Coronavirus Fraud Prevention – Malicious links, websites & summary

John:

So one area that appears to be on the increase is the use of malicious links and websites that are being created so that fraudsters can download software onto people's computers in order to gain more information on them. We even had one report where we saw a fraudulent website that was supposedly going to be tracking the number of cases related to COVID-19, and using it to get people to download the malware in order for them to be able to steal the customer's money.

John:

Chris, are you seeing a lot of this? What are your comments, please?

Chris:

John, thank you. This of course is another example of a repurposed common scam to fit our COVID scenario. Our advice has always been as straightforward as we can put it really with regards to emails, unless you are 100% certain in terms of where that email has come from, then it is really dangerous to access any links attached to the email. Because of course, if it's from a fraudster or a scammer, then that could very well give them direct access into your data, your money, your computer. So we know that there are more COVID-19 emails flying around, but please be very, very wary of accessing any links. If the email suggests a subject that you're interested in, then once again, do your own research, go to official sites and access it that way, as opposed to using a link on an email that you are not at all sure where it comes from. So COVID-19, be extra specially careful, especially when it comes to emails and links.

John:

So thank you so much for taking the time to watch these videos. We really hope that you found them to be beneficial and that you'll be able to use the learnings from these to be able to recognise a scam and to keep yourself safe during these difficult times.

John:

Chris, would you like to summarise the key points that you'd like customers to take note of?

Chris:

Yes, absolutely, John, no problem.

Chris:

Very simply, always double- or triple-check where you are sending your money and who you were responding to. Please be very wary of links in emails and do not use them unless you are 100% certain of where the email came from or the fact that you were actually expecting it. Just because someone's asking you to donate to charity of course doesn't always mean that that particular site is legitimate, so please do your research. Banks, police, and government will never ask you to send money or move it to a safe account. And finally, if you are unsure about who is contacting you and they are claiming to be from your bank, then please have the confidence to terminate the call and to re-establish that communication via alternative means. Thank you for your time.

John:

Thank you.

HSBC