superhighways
harnessing technology for community benefit

Cyber Security in 60 mins

Part 2: Phishing emails & other scams

#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

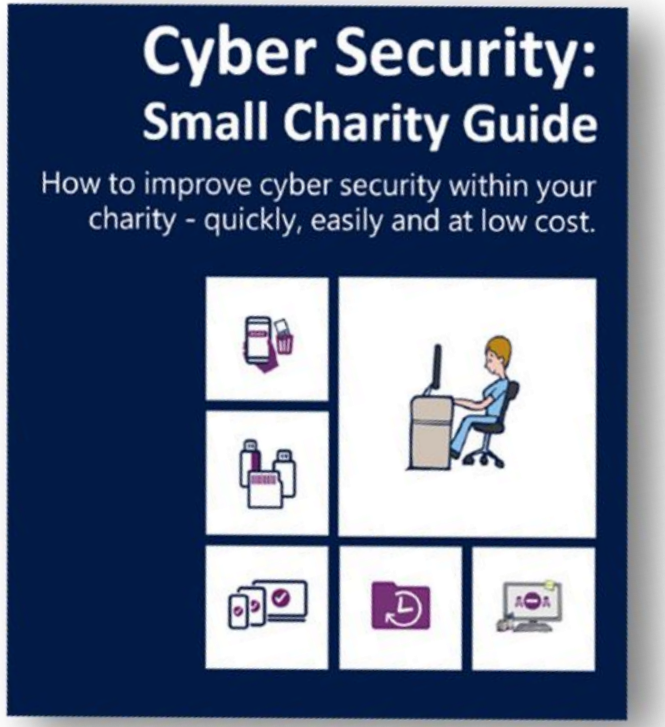
Which of the following breaches or attacks has your organisation identified in the last 12 months?	Businesses	Charities
Phishing attacks	83%	87%
Other impersonating organisation in emails or online	27%	26%
Viruses, spyware or malware (excluding ransomware)	12%	11%
Denial of service attacks	10%	2%
Hacking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

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

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.

Phishing: overview

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]

Discussion

- ✓You receive an email that contains the same logo, phone number, and address as a trusted organisation. How would you determine whether it is a phishing email?

- ✓What solutions would you suggest for someone who is a victim of a phishing scam?

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

Configure accounts appropriately

- ✓ Use the principle of 'least privilege'. Give trustees, staff and volunteers the lowest level of user rights required to perform their role, so if they are the victim of a phishing attack, the potential damage is reduced.

- ✓ Ensure users aren't logged on with Administrator privileges. Administrators can change security settings, install software and hardware, and access all files on the computer. An attacker having unauthorised access to an Administrator account can be far more damaging than accessing a standard user account

- ✓ Use two factor authentication (2FA) on your important accounts such as email. This means that even if an attacker knows your passwords, they still won't be able to access that account if someone has given away their password.

- ✓ Check what other security measures your tech providers offer e.g. Office 365 has features to detect spoof emails and e.g. quarantine them before reaching your inbox

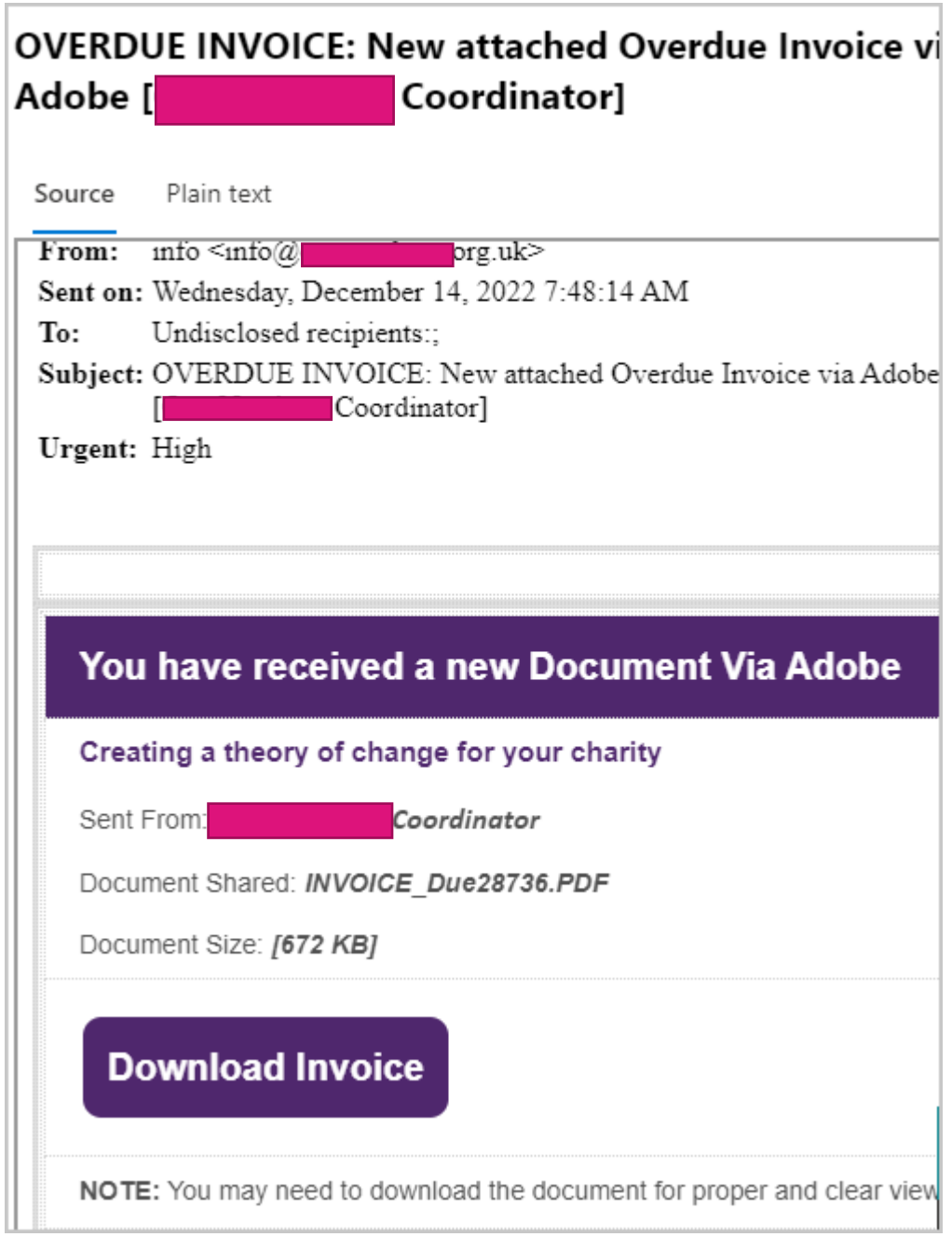
Think about how you operate

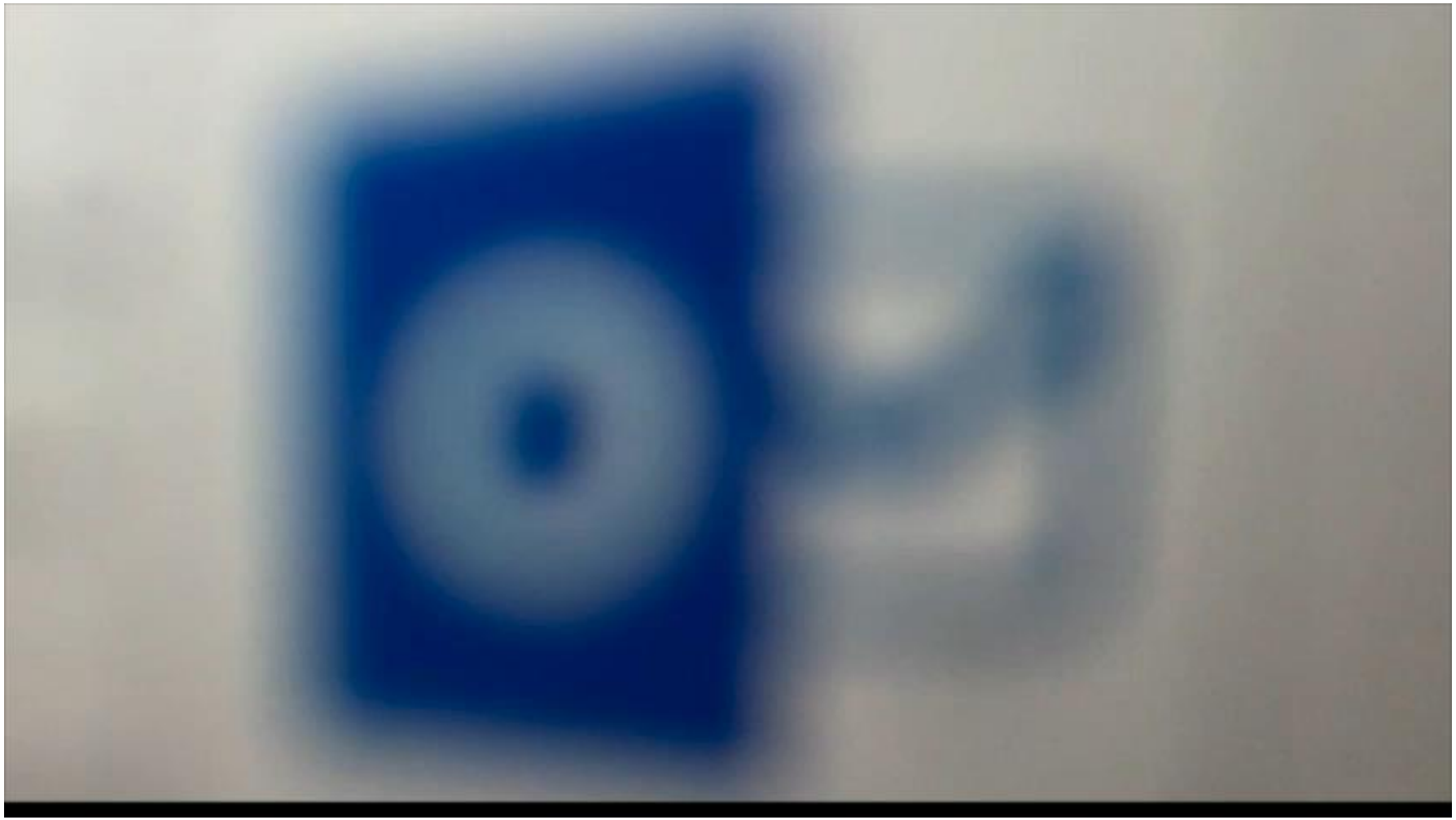
- ✓A common scam is to trick staff into transferring money or information by sending emails that look authentic. Think about your usual practices and how you can help make these tricks less likely to succeed e.g. picking up the phone and checking
- ✓Scammers will often send phishing emails from large organisations (such as banks) in the hope that some of the email recipients will have a connection to that company. Does the team know enough about companies you work with or use services from so that if they get an email from an organisation you don't do business with, they treat it with suspicion?
- ✓Encourage and support people in your charity to question suspicious or just unusual requests, even if they appear to be from important individuals.
- ✓Do you follow best practice re other procedures e.g. financial. Having more than one person required to authenticate payments for example which could save you from being a victim of financial fraud.

Know the obvious signs of phishing

- ✓ Is the spelling, grammar and punctuation poor? Is the design and quality what you'd expect from a credible, large organisation?
- ✓ Is it addressed to you by name, or does it refer to 'valued customer', or 'friend', or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.
- ✓ Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
- ✓ Does it appear to come from a trustee or manager, requesting a payment is made to a particular bank account. Look at the sender's name. Does it sound legitimate, or is it trying to mimic someone you know?
- ✓ If it sounds too good to be true, such as a large donation in return for banking details, it probably is!

Here's an example from today!





https://youtu.be/TFlCLREWxfU

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)

Text scams

If you receive a suspicious text message

- ✓Most phone providers are part of a scheme that allows customers to report suspicious text messages for free by forwarding it to **7726**.
- ✓If you forward a text to **7726**, your provider can investigate the origin of the text and arrange to block or ban the sender, if it's found to be malicious.
- ✓Find further information on the Action Fraud website.

Phone scams

If you receive a suspicious phone call

- ✓Phone scammers will call you unsolicited, pretending to be from an organisation you trust, such as your bank, a service provider or even the police.
- ✓These scam calls may be automated, or from a real person. They may ask you for your personal information like banking details, or tell you you need to transfer money.
- ✓If you've lost money or have been hacked as a result of responding to a call, you should report it to Action Fraud online or call 0300 123 2040.

I'm pretty alert to scammers, I think I'm safe...

https://youtu.be/Ic7scxvKQOo

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?

NCSC Small Charity Cyber Security Guide Infographic

Defending against phishing

✓Defending against phishing (online learnng)

(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