An Rialálaí Carthanas
Charities Regulator

Protecting your charity from cybercrime

Protecting your charity from cybercrime

Charity trustees have a responsibility to protect their organisation's interests, as well as any potentially sensitive organisational or supporter / beneficiary data.

There are many things charity trustees, staff and volunteers can do to help protect your organisation from cybercrime including:

Keep devices and anti-virus software up-to-date:

- Make sure your devices always have the latest software installed and are protected against viruses using specific malware / virus protection software.
- Ensure the latest operating systems, browsers, and apps are installed on computers and devices that connect to the Internet.
- Encrypt sensitive data and install remote locking and blocking / wiping, in the event that the device is lost or stolen.
- Make sure that you set your devices to update the operating system and malware protection automatically.

If you are unsure how to check whether your devices and virus software are up-to-date, reach out to others within your organisation to identify someone who has the technical skills to assist; if that is not possible then go outside your organisation for IT assistance. Suppliers of laptops, tablets and phones will also be able to advise you on required software updates.

Set strong passwords:

- Ensure you have set strong passwords for your devices and email. A strong password is one which is long, ideally 12-15 characters, and contains a random mix of upper and lower case letters, numbers and characters
- Regularly change passwords and do not share them
- Use different passwords for each application / website

Make sure you keep regular backups of your data:

Cyber criminals are increasingly using ransomware to infiltrate systems and lock down data. They then seek payment to release it.

If you are unsure whether backups of your data are being taken regularly and can be restored easily, or you do not know who is responsible for taking backups, check with others within your organisation to ensure that this is being done. If it is not, make sure a process is put in place immediately to ensure regular backing up of data. If this is not possible, go outside your organisation to secure the required technical expertise.

If your device has been locked by ransomware, seek professional advice from a trustworthy source.

Always use a secure network connection:

When working remotely never use public Wi-Fi, e.g. that offered on public transport, in cafes, airports etc. or a Wi-Fi connection which does not require any kind of log in or screening before you access it.

Beware of Phishing:

Phishing is a crime in which a target is contacted by email, telephone or text message by someone posing as a legitimate institution, such as a bank, government office or well-known organisation, in an attempt to trick them into providing sensitive data such as personal information, bank and credit card details, PINs or passwords.

Take extra caution with every email, phone call, voicemail or text message you receive and verify the identity of the person you are dealing with. If you are unsure, get in touch with the institution / person that the communication claims to be from using a different contact method first, and verify the source before providing any personal or confidential information.

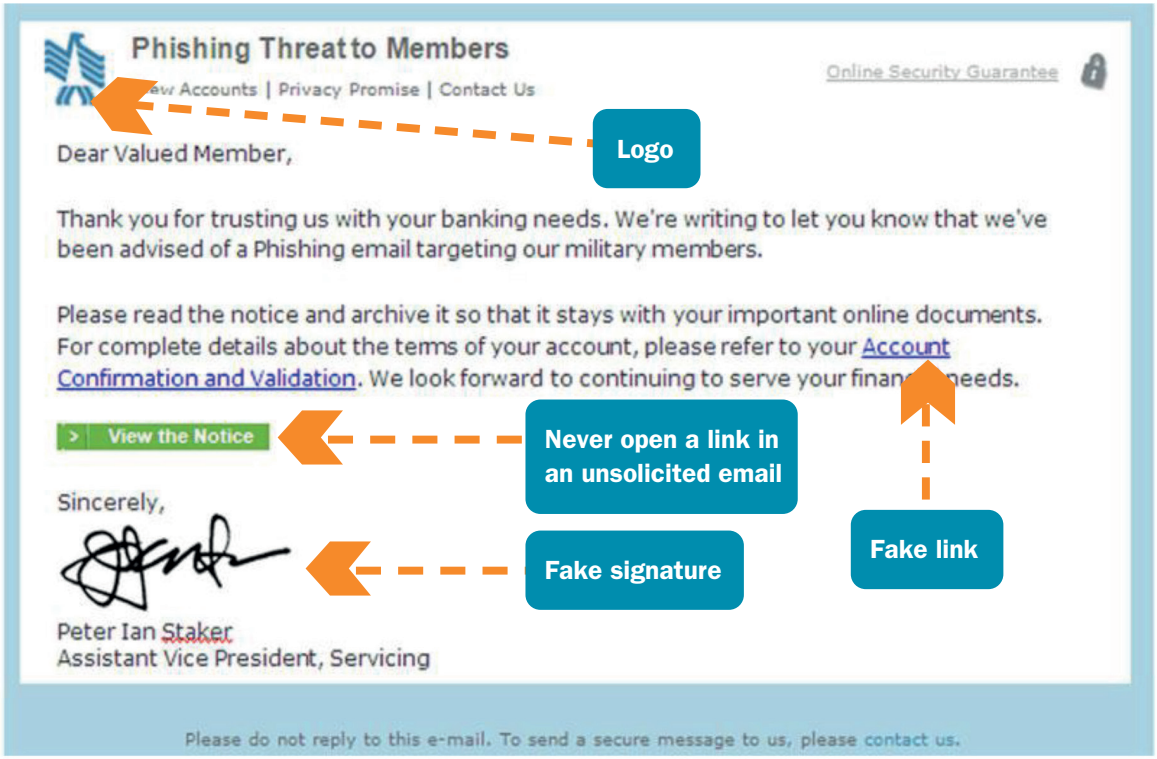
It's especially important to check unsolicited communications. For example, banks will never contact you by phone, email or text message, asking you to confirm any kind of information about your account(s), personal or charity details, and will never ask to you transfer funds between your accounts.

Be cautious of clicking on links or opening attachments from external senders. Even if you recognise the sender, look at the email address and check it to make sure it is from who you think it is – cyber criminals could do something as simple as change one letter in a familiar email address in an attempt to convince you that the email comes from a legitimate source.

In general, unless you are expecting a message with attachments or links and the sender often sends them to you, you should never click on either the attachment or a link.

It's particularly important to check unsolicited messages, even when they appear to be from a legitimate source. Even if you do recognise the sender, if the sender does not explain in the message what is in the attachment, or if the attachment or link has a name which is unusual or incompatible with the subject matter, this is definitely a warning and should be checked. Remember the basic principle that if you are contacted with an offer which sounds too good to be true, unfortunately there's a strong chance that it is, so take your time and do your research before you commit.

The screen shot below shows an actual example of a phishing message containing links and attachments. This email, sent to members of the U.S. defence forces, claims to be a warning but is in fact fake. These emails can display logos from well-known companies such as banks, insurance companies or internet providers. Note that this fake email features a logo, a signature and a link.



Turn off network discovery and folder sharing*

Network discovery is a setting that affects whether your computer or device can find other computers and devices on the network and whether other computers on the network can find your computer. Folder sharing (or file sharing) means your computer or device recognises other devices in that network such as other computers and printers and shares all data in the relevant folders. These options can usually be found under 'Network and Sharing' on the control panel or under the 'Settings' icon of your device.

When connecting to a new network, you will be asked something like, *'Do you want to find PCs, devices, and content on this network, and automatically connect to devices like printers?'*

You should indicate that you do not want this to occur by selecting the relevant option.

*Note that changing these settings within your own network or device may affect your access to shared systems and data within your organisation so you should only do so after checking with colleagues or your organisations' IT provider.

A few final points:

- Consider training for charity trustees, staff and volunteers to ensure that they are able to identify and take steps to protect the charity from cybercrime.
- Remember that the General Data Protection Regulation applies to the processing of all personal data. Take extra steps where necessary to ensure that personal data being processed remotely is as secure as it would be if being processed in your office environment.
- If you think your charity has been a victim of cybercrime, report it to An Garda Síochána.

For further information, advice and tips please see the following websites:

The National Cyber Security Centre www.ncsc.gov.ie

The Data Protection Commissioner
www.dataprotection.ie

An Garda Siochána
www.garda.ie/en/Crime-Prevention/Fraud-Prevention-Brochure.pdf

Banking & Payments Federation Ireland
https://www.FraudSmart.ie

Document Reference No SE GLS 8.2.1 024

Charities Regulator
3 George's Dock
IFSC
Dublin 1
D01 X5X0
Telephone: 01 633 1500
www.charitiesregulator.ie