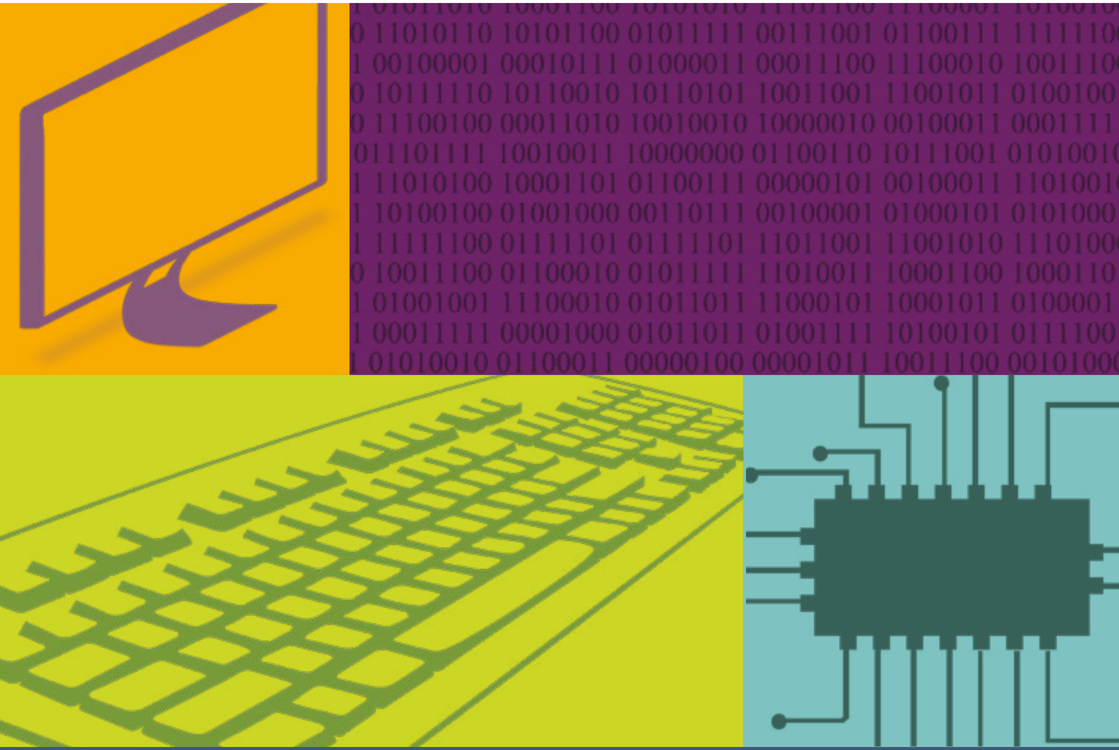
OSCR
Scottish Charity Regulator



Cybercrime Factsheet

November 2020
Scottish Charity Regulator

Introduction & Contents

Fraud comes in many forms and anyone can be a target. Cyber-crime is any criminal act committed by digital means.

With more organisations using digital methods of operating it is essential that charities protect themselves against any potential attacks. It is important charities report incidents of cybercrime and fraud both to the appropriate authorities, and to OSCR. We need to understand the scale of what we understand to be a growing problem, and potentially one of the biggest threats that charities face in a modern world.

This factsheet is split into sections that explain steps that charities can take to protect themselves and what to do if your charity has been the victim of cybercrime. It has been produced in conjunction with Alison Stone, Cyber Resilience Co-ordinator for the third sector, who is based at SCVO.

Cybercrime and risk

What is a cyber attack?

A cyber-attack is where someone maliciously tries to:

- Damage – for example by deleting a database (potentially also stealing a copy of it at the same time)
- Disrupt – for example a Denial of Service Attack, where someone uses a program to visit a website from lots of different devices at once in an effort to overload its capacity and cause it to crash.
- Gain unauthorised access – for example by trying to guess your email password or getting you to hand it over to them by filling in a legitimate looking form. This will then give them access to your emails and any accounts where you are using the same email and password combination.

What is cyber security?

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

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

Cyber security is important because smartphones, computers and the internet are now such a fundamental part of modern life, that it is difficult to imagine how we'd function without them. From online banking and shopping, to email and social media, it is more important than ever to take steps that can prevent cyber criminals getting hold of our accounts, data, and devices.

Why are charities at risk?

Charities hold funds, personal, financial and commercial data

- Funds and data have a financial value to a cyber-criminal, whether to use to try and attack another person or to sell on to other criminal entities.
- In holding funds and data, often with low levels of security protecting it; charities become an easy target to cyber criminals and attackers.
- While most small charities will not hold a lot of funds, cyber attackers approach most things with a cost vs benefit analysis. If they can get a quick win and get say £1,000 from a poorly protected organisation it's probably still worth their while. If you put in place the simple, sensible controls, it will add a layer of protection that could be the difference between you being an attractive target or one that is too time/cost consuming to be worthwhile to criminals.

Potentially a route into a 'bigger fish' such as a local authority or corporation

- Many charities, through commissioned services, or grants from local authorities, are now fulfilling roles which were previously done by government, local authorities or larger companies. It is likely that to carry out these roles, the charity will need to share systems with the 'bigger fish' and a cyber attacker could use the charity as a route in; causing significant damage along the way.

Low levels of awareness, particularly amongst smaller charities

- The NCSC's assessment conducted in late 2017 found that there were low levels of awareness, particularly amongst smaller charities who do not perceive themselves as a target; or even holding anything of value to an attacker.

Culture of trust

- To be able to achieve their goals, charities have to be open, transparent and trusting of beneficiaries and the public. For example, it is not uncommon for someone to call or email a charity and offer to give them money, no strings attached. This would never happen in a business, because everything is a commodity; which means that charities, by their very nature are potentially open to having their trust exploited by criminals.

How are charities at risk?

Ransomware and extortion

Ransomware is where a cyber attacker gains access to an organisations systems or website, locks it down so you can't access it and then offers to unlock it in exchange for payment of a ransom. Charities may be targeted directly, be inadvertently affected by an attack aimed elsewhere, or by mass indiscriminate campaigns seeking to exploit as many victims as possible. Attackers may not only steal or deny access to data; they may delete or change it.

Extortion is where a cyber attacker steals data or commercial information and threatens to release it publicly or sell it if you don’t pay them a fee. Charities involved in the protection of vulnerable individuals or holding sensitive medical data could be particularly susceptible to this form of extortion.

Malware and spyware

Malware simply means malicious software. Attackers often try to get malware and spyware onto an organizations' systems and devices to steal data or look for other more valuable leads for to use in future criminal acts. There are many ways to get malware onto your system or devices but common ones are by clicking on links on phishing emails or by visiting unsecure websites.

Business email attacks (phishing)

There are many ways that criminals can use email to launch cyber-attacks. The most common ones are:

- Tricking staff, trustees or volunteers into clicking on a link or attachment that seems genuine but in reality contains malicious software or sends you to a fake website.
- Tricking employees with financial authority into transferring money to criminals is increasing. A UK charity lost £13,000 after the email of its CEO was hacked and a fraudulent message sent to the charity's financial manager with instructions to release the funds.
- Gaining access to a staff member/volunteer work email address to send emails purporting to be from the organisation to build trust with a third party. This could be hugely damaging to your charity's reputation if it led to losses by a third party or supplier of yours.

Fake organisations and websites

Criminals exploit the credibility and appeal of charities to trick donors into giving money to what appears to be a legitimate charity. This is often achieved through the creation of fake organisations and accompanying websites.

Criminals react quickly to exploit disasters and global events to steal donations. Although not directly targeting charities by cyber means, this activity has potential financial and reputational ramifications for genuine charities.

What steps can your charity take to protect itself?

There are a lot of resources with great advice on how to improve the cyber resilience of your third sector organisation. The advice below is taken from the NCSC Small Charity Guide which was published in March 2018 and gives you simple steps to protect your charity.

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 should take regular backups of their important data. By doing this, you are ensuring your charity can still function following the impact of flood, fire, physical damage or theft and you will be more resilient to cybercrime.

Identify what you need to back up

Your first step is to identify your essential data. That is, the information that your charity could not function without, your "crown jewels". 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.

Keep your back up separate

Whether it is on a USB stick, on a separate drive or a separate computer; your back-up is no good if its left connected to the device that is stolen, damaged or suffered a cyber attack. Access to back ups should also be restricted so that they are not accessible by all staff or volunteers as this will reduce the risk of someone accidentally damaging or deleting the back up.

Consider the cloud

You have 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 means your data is in a physically separate location meaning it cannot be damaged by a fire, theft or loss in your charity.

Cloud Service Providers can supply your charity with data storage and other services without you needing to invest in expensive hardware up front. They typically have higher levels of security than you could achieve for a similar investment to your subscription. Most providers offer a limited amount of storage space for free, and larger storage capacity for minimal costs to charities.

If you operate in a rural area with poor internet speeds, backing up to the cloud might not be possible due to the speed needed to upload regularly. The required internet speed is usually available from suppliers, and you can then compare this to the speed provided by your broadband supplier.

Make it part of your everyday routine

Backing up is not an exciting task, and there are always things that are ‘more important’ but the majority of cloud storage now allows you to make back-ups automatically. Ensuring this is turned on will allow you to always have the most up to date version of your files if something goes wrong and also means you don’t have to think about it every day.

Protecting your charity from Malware (malicious software)

Antivirus software

Antivirus software is included for free with most popular operating systems. It is usually just a case of making sure it is turned on. Antivirus should be used on all computers and laptops. This is a hugely simple but effective way to detect and prevent malware from infecting your systems.

Smartphones and tablets differ in their need and availability of antivirus. The NCSC has produced guidance for the popular types of devices (visit ncsc.gov.uk) or consult your device supplier.

Prevent users from downloading ‘dodgy apps’

Users should only have enough ‘permissions’ on their account to carry out their role at the charity. By giving them permissions such as ‘administrator’ they have the ability to download a piece of dodgy software; probably by accident but it could have very damaging consequences.

Check what permissions your users have an unless they are in charge of the IT, make sure they do not have an administrator account. Some organisations may want to consider looking at our “bring your own device” guidance at www.ncsc.gov.uk/guidance/byod-executive-summary

Keep everything up to date

All of your devices will prompt you to ‘download and install’ the latest update. Carrying out these updates (a process often called patching) is one of the most important things you can do to improve security. Each update brings with it fixes for new vulnerabilities or defences against known attacks. If you have the option to set your devices to update automatically then select that. It will mean you do not need to worry about it again.

Control the use of USB drives

It is common practice to use USB drives or memory cards to transfer files between users and other organisations. However it only takes one person to put an USB stick or memory card infected with malware into one of your computers and it could cause significant damage to your systems. To counter this you can:

- Block access to USB ports on your computers – make a policy that all files should be transferred over email or cloud storage instead
- Use an antivirus package that scans USB sticks when you plug them in before it lets you open them
- Only allow approved USB sticks which are monitored and audited regularly. Some charities have a couple of numbered USB sticks which must be hung up in a secure cupboard at the end of each day and users are only allowed to use these.

Switch on your firewall

Firewalls simply create a buffer zone between your network and the internet. Most popular systems include a firewall for free, all you need to do is make sure it is switched on.

Keeping your smartphones and tablets up to date

Smartphones and tablets leave your office and home on a regular basis, it's the benefit of their portability; however, it is also a weakness as they exposed to things that devices that are solely based in the office aren't such as being lost or stolen and connecting to public Wi-Fi which can be insecure or being run by cyber criminals.

Switch on password protection

Virtually every device, whether it is a phone or tablet (like an iPad) can be locked with a password or pin number. These security settings are not always enabled when you first receive the device, simply go to your settings menu and set your pin/password. Make sure it is not the same across all your devices and isn't the same and the pin number for your debit/credit cards.

Prepare for lost or stolen devices

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. These are very handy if there is sensitive data stored on the device which you don't want to fall into the hands of others. Most devices allow 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

As all devices are different, it's easiest to look at the support pages on the website of your device manufacturer (for example Apple, Samsung, Windows, Google etc.).

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 and if your devices allows it you can save a lot of time by turning on automatic updates in the settings menu.

Its best practice to show your trustees, staff and volunteers how to check for updates and install them when you first give them a device, this opportunity also allows you to explain how important they are.

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.

Similarly to keeping your device up to date, most apps now allow you to turn on auto-update in your settings which will make sure you don't forget.

Use public Wi-Fi safely

We know that it is incredibly convenient to connect to Wi-Fi in public spaces when you are out and about, both personally and professionally. However, 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, somebody could access what you are working on and your private login details for many apps and websites you are using.

The simplest way to avoid the risk is not to connect to public Wi-Fi, instead use the 3G/4G connection on your smartphone or tablet. 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.

If you're regularly out of the office or handle sensitive data, it's worth asking your IT provider about setting up a Virtual Private Network (VPN) which encrypts your data before it is sent across the internet.

Using passwords

Switch on password protection

As with your mobile devices, one of the best and easiest ways you can protect your devices and accounts is by using passwords (or pin numbers on some devices). You can also use other authentication methods such as fingerprint or 'face unlock', this means you won't be needing to enter your password as often.

Use two factor authentication

Two factor authentication 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 is sent to your smartphone (or a code that is generated from a bank's card reader) that you must enter in addition to your password. Using this service means that an attacker needs to have something you know (your password) and something you have (card reader/phone to receive text message) which makes it much more secure.

For detailed guidance on how to turn on two factor authentication on most well-known services visit www.turnon2fa.com

Avoid 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 on setting secure passwords that is easy for them to understand.

A good rule is to use three random words to create a strong password. Avoid using the most common passwords, which criminals can easily guess (such as P4$$w0rd or QWERTY).

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. You should only give 'administrator' access to those who need it or manage the systems like the IT person.

Help users cope with 'password overload'

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 may also have heard of 'password managers', 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 is a strong one, for example by using three random words. Have a look at the star ratings in your devices App Store to make sure you're choosing a reputable one. The NCSC has further advice on password managers on their website – www.ncsc.gov.uk

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. Often credentials they are issued with are as simple as Username: Admin; Password: Password – which means if you know what they are then so does a cyber attacker.

Avoid all 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 or steal your details to sell on to a 3rd party.

Configure accounts appropiately

It is important to make sure that your charity's IT is set up to protect your charity if you suffer a phishing attack. Simple steps you can take are;

- Give everyone their own account
- Make sure users have the 'least privileges' needed to carry out their role – for example only able to access data that they need to see
- Only give full system access (Adminstrator access) to those who need it – for example the person that manages your IT.
- Use two factor authentication (2FA) on your important accounts such as email. This means that even if an attacker knows your passwords, they still will not be able to access that account.

These steps will help minimise the damage that is caused by preventing an attacker gaining access to as much of your system as possible.

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. For example, do your users know who your organisation works with – would they open an email from just anyone? 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. Work with your trustees, staff and volunteers to see how you can help make these tricks less successful. For example;

- Do users know what to do with unusual requests, and where to get help?
- Would users be willing to challenge an important individual (a trustee perhaps) if the request was unusual or asked them to circumvent the normal process?
- 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 do not do business with, treat it with suspicion.
- Encourage staff to have the confidence to ask 'is this genuine?' can be the difference between staying safe, or a costly mishap

Know 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 there are some obvious signs which you can help your users be on the look out for;

- Poor spelling, grammar and punctuation
- Is the design (and quality) what you would expect from a credible, large organisation?
- Is it addressed to you by name, or does it refer to 'valued customer', or 'friend', or 'colleague'?
- 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 asking you to do something they would not normally ask.

- If it sounds too good to be true, such as a large donation in return for banking details, it might well be. Try picking up the phone (using a number you already know to be correct) and check with the sender that it is genuine.

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’).

Check whether the information you have on your website is completely necessary for your normal visitors - could attackers utilise information about managers or trustees to trick an unsuspecting staff member or volunteer?

Help your staff understand how sharing their personal information can affect them and your charity. People should not remove all trace of themselves from the internet but understanding the consequences of publicising information about themselves and your charity will help stop your charity becoming a target.

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. It is important to get the person who manages your IT 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.

Where to get advice for your third sector organisation

National Cyber Security Centre (NCSC)

The main source of good cyber advice here in the UK is the National Cyber Security Centre (NCSC) who are the cyber resilience part of the intelligence agency, GCHQ. NCSC was launched in October 2016 and provides a single point of contact for SMEs, larger organisations, government agencies, the general public and departments. They also work collaboratively with other law enforcement, defence, the UK’s intelligence and security agencies and international partners.

The NCSC’s mission is to "make the UK the safest place to live and work online” and, as part of this, they provide lots of useful advice to both organisations and individuals. Of particular interest for the third sector are the following publications:

- Small Charity Guide
- Cyber threat assessment for the charity sector
- The Board Toolkit
- Top tips for staff e-learning
- New – Home working guidance during Covid-19

Test the cyber preparedness of your organisation by using the NCSC tool Exercise in a Box.

There are also a range of cohosted training videos for the third sector in association with Charity Digital.

Other sources of Cyber Resilience information for Charities in Scotland

- Scottish Government Third Sector Action Plan
- Get Safe Online: a UK website offering free expert personal and business advice
- Take 5 to stop Fraud: a UK initiative which offers straight-forward and impartial advice to help everyone in the UK protect

themselves against financial fraud

- Scottish Business Resilience Centre – Incident Helpline
- SCVO remote working guides - Cyber

Response and Recovery

Should your charity become subject to a cyber-attack or data breach, there is support available to help you:

- Review the NCSC Response and Recovery guidance
- Report to Police Scotland on 101
- Contact the Scottish Business Resilience Centre's Incident Helpline for practical advice and remedial action
- Contact the Information Commissioners Office (ICO) within 72 hours if you suspect a data breach that may impact the rights and freedoms of individuals included within the breach
- Follow the OSCR notifiable event procedure.

The Scottish Charity Regulator (OSCR)
2nd Floor
Quadrant House
9 Riverside Drive
Dundee
DD14NY

T 01382 220446
E info@oscr.org.uk
@ScotCharityReg
ScottishCharityRegulator
www.oscr.org.uk

This booklet was updated in November 2020