superhighways
harnessing technology for community benefit

Cyber Security in 60 mins

Part 5: Securing mobile devices

#DigitalFoundations

Some context about Cyber Attacks

Question:

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

26% 30% 62% 76%

Official Statistics

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

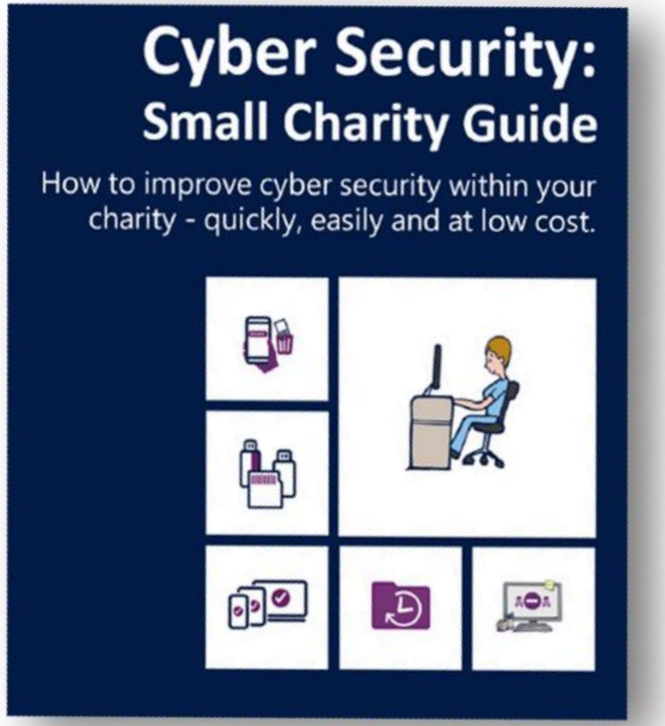
Data protection – GDPR principles

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

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. Securing your mobile devices
4. Password best practice
5. Avoid phishing attacks



Download the full guide

Download the infographic

Mobile devices – what do you use?

- ✓Laptops
- ✓Desktop PCs
- ✓Smartphones
- ✓Tablets

- ✓Organisational devices
- ✓Personal devices

Mobile safety and security

[Mobile Safety and Security (captioned) Explained by Common Craft (VIDEO)]

Discussion

- ✓ How do you protect your smartphone or mobile device?
- ✓ How could you improve upon the actions you take already?
- ✓ If you connect to unsecured wifi in a public place, you may connect to a criminal's computer and give the criminal remote access to your device?
  - ✓ True or False?
- ✓ Which of the following actions would not help you protect your mobile device?
  a) Keep the software up to date
  b) Back up your device consistently
  c) Ignore the privacy policies of the apps and websites you use
  d) Turn off location services on apps

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

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 65 account. But it can't be use to sign on another device. (See Why a PIN is better than a password)
- Check out our Bitesize 1 session – Passwords and multi factor authentication for further info on best practice

Configure tracking on your devices

- Configure devices so that when lost or stolen they can be tracked, remotely wiped or remotely locked
  - For Android devices – find out how you can find, lock or erase here
  - For Apple devices – learn how to use the Find My service
- Remember if you are using cloud solutions e.g. Office 365 or Google Workspace – you'll have options to:
  - sign users out of devices
  - reset passwords / block future sign ins

Keep devices up to date

- Keep your devices (and all installed apps) up to date
- Don't ignore any update reminders!
- This protects against identified vulnerabilities and is needed for mobile devices as well as laptops & desktops
- Use 'automatic update' options where available – see further guidance from NCSC here
- Be aware of software 'end of life' e.g. Windows & Office suites, where security updates are no longer provided

Avoid using public Wi-Fi hotspots

- When sending sensitive data, don't connect to public Wi-Fi hotspots
- Instead use 3G or 4G connections (including tethering or hotspotting to your phone and wireless dongles) or use VPN's
- Read our Using public Wi-Fi securely guide

Tethering / hotspotting to your phone

This is when you connect your laptop to your phone to access Internet data either via a cable – '**tethering**' or through Wi-Fi - '**mobile hotspot**'.

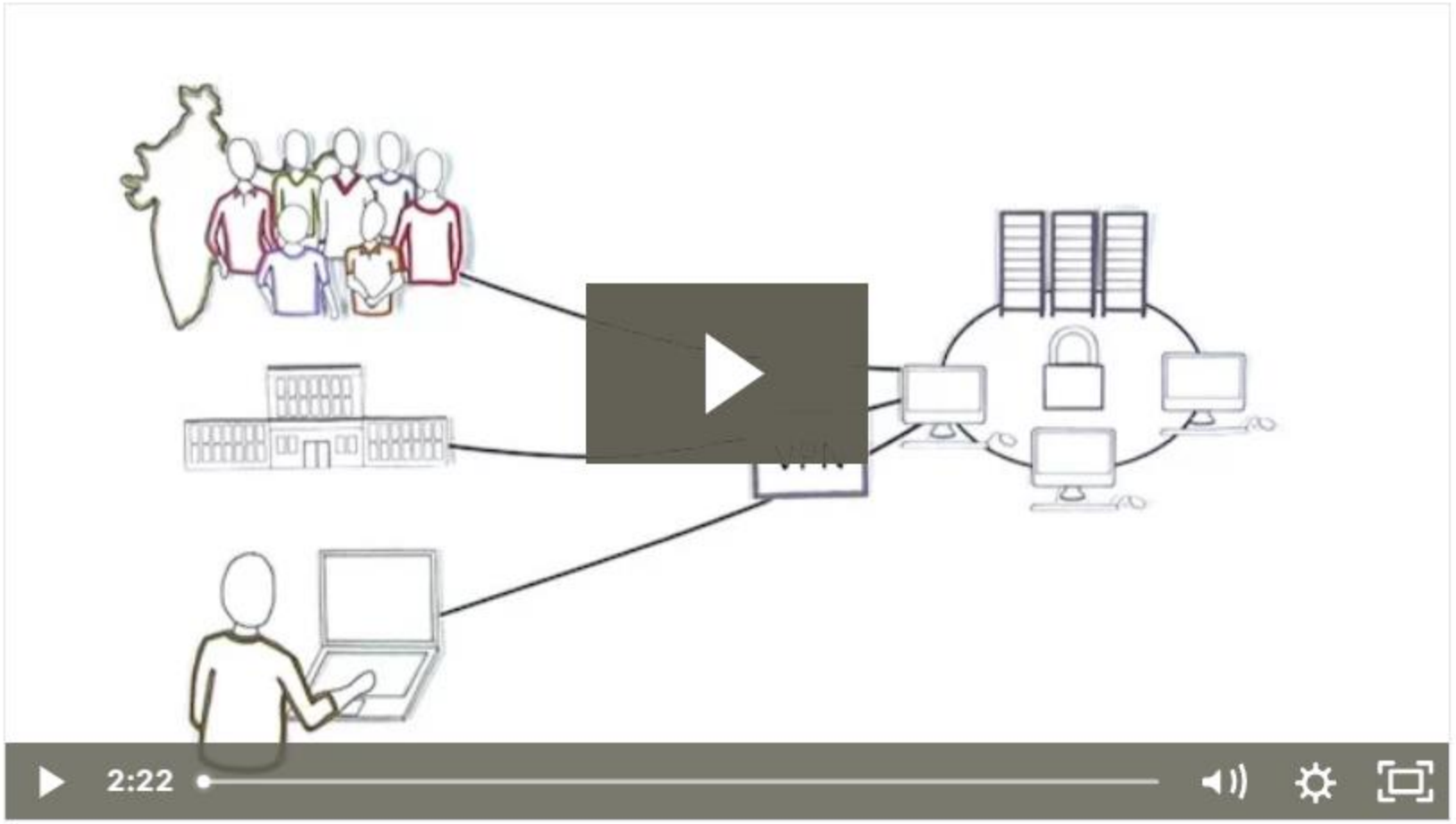
To points to bear in mind:

- ✓Both will use the data included with your phone package, so could potentially result in an additional charge for extra data used
- ✓Both use a lot of power so can quickly drain your mobile battery - it's a good idea to have a charging cable with you just in case

Haven't done this before?

- ✓Instructions for android
- ✓Instructions for iphone / ipad

Virtual Private Networks (VPNs)



[Virtual Private Networks (captioned) Explained by Common Craft (VIDEO)]

Discussion

- ✓Why do some companies limit employee access to the company network to headquarters?
- ✓What is a Virtual Private Network (VPN)?
- ✓What is encrypted information?

Replace older devices

- Replace older devices as these more vulnerable to cyber attacks
- Cyber Essentials accreditation relies on confirmation that older devices using End of Life (EOL) operating systems that are out of regular support are not being used
  - These include Windows XP/Vista/Server 2003/Server 2012(as of Oct 2023), Mac OS Mojave, iOS 12, iOS 13, Android 8

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.

https://www.ncsc.gov.uk/collection/device-security-guidance

Mobile Device Management

- ✓See NCSC blog - https://www.ncsc.gov.uk/blog-post/ncsc-it-mdm-products-which-one-best-1
- ✓Contact us to discuss further!

Action planning – questions to ask

1. What devices are staff, trustees & volunteers using to access organisational systems and data – do you have a record?
2. Are they protected with PINS / passwords / biometrics?
3. Are they still supported with updates (or are they too old)?
4. Do you have a policy re using public Wi-Fi?
5. Can you track lost or stolen devices and block / remove data

Keeping your devices secure

[Keeping your devices secure](#) (online learning)

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

Digital Foundations programme

There are many ways we can help small community organisations make sound choices about the digital tools and technology they use.

Communications made easy

Raise your profile using digital tools to engage supporters and fund your future

Read more »

Digital basics

Work and collaborate online using free and affordable digital tools and technology

Read more »

Websites for communities

Put your website at the heart of your charity or community organisation's story

Read more »

[Find out more about the Digital Foundations programme]

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

info@superhighways.org.uk
@SuperhighwaysUK

#DigitalFoundations