

7th August 2020

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

Criminals have been using a variety of sophisticated methods to exploit the coronavirus pandemic to get people to part with their hard earned money.

As part of their Take Five to Stop Fraud campaign, UK Finance have revealed the top ten Covid-19 and lockdown scams the public should be on the lookout for.



**TO STOP FRAUD™**

### Health Scams

1

#### Hand Sanitizer & Face Masks

Victims are also being targeted by fake adverts for Covid-related products and Personal Protective equipment (PPE) that do not exist.

2

#### NHS Test and Trace

Criminals are preying on an anxious public by sending phishing emails and cold calls claiming that the recipient has been in contact with someone diagnosed with Covid-19. These are designed to steal personal and financial information.

Contact Tracers will **never**:

- Ask you to make any form of payment
- Ask for details about your bank account
- Ask you for passwords or PINs
- Ask you to download anything

## Covid-19 Financial Support Scams



3

### Fake Government Emails

Criminals are sending emails designed to look like they are from government departments offering grants of up to £7,500. These emails contain links which steal personal and financial information.

4

### 'Covid-19 Relief Funds'

Fraudsters have also been sending scam emails which offer access to relief funds, encouraging victims to fill in a form with their personal information.

5

### 'Council Tax Reduction'

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

6

### Universal Credit Applications

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

## Lockdown Scams

7

### TV Subscription Services

Amid a rise in the use of 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.



8

### Dating Scams

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

9

### Fake Investment Opportunities

Criminals are using social media websites to encourage victims to “take advantage of the financial downturn”. Bitcoin platforms are using emails and adverts on social media platforms to encourage unsuspecting victims invest money into fake companies.

10

### TV Licensing Scams

Criminals are sending fake emails and texts claiming to be from TV Licencing 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.



## Remember

Criminals are experts at impersonating trusted organisations and manipulating people into parting with their money or personal information.

Consumers are reminded to stop and take a moment to think before parting with any money or information, in case it's a scam.

### 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 on **0300 123 2040** or at [www.actionfraud.police.uk](http://www.actionfraud.police.uk).



TO STOP FRAUD™

# STOP. CHALLENGE. PROTECT.