This factsheet has been produced with help from Police Scotland. It provides steps that charities can take to protect themselves and what to do if your charity has been the victim of cybercrime

Pg 3.  1.  What is cybercrime?

Pg 4.  2.  What steps can my charity take to protect itself?

Pg 6.  3.  I think my charity may be a victim of cybercrime, what should I do?

Pg 7.  4.  Where can I get more advice?
1. What is cybercrime?

Cybercrime is any criminal act committed by digital means.

**Fraud comes in many forms** and **anyone** can be a target.

Although the number of cybercrime notifications we get in is low, with more organisations using digital methods of operating it is essential that charities protect themselves against any potential attacks.
2. What steps can my charity take to protect itself?

Here are 10 steps your charity can take to help protect itself from cybercrime:

• If your charity provides services digitally, make sure any systems have been designed to deter cyber-attacks. Advice on digital service security can be found on the NCSC website - www.ncsc.gov.uk/guidance/digital-service-security.

• Know you customers, suppliers and employees. Always verify credentials before providing any personal or confidential information – and be aware of your responsibilities under data protection laws.

• Make sure your devices always have the latest software installed and are protected against viruses using specific virus protection software. Software updates usually contain new barriers to stop viruses stealing information.

• Beware of emails that are not legitimate. Banks will never email you with a link asking for a confirmation of your details. If you are unsure, please get in touch with a bank using a different contact method from other official correspondence (website, telephone number, customer service email, etc.)

• Check your bank statements and invoices – if something has been purchased that you haven’t bought, your charity’s details may have been stolen.

• If you get an offer by post or email that looks too good to be true, there is a chance that it is. Take your time when asked for a decision – don’t be rushed.

• If you are taking a device out in public make sure it is secure and the screen cannot be seen. This also goes for documents with personal information – don’t leave them lying around and be careful.
how you dispose of them.

- Regularly change passwords and don’t give them out to anyone who shouldn’t have them.

- Make sure you keep back-ups of the data you need. Ransomware, a crime where you could be held to ransom for stolen data, is on the rise.

- Consider training for charity trustees and staff to ensure that they are able to identify and take steps to protect the charity.
3. I think my charity may be a victim of cybercrime, what should I do?

Report it to the Police Scotland by phoning 101 immediately.

You also need to tell OSCR by sending us a notifiable event.
4. Where can I get more advice?

Guidance for individuals, charities and small businesses

• mygov.scot’s Guide to Staying Safe Online
• mygov.scot’s Guide to Keeping Your Business Safe Online
• NCSC’s Small Business Guide
• NCSC’s Small Charity Guide
• Cyber Aware: a UK initiative designed to make good cyber security habits second nature for individuals and small businesses
• Get Safe Online: a UK website offering free expert personal and business advice
• Take Five – To Stop Fraud: a UK initiative which offers straightforward and impartial advice to help everyone in the UK protect themselves against financial fraud.

Guidance for large organisations

• The National Cyber Security Centre provides support and incident management response to the most critical organisations in the UK, in both the public and private sectors.