Charities offered latest insight into key cyber threats to help keep out attackers

Latest report published by the NCSC outlines key threats facing the UK charity sector.

> This report is no longer available on the NCSC's website. You can access the report through The National Archives.

- New report outlines major threats facing the charity sector online, including from ransomware and phishing attacks
- GCHQ's National Cyber Security Centre issues latest threat information, case studies and guidance to help charities operate safely
- Charities encouraged to follow NCSC guidance to improve their cyber resilience to prevent future attacks

Charities have today (Friday) been issued with fresh advice on the emerging threats to their vital work from cyber attackers and the steps they can take to protect themselves.

The National Cyber Security Centre's latest Cyber threat to UK charity sector report outlines the key threats charities face in 2023 and beyond. It reflects the ongoing threat to the sector as more charities run services and fundraising online and highlights how the sector is particularly attractive to attackers seeking financial gain.

It provides case studies showing how disruptive and costly incidents can be, including a ransomware attack on the Edinburgh Festival Fringe Society costing £95,000 and a business email compromise incident which cost a hospice in the West Midlands £17,000.

The report also warns about the threat from cyber criminals taking advantage of public generosity during times of hardship by masquerading as charities to

receive donations. This has been observed recently following the Russian invasion of Ukraine.

Charities are encouraged to follow the NCSC's guidance to help improve their cyber resilience and sign up to free Active Cyber Defence tools to help mitigate the highlighted threats.

NCSC CEO Lindy Cameron said:

> "The UK's charities are doing fantastic work every day, and digital services and online fundraising are now playing a crucial role in this.
>
> "While it is right that technology should play a part in helping charities, this does open up the possibility of cyber attacks and it is important they understand the risks.
>
> "The NCSC is here to help and I urge all charities to reduce their vulnerability by reading our latest report, following our guidance and making use of the tools available to them."

Minister for Civil Society and Youth Stuart Andrew said:

> "As charity fundraising and services increasingly move online, charities are more susceptible than ever to cyber attacks and it's vital they're aware of how to stay safe and mitigate against risks.
>
> "This new report from the NCSC provides crucial guidance when it comes to protection from cyber harm and I'd urge all charitable organisations to follow the advice."

Helen Stephenson, Chief Executive of the Charity Commission for England and Wales said:

> "Charities play a crucial role in our society and in every community – they save lives, and they provide many of the services that make life worth living. All charities ultimately rely on public trust and continued public generosity.

> “So the impact of any cyber attack on a charity can therefore be devastating, not just for the organisation and those who rely on its services, but also in undermining public confidence and support.
>
> “Taking steps to stay secure online is not an optional extra for trustees, but a core part of good governance. We welcome this report and urge trustees to take early action to protect their charities from cyber harm.”

The report aims to highlight the overarching cyber threats to the sector and equip UK charities with the information they need to take action and boost their cyber resilience. It outlines how charities are vulnerable to the same cyber risks as commercial businesses but might be seen as attractive targets.

The key threats for charities to stay vigilant against include phishing, ransomware, business email compromise and fake organisations and websites.

The NCSC has published a range of free guidance and advice to help charities improve their cyber defences, including the Small Charities Guide and Free Training for Small Charities.

Charities are also eligible to take up some services offered as part of the NCSC’s Active Cyber Defence (ACD) programme. This includes free tools and services, including Web Check, Mail Check and Exercise in a Box.

Organisations looking to ensure they have baseline cyber security protections in place should consider taking up Cyber Essentials, a government-backed certification scheme, to help mitigate the majority of cyber attacks.

Smaller organisations in the charity sector can now access free support with putting these controls in place under the new Funded Cyber Essentials Programme, which the NCSC launched last month.

View the report

PUBLISHED

20 January 2023

WRITTEN FOR

Small & medium sized organisations

NEWS TYPE

General news