Government Warnings Over Coronavirus Scams - Here's How to Protect Yourself

Submitted by: Key Loans & Mortgages Limited t/a KIS Finance
Wednesday, 6 May 2020

As the number of COVID-19 related scams reaches new heights, the government is now including up-to-date statistics and information in the daily Coronavirus briefings at Downing Street.

KIS Finance (https://www.kisbridgingloans.co.uk/) have put together a clear and simple guide on the most common Coronavirus related scams, including how to protect yourself from them and what to do if you have fallen victim.

Amid the fear and confusion of the current Coronavirus pandemic, scammers are out taking full advantage of scared and vulnerable people. Over £800,000 has been lost to Coronavirus scams since February 2020, according to reports made to the National Fraud Intelligence Bureau. The NCSC has also removed over 2,000 online scams related to COVID-19 in the last month.

In a time where most of us are heavily relying on technology to work or to stay in contact with family and friends, scammers are using this to their advantage and cyber security is more important than ever. Most of these scams are online and are coming in the form of phishing emails (https://www.kisbridgingloans.co.uk/guide-to-fraud-prevention/what-is-a-phishing-email-scam-and-simple-ways-to-protect-your malicious social media adverts, fake online sellers and hacking of video conferencing websites.

This article will outline the details of some of the Coronavirus scams that have been reported so far so you can keep your money safe.

Phishing Emails

You've probably received many emails related to COVID-19 from businesses, your children's school, your employer and other well-known companies. This makes it even easier for phishing emails to slip through the net.

'Names of patients revealed'

In this phishing attempt, scammers are posing as representatives from the World Health Organisation (WHO) or the Centres for Disease Control and Prevention (CDC) and offering to release names of those infected with COVID-19 in your area in exchange for payment. They may ask you to perform a bank transfer or ask for a payment in Bitcoin or other cryptocurrencies.
The email will contain a link which you are urged to click on so you can make the payment. You will be asked for your bank details as well as personal information such as your name, address and date of birth.

‘Get the latest statistics’

This is another phishing email where the scammers pose as The World Health Organisation (WHO) but this time they are offering you up-to-date Coronavirus statistics and all you have to do is follow a link. However, the link will infect your device with malicious malware of viruses that could lock you out of your computer, take control of your computer, or access your personal and financial details in order to commit identity theft.

‘Coronavirus safety measures’

Scammers are sending out phishing emails where they’re offering medical advice and various ‘safety measures’ you can take in order to protect yourself from Coronavirus. Again, they ask you to follow a link or to download a PDF file which will infect your devise with viruses or malware.

HMRC tax refund’

Some scammers are posing as HMRC and saying that tax refunds are part of the government’s action plan to help people cope with income shortages amid the crisis. This is not part of the government’s plan and HMRC will never, under any circumstances, contact you via email, text or phone call to offer you a tax refund. This is an attempt to steal your personal information and bank details.

‘Donate to the cause’

This scam involves fake donation pages set up by scammers. You will be urged to click on a link in the email which will take you to a fake website where you’ll be asked to make a donation to help find a cure to the Coronavirus. This website has actually been set up to steal your money as well as capture your personal information and bank details. There has only been one fund set by The World Health Organisation and that can be found on their official website – they will not email you asking for donations.

How to avoid Coronavirus phishing scams

•The World Health Organisation (WHO) have stated on their website that they will never ask for your personal details or password via email, they will never send email attachments that you didn’t ask for and they will never ask you to go on to a website outside of www.who.int. WHO say that you can verify whether a form of communication is legitimate by contacting them directly using the contact details on their website.

•Verify the sender by checking their email address. If they’re claiming to be from WHO and the email address ends in anything other than ‘@who.int’, it is a scam so do not click on any links in the email.

•Never give personal information to someone you don’t know, or to someone you haven’t initiated the contact with. Use some common sense and decide whether it’s an appropriate reason for this person to be

asking for your details. You shouldn't have to give anything to access public information.

•If you see a scam, report it. This is essential in helping you and others.

Video Conferencing Scams

Many people are taking to video-conferencing in order to work from home or to stay in touch with family friends during the UK lockdown. And some are doing this for the first time, so it's very important to be aware of how to stay safe.

Scammers are creating their own fake versions of well-known apps and websites in order to steal peoples' personal and banking information. They are also hacking into public video calls in order to try and obtain sensitive data about individuals.

How to avoid Coronavirus video conferencing scams

•Make sure you only download apps and software from trusted sources like your app store or from the provider's official website (https://www.kisbridgingloans.co.uk/guide-to-fraud-prevention/5-simple-ways-to-tell-if-a-website-is-safe-and-secure/). Never click on links which have been sent to you in the form of unsolicited emails, SMS messages or on social media messaging platforms or adverts,

•Use a strong and unique password so scammers who are trying to hack into your account can't guess it easily or find it out from your social media profiles. You should also set up two-factor authentication if this is an option as it adds an extra layer of security and stops people from being able to access your account even if they know your password.

•Do not make your calls public meaning anyone can join. Only connect with your colleagues, friends, or family directly from their information in your address book. Some video conferencing services allow you to set up a password which people must enter before they can join the call which adds an extra layer of security. Never share this password publicly.

Fake Social Media Adverts

A lot of online scammers are taking to social media to post malicious adverts. Most of these promote miracle cures and treatments for the Coronavirus and try to create a sense of urgency by saying things like 'Buy now, very limited stock'.

There are two possible bad outcomes for clicking on a malicious advert. Number one, it could download viruses and malware onto your device or, number two, they may allow you to purchase one of these fake products, but nothing will turn up and the fraudsters disappear with your money and personal details.

Avoid anything on social media that advertises things like this and is clearly trying to profit out of the crisis. Only go to trusted sources like the NHS or government websites for information.

In-person Scams

Offer to do shopping

Recent reports have revealed that some particularly nasty fraudsters are attempting to steal money from elderly and vulnerable people by offering to do their shopping for them. These criminals are posting on social media community pages offering anyone who can't get themselves to the shops to go for them. They ask for the cash upfront in order to pay for the shopping but disappear with the money and never return. They will usually post the messages on social media under a fake name so they can't be traced or arrested.

If you are in a vulnerable position and you are having to stay at home in isolation, only trust people you know - neighbours, friends, and family – and ask them for help. Don't turn to somebody you don't know. Some people do genuinely want to help and will offer genuine services like this, but it's not worth the risk.

Door-to-door testing

Some scammers have been knocking on people's doors claiming to be from the NHS and offering Coronavirus tests for a small fee. These tests are not real, and the scammers are targeting vulnerable and elderly people. You should call the police if someone knocks on your door and offers you a COVID-19 test.

What to do if you have fallen victim to a Coronavirus scam

The NCSC and the City of London Police have recently launched a new suspicious email reporting service which can be used if you receive anything that looks fraudulent. You must forward any dubious emails to report@phishing.gov.uk so the NCSC can look into it and remove any fraudulent websites. More information about this can be found on the NCSC website.

If you have lost money because of a Coronavirus scam, you must report it to your bank and to Action Fraud UK.

For up to date information on the latest COVID-19 scams, take a look at KIS Finance's Latest Fraud News (https://www.kisbridgingloans.co.uk/guide-to-fraud-prevention/latest-fraud-news/) page.

If you would like any more information on this, or for us to provide expert comment for an article, don't hesitate to contact us.

Alan Andrews
alan@kisfinance.co.uk
01884 820110