superhighways
harnessing technology for community benefit

Cyber Security in 60 mins

Part 3: Malware - viruses, spyware and more...

#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

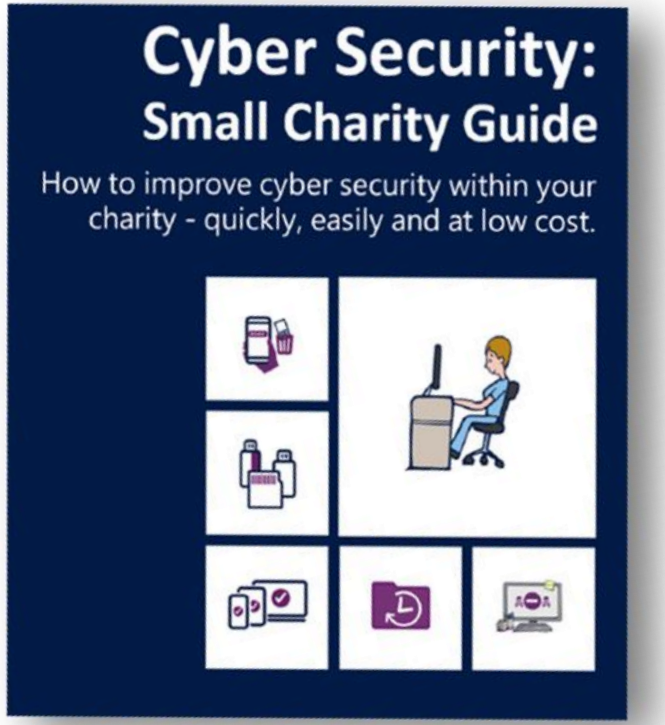
Which of the following breaches or attacks has your organisation identified in the last 12 months?	Businesses	Charities
Phishing attacks	83%	87%
Other impersonating organisation in emails or online	27%	26%
Viruses, spyware or malware (excluding ransomware)	12%	11%
Denial of service attacks	10%	2%
Hacking 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

How 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

What is Malware (& 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.

- ✓**Ransomware** - a type of malware that makes data or systems unusable until the victim makes a payment


3:13

Discussion

- ✓What negative consequences might arise if your PC contracts malware?

- ✓What's the best defence against viruses?
  - ✓Antivirus software to prevent viruses from entering your computer and to remove them if they are found.
  - ✓Avoid opening untrusted attachments or downloadable files

- ✓What's the best defence against worms?
  - ✓Keep your computer software up to date

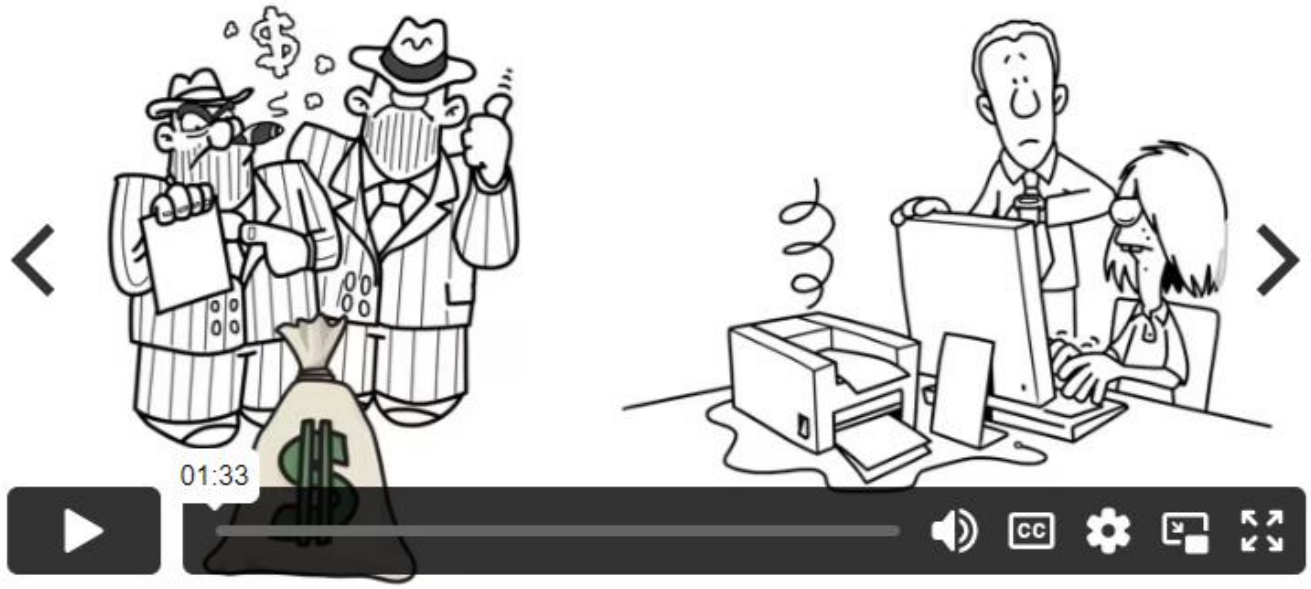
- ✓How do you avoid trojans?
  - ✓Download software from only trusted sites. Avoid clicking on links from untrusted sites

What is Ransomware?

STEP 4

Prevent Phishing and Malware

Every year many small organizations fall victim to costly malware and phishing attacks, and it can be difficult to survive. These attacks can infect your systems resulting in revenue loss, expensive recovery costs, data loss, damage to reputation and more.



Donated by [Wizer Security Awareness Training]

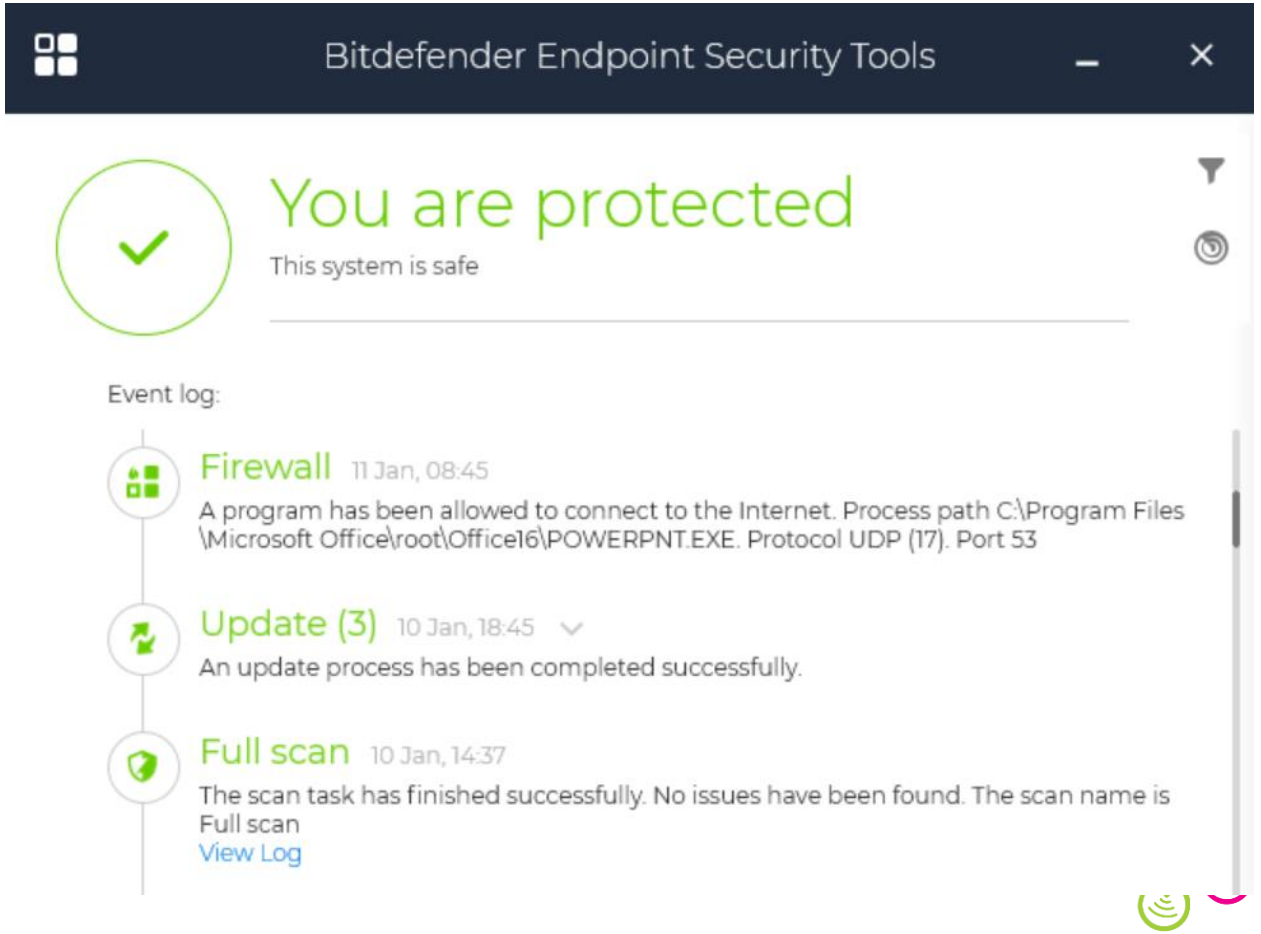
[GCA cyber security toolkit for small business]

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

Use antivirus software

- ✓Install antivirus software on all desktops and laptops
- ✓Ensure automatic updates, scans & full scans are switched on
- ✓Remind staff to check alerts and report if issues flagged
- ✓See NCSC advice on mobile devices



Antivirus options

- ✓Free or paid options – better to go with paid options (watch out for personal use vs organisational/business use criteria)

CHARITY DIGITAL

- ✓Security products catalogue with discounts for registered charities including Bitdefender, Avast & Norton
- ✓Alternatively purchase via e.g. Amazon
- ✓Check pricing at point of renewal – it may be cheaper to rebuy the product

Keep everything up to date

- ✓Patch all software and firmware by promptly applying the latest software updates (don't ignore these!)provided by manufacturers and vendors
- ✓This protects against identified vulnerabilities and is needed for PCs & laptops as well as mobile devices
- ✓Use 'automatic update' options where available.
- ✓Be aware of software 'end of life' e.g. Windows & Office suites, where security updates are no longer provided

Control software installation

- ✓Only install approved software on tablets and smartphones from your relevant app stores
- ✓Stop users from downloading third party apps from unknown sources
- ✓Prevent users from routinely logging on with administrative privileges (limits potential damage malware can carry out)

Control removable media

- ✓Control access to removable media such as memory cards and USB sticks
- ✓Consider disabling ports or limiting access to specific media (e.g. with shared PCs)
- ✓Encourage staff instead to transfer files via email or cloud storage

Switch on your firewall

- ✓Switch on your firewall to create a buffer zone between your network and the Internet
- ✓Included with most operating systems. If using Windows 10 or 11 – follow these instructions to check if your firewall is on
- ✓If using a 3rd party anti-virus solution this might include an additional firewall

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.

NCSC Small Charity Cyber Security Guide Infographic

NCSC online training

Protecting against malware

(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