30% 62% 76%



Cyber Security Breaches Survey 2022

Updated 11 July 2022

Which of the following breaches or attacks has your organisation identified in the last 12 months?	Businesses	Charities
Phishing attacks	83%	87%
Other impersonating organisation in emails or online	27%	26%
Viruses, spyware or malware (excluding ransomware)	12%	11%
Denial of service attacks	10%	2%
Hacking or attempted hacking of online bank accounts	8%	6%
Takeover of organisation's or users' accounts	8%	6%
Ransomware	4%	4%
Unauthorised accessing of files or networks by outsiders	2%	2%

[Visit the full report](#)



Data protection – GDPR principles

1. Process lawfully, fairly and in a transparent manner
2. Collect for specified, explicit and legitimate purposes
3. Only keep what is adequate, relevant and limited to what is necessary
4. Store accurate information and keep up to date
5. Retain only for as long as necessary
6. Process in an appropriate manner to maintain security



ICO Data security incident trends - 2021/22

1,411

Incidents Reported

Non-Cyber

1,019

Incidents Reported

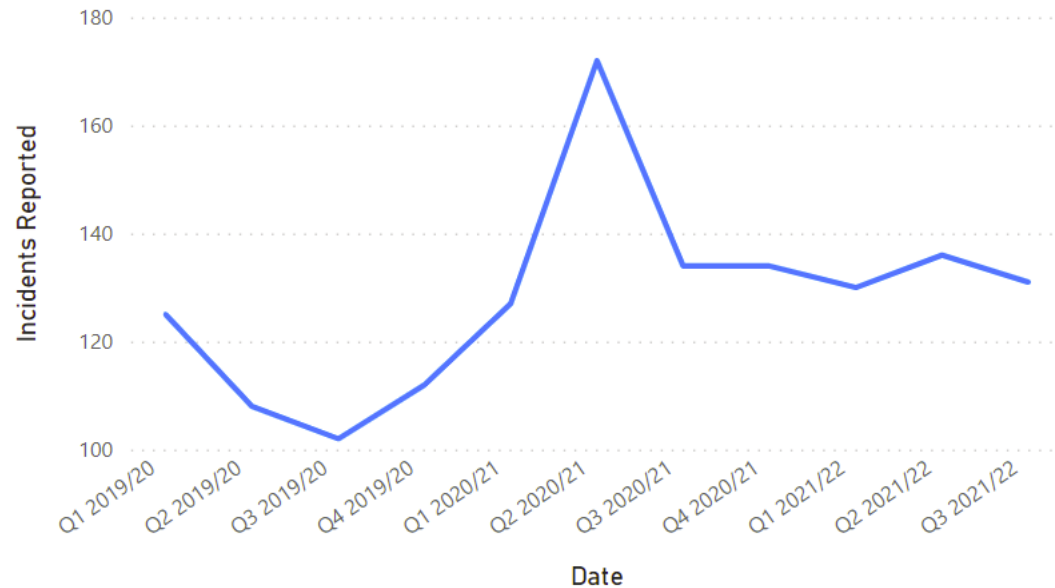
Cyber

392

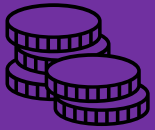
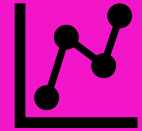

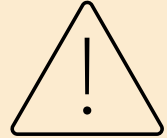


Incidents Reported

Number of reported cyber security incidents in 2021/22 – Charity & voluntary sector

Incidents Reported



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> 

Who are charities at risk from?



▼
Cyber
criminals

- Usually for financial gain
- Ransomware attacks on charities
- Can steal money by other means



▼
Nation
States

- No evidence of direct targeting
- Wannacry affected NHS and Schools
- Untargeted threats/opportunists



▼
Insider

- By staff or employees accidental or on purpose
- Overwhelmingly accidental
- Net result the same

How are charities being attacked?

➤ Ransomware

A type of malware that makes data or systems unusable until the victim makes a payment.

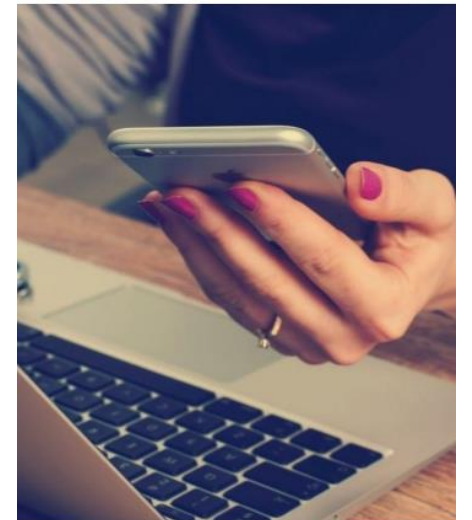
➤ Malware and Spyware

Malicious software that is designed to interfere with a computer's normal functioning and that can be used to obtain information and commit cybercrimes.

➤ Business email attacks (phishing)

Scam emails sent to people asking for sensitive information (such as bank details) or encouraging them to visit a fake website

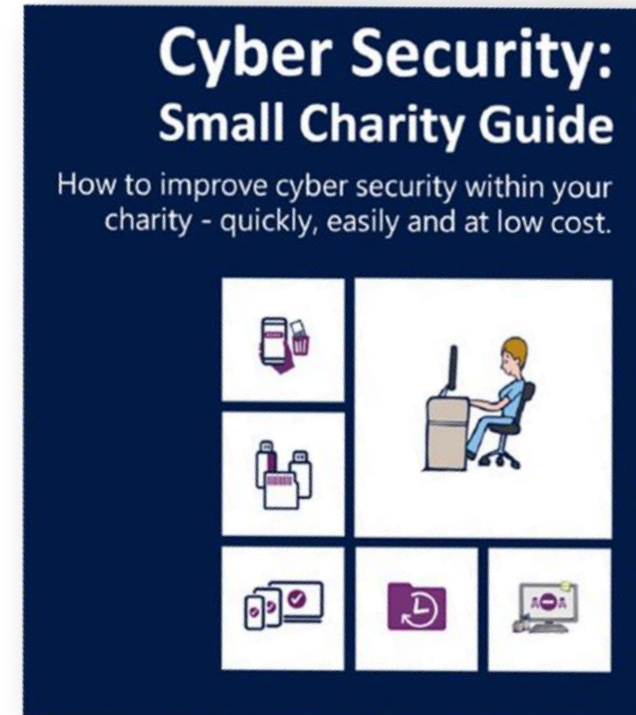
➤ Fake organisations and websites



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

1. Identify what you need to back up
2. Keep your back up separate
3. Consider the cloud
4. Make it part of your everyday routine

Protecting against 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



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



Keeping your devices secure

1. Switch on password protection
2. Prepare for lost or stolen devices
3. Keep your device up to date
4. Keep your apps up to date
5. Use public Wi-Fi safely

Passwords: protecting accounts & devices

- ✓ Emails
- ✓ Files
- ✓ Databases / CRMs
- ✓ Websites
- ✓ Social Media
- ✓ And more!

- ✓ Phones
- ✓ Tablets
- ✓ PCs & laptops

But also

- ✓ Firewalls
- ✓ Routers
- ✓ Servers



Poll

✓ How long does it take to crack these passwords?

✓ QwErTy987123! 15 seconds

✓ CoffeeTinyFish 6 hours

✓ CoffeeTinyFish#9 6 days





[Two Factor Authentication \(captioned\) Explained by Common Craft \(VIDEO\)](#)



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.



Here's an example from today!

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*

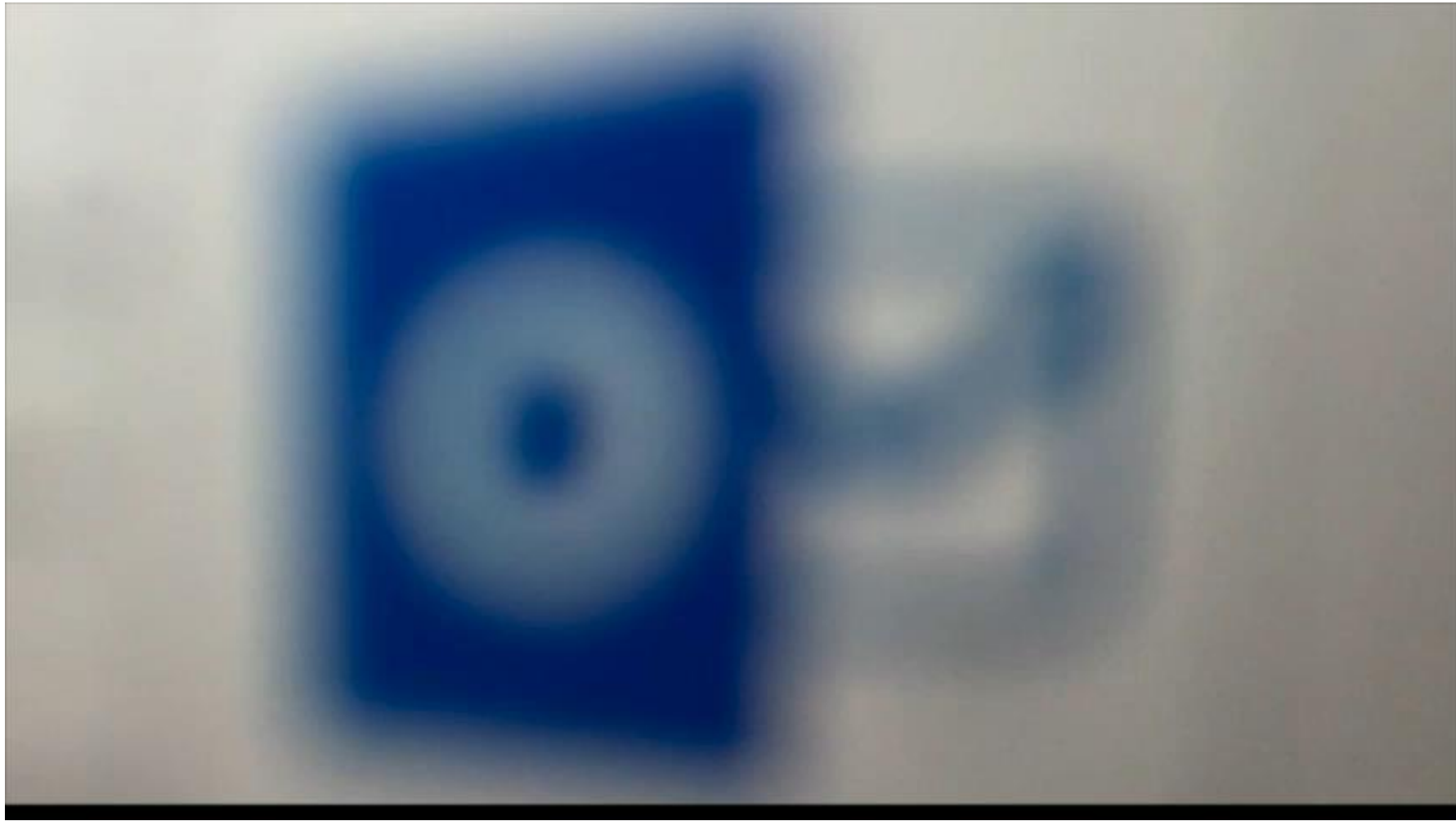
Document Shared: *INVOICE_Due28736.PDF*

Document Size: *[672 KB]*

Download Invoice

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





<https://youtu.be/TFICLREWxfU>

NCSC's 5 tips to avoid phishing scams

1. Configure accounts appropriately to reduce the impact of successful attacks
2. Think about how you operate
3. Know the obvious signs of phishing
4. Report all attacks
5. Check your digital footprint



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.



What can people see about me online?



https://youtu.be/_YRs28yBYuI

[See NCSC guidance on using social media safely](#)

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 (see next slide)
 - ✓ Charity Commission – where there's been a serious incident
 - ✓ Information Commissioners Office – where this has led to a data breach



Action Fraud



- ✓ Visit the [Report phishing web page](#)
- ✓ Forward any email you're not sure about to the Suspicious Email Reporting Service (SERS) at report@phishing.gov.uk
- ✓ The NCSC will investigate and may:
 - ✓ Block the address the email came from so it can no longer send emails
 - ✓ Work with hosting companies to remove links to malicious websites
 - ✓ Raise awareness of commonly reported suspicious emails and methods used (via partners)



- An independently verified self-assessment.
 - Organisations assess themselves against five basic security controls and a qualified assessor verifies the information provided.
 - All the self assessment questions are available to download for free in advance.
 - Cyber Essentials certification includes automatic cyber liability insurance for any UK organisation who certifies their whole organisation and have less than £20m annual turnover (terms apply).

<https://iasme.co.uk/cyber-essentials/>



Stay Safe Online

Top tips for staff

Regardless of the size or type of organisation you work for, it's important to understand why you might be vulnerable to cyber attack, and how to defend yourself. The advice summarised below is applicable to your working life and your home life. You should also familiarise yourself with any cyber security policies and practices that your organisation has already put in place.

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.



© Crown Copyright 2018

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'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>



NCSC online training



The image shows a promotional banner for an online training course. On the left, there is a teal circle with the letters 'SU' and the text 'Sponge UK' next to it. Below this, the title 'Cyber Security for small organisations' is written in large, bold, white font. Underneath 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 yellow necklace, looking thoughtful with her hand on her chin. To the right of the woman, there are several grey icons connected by lines, representing various cybersecurity concepts: a credit card, a USB drive with a warning sign, a shield with a checkmark, a bell with a notification icon, a padlock, and a bug.

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



About Superhighways

Providing tech support to small local charities in London for over 20 years

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





Thank you for listening

KATE WHITE & COLIN CREGAN

info@superhighways.org.uk

@SuperhighwaysUK

#DigitalFoundations