What Will Be The Biggest Scams and Fraud Threats of 2020

Submitted by: KIS Finance
Friday, 31 January 2020

Scammers are continuously adapting and developing their techniques in order to trick more and more people every day.

Based on data from UK Finance and analysis from KIS Finance (https://www.kisbridgingloans.co.uk/guide-to-fraud-prevention/what-will-be-the-biggest-scams-of-2020/), these are what we predict will be the biggest scams and fraud threats of 2020.

Authorised Push Payment (APP) Scams

Authorised push payment scams are one of the largest growing threats to consumers. According to trade body UK Finance, there were 57,549 reported cases of APP fraud in just the first half of 2019 – a rise of 69% year on year. Total monetary losses of reported cases reached £207.5 million.

An authorised push payment scam is when a criminal tricks you into transferring money into an account controlled by them by making you believe they are a genuine organisation such as a bank, a utilities company or even the police. This tactic is known as social engineering and criminals are continuously developing and adapting their techniques in order to trick consumers into handing over personal details or transferring money.
Although banks are starting to introduce various defences in order to try and prevent these types of scams from happening, there haven't been any signs yet to show them slowing down.

Read here for further details on how to protect yourself from APP scams (https://www.kisbridgingloans.co.uk/guide-to-fraud-prevention/complete-guide-to-protection-against-authorised-push-payment-

Investment Scams

Investment scams involve criminals convincing you to move money into a fictitious fund to pay for an investment.

They will promise very high returns and ensure that your money is safe, although the investment is entirely fake. You may be cold called by the scammer, or they may entice you with an advert on social media.

Investment products offered are usually gold, diamonds, expensive wine, property and, more recently, cryptocurrencies.

In the first half of 2019, losses that resulted from investment scams equalled £43.4 million, and this was an increase of 108% year on year.

With scammers adapting their techniques to lure in victims; now creating full websites, social media adverts and even sending out official looking paperwork, it looks like investment scams will be another big one for 2020.

Windows 7 Hacking

There is now a security concern for people still using Windows 7 as it entered into its ‘End of Life’ phase at the beginning of this year. This means that Windows will no longer be offering updates or security fixes for the operating system.

While it won’t be an overnight security risk and your PC will continue to run as normal, the worry is that eventually hackers will be able to find vulnerabilities in the system and exploit them in order to steal peoples’ personal data.

Another concern is that you could still be vulnerable to this even if you updated your own PC from Windows 7 years ago. Any company that you’ve trusted to give your data to, a doctor’s surgery would be one example, could also be putting your information at risk if they are still running their systems on Windows 7 and they succumb to a data breach.

So, if your PC is still running on Windows 7, I would suggest updating to Windows 10 as soon as possible to make sure you’re not putting yourself at a higher risk of being defrauded.

SIM-swapping Scams

The number of SIM-swap scams has been growing rapidly over recent years with little protection in place against this type of fraud.

SIM-swapping fraud is when a criminal manages to convince your mobile network provider, by impersonating you over the phone, that you want to switch your phone number to another company.

They are able to bypass security questions as they would have already collected a lot of your personal data before attempting the scam – this is usually through companies who have had a data breach, or by hacking into your email and/or social media accounts.

Once they have successfully pulled off the switch, they will be able to benefit from everything that having your phone number provides including making and receiving phone calls and sending and receiving SMS messages.

The criminal will also receive any two-factor authentication or one-time passcode texts meaning they will be able to log-in to your personal accounts and perform online banking transactions without you being

notified.

Here are the warning signs of SIM-swapping fraud (https://www.kisbridgingloans.co.uk/guide-to-fraud-prevention/what-is-sim-swapping-fraud-and-how-to-protect-yourself/).

Remote Access Fraud

This type of fraud occurs when a fraudster cold calls you and explains that they are from a tech support company and there is something wrong with your computer or internet connection. This scam is often targeted towards people who are likely to have less of an understanding of modern technology, for example, the elderly.

The scammer will usually ask you to download a piece of software that allows them remote access of your computer - 'Team Viewer' is often used as it's a well-known and trusted programme. Once you have downloaded it and connected to the scammer, they can see and control your computer screen.

They will then download (or tell you to download) a piece of software which they insist is needed to sort out the supposed problem. This piece of software is likely to spread viruses and malware onto your computer.

Information on how to protect yourself from all these types of scams can be found in this article by KIS Finance (https://www.kisbridgingloans.co.uk/guide-to-fraud-prevention/what-will-be-the-biggest-scams-of-2020/).

[ENDS]

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

Contact Details:

Phoebe Griffits
phoebe@kisfinance.co.uk