acosvo
For Scotland's Third Sector Leaders

Protect Your Network

Top Tips to Improve Cyber-Security

Top Tips for Chief Officers

Back-Up Your Data

Ensure there are *regular* back-ups of your essential data, and safely store the back-up separately from the main source (e.g. in the cloud, or on an external hard-drive in a different building).

Use Strong Passwords on All Your Devices

The most secure passwords consist of three or more words. Use strong passwords on any device used for work purposes (even staff's personal phones that can access emails).

Turn on 2nd Factor Authentication

2nd Factor Authentication (2FA) is used so that even if someone knows your password, they still need something else (like a code texted to your phone) to access your account. Turn it on for your emails, cloud storage, and even social media.

Install Anti-Malware Software

Malware and viruses are malicious software that can harm your organisation's computers. Prevent malware by installing anti-virus software on all devices and making sure staff know to keep it enabled.

Keep your Devices Up-To-Date

Updates can be annoying when they take a while to install - but they're used by manufacturers to keep your devices protected from new threats. Take a minute to turn on your devices' auto-updates feature, and then you never have to worry about it again.

Top Tips for Chief Officers

Learn to Spot the Signs of Phishing

Phishing is when someone pretends to be from a trustworthy source to trick you into giving up important information. Take Five can teach you and your staff the key signs of phishing.

If You Suspect Phishing: TAKE FIVE

The most common sign of a phishing attempt is a sense of urgency from the perpetrator. Stop. Slow down. Take a moment. Take another. Take five minutes to think it over before responding – even if that means ending the call and phoning back later.

Report any Phishing Attempt

Encourage your staff to report a suspected phishing attempt – even if they've already clicked. Foster a "no-blame" culture so incidents are reported and learned from.

Use Mobile Device Management Software

Install Mobile Device Management software on your devices. This will allow you to track, lock, or even wipe the device remotely, should it be lost or stolen.

Don't Connect to Unknown Wi-Fi Sources

Always find out who's controlling the wi-fi before you connect (just because the wi-fi has the same name of the coffee shop you're in, doesn't mean it's theirs).

Top Tips for Boards

Put Cyber-Security on your Risk Register

Cyber risks include computer viruses and malware on any of your networks or devices, criminal activity (fraud and extortion), and loss of data by accident or a deliberate act. Make sure these topics are on your **Risk Register** and board agenda, and discussed regularly.

Manage Administrator Privileges

Staff should only have enough network access as required to perform their role. Use “admin accounts” only for their intended purpose; and use standard user accounts for general work.

Have Robust Mobile-Working Policies

Mobile devices such as phones, tablets, and laptops provide huge advantages in terms of flexible working; but if staff are using personal devices for work purposes, that could be a risk. Make sure your organisation has policies and practices regarding Mobile Device Management Software.

Raise Awareness within your Staff Team

Make sure staff are thinking about Cyber-Security too. Consider further training, and/or recruiting any necessary skills through specialised consultants or volunteers.

Top Tips for Boards

Have an Incident Management Policy

Post-incident analysis provides insight that can help you reduce the likelihood of incidents occurring in the future and reduce their potential impact. Foster a “no-blame” culture so incidents are reported and learned from.

Monitor Cyber Risks

The Cyber Security Information Sharing Partnership (CiSP) is a joint industry and government initiative that shares news and updates about cyber threats. Register your organisation now for free, and ensure members of your staff receive these notifications.

Develop Anti-Malware Policies

Viruses and malware are malicious software that can harm your organisation’s computers. Prevent your network being infected with policies to keep devices up to date, keep firewalls switched on, and keep anti-virus and anti-malware software enabled.

Become Cyber-Security Accredited

There are many cyber-security accreditations out there, which will take members of your staff and board teams through the essential information they need to know to mitigate risks. One option is Cyber Essentials.

The vast majority of organisations in the UK rely on digital technology to function.

Good cyber-security protects that ability to function, and ensures organisations can exploit the opportunities that technology brings. Cyber-security is therefore central to an organisation's health and resilience.

- The National Cyber Security Centre

You can find this guide at

www.acosvo.org.uk/acosvo-research-guidance

Next Steps:

These top tips should be considered only a starting point to making your organisation more cyber-secure.

For more information about all of these tips, including more detailed templates and guides, look for:

National Cyber Security Centre: Small Charity Guide

www.ncsc.gov.uk/collection/charity

National Cyber Security Centre: Board Toolkit

www.ncsc.gov.uk/collection/board-toolkit

SCVO: Cyber Resilience Evolution

www.scvo.org.uk/digital/evolution/cyber-resilience