AN INTRODUCTION TO CYBER SECURITY

Some simple, low-cost security measures can go a long way towards improving a charity's cyber defences and protecting its funds, people and data.

HELPSHEET

Introduction

Charities are vulnerable to cyber attacks that can deprive them of their data and funds and potentially cause reputational damage. However, there are some simple steps that your charity can take to help protect itself and minimise and mitigate the effects of such attacks.

What is cyber security?

Cyber security is the means by which individuals and organisations reduce the risk of becoming victims of cyber attacks.

Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access – both at home and at work – from theft or damage. It's also about preventing unauthorised access to the vast amounts of personal information we store on these devices, and online.

Why is it important?

Charities fall victim to a wide range of cyber attacks because they hold funds and personal, financial and commercial data that have a financial value to cybercriminals. The cybercriminals might use the data to try and attack another person or they might sell it to other criminals.

Charities can be targeted by cybercriminals and attackers due to the fact that they often hold funds and data in low-security sites.

Common risks

There are various different cyber threats that range from malicious software (malware) to phishing emails and even fake websites that seek to mimic your own legitimate ones. By following five simple steps you can dramatically reduce the chances of a successful cyber attack.

Five steps of basic cyber security

1. **Use passwords:** Switch on password protection on all devices. Consider using multifactor authentication to access devices and ensure any manufacturer's default passwords are changed. Don't use predictable passwords, and consider using password managers to avoid password overload.

2. **Back up your data:** Identify your essential data and keep a backup copy of this separate from your computer. This could be on a USB stick, separate drive or on some form of cloud-based storage platform.

3. **Protect yourself from malware:** Install and turn on antivirus software. Prevent your staff from downloading apps from unknown vendors or sources, and keep all of your IT equipment and software up to date by applying security patches as soon as they are available. Switch on your firewall and control how people can use external storage devices.

4. **Protect your devices:** Ensure your devices can be tracked, locked and remotely wiped if they are ever lost or stolen. Keep your device operating system and your apps up to date and do not connect to unknown wi-fi hotspots – use 3G or 4G mobile networks instead.

5. **Avoid phishing attacks:** To reduce risk, minimise the number of people who have administrator access on your network. Train your staff to spot phishing emails and tell them what to do if they have any concerns. Publicly accessible information will often be used to make phishing emails seem more plausible, so think carefully about what you post online and review this information regularly.

CHARITY FRAUD AWARE

Taking action

If you suspect a cyber security breach act promptly.

- Ideally have a cyber response plan so that everyone knows what to do and when.
- Report the incident to your relevant national law enforcement agency. In the UK this is Action Fraud (England, Wales and Northern Ireland) or Police Scotland (Scotland).
- Report matters promptly to your charity regulator. For reports to the Charity Commission for England and Wales treat it as a serious incident. Use the **online form** to make your report, stating what happened and how you're dealing with it.

CHECKLIST

BUILDING YOUR CHARITY'S DEFENCES

ASK YOURSELF:

- ☐ Do we follow the five steps of basic cyber security? If not, how quickly can we introduce them and make sure they carried out?
- ☐ Do we have an information security policy and cyber response plan that is regularly reviewed, tested and updated?
- ☐ Do we have a policy or set of rules for staff and volunteers that connect to our charity's network for business purposes using their personally owned devices? Are staff told about it?
- ☐ Are staff made aware of common cyber attacks and how to spot and report them?

OTHER RESOURCES

The UK's National Cyber Security Centre has produced guidance for charities on how to improve cyber security quickly, easily and at low cost. See '**Cyber security: small charity guide**', '**Mitigating malware and ransomware attacks**' and '**Using passwords to protect your devices and data**'. It also offers free tools and exercises to help you practice your response to a cyber incident as part of its '**Active cyber defence programme**'.

The UK's Information Commissioner's Office has produced guidance on how and when to report a cyber security incident to them. See '**Responding to a cyber security incident**'.

Get Safe Online provides easy-to-understand information on online safety.

Preventing Charity Fraud contains resources to help charities prevent, detect and respond to fraud.

ACKNOWLEDGEMENT

This helpsheet was kindly prepared by the UK's National Cyber Security Centre.