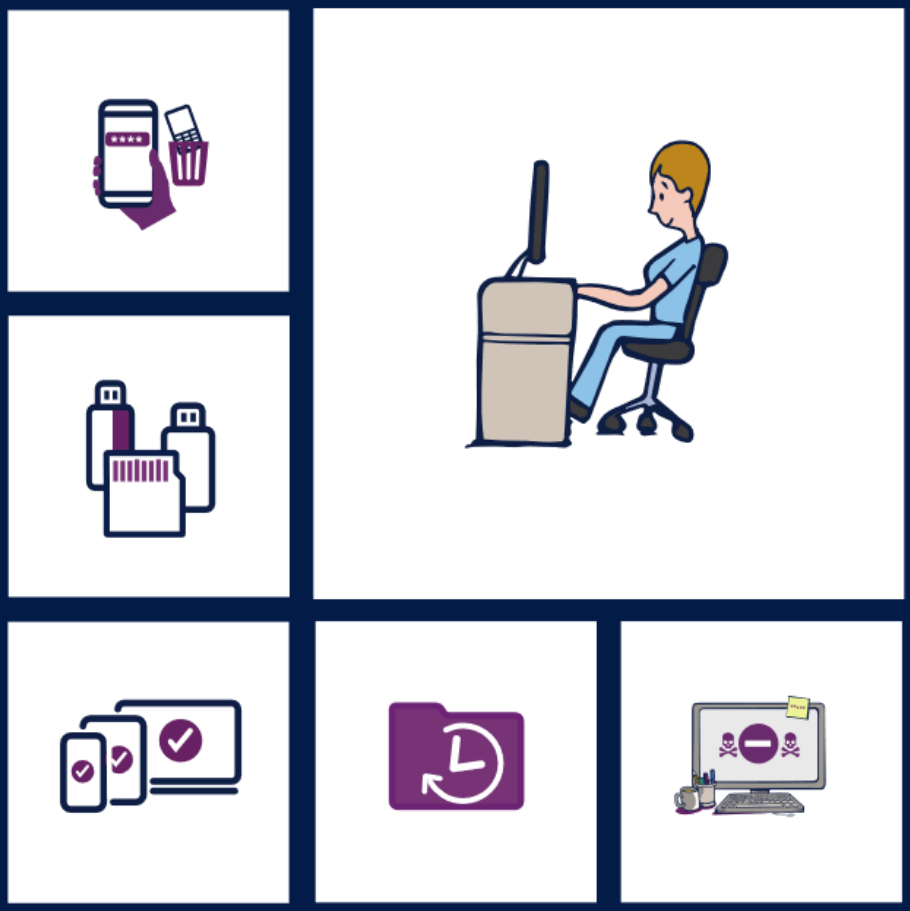
National Cyber Security Centre
a part of GCHQ

Cyber Security:
Small Charity Guide

How to improve cyber security within your charity - quickly, easily and at low cost.





Contents

Foreword: Ciaran Martin **4**

Foreword: Helen Stephenson **5**

Backing up your data **6**

Protecting your charity from malware **8**

Keeping your smartphones (and tablets) safe **10**

Using passwords to protect your data **12**

Avoiding phishing attacks **14**

Infographic summary **17**

Glossary **18**



Foreword: Ciaran Martin

I am extremely proud to present this cyber security guide for charities, which has been produced to help you protect yourself from the most common cyber attacks.

Like businesses, charities are increasingly reliant on IT and technology and are falling victim to a range of malicious cyber activity. Losing access to this technology, having funds stolen or suffering a data breach through a cyber attack can be devastating, both financially and reputationally. Whilst this guide has been created for small charities, its advice is applicable to charities of any size.

The National Cyber Security Centre (NCSC) aims to make the UK the safest place to live and work online. We want to help you to feel better armed to face the challenges that come with such rapid advancement, and although we can't guarantee protection from all types of cyber attack, following the advice in this guide will significantly increase your protection from the most common types of cyber crime. The five topics covered are easy to understand, are free or cost little to implement. We hope this guide demonstrates how easy it can be to protect your charity's data, assets, and reputation.

The 'find out more' sections at the bottom of each topic offer extra help. If you need to improve your cyber security further, then you can also seek certification under the Cyber Essentials[1] scheme, which has the benefit of demonstrating to your supporters, donors and beneficiaries that you take the protection of their data seriously. And if you're a larger charity, or face a greater risk from cyber crime, then the 10 Steps to Cyber Security[2] can help you further.

The NCSC is not just here to look after the IT systems of UK government and business. We are committed to supporting the charity sector and we encourage you all to implement the five quick and easy steps outlined in this guide.



Ciaran Martin
Chief Executive Officer, NCSC

[1] https://www.cyberessentials.ncsc.gov.uk/
[2] https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

Foreword: Helen Stephenson

Charities are not immune to cyber crime. Perpetrators do not distinguish between their victims and charities are as likely to be targeted as private firms or the general public. The valuable funds, assets and good reputation of charities are at risk from the increasing threat of cyber crime. That is why everybody involved with charities - donors, volunteers, employees, professional advisers and, above all, trustees - have a role to play in protecting the charity sector from cyber-related harm.

The Charity Commission is proud to have supported the National Cyber Security Centre (NCSC) in the development of the first cyber security guide for charities. The advice contained in this guide will be relevant to all charities, though it's likely that smaller charities will especially benefit from the practical tips and guidance on offer. However, good practice will only be effective if everyone plays their part, seeking out and applying relevant advice to help improve their charity's resilience to the growing threat of cyber crime. Taking even a few of the simple steps recommended in this guide will be a good start to better protecting your charity from harm.

I encourage you all to read this guide, adopt good practice and share key messages with your charity peers. By consistently applying the guidance contained in this guide, you'll be going some way to tackling the scourge of cyber crime and ensuring the sector is well equipped for the future. Prevention really is better than cure.



Helen Stephenson
Chief Executive, Charity Commission for England and Wales

Backing up your data

Think about how much you rely on your charity's critical data, supporter details, information on beneficiaries, volunteer data, governing documents, as well as invoices and payment details. Now imagine how long you would be able to operate without them.

All charities, regardless of nature and size, should take regular backups of their important data, and make sure that these backups are recent and can be restored. By doing this, you're ensuring your charity can still function following the impact of flood, fire, physical damage or theft. Furthermore, if you have backups of your data that you can recover quickly, your charity will be more resilient to cyber crime.

This section outlines 5 things to consider when backing up your data.

Tip 1: Identify what data you need to back up

Your first step is to identify your essential data. That is, the information that your charity couldn't function without. Normally this will comprise documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases; most of which are kept in just a few common folders on your computer, phone, tablet or network.

Tip 2: Keep your backup separate from your computer

Whether it's on a USB stick, on a separate drive or a separate computer, access to data backups should be restricted so that they:

- are not accessible by all staff or volunteers
- are not permanently connected (either physically or over a local network) to the device holding the original copy

Ransomware (and other malicious software) can often move to attached storage automatically, which means any such backup could also be infected, leaving you with no backup to recover data from. For more resilience, you should consider storing your backups in a different location, so fire or theft won't result in you losing both copies. Cloud storage solutions (see below) are a cost-effective and efficient way of achieving this.

Tip 3: Consider the cloud

You've probably already used cloud storage during your everyday work and personal life without even knowing - unless you're running your own email server, your emails are already stored 'in the cloud'.

Using cloud storage (where a service provider stores your data on their infrastructure) means your data is physically separate from your location. You'll also benefit from a high level of availability. Service providers can supply your charity with data storage and web services without you needing to invest in expensive hardware up front. Most providers offer a limited amount of storage space for free, and larger storage capacity for minimal costs to charities.

Tip 4: Read our cloud security guidance

Not all service providers are the same, but the market is reasonably mature and most providers have good security practices built-in. By handing over significant parts of your IT services to a service provider, you'll benefit from specialist expertise that smaller charities would perhaps struggle to justify in terms of cost. However, before contacting service providers, we encourage you to read the NCSC's Cloud Security Guidance[3]. This guidance will help you decide what to look for when evaluating their services, and what they can offer.

Tip 5: Make backing up part of your everyday business

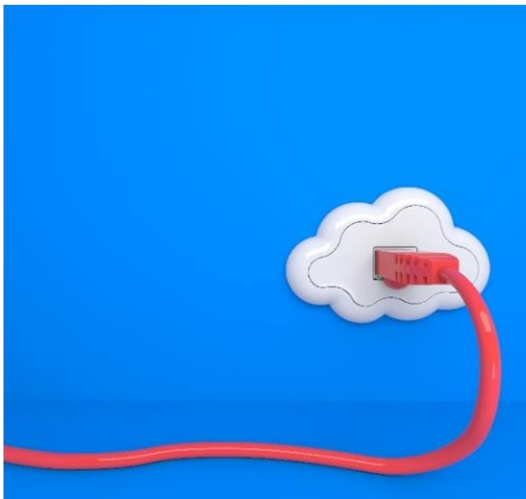
We know that backing up is not a very interesting thing to do (and there will always be more important tasks that you feel should take priority), but the majority of network or cloud storage solutions now allow you to make backups automatically. For instance, when new files of a certain type are saved to specified folders. Using automated backups not only saves time, but also ensures that you have the latest version of your files should you need them.

Many off-the-shelf backup solutions are easy to set up, and are affordable considering the business-critical protection they offer. When choosing a solution, you'll also have to decide how much data you need to back up, and how quickly you need to be able to access the data following an incident.

Find out more

For further guidance on backups, please see our Securing Bulk Data guidance[4], which discusses the importance of knowing what data is most important to you, and how to back it up reliably.

The Information Commissioner's Office website also has a useful introduction to cloud computing[5].



[3] https://www.ncsc.gov.uk/guidance/cloud-security-collection
[4] https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-main
[5] https://ico.org.uk/for-the-public/online/cloud-computing/

Protecting your charity from malware

Malicious software (also known as 'malware') is software or web content that can harm your charity, such as the WannaCry outbreak[6] in 2017. The most well-known form of malware is viruses, which are self-copying programs that infect legitimate software.

This section contains 5 free and easy-to-implement tips that can help prevent malware damaging your organisation.

Tip 1: Install (and turn on) antivirus software

Antivirus software - which is often included for free within popular operating systems - should be used on **all** computers and laptops. For your office equipment, you can pretty much click 'enable', and you're instantly safer. Smartphones and tablets might require a different approach and if configured in accordance with the NCSC's End User Device guidance[7], separate antivirus software[8] might not be necessary.

Tip 2: Prevent trustees, volunteers or staff from downloading dodgy apps

You should only download apps for mobile phones and tablets from manufacturer-approved stores (like Google Play or Apple App Store). These apps are checked to provide a certain level of protection from malware that might cause harm. You should prevent charity personnel from downloading third party apps from unknown vendors/sources, as these will not have been checked.

Staff accounts should only have enough access required to perform their role, with extra permissions (i.e. for administrators) only given to those who need it. When administrative accounts are created, they should only be used for that specific task, with standard user accounts used for general work.

Tip 3: Keep all your IT equipment and software up to date (patching)

For all your IT equipment (so tablets, smartphones, laptops and PCs), make sure that the software and device(s) operating system are always kept up to date with the latest versions from software developers, hardware suppliers and vendors. Applying these updates (a process known as patching) is one of the most important things you can do to improve security - the IT version of eating your fruit and veg. Operating systems, programs, phones and apps should all be set to 'automatically update' wherever this is an option.

At some point, software and device suppliers will end their support for older models and updates will no longer be available, at which point you should consider replacing them with modern alternatives. For more information on applying updates, refer to the NCSC's guidance on Vulnerability Management[9].

[6] https://www.ncsc.gov.uk/WannaCry-guidance-for-home-users-and-small-businesses
[7] https://www.ncsc.gov.uk/guidance/end-user-device-security
[8] https://www.ncsc.gov.uk/blog-post/av-or-not-av
[9] https://www.ncsc.gov.uk/guidance/vulnerability-management

Tip 4: Control how USB drives (and memory cards) can be used

We all know how tempting it is to use USB drives or memory cards to transfer files between organisations and people. However, it only takes one person to inadvertently plug-in an infected device (such as a USB drive containing malware) to cause lasting damage to your charity's assets and good reputation.

When drives and cards are openly shared, it becomes hard to track what they contain, where they've been, and who has used them. You can reduce the likelihood of infection by:

- blocking access to the physical ports (such as USB ports) on the devices being used
- using antivirus tools
- only allowing approved USB drives and memory cards to be used within your charity - and prohibiting their use in other devices (such as home computers)

Make these directives part of your charity's policies and procedures, to prevent it being exposed to unnecessary risks. You can also ask trustees, volunteers or staff to transfer files using alternate means (such as by email or cloud storage), rather than via USB.

Tip 5: Switch on your firewall

Firewalls create a 'buffer zone' between your own network and external networks (such as the Internet). Most popular operating systems now include a firewall, so it may simply be a case of switching this on. For more detailed information on using firewalls, refer to the Network Security section of the NCSC's 10 Steps to Cyber Security[10].

Find out more

More detailed, technical advice on preventing malware is available from the NCSC's 10 Steps to Cyber Security[11].

For detailed information on removable media, refer to the removable media section of the NCSC's 10 Steps to Cyber Security[12].

How to protect your PC from viruses (Microsoft guide)[13].



[10] https://www.ncsc.gov.uk/guidance/10-steps-network-security
[11] https://www.ncsc.gov.uk/guidance/10-steps-malware-prevention
[12] https://www.ncsc.gov.uk/guidance/10-steps-removable-media-controls
[13] https://support.microsoft.com/en-us/help/17228/windows-protect-my-pc-from-viruses

Keeping your smartphones (and tablets) safe

Mobile technology is now an essential part of life in a small charity, with increasing amounts of data being stored on tablets and smartphones. What's more, these devices are now as powerful as traditional computers, and because they often leave the safety of the office (and home), they need even more protection than 'desktop' equipment.

With this is mind, here are 5 quick tips that can help keep your mobile devices (and the information stored on them) secure. This applies whether you are using your own personal device, or a device provided by your charity.

Tip 1: Switch on password protection

A suitably complex PIN or password[14] (opposed to a simple one that can be easily guessed or gleaned from your social media profiles) will prevent the average criminal from accessing your phone. Many devices now include fingerprint recognition to lock your device, without the need for a password. However, these features are not always enabled when you first receive your devices, so you should always check they have been switched on.

Tip 2: Make sure lost or stolen devices can be tracked, locked or wiped

Trustees, staff and volunteers are more likely to have their devices stolen (or lose them) while out of the office or their home. Fortunately, the majority of devices include free web-based tools that are invaluable should you lose your device. They can help you to:

- track the location of a device
- remotely lock access to the device (to prevent anyone else using it)
- remotely erase the data stored on the device
- retrieve a backup of data stored on the device

Setting up these tools may seem daunting at first, but by using mobile device management software[15], you can set up your devices to a standard configuration with a single click.

Tip 3: Keep your device up to date

No matter what phones or tablets your charity is using, it is important that they are kept up to date at all times. All manufactures (for example Windows, Android, Apple) release regular updates that contain critical security fixes to keep the device protected. This process is quick, easy, and free; devices should be set to automatically update, where possible. Ensure your trustees, staff and volunteers know how important these updates are, and explain how to do it, if necessary. At some point, manufacturers will discontinue their support for older devices, at which point you should consider replacing them with a newer model or version.

[14] https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0
[15] https://www.ncsc.gov.uk/blog-post/ncsc-it-mdm-products-which-one-best-1

Tip 4: Keep your apps up to date

Just like the operating systems on your charity's devices, all the applications that you have installed should also be updated regularly with patches from the software developers. These updates will not only add new features, but will also fix any security issues that have been discovered. Make sure trustees, staff and volunteers know when updates are ready, how to install them, and that it's important to do so straight away.

Tip 5: Don't connect to unknown Wi-Fi Hotspots

When you use public Wi-Fi hotspots (for example in hotels, coffee shops or public transport), there is no easy way to find out who controls the hotspot, or to be assured it's secure. If you do connect to these hotspots, somebody else could access:

- what you're working on whilst connected
- your private login details that many apps and web services maintain whilst you're logged on

The simplest precaution is to not connect to the Internet using unknown hotspots, and instead use your mobile 3G or 4G mobile network, which will have built-in security. This means you can also use 'tethering' (where your other devices such as laptops share the 3G/4G connection from your phone), or a wireless 'dongle' provided by your mobile network. You can also use Virtual Private Networks (VPNs), a technique that encrypts your data before it is sent across the Internet. If you're using third party VPNs, you'll need the technical ability to configure it yourself, and should only use VPNs provided by reputable service providers.

Find out more

For more technical information about how to ensure your trustees, staff and volunteers can work safely whilst on the move or at home, please refer to the 10 Steps: Home and Mobile Working guidance[16].

If you're about to invest in a new device, we recommend you read the Buyer's Guide to Choosing and Using Mobile Devices[17] produced by the Home Office.

[16] https://www.ncsc.gov.uk/guidance/10-steps-home-and-mobile-working

[17] https://www.gov.uk/government/publications/mobile-device-security-a-buyers-guide-to-choosing-and-using-mobile-devices

Using passwords to protect your data

Your charity's laptops, computers, tablets and smartphones will contain a lot of important and sensitive data such as the personal information of your beneficiaries and supporters, as well as details of your online accounts such as banking. It is essential that this data is available to you, but not available to unauthorised users.

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised users accessing your devices. **This section outlines 5 things to keep in mind when using passwords**.

Tip 1: Make sure you switch on password protection

Set a screenlock password, PIN, or other authentication method (such as fingerprint or face unlock on your mobile devices). The NCSC blog[18] has some good advice on passwords. If you're mostly using fingerprint or face unlock, you'll be entering a password less often, so consider setting up a long password that's difficult to guess.

Having said this, password protection is not just for smartphones and tablets. Make sure that your office equipment (so laptops and PCs) all use an encryption product (such as BitLocker for Windows) using a Trusted Platform Module (TPM)[19] with a PIN, or FileVault (on macOS)[20] in order to start up. Most modern devices have encryption built in, but you'll need to ensure it's turned on and configured, so check you have set it up.

Tip 2: Use two factor authentication for 'important' accounts

If you're given the option to use two-factor authentication (also known as 2FA) for any of your accounts, you should do; it adds a large amount of security for not much extra effort. 2FA requires two different methods to 'prove' your identity before you can use a service, generally a password plus one other method. This could be a code that's sent to your smartphone (or a code that's generated from a bank's card reader) that you must enter in addition to your password.

Tip 3: Avoid using predictable passwords

Using strong passwords is an important way to protect your charity's valuable data. Make sure trustees, staff and volunteers are given actionable advice[21] on setting secure passwords that is easy for them to understand.

[18] https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0
[19] https://technet.microsoft.com/en-us/library/cc766295(v=ws.10).aspx
[20] https://support.apple.com/en-gb/HT204837
[21] https://www.ncsc.gov.uk/guidance/helping-end-users-manage-their-passwords

Passwords should be easy to remember, but hard for somebody else to guess. A good rule is to use three random words to create a strong password. Avoid using the most common passwords[22], which criminals can easily guess (such as P4$$w0rd or QWERTY). The NCSC have some useful advice on how to choose a non-predictable password[23].

Your charity's IT systems should **not** require trustees, volunteers or staff to share accounts or passwords in order to get their job done. Make sure that every user has personal access to the right systems, and that the level of access given is always the lowest needed to do their job whilst minimising their access to systems they don't need to use. This will lower the risk of wider damage if a user downloads malicious software (like a virus).

Tip 4: How to cope with 'password overload'

Only enforce password access to a piece of software or system if you really need to. Where you do use passwords to access a service, do not enforce regular password changes. Passwords really only need to be changed when you suspect a compromise of the login credentials.

You should also provide secure storage, so staff can write down passwords for important accounts (such as email and banking), and keep them safe (but not with the device itself). People will forget passwords, so make sure they can reset their own passwords easily.

Consider using password managers[24], which are tools that can create and store passwords for you that you access via a 'master' password. Since the master password is protecting all of your other passwords, make sure it's a strong one, for example by using three random words.

Tip 5: Change all default passwords

One of the most common mistakes is not changing the manufacturers' default passwords that smartphones, laptops, and other types of equipment are issued with. Change all default passwords before devices are distributed within your charity. You should also check devices and software regularly to detect unchanged default passwords.

Find out more

If you're in charge of setting up passwords in your charity, please refer to our password policy guidance[25].



[22] https://www.teamsid.com/worst-passwords-2015/
[23] https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0
[24] https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers
[25] https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

Avoiding phishing attacks

In a typical phishing attack, scammers send fake emails to thousands of people, asking for sensitive information (such as bank details), or containing links to bad websites. They might try to trick you into sending money, steal your details to sell on, or they may have political or ideological motives[26] for accessing your charity's information.

Phishing emails are getting harder to spot, and some will still get past even the most observant users. Whatever the size and nature of your charity, you will receive phishing attacks at some point. This section contains some easy steps to help you identify the most common phishing attacks, but be aware that there is a limit to what you can expect your users to do[27].

Tip 1: Configure accounts to reduce the impact of successful attacks

You should configure your charity's IT systems in advance using the principle of 'least privilege'. This means giving 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.

To further reduce the damage that can be done by malware or loss of login details, ensure that your personnel don't browse the web or check emails from an account with **Administrator** privileges. An Administrator account is a user account that allows you to make changes that will affect other users. 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.

Tip 2: Think about how you operate

Consider ways that someone might target your charity, and make sure your trustees, staff and volunteers all understand normal ways of working (especially regarding interaction with other organisations), so that they're better equipped to spot requests that are out of the ordinary. Common tricks include sending an invoice for a service that you haven't used, so when the attachment is opened, malware is automatically installed (without your knowledge) on your computer.

Another 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. For example:

- Do trustees, staff and volunteers know what to do with unusual requests, and where to get help?
- Ask yourself whether someone impersonating an important individual (a trustee, beneficiary or manager) via email should be challenged (or have their identity verified another way) before action is taken.

[26] http://www.bbc.co.uk/news/uk-38332266
[27] https://www.ncsc.gov.uk/blog-post/im-gonna-stop-you-little-phishie

- Do you understand the day-to-day relationships your charity has? 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. If you get an email from an organisation you don't do business with, treat it with suspicion.
- Think about how you can encourage and support people in your charity to question suspicious or just unusual requests, even if they appear to be from important individuals. Having the confidence to ask 'is this genuine?' can be the difference between staying safe, or a costly mishap.

You might also consider looking at how your outgoing communications appear. For example, do you send unsolicited emails asking for money or passwords? Will your emails get mistaken for phishing emails, or leave people vulnerable to an attack that's been designed to look like an email from you? Consider telling your trustees, staff and volunteers what they should look out for (such as *'we will never ask for your password'*, or '*our bank details will not change at any point*').

Tip 3: Check for the obvious signs of phishing

Expecting your trustees, staff and volunteers to identify and delete all phishing emails is an impossible request and would have a detrimental effect on a charity's productivity. However, many phishing emails still fit the mould of a traditional attack, so look for the following warning signs:

- Many phishing scams originate overseas and often the spelling, grammar and punctuation are poor. Others will try and create official looking emails by including logos and graphics. 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'.
- Look out for emails that appear to come from a high-ranking person within your organisation, such as 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. It's most unlikely that someone will want to give you money, or give you access to some secret part of the Internet.

Tip 4: Report all attacks

Make sure that your trustees, staff and volunteers are encouraged to ask for help if they think that they might have been a victim of phishing, especially if they've not raised it before. It's important to take steps to scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred.

Do not punish staff if they get caught out. It discourages people from reporting in future, and can make them so fearful that they spend excessive time and energy scrutinising every email they receive. Both these things cause more harm to your charity in the long run.

If you believe that you or your charity has been the victim of online fraud, scams or extortion, you should report this through the Action Fraud website[28]. If you are in Scotland contact Police Scotland on 101. You should also report it as a serious incident to the Charity Commission via RSI@charitycommission.gsi.gov.uk, or the Office of the Scottish Charity Regulator (OSCR) in Scotland[29]. The OSCR has also produced guidance on fraud and cybercrime[30], and a separate factsheet[31].

Reporting demonstrates that you have taken responsible action to identify problems within your charity. It also helps the Commission to gauge threats that may affect the wider sector, and to take steps to address these with targeted advice and guidance. For more information, see How to report a serious incident in your charity[32].

Tip 5: Check your digital footprint

Attackers use publicly available information about your charity and staff to make their phishing messages more convincing. This is often gleaned from your website and social media accounts (information known as a 'digital footprint').

- Understand the impact of information shared on your charity's website and social media pages. What do visitors to your website need to know, and what detail is unnecessary (but could be useful for attackers)?
- Be aware of what your trustees, staff and volunteers give away about your charity online.
- Help your staff understand how sharing their personal information can affect them and your charity. This is not about expecting people to remove all traces of themselves from the Internet. Instead support them as they manage their digital footprint, shaping their profile so that it works for them and the charity.
- CPNI's Digital Footprint Campaign contains a range of useful materials (including posters and booklets) to help charities work with employees to minimise online security risks.

[28] http://www.actionfraud.police.uk/report_fraud

[29] https://www.oscr.org.uk/

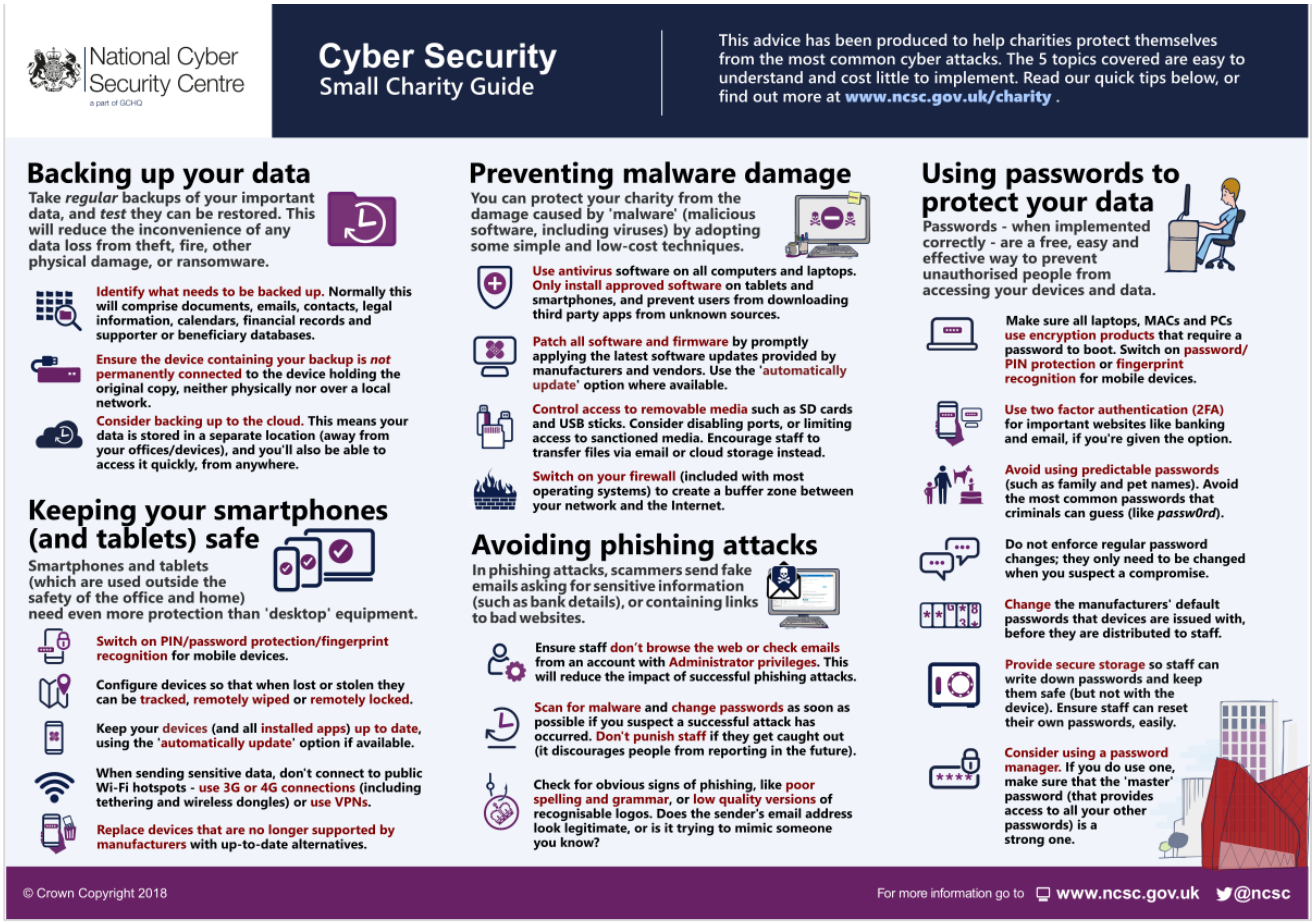
[30] https://www.oscr.org.uk/guidance-and-forms/fraud-how-to-reduce-the-risks-in-your-charity

[31] https://www.oscr.org.uk/guidance-and-forms/managing-a-charity-guidance/cybercrime-factsheet

[32] https://www.gov.uk/guidance/how-to-report-a-serious-incident-in-your-charity

Infographic summary

The following infographic summarises the tips provided in this guidance. You can download a high-quality PDF version of this at the NCSC website at http://www.ncsc.gov.uk/charity .



Glossary

2FA	Two factor authentication. The use of two different components to verify a user's claimed identity. Also known as multi-factor authentication.
Antivirus	Software that is designed to detect, stop and remove viruses and other kinds of malicious software.
Backup	A copy of a file or other item of data made in case the original is lost or damaged.
Breach	An incident in which data, computer systems or networks are accessed or affected in a non-authorised way.
BYOD	Bring Your Own Device. An organisation's strategy or policy that allows employees to use their own personal devices for work purposes.
(the) Cloud	Where shared computer and storage resources are accessed as a service (usually online), instead of hosted locally on physical devices. Well known examples include; Apple iCloud, Microsoft 365, Dropbox, Amazon Web Services.
Cyber Attack	Malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means.
Default Password	The password that your device or service was issued with. The NCSC recommends changing these as soon as you receive the device (or set up the service), as default passwords are often easy to guess or identical to other users'.
Encryption	A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.
EUD	End User Device. Collective term to describe modern smartphones, laptops and tablets that connect to an organisation's network.
Firewall	Hardware or software which uses a defined set of rules to constrain network traffic to prevent unauthorised access to or from a network.
Malware	Software intended to infiltrate and damage or disable computers. Shortened form of malicious software.
Mobile Data (3g/4g)	The networks that your phone (and some tablets and laptops) use to communicate, without needing to be connected to Wi-Fi.
Patching	Applying updates to firmware or software to improve security and/or enhance functionality.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that makes data or systems unusable until the victim makes a payment – The 'WannaCry Attack' in 2017 was an example of Ransomware.

Social Engineering	Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker.
Spear-Phishing	A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.
Spyware	Malware that passes information about a computer user's activities to an external party.
VPN	Virtual Private Network. A VPN allows you to connect securely to your organisation's network whilst away from your normal office.
Virus	Programs which can self-replicate and are designed to infect legitimate software programs or systems. A form of malware.
Wi-Fi	A facility allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.

National Cyber Security Centre
a part of GCHQ

Cyber Security:
Small Charity Guide

© Crown Copyright 2018

Photographs produced with permission from third parties. This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.