Cybercriminals exploit the spread of coronavirus

Since February 2020, the National Fraud Intelligence Bureau (NFIB) has identified 21 reports of fraud where coronavirus was mentioned, with victim losses totalling over £800k. It's expected that reporting numbers will rise as the virus continues to spread across the world.

What are the risks?

The two most common risks are:

- Viruses — These are malicious software programmes loaded onto the user's computer without their knowledge and performs malicious actions, leading to corruption of data/files, or even altogether disabling the computer.
- Phishing — This is the fraudulent attempt to obtain sensitive information such as usernames, passwords and bank details by disguising oneself as a trustworthy entity in an electronic communication.

Of the reported coronavirus related fraud cases, ten of these reports were made by victims that attempted to purchase protective face masks from fraudulent sellers. Fraudsters are also sending out coronavirus-themed phishing emails in an attempt to trick people into opening malicious attachments or revealing sensitive personal and financial details.

Some of the tactics we've identified from victim reports include fraudsters purporting to be from research organisation's affiliated with the Centres for Disease Control and Prevention (CDC) and the World Health Organisation (WHO) contacting potential victims over email. They claim to be able to provide the recipient with a list of coronavirus infected people in their area. To access this information, the victim needs to click on a link which takes them to a malicious website or requested to make a payment in Bitcoin.

What should I do next?

- Watch out for scam messages — Don't click on the links or attachments in suspicious emails, and never respond to unsolicited messages and calls that ask for personal or financial details,
- Protect devices from the latest threats — Always install the latest software and app updates to protect devices from the latest threats. The National Society for Cyber Security provides useful information on **how to update your devices**.
- Shopping online — If you're making a purchase from a company or person you don't know and trust, carry out some research first and ask a friend or colleague for advice before completing the purchase. If you decide to go ahead with the purchase, use a credit card if you have one, as most major credit card providers insure online purchases. Action Fraud, the UK's national reporting centre for fraud and cybercrime, has produced **advice on how to shop online safely**.