Coronavirus (COVID-19): increased risk of fraud and cybercrime against charities

Fraudsters are exploiting the spread of coronavirus (COVID-19) in order to carry out fraud and cybercrime. Police have reported an increase in coronavirus related scams.

We are issuing this alert to help charities minimise the risk of becoming a victim of such frauds and cyber-attacks.

All charities, but especially those providing services and supporting local communities during the coronavirus crisis, could be targeted by fraudsters.

Webinar about the risks of coronavirus frauds: what to watch out for and how to stay safe

The Fraud Advisory Panel and Charity Commission have pre-recorded a webinar with sector partners to help you spot COVID-19 related fraud, and better protect your charity from harm.

We are joined by fraud experts from the City of London Police and Chartered Institute of Public Finance & Accountancy who share practical advice and tips.

Scam emails ('phishing')

Be vigilant. Do not click on links or attachments in unexpected or suspicious emails. Never respond to unsolicited messages or phone calls that ask for your personal or financial details.

The police have already noted an increase in phishing attacks.

National Cyber Security Centre (NCSC) guidance about phishing attacks.

Report potential phishing messages to the NCSC through the Suspicious Email Reporting Service (SERS).

Example of this type of fraud

Fraudsters claim to be from a legitimate organisation and able to provide information that could be of assistance to local charities, such as a list of at-risk elderly people in a local community who may require support from the charity. The victim has to click on a link to get the information. This leads to a fake website or asks the victim to make a cryptocurrency (such as Bitcoin) payment.

Protect your devices

Always install the latest software and app updates to protect your devices from the latest threats.

National Cyber Security Centre (NCSC) guidance on keeping devices secure.

Consider if you need to take any extra steps if you have staff working at home.

NCSC guidance on minimising the risk of cybercrime with staff working at home.

NCSC guidance about using video conferencing services securely.

Ensure that you keep people safe by protecting the personal data of staff and beneficiaries when using, or switching to, digital communications and delivery platforms.

Procurement fraud

There are a number of ways in which charities can be defrauded. Some scams involve the sale of vital personal protective equipment (PPE), such as face masks and gloves, online.

Some sellers have been fraudulent. Once the payment has been made, no products are delivered or the products do not meet required standards.

Carry out due diligence if you're making a purchase on behalf of your charity from a company or person you do not know.

Discuss with fellow trustees, colleagues or volunteers if you're unsure.

Action Fraud guidance about shopping safely online.

Mandate or Chief Executive Officer frauds

Always be cautious if you are asked to make changes to bank details or make payments to a new account. Wherever possible, follow your charity's validation procedures and check the authenticity of such messages before making any payments or actioning banking changes.

Commission prevention advice for this type of fraud.

Action Fraud guidance about mandate fraud.

Example of this type of fraud

A charity employee working from home receives an email purporting to be from a legitimate company providing services for the charity. The email asks that future payments be made to an alternative bank account, which is controlled by the fraudster.

Unsolicited offers of goods, services or financial support (advanced fee fraud)

Always question unsolicited offers of goods or other financial support where an advanced fee payment is required. Just because someone knows your name and contact details, it does not mean they are genuine. Don’t be rushed or pressured into making a decision that could harm your charity or your beneficiaries.

Action fraud guidance about computer software service frauds.

Reporting fraud and cybercrime

If your charity is a victim of fraud or cybercrime, aim to report it promptly to:

1. Action Fraud
2. The Charity Commission

Report potential phishing messages to the Suspicious Email Reporting Service (SERS): report@phishing.gov.uk

Read the Commission’s guidance for more information and advice about how to protect your charity from fraud and cybercrime.

Notes

The Charity Commission, the independent regulator of charities in England and Wales, is issuing this alert to charities as regulatory advice under section 15(2) of the Charities Act 2011.