You’re a not for profit, but don’t let scammers profit off you

As a not-for-profit (NFP), your relationship with your community is based on trust – you receive donations because your donors trust you will use their money towards the right cause, and the beneficiaries you serve trust you to look after them.

While there’s no doubt that fraud within your organisation is an area of concern,[1] with Charity Fraud Awareness Week wrapping up, we’d like to also highlight the external risks you may face as an NFP or charity. Cyber security is an area which has gained more and more attention over the last few years. As an NFP, you may handle personal or sensitive information, so it’s especially important that you’re careful about how it is protected. Scammers have increasingly focused their efforts towards smaller organisations.[2]. This could be due to a lack of sophistication in cyber security systems and technology to protect against threats.

Here are some examples of scams NFP’s and charities may be susceptible to, how you can spot them, and minimise their impact if they do happen. All these scams have similar objectives – to gain access to personal information which can then be used for financial gain, or to install malware onto a device to enable access to your data.

Hacking

This is when a scammer gains unauthorised access to your computer network and the personal information you have stored – this could include information about your donors and beneficiaries. The information you store, particularly about the beneficiaries you serve can be extremely sensitive – from medical records/history to personal stories of the trauma they’ve faced. If this information fell into the wrong hands, not only would this be detrimental to your organisation or charity, imagine the impact it would have on your beneficiaries who may already be vulnerable?

Phishing

Phishing is an attempt by scammers to trick you into giving out personal information. For example, a scammer may contact a staff member or volunteer pretending to be from a legitimate business - such as a bank, phone or internet provider - with the objective of either gaining access to your organisation’s data. The most common methods of phishing are email and phone calls or luring your staff member or volunteer to download malware.

During the earlier days when this was starting to emerge, phishing emails were easy to spot, but due to advances in design software, scammers have perfected their craft - many phishing emails now look identical to genuine communications sent by the organisation, making them tricky to distinguish.

False billing

False billing scams request your organisation to make payment on fake invoices and bills. The invoices might be for ‘advertisements’ you’ve supposedly placed or offers to list in a directory you may not have heard of. As an NFP or charity, your support functions such as finance and marketing may be carried out by volunteers who might not have full information about the promotional activities or bills which have or have not been paid, and scammers may take advantage of these gaps in knowledge.

Malware & ransomware

Malware is any software which is harmful for your computer or device. Ransomware is a type of malware that blocks or limits access to your computer or files and demands ransom to be paid for them to be unlocked (although even if you pay the ransom, there is no guarantee that your devices will be unlocked). Warning signs also include websites which require you to download a particular program to access the content, or even seeing unusual pop-up boxes appear on your computer screen which have simple questions or a button that says 'close'[3]. If you notice your computer is suddenly running unusually slow, it may be affected by malware, so it is best to get it checked by an IT expert.

Importance of training your staff and volunteers

Whilst there are many different types of scams surfacing, the common thread is that they can be prevented, or at least minimised if your staff and volunteers are vigilant in spotting the early signs, which can allow you to act. Teaching your staff and volunteers how to catch phishing emails and malicious websites, training them to always lock devices and ensuring adequate record keeping of invoices and bills can all help to build up your line of defence against cyber security threats.

What to do if you suspect a cyber breach

If you suspect you've experienced a cyber security breach, it is important to act quickly and engage cyber security specialists. If you have cyber insurance, your insurance policy may identify specialists who can provide services. While cyber insurance policies vary, they may provide an incident manager and notification services for individuals whose privacy has been breached. Cyber insurance policies may also pay costs for legal advice, notification of authorities, data recovery, measures to improve IT security and public relations services to restore your reputation.

To find out more about Aon's Cyber Insurance, please visit our website.

1 https://www.acnc.gov.au/media/news/looking-ahead-charity-fraud-awareness-week-2019

2 https://www.asbfeo.gov.au/sites/default/files/documents/ASBFEO-cyber-security-guide.pdf

3 https://www.scamwatch.gov.au/types-of-scams/threats-extortion/malware-ransomware