Five ways to avoid scams due to Coronavirus

Criminals are using the publicity around Coronavirus as a chance to pose as a genuine organisation, including banks, police officers, government, the World Health Organisation or other health service providers.

Bogus emails, phone calls, text messages or social media posts often claim to be able to help customers by providing a safe haven for your money, investment opportunities or even provide medical guidance.

Using Coronavirus as a cover story, the criminal will then attempt to get recipients to disclose personal or financial information or click on links that may contain malware which they will then use for their own fraudulent purposes.

Security experts say an increase in email scams linked to coronavirus is the worst they have seen in years. Here are five examples of scams that are currently circulating and that could impact you.

1. '**Click here for a cure' - personal details could be stolen from victims looking for a Covid-19 cure**

People who click on the attached document are taken to a spoof webpage designed to harvest login details or personal and financial information.

Action: The best way for you to see where a link will take you is to hover your mouse cursor over it to reveal the true web address. If it looks dodgy, don't click. Remember, never share your personal or financial information following an unexpected email

2. **HM Revenue and Customs is not trying to give you a Covid-19 tax rebate**

If a member of the public clicked on "access your funds now", it would take them to a fake government webpage, encouraging them to input all their financial and tax information.

Action: You should never respond to any electronic communication in relation to monies via email. And certainly do not click on any links in any related message. HMRC do not use this method to advise you of a potential tax refund.

3. **The World Health Organization is being impersonated**

Criminals pretending to represent the World Health Organization (WHO) claim that an attached document details how recipients can prevent the disease's spread.

"This little measure can save you," they claim.

The attachment doesn't contain any useful advice, and instead infects computers with malicious software.

This software records your keystrokes and sends it to the criminals, a tactic that allows them to monitor their victims' every move online.

Action: To avoid this scam, be wary of emails claiming to be from WHO, as they are probably fake. Instead visit its official website or social media channels for the latest advice.

4. **Donate to help the fight!**

There are many fake emails and social media adverts circulating encouraging people across the world to donate money, whether that be to find a cure or to help the vulnerable.

Action: Be vigilant, many of these requests will be fake. Do not respond to emails or adverts requesting donations. Instead visit official websites to look at how you can help.

5. **Knock Knock!**

There have been numerous reports across the UK that criminals are knocking door to door, imitating health authorities in relation to coronavirus testing, asking for personal information or asking to enter your home. There is even reports of criminals pretending to be good Samaritans to help those in need.

Action: There is no door to door testing for coronavirus, if anybody knocks on your door out of the blue, it's likely to be a scam. Close the door immediately and report it to your local Police.

March 2020