Avast Business

Robust Cybersecurity on a Budget

James Bevan, Avast Senior Territory Manager

Avast Business

The Charity Sector at a Glance

There are over 200,000 charities registered in the UK with a combined annual income of around £100bn.

In England and Wales alone over 1 million people are employed in the charity sector with over 7.4 million volunteers.

https://register-of-charities.charitycommission.gov.uk/sector-data/sector-overview

A Cyber Security Breaches Survey questioned 2000 charities from September 2023 to January 2024 and it showed that 32% experienced a cyber attack in the last 12 months.

https://fundraising.co.uk/2024/04/12/almost-a-third-of-charities-experienced-a-cyber-breach-or-attack-in-last-12-months-survey-finds/

Avast Business

Why Charities Are Especially Vulnerable

1. Attractive Targets – Criminals Seek financial Gain from sensitive data
2. Limited Resources – Many Charities hesitate to divert funds from frontline services
3. Fewer Technical Controls – Often lack dedicated IT security
4. Part-Time & Volunteer Staff – High Turnover and Limited Training increases risk
5. Bring Your Own Devices (BYOD) – 64% of Charities rely on personal devices

Avast Business

Understanding the Threat Landscape - Phishing

Phishing happens when scammers try to trick you into revealing sensitive information, like passwords, credit card numbers, or personal details. They usually do this by pretending to be a trusted company, like your bank, a streaming service, or even your boss.

83% of charities reported phishing attacks in the past year (UK Government Cyber Breaches Survey 2024).

A single click can compromise your entire system—leading to **data breaches**, **financial loss**, or even **reputational damage**.

Avast Business

Phishing – Help to Protect Your Charity

1. Train Staff and Volunteers
2. Use Email Filtering Tools
3. Enable Multi-factor authentication (MFA)
4. Report Phishing attempts
5. Scan for Malware and change Passwords

Avast Business

Understanding the Threat Landscape - Ransomware

Ransomware is a type of malware (malicious software) that typically:

1. Gains access to, and blocks user access to, files or systems
2. Holds data ‘hostage’ - files, entire devices, exfiltrated (stolen) data, until:
3. The victim pays a ransom in exchange for either a decryption key, or to get their data ‘back’, or a promise not to publish or leak data in double / triple extortion attacks



Avast Business

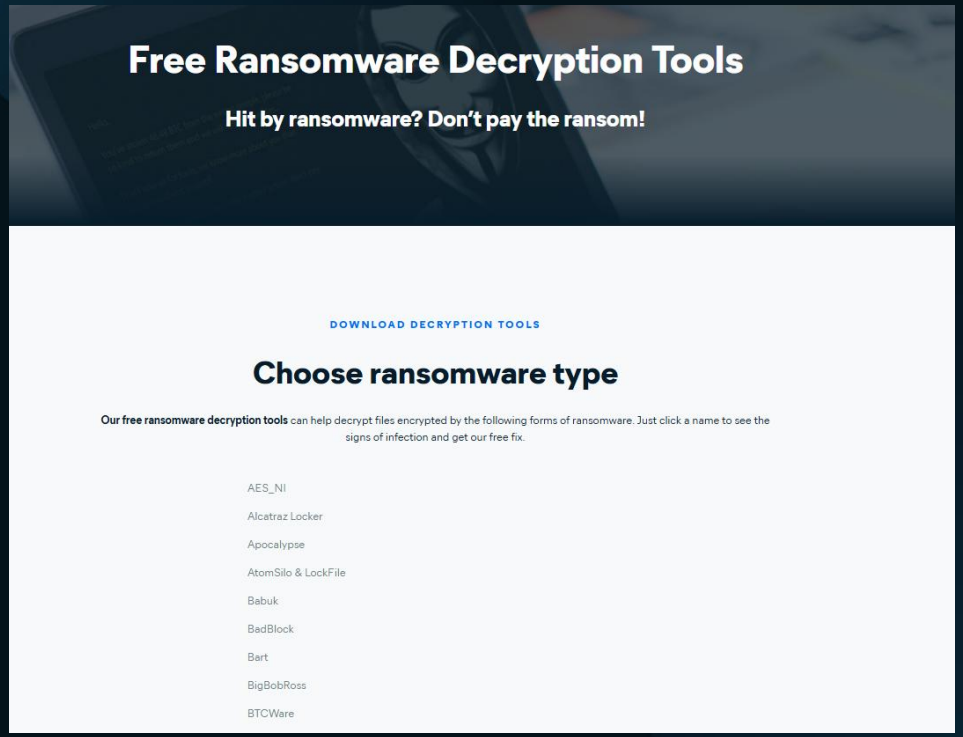
Real World Examples - Edinburgh Festival Fringe Society case study

The Edinburgh Festival Fringe Society (a charity that underpins the Festival) was victim of a ransomware attack in January 2022.

They informed their staff straightaway and arranged for disaster recovery help from a cyber security company.

Recovering from the attack cost £95k, of which only £25k was covered by insurance so the Society had to fund the difference from their charity reserves.

Avast Business



Avast Free Decryption Tools

https://www.avast.com/en-gb/ransomware-decryption-tools#pc

Avast Business

Cyber Essentials – What is it and how can it help?

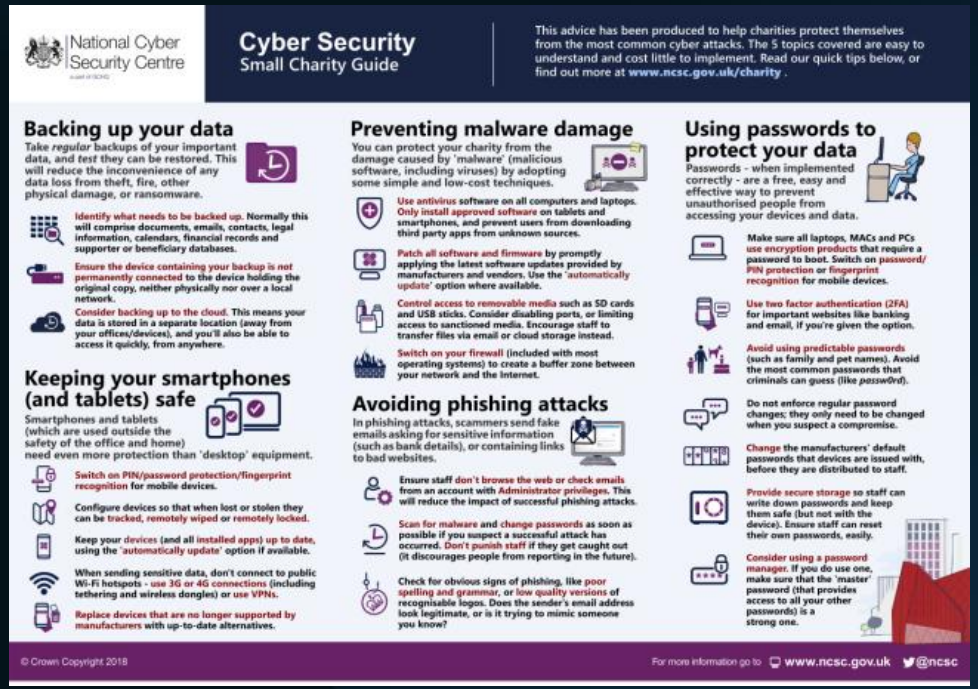
Cyber Essentials is an effective, government-backed cyber security scheme, centered on five core controls that, if implemented correctly, will help you to protect your charity against the most common cyber attacks

1. Builds Trust with Donors and Stakeholders
2. Reduces Risk of Disruption
3. Affordable and Achievable
4. Improves Staff Awareness

Cyber Essentials scheme: overview - GOV.UK

Avast Business

Resource and Support



National Cyber Security Centre

Cyber Security
Small Charity Guide

This advice has been produced to help charities protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/charity** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

Identify what needs to be backed up. Normally this will comprise documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases.

Ensure the device containing your backup is not permanently connected to the device holding the original copy, neither physically nor over a local network.

Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

Switch on PIN/password protection/fingerprint recognition for mobile devices.

Configure devices so that when lost or stolen they can be **tracked, remotely wiped or remotely locked.**

Keep your **devices (and all installed apps) up to date,** using the **'automatically update'** option if available.

When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs.**

Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your charity from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

Use antivirus software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.

Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the **'automatically update'** option where available.

Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges.** This will reduce the impact of successful phishing attacks.

Scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).

Check for obvious signs of phishing, like **poor spelling and grammar,** or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

Make sure all laptops, MACs and PCs **use encryption products** that require a password to boot. Switch on **password/ PIN protection or fingerprint recognition** for mobile devices.

Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.

Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *password*).

Do not enforce regular password changes; they only need to be changed when you suspect a compromise.

Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.

Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.

Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

© Crown Copyright 2018

For more information go to www.ncsc.gov.uk @ncsc

https://www.ncsc.gov.uk/files/Charity-Guide-v3.pdf

Avast Business

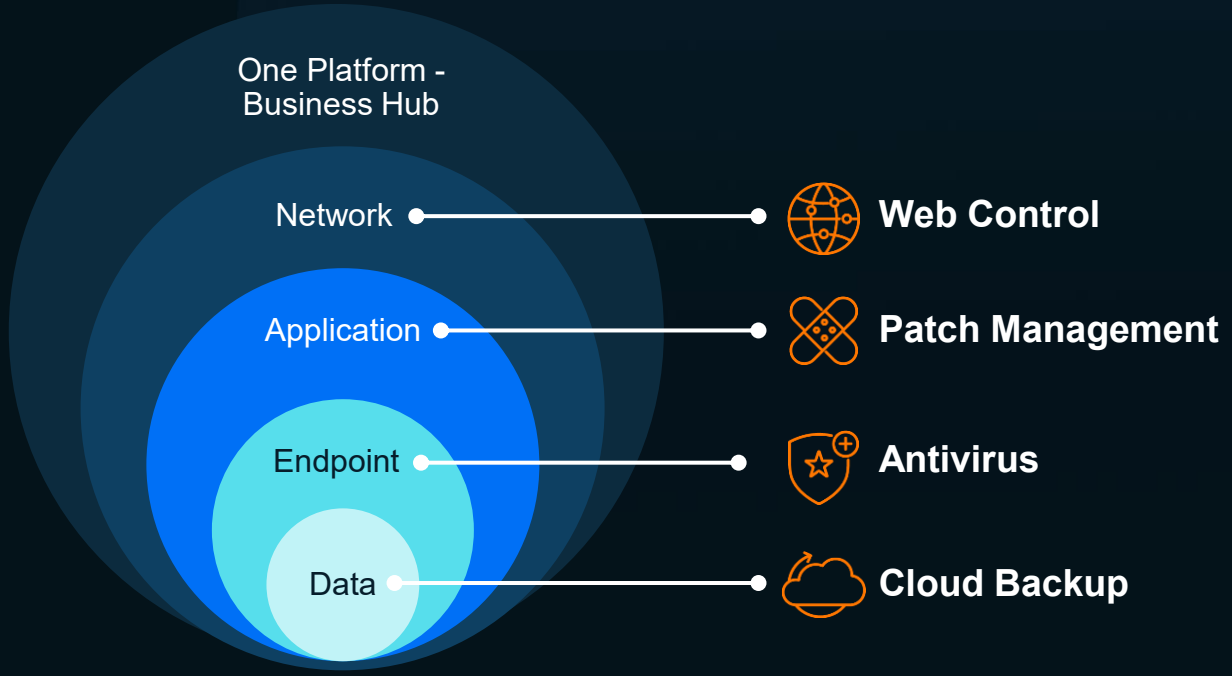
What You Can Do – 4 Key Principles (NSCS Guidance)

1. Backing Up Your Data
2. Protecting Malware Damage – Using An Anti-Virus
3. Keep All IT Equipment And Software Up To Date (Patching)
4. Don’t Connect To Unknown WI-FI Hotspots (VPN)



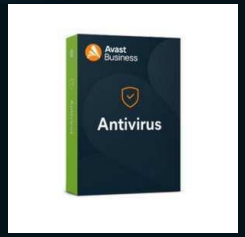
Small Charity Guide

Integrated layered security for charities managed through a single cloud platform



Avast Business

Avast Solutions available through Charity Digital



Web, File, Email, & Behaviour Shields work together to actively analyze suspicious activity, block malicious files, dangerous websites, and other threats.



Identify critical vulnerabilities and easily deploy patches across all endpoints from one central dashboard.

Avast Business

What's in a Password?

Staff hate passwords – Criminals love passwords

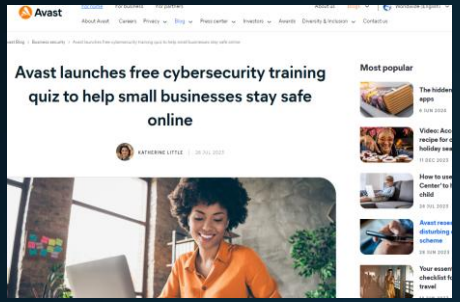
1. Encourage strong, Unique Passwords
2. Enable Multi-Factor Authentication MDF
3. Use a Password Manager
4. Avoid Reuse

Password managers: using browsers and apps to safely store... - NCSC.GOV.UK

Avast Business

Avast Blog

https://blog.avast.com/avast-launches-free-cybersecurity-training-quiz-for-smbs



Avast Academy

https://www.avast.com/c-academy

Avast Free Decryption Tools

https://www.avast.com/en-gb/ransomware-decryption-tools#pc

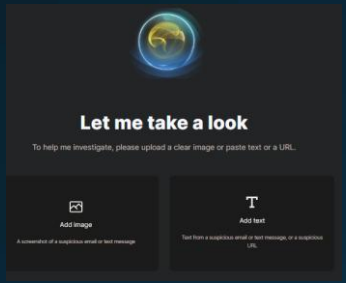


Avast Hack Check

https://www.avast.com/hackcheck/#pc

Norton Genie

https://uk.norton.com/products/genie-scam-detector



Avast Business

Conclusion – Small Steps, Big Impact!

James Bevan, Avast Senior Territory Manager

Avast Business

Q&A

Avast Business

Thank You