National Cyber Security Centre

Cyber Security for Small Charities

Richmond CVS

superhighways
harnessing technology for community benefit

Background

- The National Cyber Security Centre (NCSC), created in Oct 2016, is the UK authority on cyber security and a part of GCHQ
- The NCSC's mission to "make the UK the safest place to live and work online"
- This awareness session has been developed jointly by The NCSC, The National Association for Voluntary and Community Action (NAVCA) and a number of CVS' who are committed to helping charities protect themselves from cyber crime.

What we'll cover today

- What is a cyber attack
- What is cyber security
- Why are charities at risk
- Attack the charity!
- 5 quick, simple, free or low cost steps
  - Backing up your data
  - Protecting against malware
  - Securing your mobile devices
  - Password best practice
  - Avoid phishing attacks
- Other useful sources of information

What is a cyber attack?

- **Malicious attempts to:**
  - Damage
  - Disrupt
  - Or gain unauthorised access

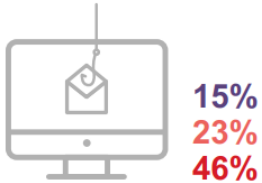
- **…to computer systems, IT networks or devices (such as laptops, phones and tablets)**

What is ‘cyber security’?

- Reducing risk of becoming a victim of a cyber attack
- Protection of devices, services, networks and the information we store on them
- The internet is a fundamental part of modern life, and so cyber security must be too.

The cost of cyber attacks – Cyber Security Breaches Survey 2019 (DCMS)

£9,470
is the average annual cost for **all charities** that lost data or assets after breaches



15%
23%
46%
of charities in each income band had phishing emails

2%
6%
18%
had viruses or other malware, including ransomware

2%
5%
22%
had others impersonating them in emails or online

[See 2021 report here]

CYBER SECURITY BREACHES SURVEY 2021

UK CHARITY TRENDS

The Cyber Security Breaches Survey is an official statistic. Since 2016, it has measured how UK organisations approach cyber security, and the impact of breaches and attacks. This infographic shows the key findings for charities, which were first included in the 2018 survey.

1.

Despite COVID-19, cyber security remains a priority for charity boards. 68% of charities say that cyber security is a high priority for their trustees or senior managers (vs. 53% in 2018).

2.

Phishing is the most commonly identified cyber attack. Among the 26% identifying any breaches or attacks, 79% had phishing attacks, 23% were impersonated and 17% had malware (including ransomware).

3.

Unprepared staff risk being caught unaware. A total of 18% of charities train staff on cyber security and 14% have tested their staff response, for example with mock phishing exercises.

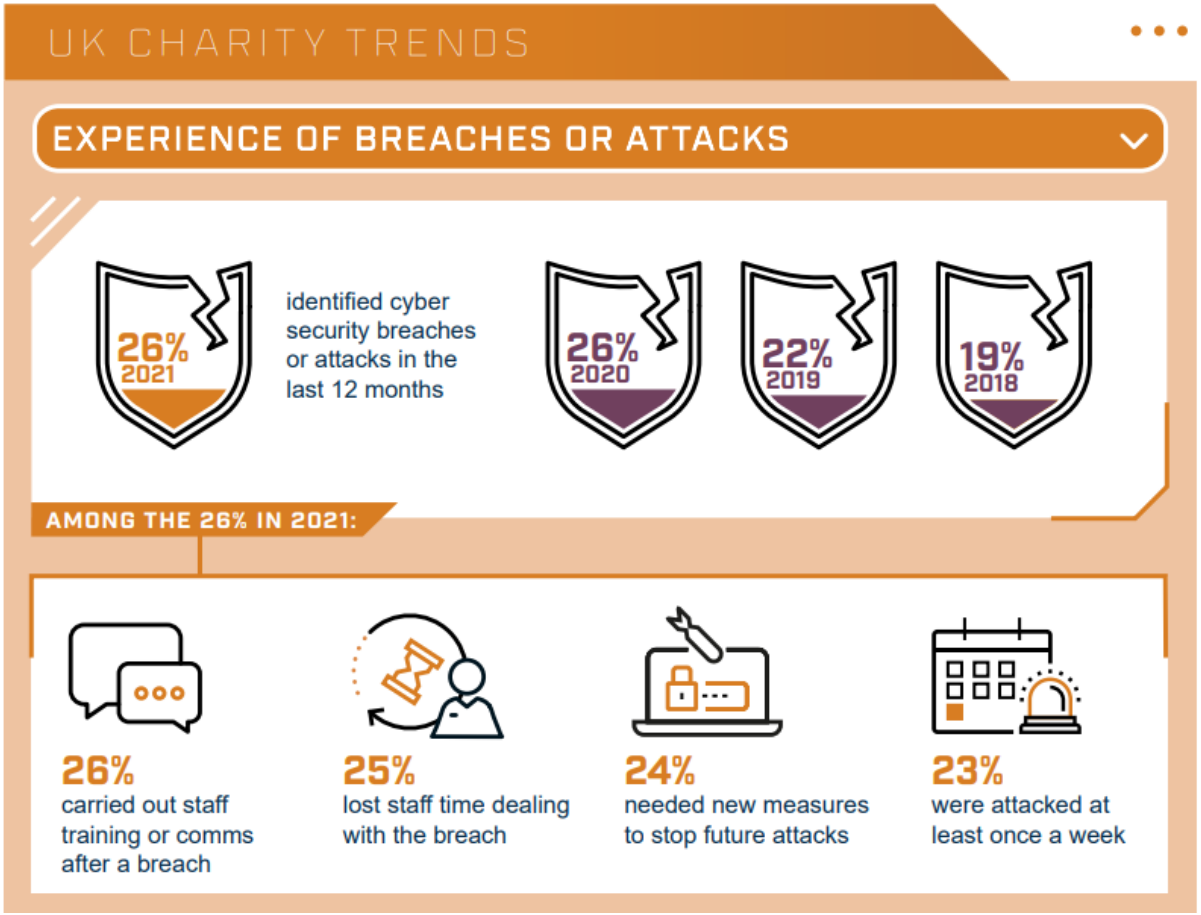
4.

COVID-19 has made cyber security harder. With resources stretched, fewer charities report having up-to-date malware protection (69%, vs. 78% in 2020) and network firewalls (57%, vs. 72% in 2020).

5.

There is room for improvement when it comes to suppliers and partners. In total, 8% of charities have reviewed cyber risks posed by their suppliers or partners (e.g. local organisations they work with).

[Download the survey summary infographic]



DEALING WITH COVID-19

67%
have staff using personal devices for work

23%
cover use of personal devices for work in a cyber security policy

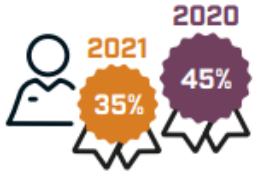
23%
cover home working in a cyber security policy

20%
have a VPN for remote working

27%
have a business continuity plan that covers cyber security

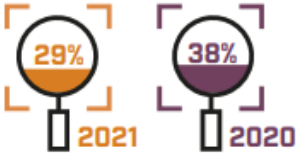
MANAGING RISKS

35%
have trustees or senior managers with a cyber security brief **(down from 2020)**



32%
have done a cyber risk assessment

29%
monitor user activity **(down from 2020)**



29%
have cyber insurance cover

Why are charities at risk?

- **Charities hold funds, personal, financial and commercial data**
- **Potentially a route into a 'bigger fish' such as a local authority or corporation**
- **Very low levels of awareness, particularly amongst smaller charities**
- **Culture of trust**

Who are charities at risk from?

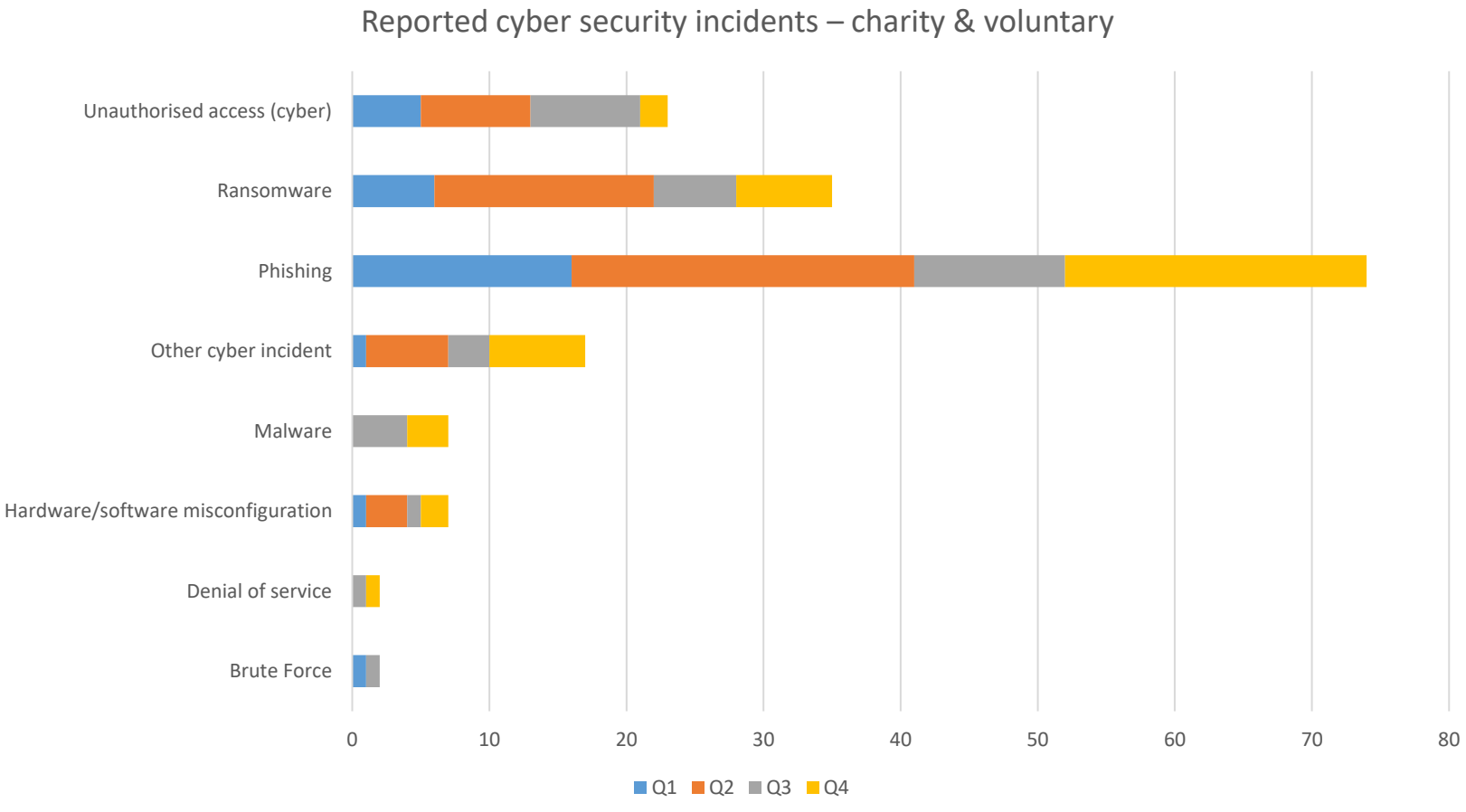
- **Cyber criminals**
  - Motivated by money
- **Indirect attacks**
- **Insiders**
  - And the inadvertent insider
- **Others but less likely for most charities**
  - Hacktivists
  - Terrorists
  - Nation states

I'm pretty alert to scammers, I think I'm safe… https://youtu.be/lc7scxvKQOo

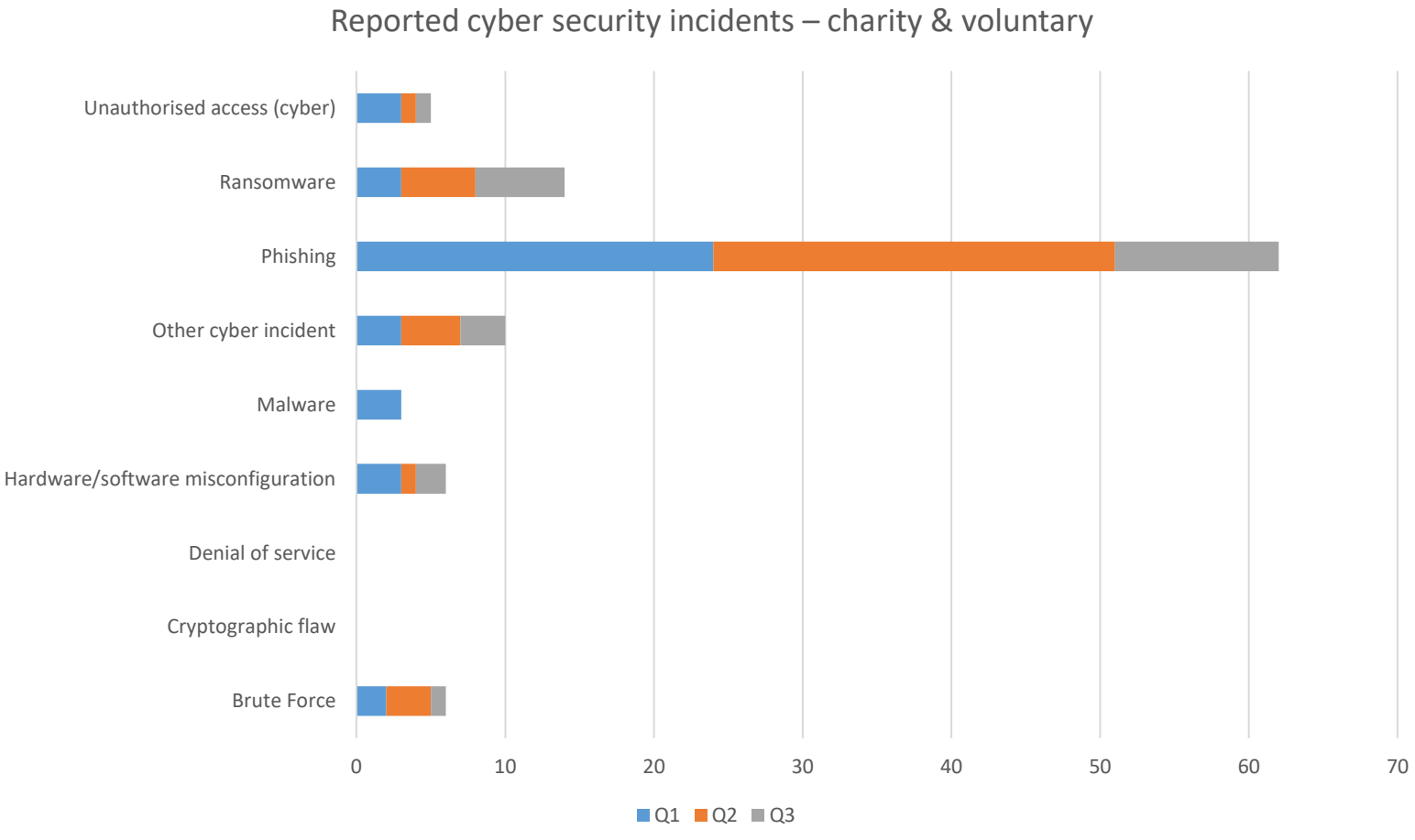
How are charities being attacked?

- **Ransomware and extortion**
- **Malware and Spyware**
- **Business email attacks (phishing)**
- **Fake organisations and websites**

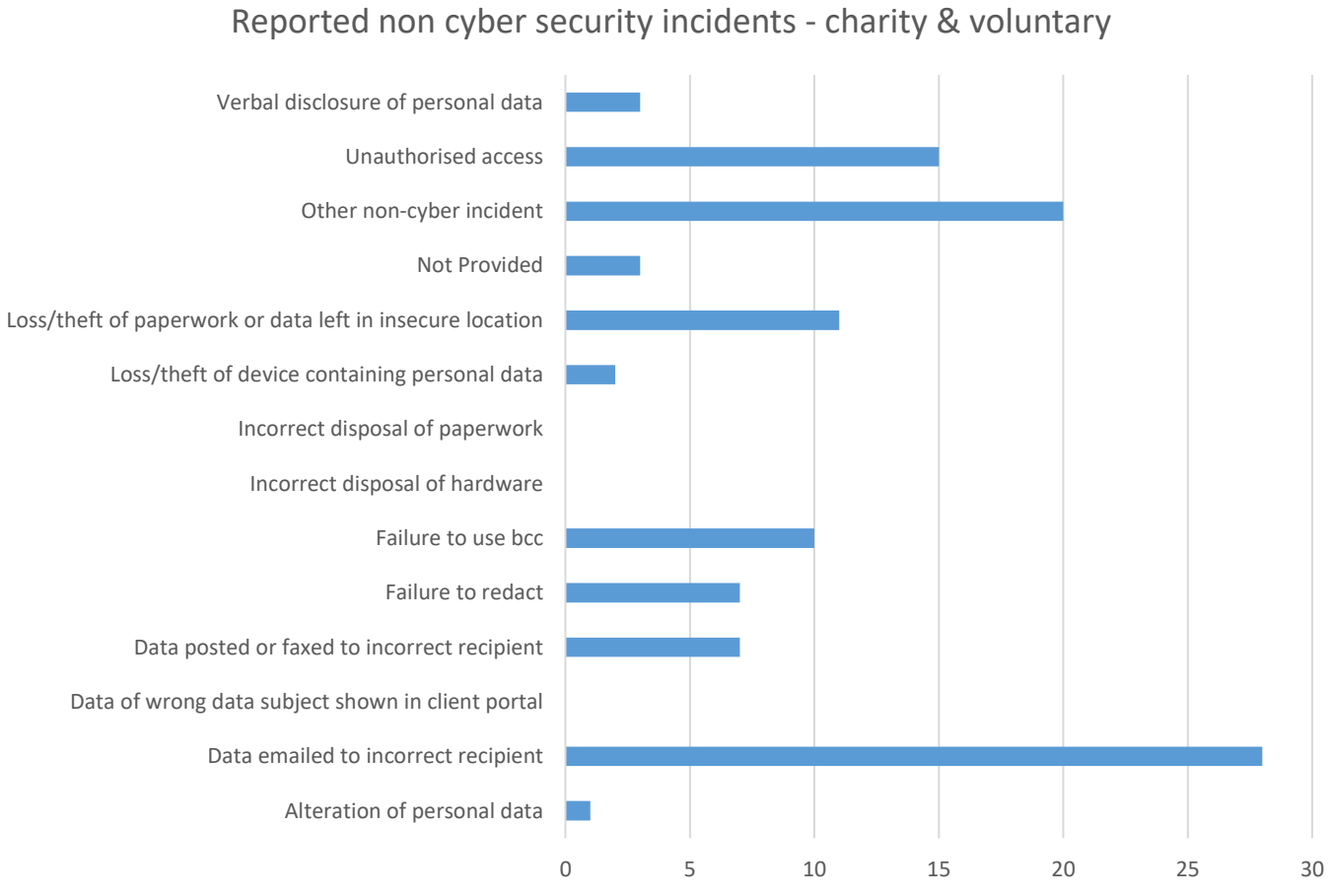
ICO Data security incident trends – 2020/21



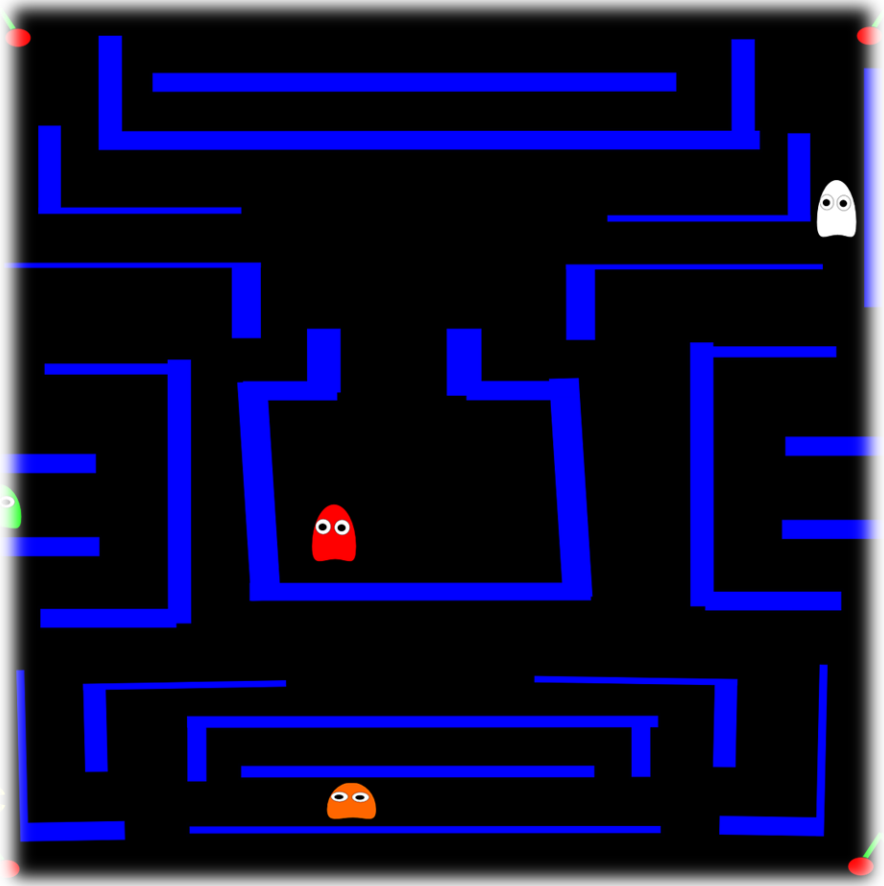
ICO Data security incident trends – 2021/22



ICO Data security incident trends – Q3 2021/22



It’s time to attack your charity…



https://youtu.be/CbETCJ8Yc-U

Cyber vulnerabilities

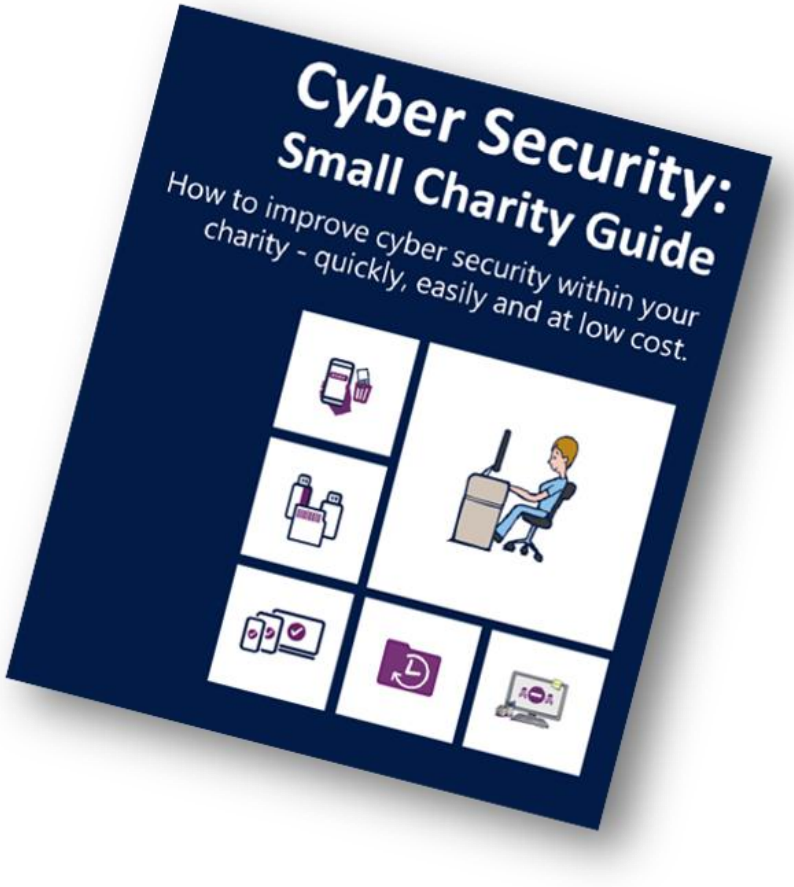
1. Volunteers / trustees using personal devices
2. Regular home & remote working – personal broadband routers
3. Staff, volunteers, trustees, clients – low levels of digital savviness
4. Staff not logging out of the House or Training room PCs
5. Publicly available info via website & social media accounts
6. Phishing - financial fraud (exploiting part time hours of financial manager), route to Local authority / other funders?

Non cyber vulnerabilities

1. Multi use office – PCs / laptops stolen
2. Outreach working – mobile devices lost or stolen
3. Confidential data viewable on office screens

What can you do to protect your charity?

- **5 quick, simple, free or low cost steps**
- **Download the full guide from https://www.ncsc.gov.uk/collection/charity**
- **There's also an infographic you can download here**



Quick Break Time!

Backing up your data

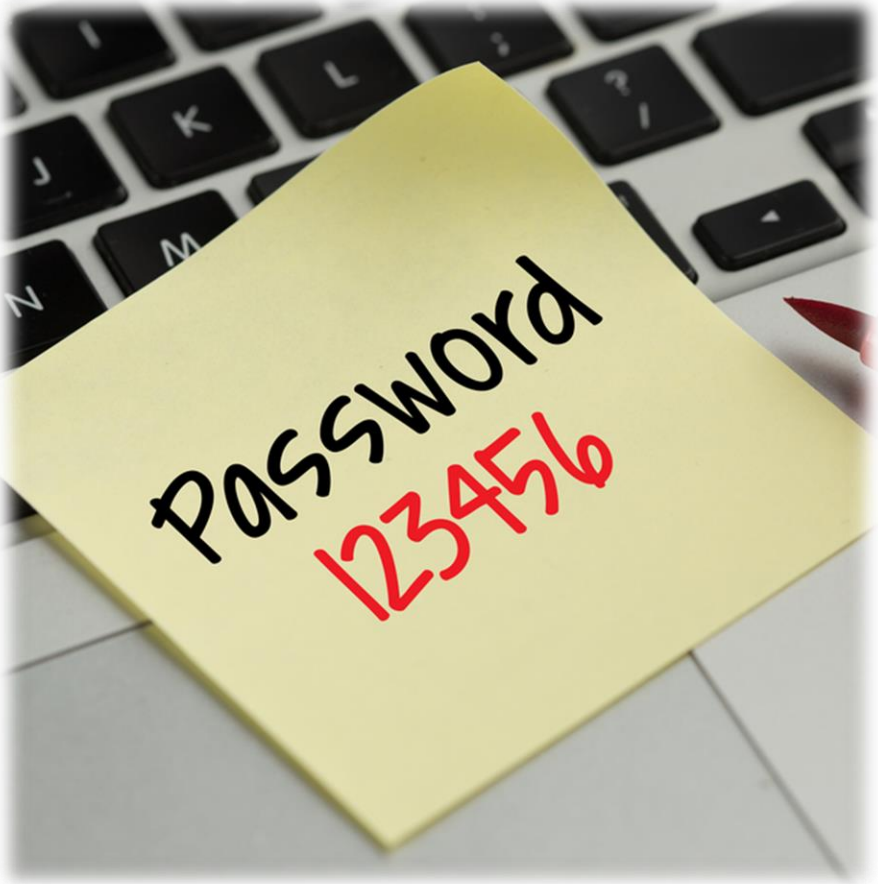
- **Identify what you need to back up**
- **Keep your back up separate**
- **Consider the cloud**
- **Make it part of your everyday routine**

Protecting your charity from malware

- **Antivirus software**
- **Prevent users from downloading 'dodgy apps'**
- **Keep everything up to date**
- **Control the use of USB drives**
- **Switch on your firewall**

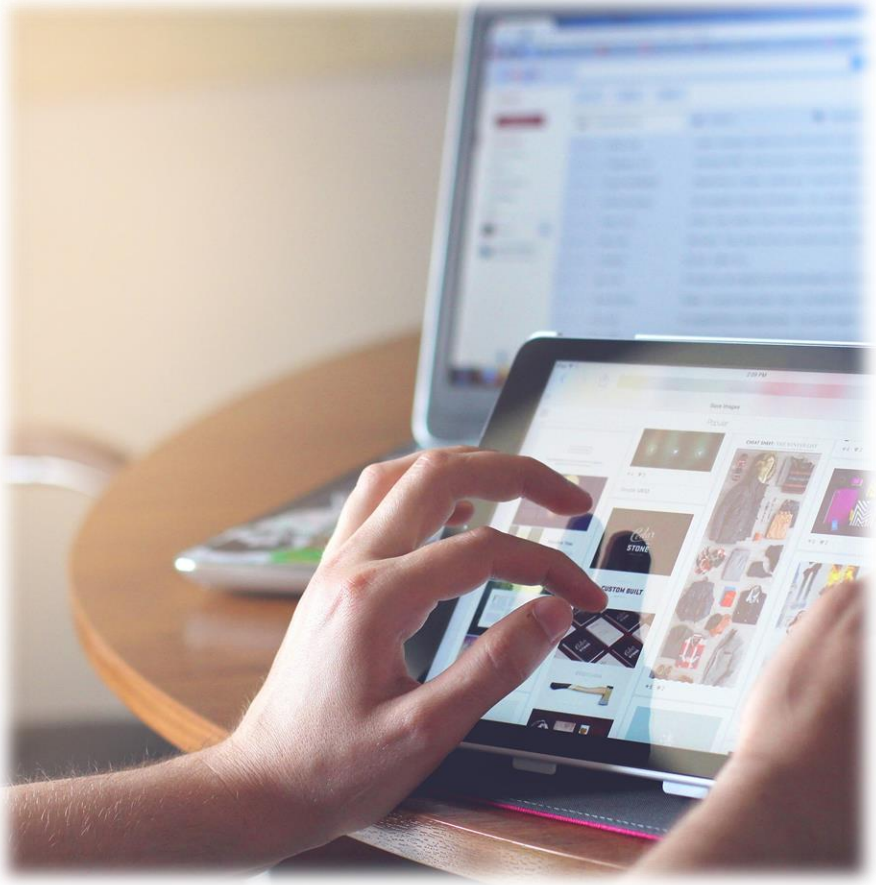
Using passwords

- **Switch on password protection**
- **Use two factor authentication**
- **Avoid predictable passwords** (What is your password video)
- **How long to crack these three passwords?**
  - QwErTy987123! – 15 seconds
  - CoffeeTinyFish – 6 hours
  - CoffeeTinyFish#9 – 6 days
  - 3 random words
- **Help users cope with 'password overload'**
  - See guidance on password managers
- **Change all default passwords**



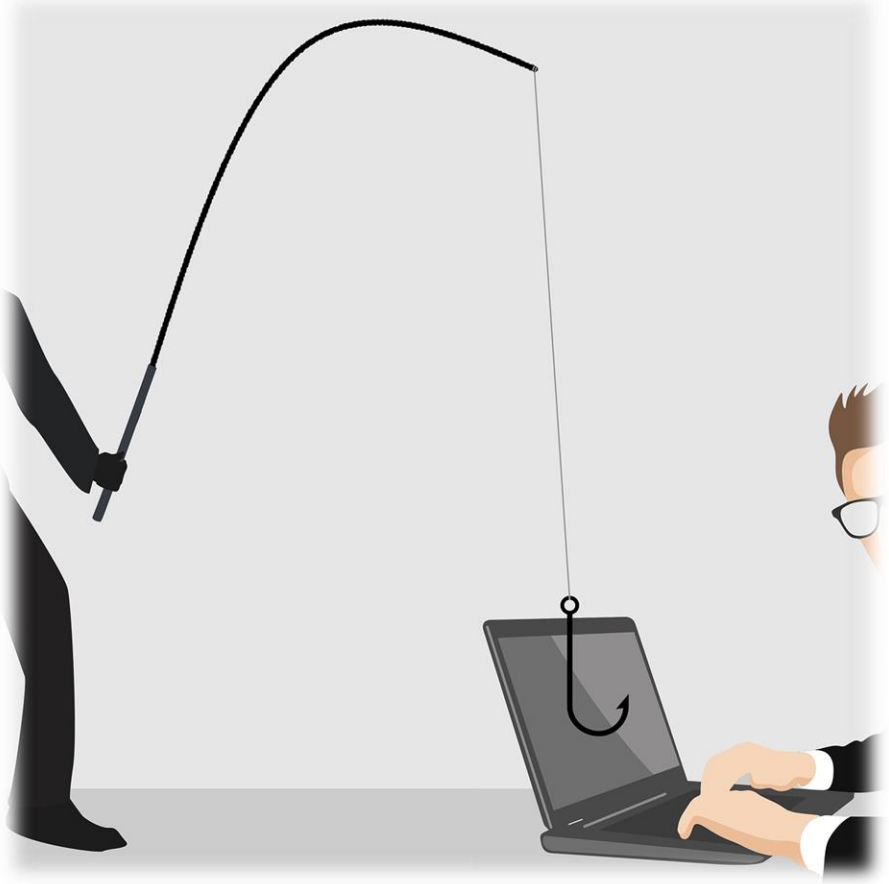
Keeping your smartphones / tablets safe

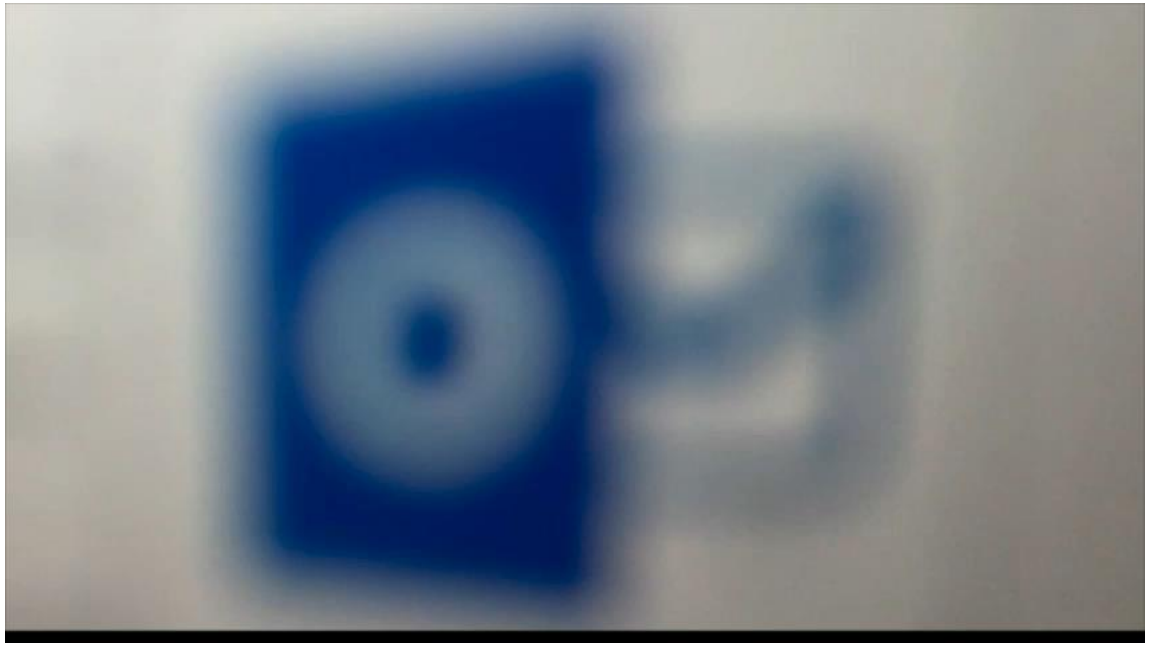
- **Switch on password protection**
- **Prepare for lost or stolen devices**
- **Keep your device up to date**
- **Keep your apps up to date**
- **Use public Wi-Fi safely**



Avoiding phishing attacks

- **Configure accounts appropriately**
- **Think about how you operate**
- **Know the obvious signs of phishing**
- **Check your digital footprint**
- **Report all attacks**





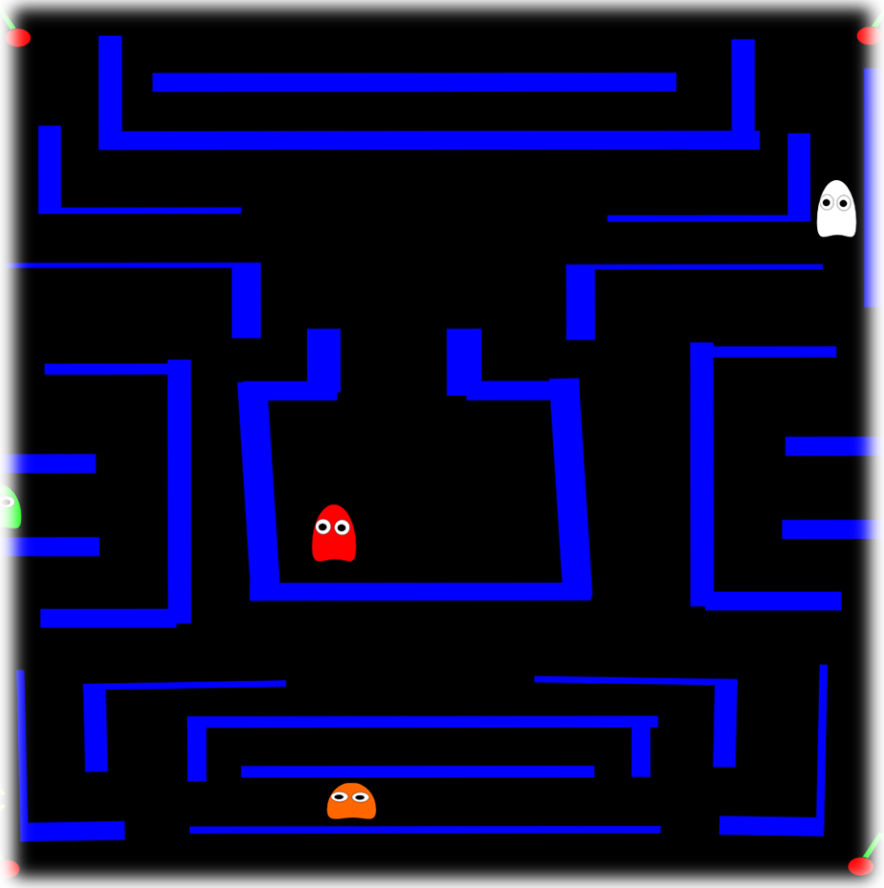
https://youtu.be/TFlCLREWxfU

How much about me can people see online?

https://youtu.be/_YRs28yBYuI

See NCSC guidance on using social media safely

It’s time to defend your charity…



Cyber vulnerabilities

1. Volunteers / trustees using personal devices
2. Regular home & remote working – personal broadband routers
3. Staff, volunteers, trustees, clients – low levels of digital savviness
4. Staff not logging out of the House or Training room PCs
5. Publicly available info via website & social media accounts
6. Phishing - financial fraud (exploiting part time hours of financial manager), route to Local authority / other funders?

Non cyber vulnerabilities

1. Multi use office – PCs / laptops stolen
2. Outreach working – mobile devices lost or stolen
3. Confidential data viewable on office screens

What to do if you fall victim

1. **Action Fraud**
   - Police Scotland if appropriate
2. **ICO Breach Notification**
   - Always within 72 hours
3. **Charity Commission**
   - Reporting a Serious Incident (RSI)
4. **Other Regulators/Funders**
   - If applicable

Discounted security products catalogue

Cyber Essentials

- Government backed scheme - https://www.cyberessentials.ncsc.gov.uk
- Cyber Essentials – an online self assessment questionnaire (see also the Get ready tool)

Pricing Structure	CYBER ESSENTIALS	
Micro Organisations	0-9 Employees	£300 +VAT
Small Organisations	10-49 Employees	£400 +VAT
Medium Organisations	50-249 Employees	£450 +VAT
Large Organisations	250+ Employees	£500 +VAT

- Cyber Essentials Plus – includes an external audit, price on application

National Cyber Security Centre

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.

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.

www.ncsc.gov.uk @ncsc National Cyber Security Centre

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

Thank you!

- **Any questions?**

- **More information**
  - www.ncsc.gov.uk/charity
  - Superhighways summary blog post

- **Get in touch**
  - **katewhite@superhighways.org.uk**
  - **colincregan@superhighways.org.uk**