SLCVO Skye and Lochalsh Council for Voluntary Organisations

Cyber Resilience - Keeping safe online

Introduction

It is nearly impossible now to imagine life without digital technologies. Almost every aspect of our daily lives relies on the internet, data and digital devices. We use them as individuals and as organisations. We use mobile phones, computers, laptops and tablets every day for communication, for shopping, banking, marketing, keeping up with friends and access to work.

In addition to this much of our national infrastructure, including transport systems, utilities and government services, depends on technology and online connectivity.

The Scottish Government Cyber Resilient Scotland Strategic Framework 2025-2030 outlines the Government's commitment to continuing to improve our nation's cyber resilience. The five-year framework takes a collaborative approach to enhance digital security building on the progress made so far. It sets the strategic direction for government and national delivery partners and provides guidance for public, private and third sector organisations to strengthen their cyber resilience

"Scotland's third sector organisations play a central role in our communities, delivering a huge range of services and support to our diverse communities. While our increasing reliance on digital systems can have huge benefits for charities and their beneficiaries, it's vital that charities also understand the risks that this can bring.
"Building cyber resilience is about ensuring that charities, indeed all third sector organisations, can continue their work safely and securely. It's the responsibility of every trustee in Scotland to act in their organisation's best interests and that must include ensuring that their organisation treats cyber security as a key part of their work, not as an optional extra."

Marieke Dwarshuis, Chair of the Office of the Scottish Charity Regulator (OSCR)

Cyber resilience touches the lives of everyone. Our digital world now connects every person and every organisation to websites, apps, systems, data and services as part of our personal and working lives. These are things we benefit from, but we need to ensure they are safe and secure to use.

Scottish Government **Cyber Resilient Scotland Strategic Framework 2025-2030**

Cyber resilience is everyone's business. It isn't just a technical necessity – it's a national imperative Scottish Government's overall aim is that by 2030 **Scotland thrives by being a digitally secure and resilient nation.**

Underlying the Framework is the clear message that we must be **proactive**. Cyber resilience is not just about responding to threats. Being aware and prepared - i.e. being cyber resilient - takes the fear out of cyber threats. It is not only about technology. It is about making sure that we as individuals and as organisations are aware of the threats and that we have the skills and ability to respond effectively when things go wrong. It's about building strength, confidence and continuity into every part of an organisation.

SLCVO Skye and Lochalsh Council for Voluntary Organisations

What is Cybercrime and Cyber Threat?

Cybercrime is happening all the time – every second of every day. It continues to grow more intense, frequent and sophisticated.

Cyber criminals (or **threat actors)** are highly organised and are capable of effective attacks –they are intelligent, and ruthless, scanning our digital footprints all the time looking for any vulnerability to exploit.

Their motives may range from financial gain, espionage, disruption, or through ideological reasons

From lone hackers to sophisticated state-sponsored groups, threat actors work intentionally carrying out activities to harm digital systems, networks, devices or data. They are ultra organised and efficient.

They include:-

- **Cyber Criminals:** organized criminal groups (close to 5000 in the UK alone) who are financially motivated. They use ransomware, data and identity theft, and fraud.
- **Espionage /State Sponsored Threat Actors:** Government-backed groups conducting espionage, sabotage, or political disruption. They might target infrastructure such as the NHS or Water or Energy supply chains and cause major disruption as well as stealing data.
- **Hacktivists:** politically driven individuals or groups promoting a social or political cause. They are the ones behind crashing servers such as DDOS attacks.
- **Insider Threats**: Current or former employees, contractors, or partners with privileged access, acting maliciously or inadvertently.
- **Terrorist Groups**: Using cyberattacks for propaganda or to cause chaos.
- **Script Kiddies**: Inexperienced individuals using pre-made tools for minor disruptions or notoriety.

CyberScotland partnership

The CyberScotland Partnership is a collaborative leadership approach to focus efforts on improving cyber resilience across Scotland.

Partners include Scottish Government, Police Scotland, SCVO, HIE, The National Cyber Security Centre, Age Scotland, LEAD Scotland, Education Scotland, Skills Development Scotland and Young Scot.

The partners work collaboratively to:-

Increase communication and knowledge-sharing

monitor impact of the **CyberScotland Portal** as a key means for organisations, businesses and individuals seeking information, guidance and support on cyber resilience issues

support planning and progress of CyberScotland Week

co-promote materials, resources and event

consider how to support the evolving cyber security community

SLCVO Skye and Lochalsh Council for Voluntary Organisations

What is a digital footprint?

Every time we use digital technology a trail is left behind – this is a digital footprint. It is the unique, often permanent, trail of data you leave behind while using the internet, encompassing both intentional actions and unintentional data collection.

- posting on social media, sending emails, filling out online forms, or leaving reviews.
- and the trails left by those actions by the devices we use- cookies from websites we look at, your IP address, or your location.

Every second across the world approx. 4.2 millionare sent globally
41,000 posts are made on Facebook

These digital footprints are constantly being monitored by threat actors looking for any vulnerability that they can identify as a way in . Depending on their motivation this might be simply a chink in the 'armour' of your digital device, providing access to knowledge about your financial status, or something about you or your organisation that they can use to trick their way in and blackmail you.

What methods do threat actors use?

- **Malware (malicious software)** is any software that is used with malicious intent to harm systems. It is deliberately damaging to computer systems. Although the motives can be varied, many criminals are looking to disrupt operations and benefit financially. Malware attacks are rising year-on-year.
- **Ransomware** is the most common malware, and often the most harmful. Typically, ransomware involves criminals encrypting an organisation's files to make them inaccessible. They then demand money in exchange for providing you a decryption key to access to the information. More recently, ransomware is being used to describe different types of cyber extortion, including information theft.

The most common start of a ransomware attack is via **phishing emails** or by exploiting remote services, for example remote desktop protocol (RDP) which is often used by administrators to remotely connect to servers on their organisation's network.

Phishing – usually in the form of scam messages (but can be texts or voice messages) are sent by cyber criminals attempting to trick individuals into sending sensitive information, paying money, or clicking on a link which contains a virus or takes you to a fraudulent website. It relies on the person believing the message originates from someone they know or an organisation they trust. Phishing threats affect organisations of all sizes and sectors.
Some phishing is more targeted (spear phishing) where attacks are tailored to use information such as names, job roles or social media profiles to make the messages seem more relevant and believable. They rely on tricking you to think that they are from someone you know and getting you to act quickly. Commonly they might suggest a health scares, the threat of money loss, or they might indicate that unless you act your account will be compromised. Sometimes they promise time-limited 'too good to be true' offers. The intention is to get you to act, click a link which will download a malware or ask you to provide further information, such as your banking details, usernames, and passwords

Phishing attacks can put all your information at risk. A successful phishing attack can have serious consequences, including:

- theft of money
- lost, or compromised information
- damage to reputation or trustworthiness
- identity theft
- disruption to business functions

How can your organisation minimize the risks?

Whilst it is virtually impossible to avoid those digital footprints we leave behind, the good news is that there are some very simple practical things we can do to help minimize the risk they present.

Know your devices and who is using them

- Does your group or organisation know what devices it has - and who is using them? These are your **IT Assets** – mobile phones, desk tops computers, laptops, tablets, printers. Make a list or asset register and keep it up to date.
- Do individuals in your group or organisation use their own devices (known as grey devices or BYOD) for their work (paid or voluntary) Do those devices have anti-virus protection?
- Think about those old devices – what happens to them when your group or organisation disposes of them? All will have data in them and that needs to be removed and destroyed – this includes old printers.
- Does your organisation have a robust IT policy setting out clear guidelines for staff and volunteers in the use of social media and posting photographs etc

Install Anti-virus software

Make sure that all computers, laptops and tablets have antivirus software on them

Further Assistance: - The National Cyber Security Centre (NCSC) has a step by step **Cyber Action Plan** for small businesses which takes 5 minutes to go through and offers tailored practical steps to help improve your cyber resilience.
Stay protected online with a Cyber Action Plan - NCSC.GOV.UK

Read:- The Cyber Essentials Knowledge Hub includes a step by step guide for 'fully remote charities'

If your organisation or staff use mobile devices including smartphones or tablets - read the NCSC guidance on keeping your smartphones and tablets safe

Privacy Settings and User Rights

Not everyone in your group or organisation will need access to everything so make sure that you set user access rights and privacy settings appropriately and on a '*need to know*' basis.

Do not allow staff or volunteers to download apps from sources or vendors that are not checked and restrict their permissions to download from manufacturer-approved stores (like Google Play or Apple App Store).

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 offline for that specific task, with standard user accounts used for general work. **When staff or volunteers leave delete their access.**

SLCVO Skye and Lochalsh Council for Voluntary Organisations

Back up your data

Make regular backups – internally, to the cloud and to another encrypted external device.

- **Cloud Storage** - 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'.
- Restrict access to **external backup devices** (USB stick, separate drive or a separate computer) and make sure that they are not permanently connected (either physically or over a local network) to the device holding the original copy. Remember that ransomware (and other malware) can often move to attached storage automatically, which means any backup could also be infected, leaving you with no backup to recover from. Keeping external back up devices in a different location to your main devices protects your back from fire or theft.

Further Assistance

Visit the NCSC website for more information on backing up your data *Backing up your data - NCSC.GOV.UK*

NSCC infographic **Using passwords to protect your devices and data**

NCSC Using passwords to protect your data

Try an online **How Secure is My Password** tool to give you an idea on how long it would take cybercriminals to hack into your password!

Passwords

- Always use **two step verification** when you can because it greatly reduces the likelihood of successful attacks. 2-step verification (2SV), sometimes referred to as multi-factor authentication (MFA) or two-factor authentication (2FA), adds that extra layer of security.
- Create passwords that are harder to crack
  either using **3 random words** or
  15-character password with a combination of characters, numbers and symbols
- **Don't use personal information** for passwords – threat actors are scanning your digital footprint all the time and can easily work out things like birthdays, memorable dates, your likes etc.
- Change the default password on your WiFi router
- Always use **different passwords for different accounts**
- If you need to keep a note of your passwords make sure you keep any notebook secure

Identifying Phishing Emails and Scam texts

Phishing emails are becoming increasingly harder to spot as the cybercriminals get more and more sophisticated in their techniques, and some will still get past even the most observant of us.

Make sure your staff / volunteers who have access to emails are familiar with the organisation and how it works – this means that they will be better equipped to spot requests that are 'out of the ordinary'.

Make sure you do NOT to open or click on any links within an email without checking it first.

- Check the email address or URL – does it look genuine? Does the email address end in ***cn*** for example (meaning it may have come from china)?
- Look for telltale signs such as poor spelling, grammar and punctuation
- Check any logos and graphics
- How is the email addressed? Emails that do not address you by name but refer to you as 'valued customer', or 'friend', or 'colleague' could be a sign that it's a scam.
- Be suspicious of emails that ask for immediate action or suggesting a veiled threat. Look for words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.

Further Assistance:

NCSC Guidance on Phishing Infographic Phishing-attacks-dealing-suspicious-emails-infographic.pdf

Read:- The Cyber Essentials Knowledge Hub includes a step by step guide for 'fully remote charities'

- Emails requesting payments – 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, 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.
- Be wary of scanning QR codes within emails, which criminals can use to trick users into visiting scam websites.

Make sure that your staff/volunteers are encouraged to ask for help if they think that they might have been a victim of phishing**.**

Ask others in your team/organization if they have received anything similar – Screen shot the email rather than sharing it with them. Forward it to your IT service provider and to **report@phishing.gov.uk**

SLCVO Skye and Lochalsh Council for Voluntary Organisations

Adopt a Cyber Incident Response Plan

Cyber Incident Response plans should be part of your organisation's policies and procedures. SCVO have created a resource to support you with creating your own incident response plan.] SCVO-A3_Amended_screen_v3.pdf

Your board, staff and volunteers should **all** be in a position where they can feel confident in detecting a cyber threat and know how to respond when an incident takes place.

Do your staff and volunteers understand their role in helping the organisation stay safe online?

Read: - SCVO's Top Tips for Trustees

Take the free 10 minute SCVO Digital Check up and see how your organisation is doing with its cyber resilience

Incident Response Process (6 Phases)

- **Preparation:** Develop policies, playbooks, training, and tools (e.g., backups, monitoring).
- **Identification:** Define how to detect, analyse, and validate incidents (e.g., monitor SIEM, alerts).
- **Containment:** Act quickly to prevent further damage. Strategies include segmenting networks or shutting down affected systems.
- **Eradication:** Remove the cause of the incident (e.g., delete malware, disable breached accounts).
- **Recovery:** Restore systems to normal operation, verify functionality, and harden systems against re-infection.
- **Lessons Learned (Post-Incident):** Conduct a "blameless postmortem" to analyse what happened, why, and how to improve the response process.

Further assistance: -

The Scottish Council for Voluntary Organisations SCVO have a Third Sector Cyber Resilience Co-ordinator, who works closely with Scottish Government through the CyberScotland partnership, to support Scotland's third sector in their journey to becoming more cyber resilient.

They are guided by a working group, made up of a range of people from across the sector, who shape and guide a programme of work to help voluntary organisations:

- prioritise cyber risk
- protect against most common threats
- prepare for cyber incident

Read: - (SCVO) infographic on how to spot and respond to a cyber incident.

Further Reading

Charities-going-digital-top-10-Data-Privacy-Tips-6-Apr.pdf

SLCVO Skye and Lochalsh Council for Voluntary Organisations

Cyber Essentials

Cyber Essentials is a cyber security UK Government approved Cyber certification scheme. The annually renewable certification gives assurance to your organisation, your customers, partners and stakeholders that your organisation has implemented basic cyber security measures - grouped under five technical controls - to give the most effective protection against common cyber-attacks.

Cyber Essentials is the government-recommended minimum level of cyber security for any organisation in the UK. The scheme is operated under the oversight of the NCSC National Cyber Security Centre - NCSC.GOV.UK the UK's technical authority on cyber security and the public facing capability to its parent agency, Government Communications Headquarters (GCHQ).

Cyber Essentials comes in two levels:

1. an online verified self-assessment
2. Cyber Essentials Plus which includes the self-assessment and a technical audit of your systems to check that the controls are implemented correctly.

More information:- Cyber Essentials - where to start? - Cyber Essentials Knowledge Hub - Cyber Essentials Knowledge Hub

The Cyber Essentials self-assessment questions can be downloaded for free from the IASME website.https://iasme.co.uk/cyber-essentials/free-download-of-self-assessment-questions/

The cost of certification depends upon the size of your organisation that you are presenting for certification, starting from £320 for an organisation with up to 9 employees.

IASME (Information Assurance for Small and Medium Enterprises) provides cyber security certifications, helping organisations manage data security and GDPR compliance, building on the Cyber Essentials Scheme.

To see whether Cyber Essentials is right for your organisation you can access the **FREE** **Cyber Essentials Readiness Tool** and work your way through the quiz-type questions which mirror the assessment questions.

SCVO offer funding to help organisations access practical support from a Cyber Advisor to either IMPROVE an organisations cyber security, through gap-analysis and implementation of the Cyber Essentials controls or ASSURE an organisation that its existing measures align with the Cyber Essentials controls.

SLCVO Skye and Lochalsh Council for Voluntary Organisations

Who to inform

The National Cyber Security Centre (NCSC)

The NCSC has the power to investigate and take down scam email addresses and websites. You can report phishing emails to report@phishing.gov.uk and report any websites that you think are scams Report a suspicious website - NCSC.GOV.UK

Your bank

If you have provided financial information to what you now think is a scam – always let your bank know.

Police Scotland

If you think you have provided personal information to a scam website, have lost money or have been hacked as a result of responding to the call, you should report this to **Police Scotland** (101 for non-emergencies or 999 in an emergency).

If you are a business, charity or organisation under a cyber-attack call Police Scotland letting the call handler know your circumstances, you should also report to OSCR and the SCVO.

Information Commissioners Office (ICO)

If your organisation experiences a cyber-attack always work on the assumption that it may have resulted in a **data breach** and alert the **Information Commissioners' Office** within 72 hours of being aware of the data breach. UK GDPR data breach reporting (DPA 2018) | ICO

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay. This should be part of your communications strategy within your Incident Response plan.

You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority or the affected individuals, or both.

You must also keep a record of any personal data breaches, regardless of whether you are required to notify.

OSCR

If your group is a registered charity in Scotland then you must also report cyber-crime to OSCR via their Raise a Concern form.