Avast Business

Best practices in cyber security

Paul Fenwick, Avast Sales Engineer

Avast Business

There are 200,000 charities registered in the UK with a combined annual income of £100 bn. In England and Wales alone over a million people are employed in the charity sector with over 5 million volunteers.

https://www.ncsc.gov.uk/files/Cyber_threat_report-UK-charity-sector.pdf

A survey by the Governments Department for Digital, Culture, Media & Sport published in 2022 showed that 30% of UK charities identified a cyber attack in the last 12 months. Of those attacks, 38% had an impact on the service with 19% “resulting in a negative outcome”.

Average estimated cost of all cyber attacks in the last 12 months of £4,200

https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022

Avast Business

Why is the charity sector particularly vulnerable.

Charities may feel reluctant to spend resources, money, oversight and staff effort on enhancing cyber security rather than on front line charitable work

Charities are more likely to rely on staff using personal IT (Bring Your Own Device) which is less easy to secure and manage then centrally issued IT

Charities have a high volume of staff who work part time, including volunteers, and so might have less capacity to absorb security procedures

Avast Business

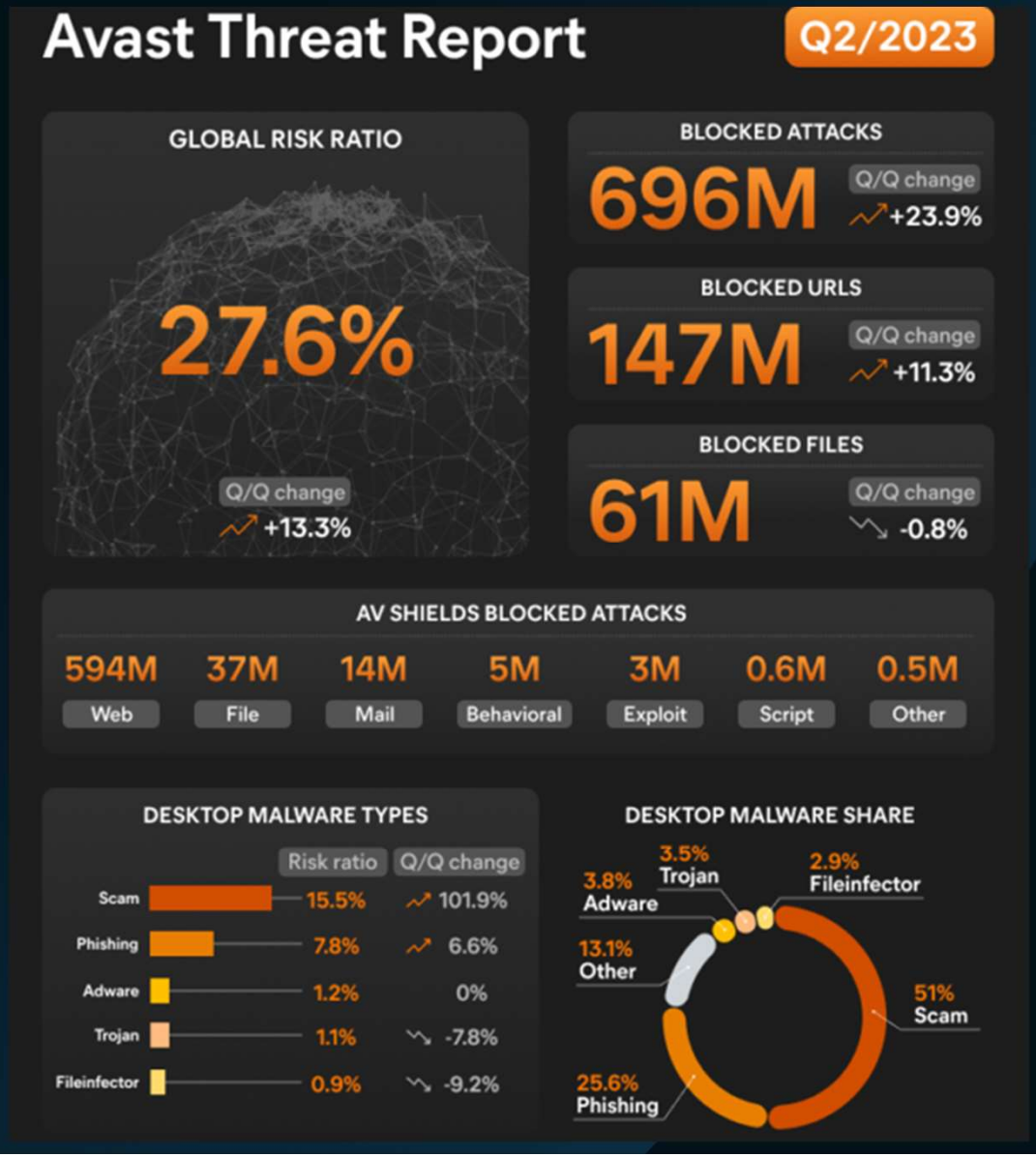
Cyber Threat activity at its highest point in 3 years, rising by 13% QonQ

Dramatic surge in social engineering and web-related threats, such as scams, phishing, and malvertising.

These threats accounted for more than 75% of our overall detections

Scams contributing to 51% ot total detections

Threat Report - https://decoded.avast.io/threatresearch/avast-q2-2023-threat-report/



Avast Business

Where to start

Backup your data

Identify data you need to back up, keeping it separate from your computer. Make backup part of your everyday procedures.

Malware Protection

Ensure Antivirus on all computers
Don't install applications from unknown vendors/sources

Patching

Make sure Operating Systems and software is up to date. Set to automatic update

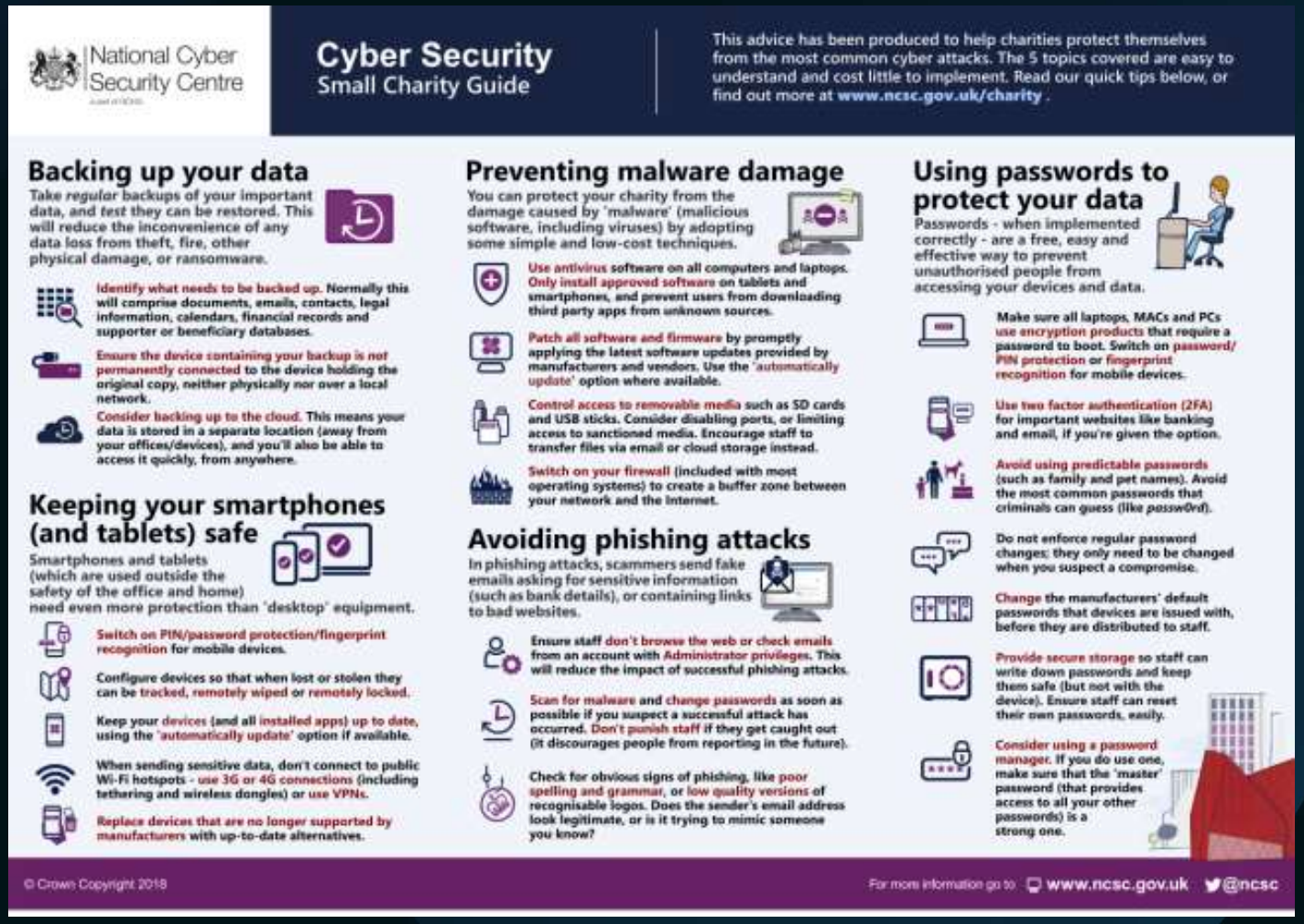
Passwords

Use strong / complex PIN or password.
Use 2FA if available.
Change default passwords.
Consider Password Manager.

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

Avast HackCheck

Avast Business



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 *passw0rd*).
- 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.

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

Avast Business

Avast Solutions available through Charity Digital

Web, File, Email, and Behaviour Shields work together to actively analyze suspicious activity, block malicious files, dangerous websites, and other threats.
Protect against zero-day attacks

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

Avast Business

Avast Blog

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

Avast Academy

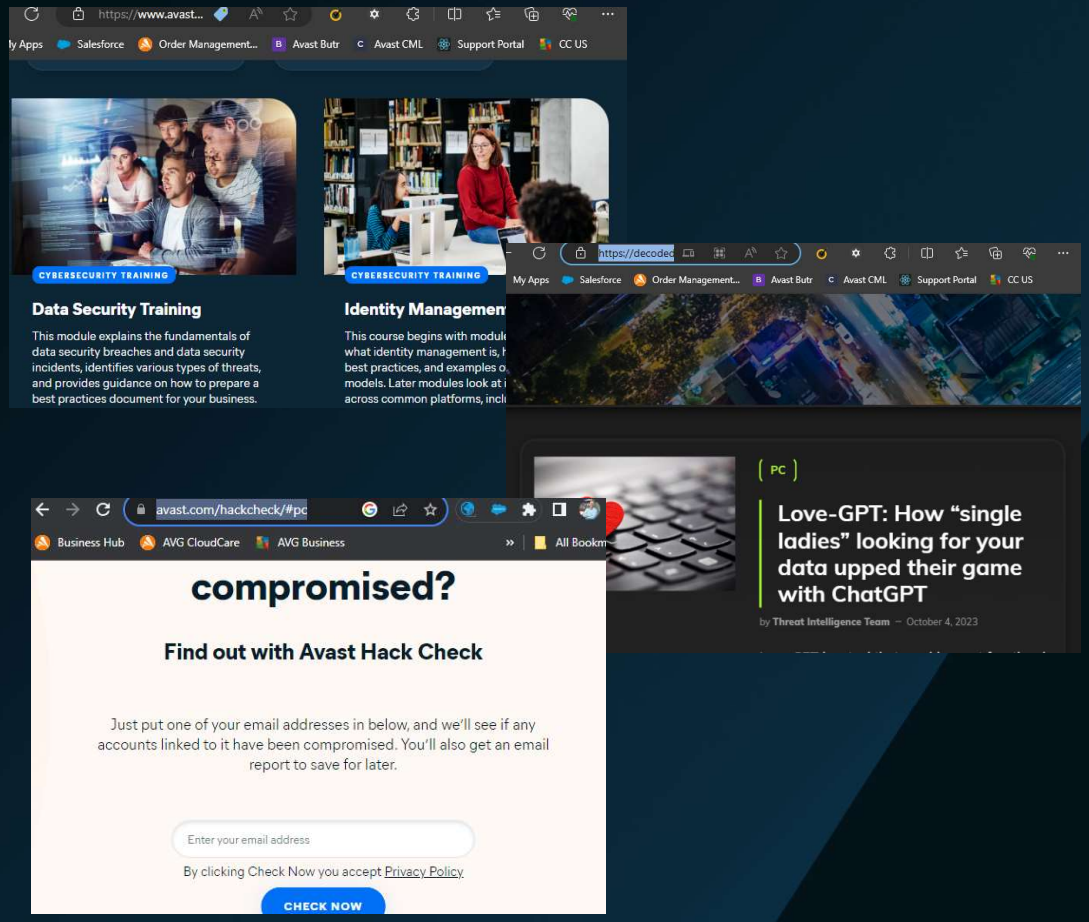
https://www.avast.com/c-academy

Avast Threat Labs

https://decoded.avast.io/

Avast Hack Check

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



Avast Business

Q&A

Thank You