Beware of scams relating to Covid-19 pandemic

Criminals will use any opportunity they can to take money from innocent people. This includes exploiting tragedies and global emergencies, such as the COVID-19 pandemic, to scam people in a variety of ways. The number of these scams are only likely to increase and we need individuals and businesses to be fully aware and prepared.

As more people stay indoors and work from computers and laptops at home, there is more opportunity for criminals to try and trick people into parting with their money at a time when they are anxious and uncertain about the future.

We have already received nearly 400 reports of fraud related to COVID-19, the majority of which are online shopping scams where people have ordered protective face masks, hand sanitiser, and other products, which have never arrived. We have also seen a large amount of phishing emails and texts circulating, that use COVID-19 as a hook, and try to get recipients to click on links or attachments which harvest information and lead to the individual revealing personal or financial details.

Is fraud rising?

While the number of reports of fraud in general is not increasing, we are warning people that the current social situation we find ourselves in could lead to any number of fraud types increasing as this immediate public health crisis unfolds. We are advising people to be particularly vigilant around:

- Computer Software Service Fraud – as more people work from home, fraudsters may capitalise on slow networks and IT problems, to commit computer software service fraud. Be wary of cold calls or unsolicited emails offering you help with your device or to fix a problem. Attached is a helpful graphic with protection advice.

- Mandate Fraud – with more people working at home, it may be easier for fraudsters to impersonate senior decision makers, with seemingly valid reasons why they cannot be contacted, and request a change in a direct debit, standing order or bank transfer mandate, by purporting to be an organisation you make regular payments to. The change they ask you to make will divert funds to their own bank account. Attached is a helpful graphic with protection advice.

Advice for businesses in regards to people working from home

Many organisations are either moving to working remotely for the first time or significantly increasing it, and this presents a number of cyber security challenges. Advice on how to respond to those challenges is set out in the NCSC’s working from home guidance.

There are a number of practical steps organisations can take to reduce the risk including:

- Supporting people to use stronger passwords and setting up two factor authentication.
- Ensuring staff know how to report problems, especially those related to security.
- Creating ‘How do I’ guides for new software and tools staff may be using.
- Using VPNs to allow users to securely access the organisation’s IT services.
- Ensuring devices encrypt data whilst at rest.

Some organisations may be allowing staff to use their own devices to work remotely. In this case, please refer to the NCSC's Bring Your Own Device (BYOD) guidance.

In addition to following the guidance set out above, it is worth being aware of phishing emails which trick users into clicking on a bad link. Once clicked, the user is sent to a website which could download malware onto your computer, or steal passwords. We know that cyber criminals are opportunistic and will look to take advantage of people’s fears, and there is evidence that the coronavirus outbreak is being exploited in this way.

Those who do fall victim shouldn’t feel bad – these scams can be extremely convincing – but what they should do as quickly as possible is report it to their IT department when the incident is work-related or Action Fraud when it is personal. They can also open their antivirus (AV) software if installed, and run a full scan, following any instructions given. If they've been tricked into providing password, they should change their passwords on all their other accounts. The NCSC's guidance on suspicious emails provides more tips on this.

Our Cyber Griffin team have also created a series of short video guides on how to keep you and your family safe while online at home which contain practical hints and tips and cover a range of topics, including passwords, phishing, vishing and multi-factor authentication.

To report a fraud please follow this link: https://www.actionfraud.police.uk/

Phishing emails can be forwarded to NFIBPhishing@cityoflondon.police.uk or via https://www.actionfraud.police.uk/report-phishing

Counter Terrorism I City of London Police
p **020 7601 2063**
e CTSA@cityoflondon.pnn.police.uk
w www.cityoflondon.police.uk **t** www.twitter.com/citypolice

It's probably nothing, but...
Confidential Anti Terrorist Hotline 0800 789 321