

# Cyber Security for Small Charities

CVS Cheshire East



# CVS Cheshire East

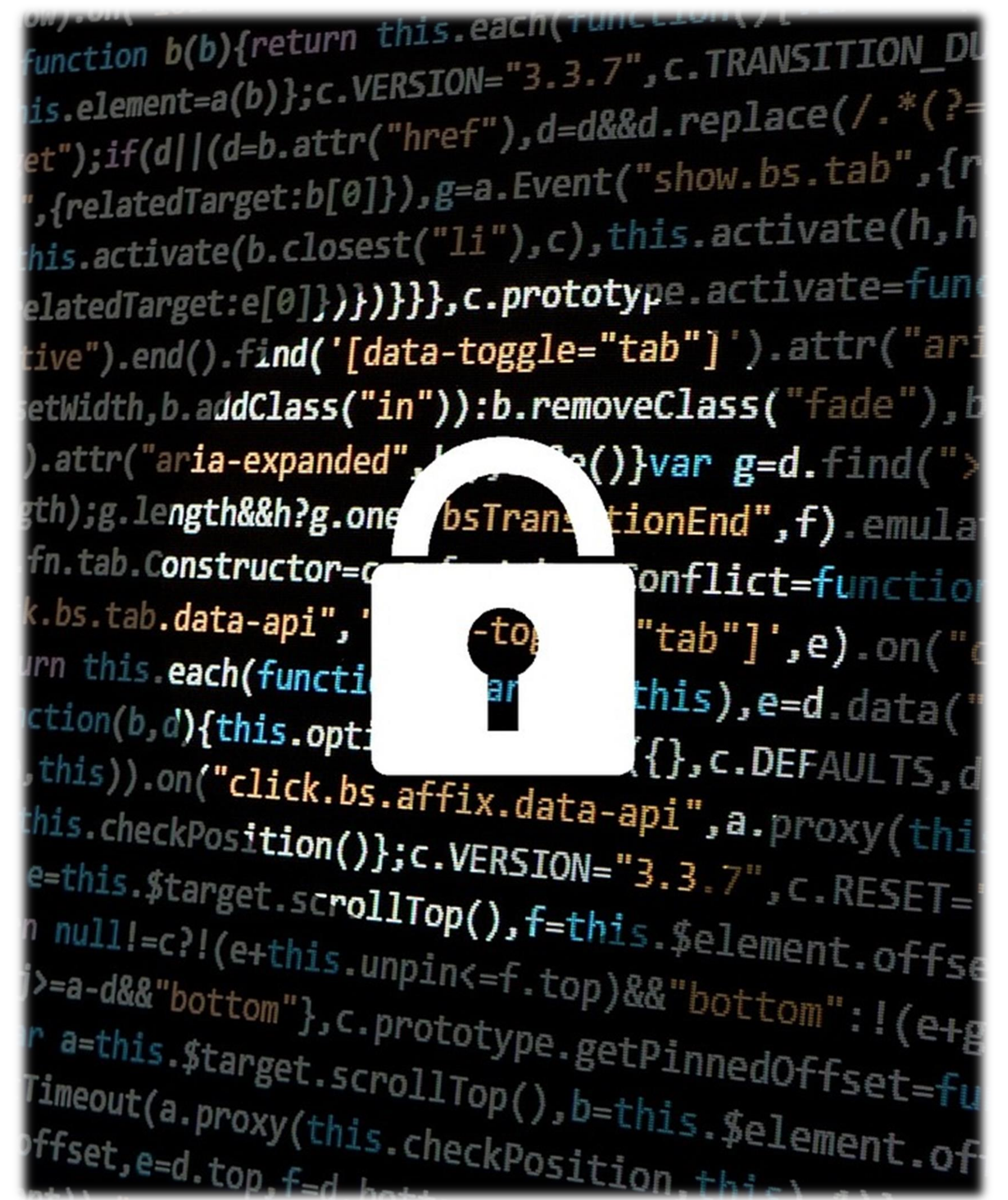
## Introduction





## Background

- The National Cyber Security Centre (NCSC) 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 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)**

010111001111  
100101010010  
101101010110  
011**HACKED**111  
101001000010  
101010101010  
001111110110



## 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.





# Cyber Breaches Survey 2020

## UK CHARITY TRENDS

### EXPERIENCE OF BREACHES OR ATTACKS



Among these 26%:



42% needed new measures for future attacks



33% lost staff time dealing with the breach



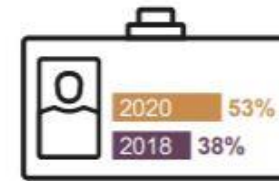
22% had staff stopped from doing day-to-day work



22% were attacked at least once a week

### MANAGING RISKS

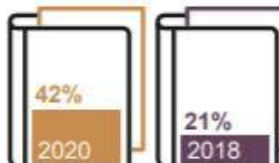
53% have staff whose job role includes information security or governance (up from 2018) ▶



45% have trustees with a cyber security brief (up from 2018) ▶



42% have cyber security policies (up from 2018) ▶



### IDENTIFYING RISKS

37% have done a cyber security risk assessment (up from 2018) ▶



### INCIDENT RESPONSE

50% assign incident management roles to specific people

43% have written guidance on who to notify of breaches

23%

## CYBER SECURITY BREACHES SURVEY 2020

### 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. This infographic shows the key findings for charities, which were first included in the 2018 survey.



**1. Cyber attacks have become more frequent.** In 2018, 19% of charities identified any cyber security breaches or attacks over a 12-month period. In 2020, this has risen to 26%.



**2. Cyber security is increasingly important for charities.** 74% of charities say that cyber security is a high priority for their trustees and senior managers, up from 53% in 2018.



**3. More charities are engaging their trustees and senior managers.** 38% of charities update their board on actions taken on cyber security at least quarterly. 12% never update them, down from 38% in 2018.



**4. Half of charities are seeking information.** 51% sought information in the last 12 months, up from 36% in 2018. But just 16% have heard of the National Cyber Security Centre's Small Charity Guide.



**5. Some are insuring themselves against the risks.** 31% of charities report being insured against cyber risks, either through a specific cyber insurance policy or as part of wider business insurance.



**6. There is room for improvement when it comes to suppliers and partners that charities work with.** Just 13% of charities have reviewed cyber security risks posed by their suppliers.

For the full results, visit [www.gov.uk/government/statistics/cyber-security-breaches-survey-2020](http://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020).

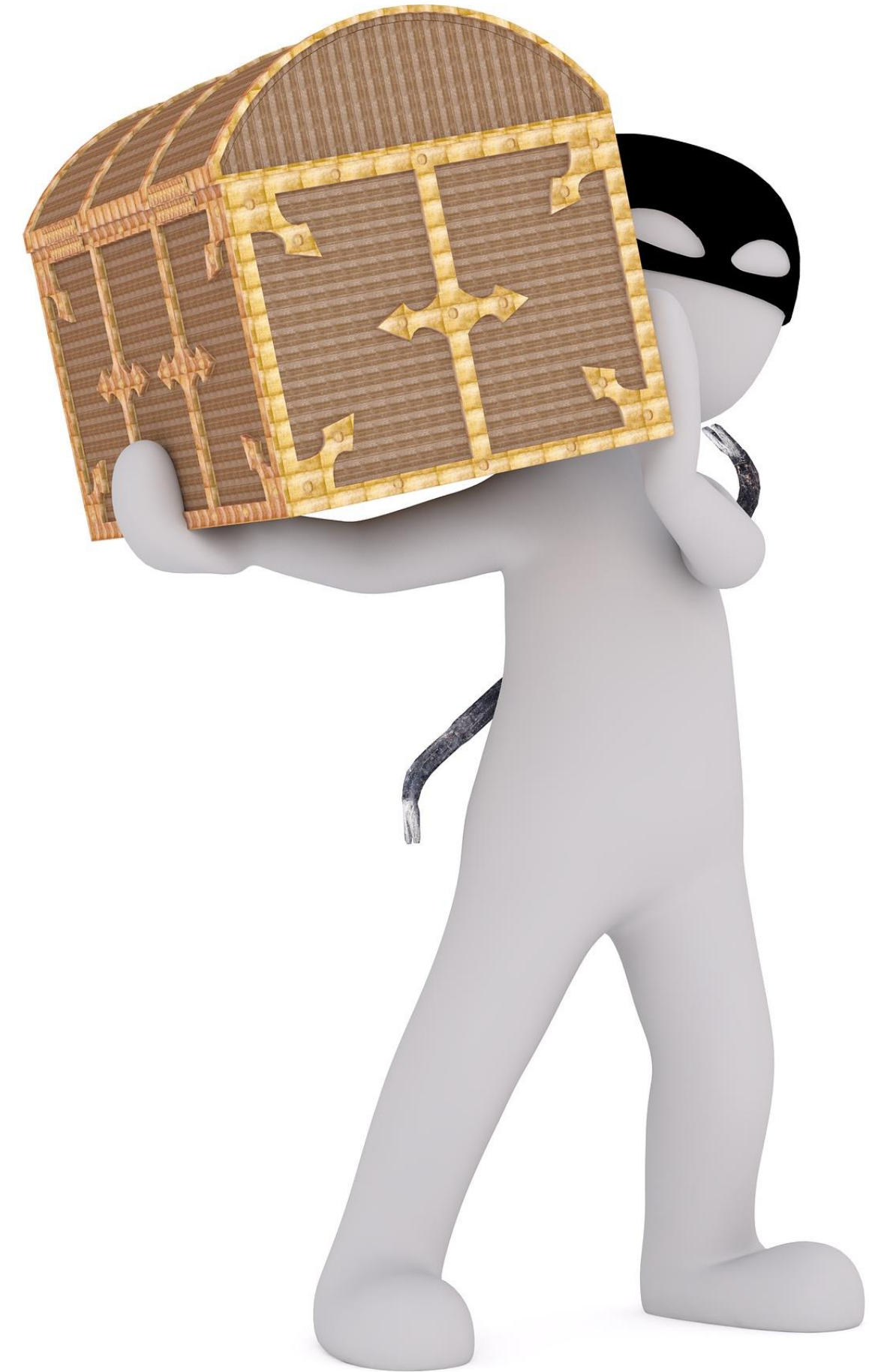
For further cyber security guidance for your charity, visit the National Cyber Security Centre website ([www.ncsc.gov.uk](http://www.ncsc.gov.uk)). This includes the Cyber Security Small Charity Guide drafted especially for charities ([www.ncsc.gov.uk/charity](http://www.ncsc.gov.uk/charity)).

Technical note: Ipsos MORI carried out a telephone survey of 337 UK registered charities from 9 October to 23 December 2019. This included 134 charities that identified a breach or attack in the last 12 months. N.B. this year's survey omitted the denial-of-service attacks category that had been included previously – this has a negligible impact on the trend. Data are weighted to represent UK registered charities by income band and country.



## 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





## 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**
- **Use of Volunteers**





## How are charities being attacked?

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





# More types of malware

**Virus** – a type of malware designed to replicate and spread, infecting computer systems. Needs a person to activate

**Worm** – a virus that doesn't need human assistance after it has been introduced. Infects a network by continuously replicating itself. Can modify or delete files or add infected software onto a computer.

**Trojan** – an attachment that looks like legitimate software and gives unauthorised access of the system to hackers

---

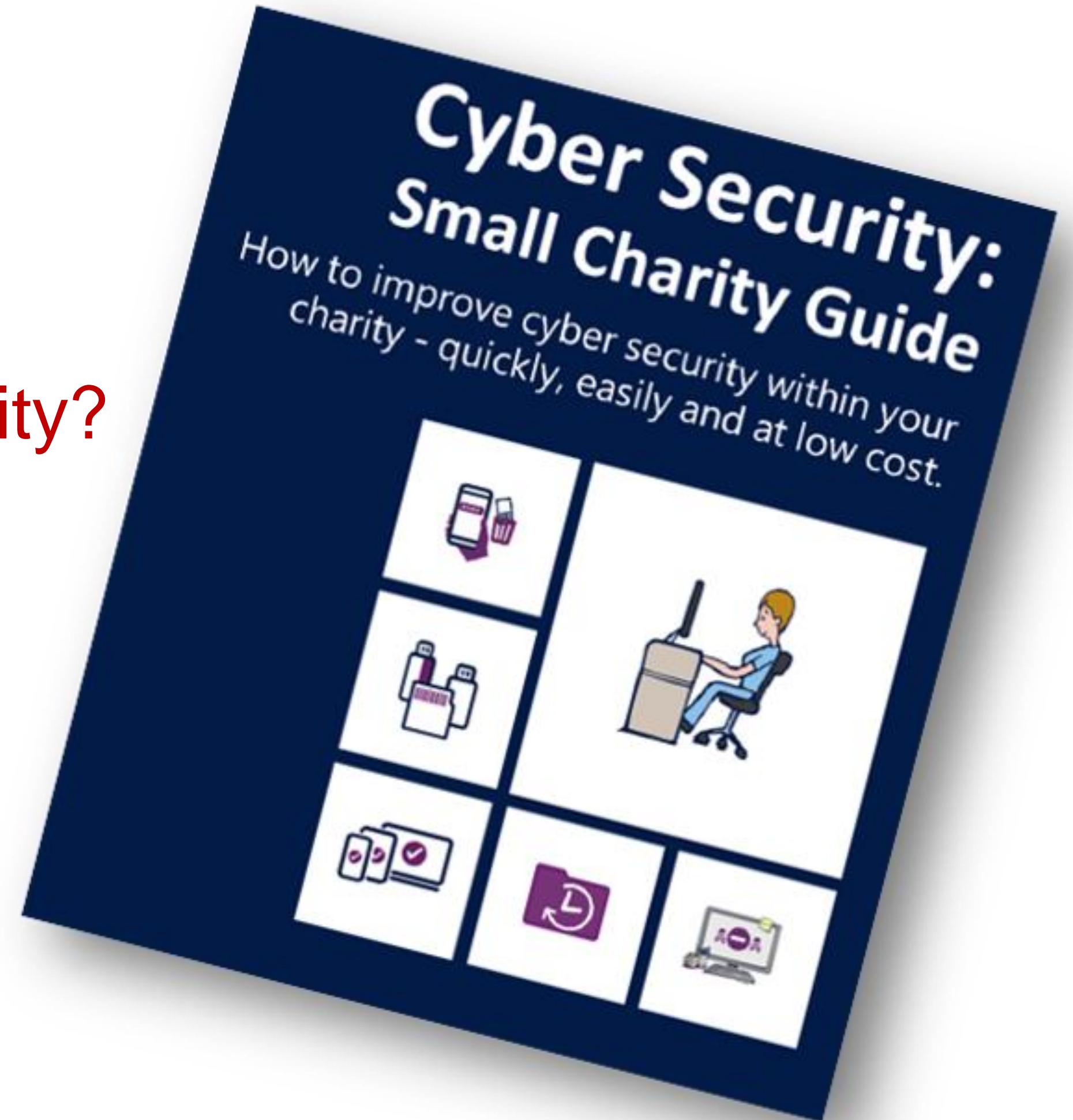


# Protecting your charity from cyber attacks



## What can you do to protect your charity?

- 5 quick, free or low cost steps...





# 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**





## Protection from malware?

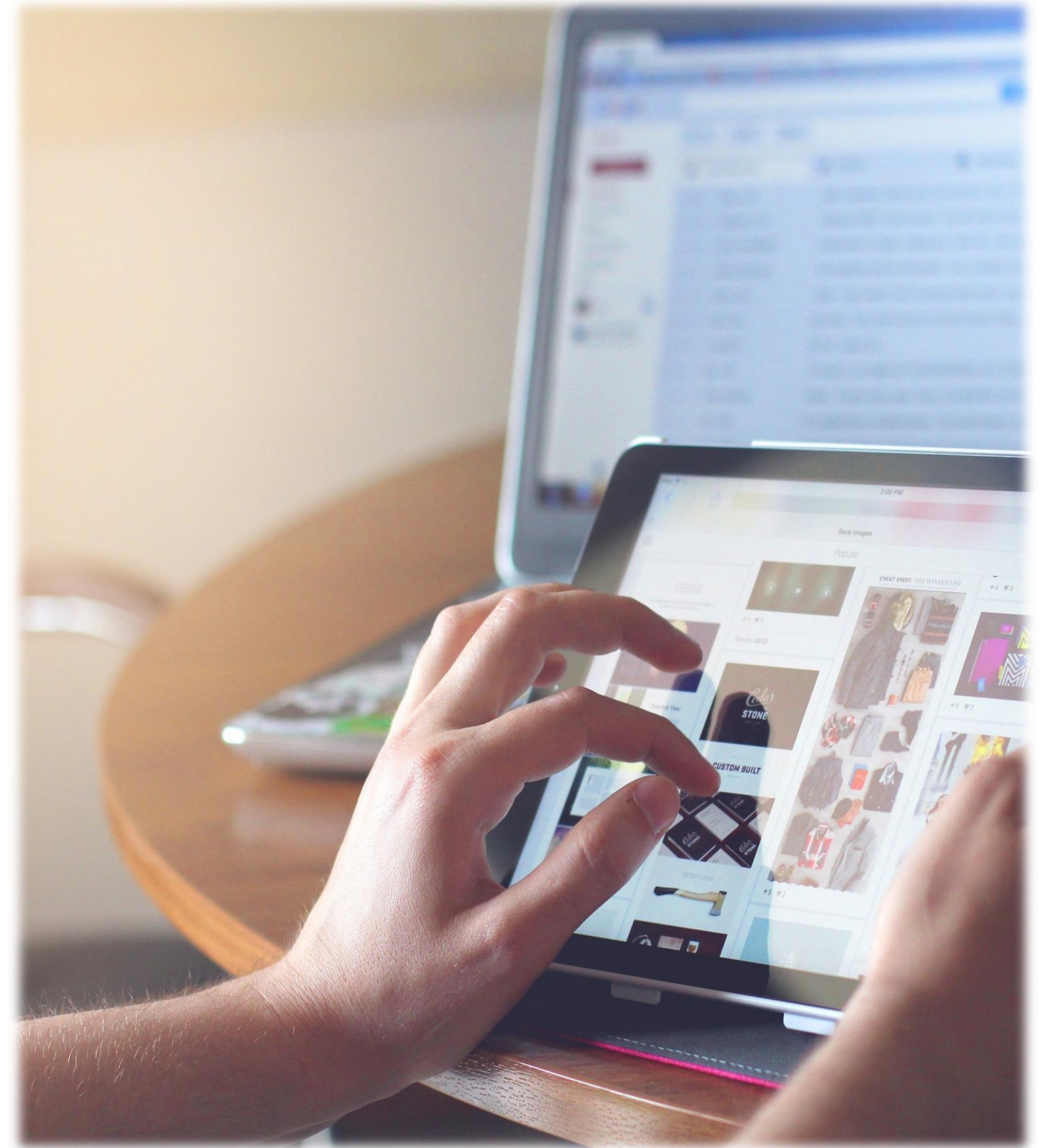
- **Antivirus software**
- **Prevent users from downloading 'dodgy apps'**
- **Keep everything up to date**
- **Control the use of USB drives**
- **Switch on your firewall**





## Keeping your smartphones /tablets safe

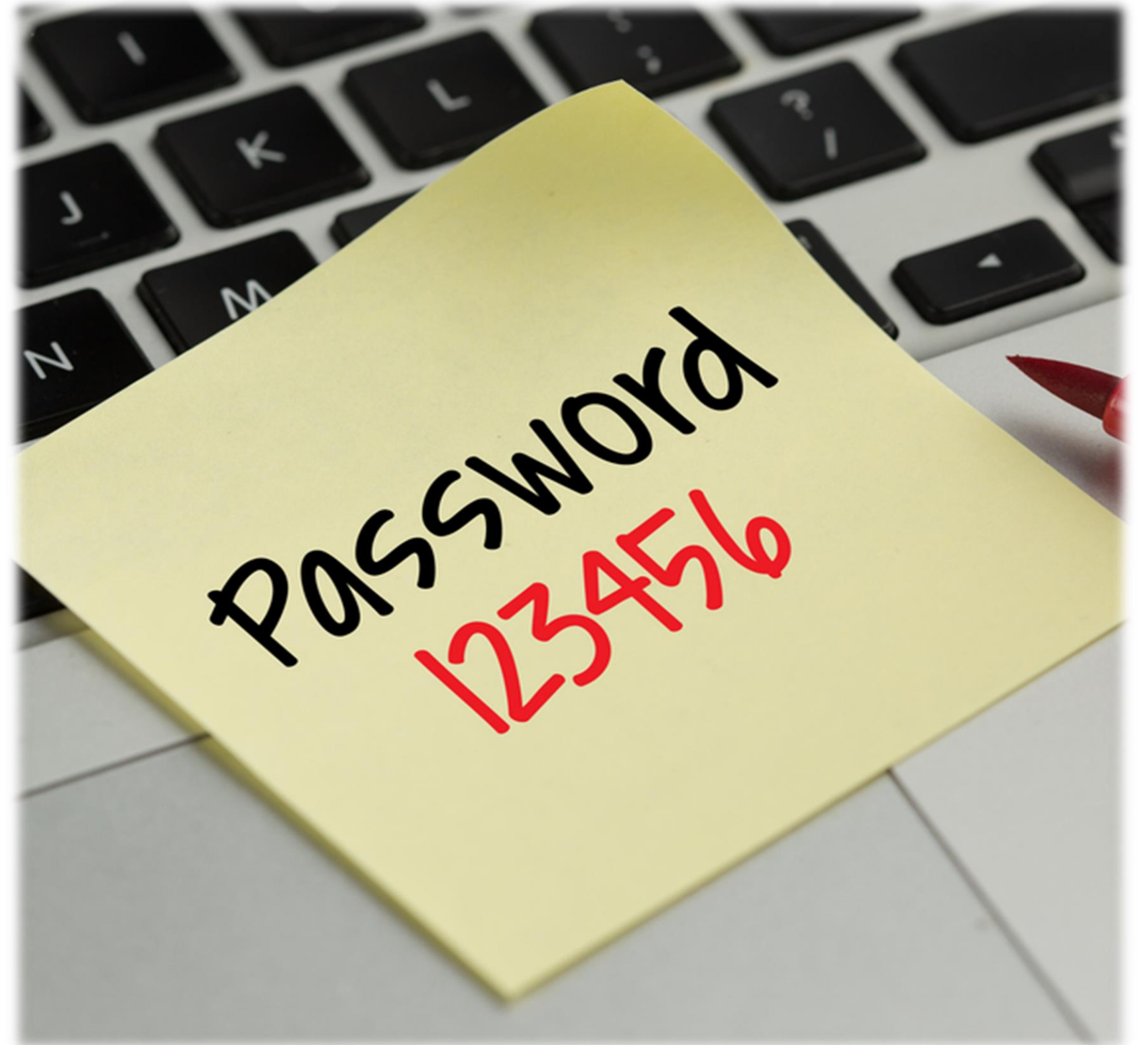
- Switch on password protection
- Prepare for lost or stolen devices
- Keep your device up to date
- Keep your apps up to date
- Use public Wi-Fi safely





## Using passwords

- Switch on password protection
- Use two factor authentication
- Avoid predictable passwords
  - 3 random words
- Help users cope with 'password overload'
- Change all default passwords





## Avoiding phishing attacks

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





## How much about me can people see online?





# What to do if you fall victim

## 1. Action Fraud

- Police Scotland if appropriate

## 2. ICO Breach Notification

- Always within 72 hours

## 3. The Charity Commission

- Reporting a Serious Incident (RSI)

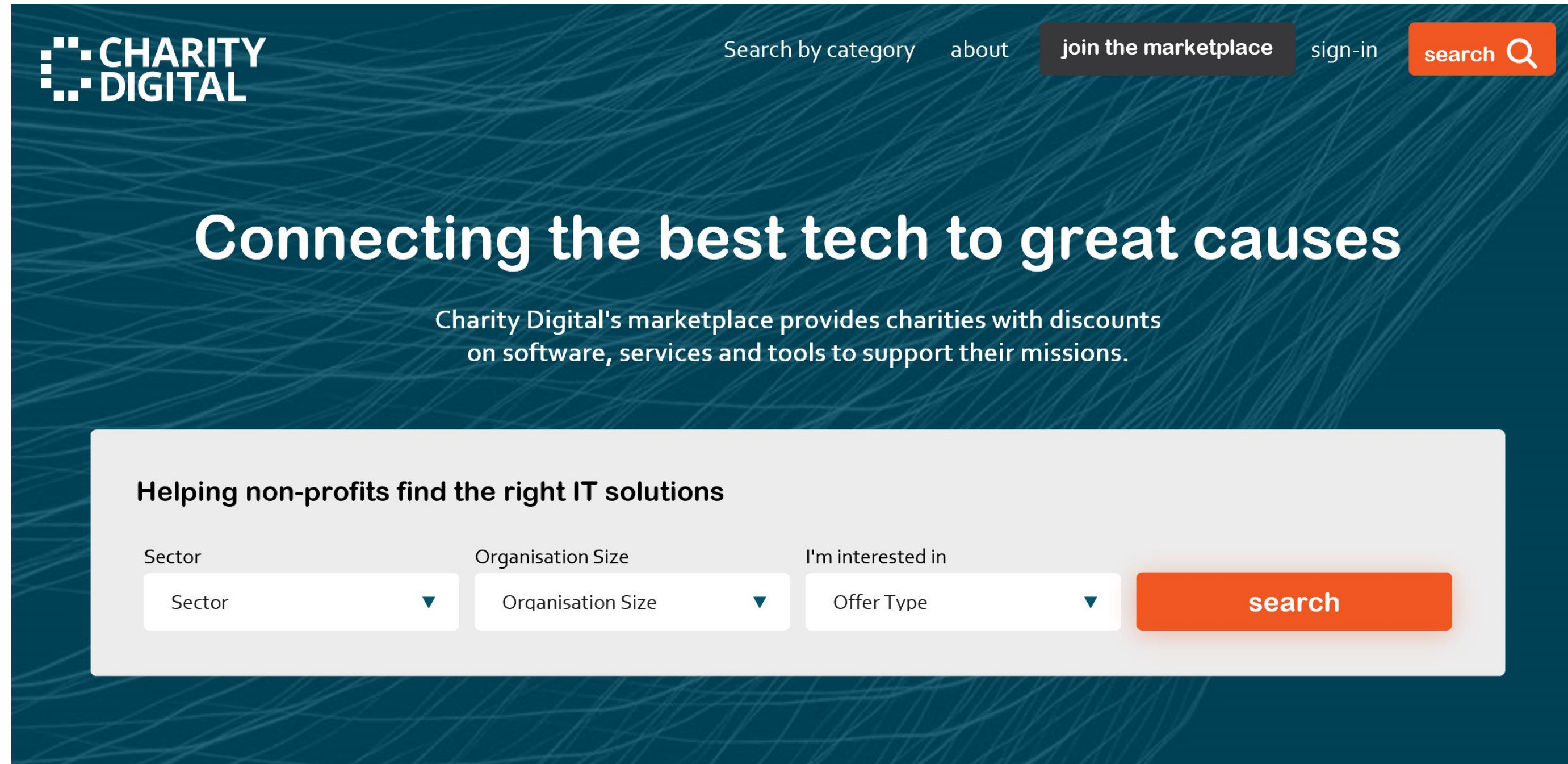
## 4. Other Regulators/Funders

- If applicable





# Charity Digital Marketplace



The screenshot shows the Charity Digital Marketplace website. At the top left is the logo for Charity Digital, which consists of a grid of dots forming the word 'CHARITY' above 'DIGITAL'. To the right of the logo are navigation links: 'Search by category', 'about', 'join the marketplace' (highlighted in a dark grey button), and 'sign-in'. Further right is a search bar with the text 'search' and a magnifying glass icon. The main heading is 'Connecting the best tech to great causes' in large white text. Below this is a sub-heading: 'Charity Digital's marketplace provides charities with discounts on software, services and tools to support their missions.' At the bottom, there is a search filter section titled 'Helping non-profits find the right IT solutions'. It contains three dropdown menus: 'Sector' (with 'Sector' selected), 'Organisation Size' (with 'Organisation Size' selected), and 'I'm interested in' (with 'Offer Type' selected). To the right of these filters is an orange 'search' button.



## What is your experience of Cyber Security?

- Does your organisation take Cyber Security seriously?
- What are your main takeaways from today's session?
- Who needs to be involved?





**Thank you.**

**Aoife Middlemass**