UK Finance reveals ten Covid-19 scams the public should be on high alert for

- UK Finance unveils ten Covid-19 and lockdown scams the public should be on high alert for and how to spot them
- Criminals are preying on a worried public by tapping into their financial concerns due to coronavirus, asking for personal and financial information
- New animation video from Take Five to Stop Fraud campaign warns people to remember criminals are sophisticated at impersonating other organisations

Using the coronavirus pandemic as an opportunity, fraudsters are using sophisticated methods to callously exploit people, with many concerned about their financial situation and the state of the economy. To coincide with the launch of its new animation urging people to follow the advice of the Take Five to Stop Fraud campaign, UK Finance today reveals ten Covid-19 and lockdown scams which criminals are using to target people to get them to part with their money.

Some scams manipulate innocent victims, urging people to invest and "take advantage of the financial downturn". Others impersonate well-known subscription services to get people to part with their cash and personal information. Criminals are even posing as representatives from the NHS Test and Trace service in an effort to trick people into giving away their personal details.

To remind people that criminals are experts at impersonating trusted organisations, UK Finance has launched a new animation video urging people to follow the advice of the Take Five to Stop Fraud campaign. Consumers are reminded to always take a moment to stop and think before parting with their money or information in case it's a scam.

The ten scams to be on the lookout for and how to spot them:

Covid-19 financial support scams

1. Criminals have sent **fake government emails** designed to look like they are from government departments offering grants of up to £7,500. The emails contain links which steal personal and financial information from victims.

2. Fraudsters have also been sending scam emails which offer access to **'Covid-19 relief funds'** encouraging victims to fill in a form with their personal information.

3. Criminals have been targeting people with official-looking emails offering a **'council tax reduction'**. These emails, which use government branding, contain links which lead to a fake government website which is used to access personal and financial information.

4. Fraudsters are also preying on benefit recipients, offering to help apply for **Universal Credit**, while taking some of the payment as an advance for their "services".

Health scams

5. One of the most shocking scams that has appeared during the pandemic has involved using the **NHS Test and Trace** service. Criminals are preying on an anxious public by sending phishing emails and links claiming that the recipient has been in contact with someone diagnosed with Covid-19. These lead to fake websites that are used to steal personal and financial information or infect devices with malware.

6. Victims are also being targeted by fake adverts for Covid-related products such as **hand sanitizer and face masks** which do not exist.

Lockdown scams

7. Criminals are sending fake emails and texts claiming to be from **TV Licensing**, telling people they are eligible for six months of free TV license because of the coronavirus pandemic. Victims are told there has been a problem with their direct debit and are asked to click on a link that takes them to a fake website used to steal personal and financial information.
8. Amid a rise in the use of **online TV subscription services** during the lockdown, customers have been targeted by criminals sending convincing emails asking them to update their payment details by clicking on a link which is then used to steal credit card information.

9. Fraudsters are also exploiting those using **online dating websites** by creating fake profiles on social media sites used to manipulate victims into handing over their money. Often criminals will use the identities of real people to strike up relationships with their targets.

10. Criminals are using social media websites to advertise **fake investment opportunities**, encouraging victims to "take advantage of the financial downturn". Bitcoin platforms are using emails and adverts on social media platforms to encourage unsuspecting victims to put money into fake investment companies using fake websites.

The banking and finance sector is working with the government and law enforcement to help identify scams and prevent people becoming victims of fraud. The industry is also encouraging everyone to remain vigilant and to follow the advice of the *Take Five to Stop Fraud campaign,* and to Stop, Challenge and Protect when they receive any messages out of the blue:

Stop: Taking a moment to stop and think before parting with your money or information could keep you safe.

Challenge: Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

Protect: Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

In order to spot a Covid-19 scam, people should be on high alert if:

- The website address is inconsistent with that of the legitimate organisation
- The phone call, text or emails asks for financial information such as PIN, passwords

- You receive a call or email out of the blue with an urgent request for your personal or financial information, or to make an immediate payment
- You're offered a heavily discounted or considerably cheaper product compared to the original price
- There are spelling and grammar mistakes, or inconsistencies in the story you're given

Managing Director of Economic Crime at UK Finance, Katy Worobec, said:

"During this pandemic we have seen criminals using sophisticated methods to callously exploit people's financial concerns, impersonating trusted organisations like the NHS or HMRC, to trick them into giving away their money or information.

"The banking and finance industry is tackling fraud on every front, investing millions in advance technology to protect customers and working closely with the government and law enforcement to stop the criminal gangs responsible and neutralise the threat.

"We would always urge people to follow the advice of the Take Five to Stop Fraud campaign to keep their money and personal information safe from fraudsters."