Press release: Ransomware threat – keep your charity safe

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.

Charities could be at risk and are urged to be vigilant.

Over 200,000 organisations, including the National Health Service (NHS), in 150 countries have been affected by a recent ransomware attack. The vulnerabilities exploited by the hackers are the same for charities as they are for individuals, public or private sector organisations.

The Charity Commission encourages all charities to follow protection advice recently issued by the City of London Police and National Cyber Security Centre (NCSC).

Key protection messages:

- install system updates on all devices as soon as they become available
- install anti-virus software on all devices and keep it updated
- create regular backups of your important/business critical files to a device that is not left connected to your network, as any malware infection could be spread to that too
- do not meet any stated demands and pay a ransom – this may be requested via Bitcoins (a form of digital or 'crypto' currency)

National Cyber Security Centre technical guidance includes specific software patches to use that will prevent infected computers on your network from becoming infected with the "WannaCry" Ransomware.

Additional in-depth technical guidance on how to protect your organisation from ransomware can also be found on the NCSC website.

Phishing/Smishing

Fraudsters may exploit this high profile incident and use it as part of phishing/smishing (SMS phishing) campaigns. Charities are urged to be cautious if they receive any unsolicited communications from the NHS.

The protect advice is:

- any email address can be spoofed – do not open attachments or click on the links within any unsolicited emails you receive, and never respond to emails that ask for personal/charity information or financial details
- the sender's name and number in a text message can be spoofed – so even if the message appears to be from an organisation you know of, continue to exercise caution, particularly if the texts are asking you to click on a link or call a number

How to report

If you think your charity has fallen victim to cyber-attack, you should report it to Action Fraud by calling 0300 123 2040, or visiting ActionFraud.

Trustees are advised to also report suspected or known fraud incidents to the Commission by emailing RSI@charitycommission.gsi.gov.uk

Serious incident reporting helps the Commission to gauge the volume and impact of incidents within charities and to understand the risks facing the sector as a whole.

Harvey Grenville, Head of Investigations and Enforcement at the Charity Commission said:

> Charities need to be aware of the imminent danger posed by ransomware threats and take appropriate steps to protect their charity from cyber-attack – a charity's valuable assets and good reputation can be put at risk from these dangerous scams.
>
> I urge all charities, if they suspect they may have fallen victim to cyber fraud, to report it immediately to Action Fraud and to the Commission, under its serious incident reporting regime.
>
> You can visit Charities against fraud for advice and top tips on how to protect your charity against cyber-fraud.

Ends.

Notes to editors

The Charity Commission is the independent registrar and regulator of charities in England and Wales.

We act in the public's interest, to ensure that:

- charities know what they have to do
- the public know what charities do
- charities are held to account