

Covid Fraud & Cyber Threats

May, 2020

Keeping vigilant | Staying safe

Our Services

Due Diligence
Assurance
Financial Crime Compliance
Strategic Intelligence

Investigations
Corporate Fraud
Litigation Support
Digital Forensics

Protection
Brand Protection
Cyber Security
Data & Privacy



*Together, Reducing
Fraud Worldwide*



Opportunity

History tells us where there is **fear, anxiety** and **vulnerability**, there is **exploitation**.

Fraudsters thrive on vulnerability, **human curiosity** and **error**.



Keep Vigilant

In the next few slides, we have highlighted several **emerging** fraud trends arising during this time.

Some of you may have seen these already or experienced these, many of you will have thankfully **spotted** them.

Yet, not everyone will see them, especially the most vulnerable, as many of these scams will **look** very authentic to the untrained or unsuspected eye.

These are a selection of **fake** awareness emails, encouraging end users to click on a link.



Re:SAFTY CORONA VIRUS AWARENESS WHO

WO World Health Organization · [redacted] ↶ ↷ → ...



Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

Safety measures

Symptoms common symptoms include fever, cough, and breathing difficulties.

Regards,

Dr. Stella Chungong
Specialist wuhan-virus-advisory

[EXTERNAL] COVID-19 - Now Airborne, Increased Community Transmission

CI CDC INFO <CDC-Covid19@cdc.gov>
To: [redacted]

↶ Reply ↷ Reply All → Forward

Wed 2/26/2020 1

As you know, the Department of Health and Human Services has declared the Coronavirus (COVID-19) a public health emergency.

At this time, three new cases have been confirmed around your location today. The risk to the Public in your city and throughout the World is very HIGH.

The World Health Organization has named the new coronavirus, Covid-19, and the Centers for Disease Control and Prevention has established precautions.

- * The CDC requires you to avoid (HIGH-RISK) zone around your city to Minimize Chances for Exposures.
- * A high-risk person is currently being monitored around your city center.

For additional information about high-risk places around <https://healing-yui223.com/cd.php?e1...>
Click or tap to follow link.

From Brianna Milne ☆

Subject **RE: IT COVID-19 Update**

To Brianna Milne ☆

To All Staff/Employee,

Due to the recent COVID-19 outbreak. IT Helpdesk is currently working on advance Staff portal in order to keep our staff/employee on task & organized schedules. All Staff/Employee are required to login Staff Portal for update.

To access the portal, Click on [STAFF PORTAL](#)

Failure to update your Staff portal, you will be deleted from our database.

Sincerely,
Brianna Milne
IT Helpdesk
©2020 All rights reserved

COVID-19 Everything you need to know

JD

• John DeFranco <

To: •

How to Protect your friends from nCov 2019 FAQ

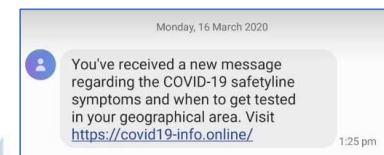
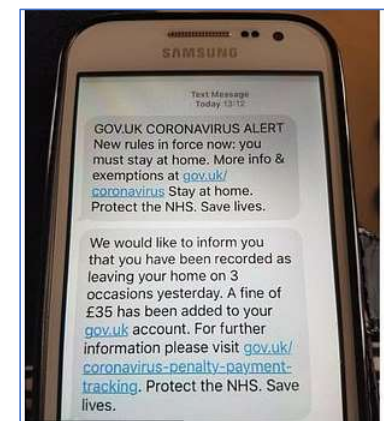
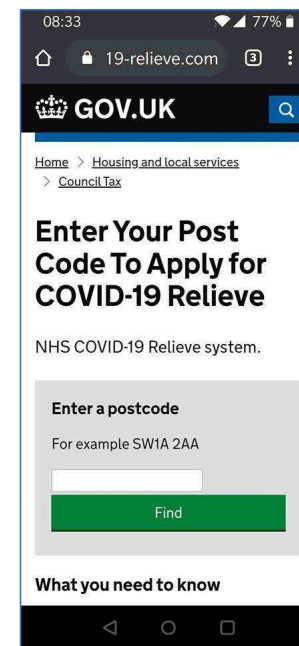
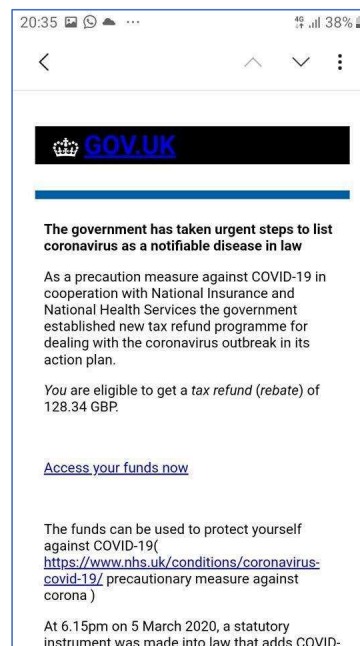
There are more than 75,000 infected COVID-19 cases all around the world!

[COVID-19-FAQ](#) - uploaded with iCloud Drive.

Regards,
John DeFranco

These are some examples of **text related** messages that users have received on their mobile phones.

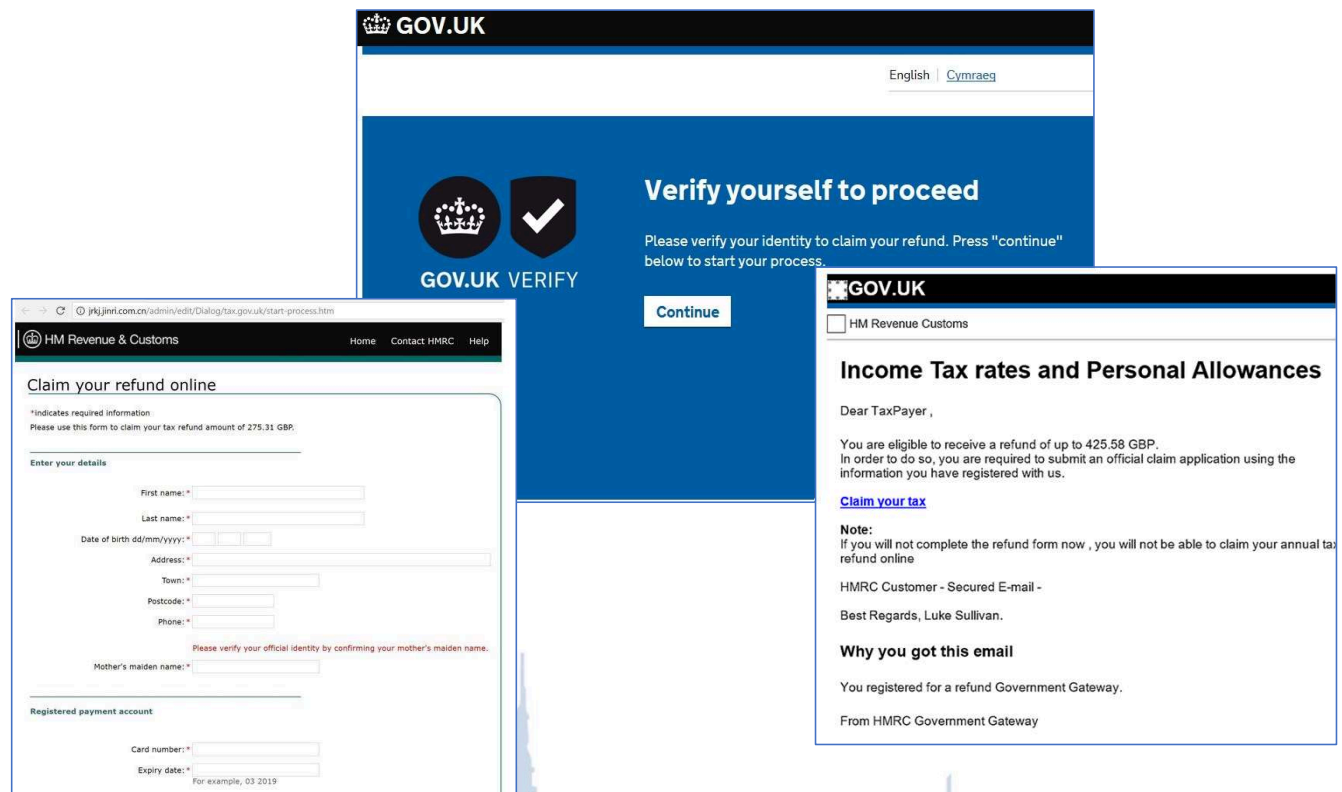
Again **enticing** the user to click through to the link, usually with an offer of “relief money”.



These are some examples
with our own UK
Government logos.

They look relatively
authentic; especially if you
have registered your email
address with the HMRC.

Many of you might actually
anticipate receiving
correspondence from the
Government and
unfortunately, click on
these links



The top screenshot shows the GOV.UK 'Verify yourself to proceed' page. It features the GOV.UK logo, a language selector (English | Cymraeg), and a 'Continue' button. The text reads: 'Please verify your identity to claim your refund. Press "continue" below to start your process.'

The bottom-left screenshot shows the HM Revenue & Customs 'Claim your refund online' form. It includes fields for 'First name', 'Last name', 'Date of birth', 'Address', 'Town', 'Postcode', 'Phone', 'Mother's maiden name', and 'Registered payment account'. A note states: 'Please verify your official identity by confirming your mother's maiden name.'

The bottom-right screenshot shows the HM Revenue & Customs 'Income Tax rates and Personal Allowances' page. It includes a 'Dear TaxPayer' greeting, a note about eligibility for a refund, and a 'Claim your tax' link. The text reads: 'You are eligible to receive a refund of up to 425.58 GBP. In order to do so, you are required to submit an official claim application using the information you have registered with us.'

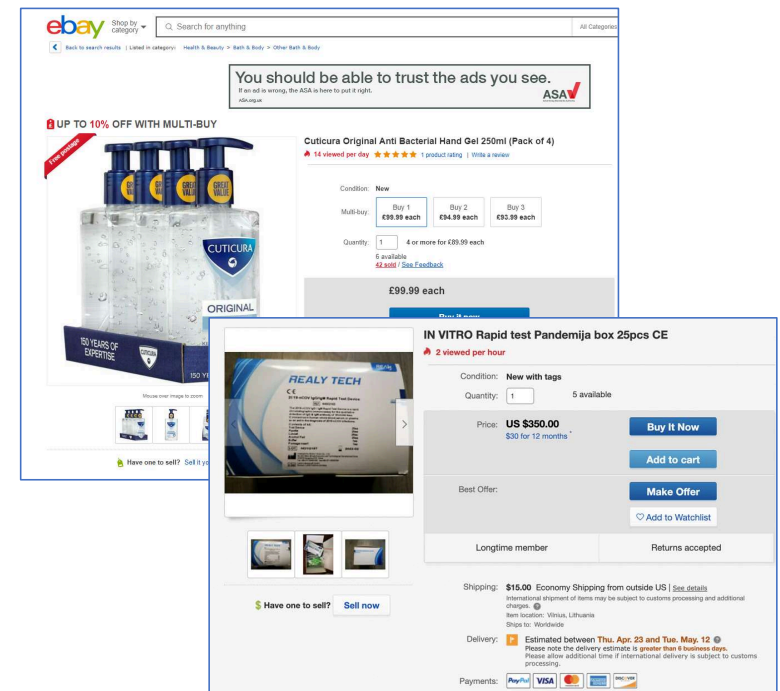
We are all probably **ordering a lot more goods** and products **online**, from auction sites and shopping sources.

Be careful. **Always** check the seller's details, verify the origin, and especially look at the feedback reviews, looking for negative **customer** comments.

"If it is **too good** to be true, it probably is" and "you pay for what you get". Or in some of these cases, what you **don't** get.

You might also be buying **counterfeit goods** which are a **danger** to your safety.

There have been examples that counterfeit "sanitisers" are actually **using bleach** instead of alcohol, causing **significant** burn injuries to hands.



Keep Vigilant

Watch out for these emerging trends:

- **Phishing emails** advising that the recipient's mailbox is full but that they can increase their storage space “free of charge” by clicking on the link provided
- Emails and text messages to parents/carers offering **free school meals** for their children subject to providing their bank details
- Unregistered **Charities** and “GoFundMe” style pages requesting financial donations and sponsorship for Covid-19 related projects
- Increase in **fake grant & funding** businesses



Keep Vigilant

Watch out for these emerging trends:

- Fraudsters requesting advance fees to assist with **emergency** supply chain procurement then **disappearing once payment has been made**
- Emails offering **TV License** refunds and **Supermarket** delivery slots
- Fake **websites** selling personal protective equipment and supplies
- Access to “free” **webinars**, online courses and **Corona tracking** Apps subject to providing personal & banking details
- An increase in PlayStation, console & **game-based malware**



Keep Vigilant

Watch out for these emerging trends:

- Illegal selling of **NHS prescription** medicines
- Delivery service phishing emails with **DHL, FedEx and UPS** logos
- Fake **payroll** and document **signing** links within emails
- Fraudulent **streaming sites** with insecure payment pages
- Department of Education **free IT equipment** emails



Keep Vigilant

Watch out for these current trends:

- Data **breaches** relating to remote working and **unauthorised** access to personal information
- There are concerns about unprotected devices that **would not be** permitted in the workplace being used by employees working at home
- **Disgruntled** furloughed/redundant employees stealing company information such as client lists and proposals
- With call centres moving to home working there are concerns that **organised crime groups** look to exploit



Stay Safe

Methods to keep you secure:

- Ensure remote laptop/device systems are secure and **updated**.
- Regularly update all **antivirus** software platforms.
- Secure your **home Wi-Fi network**.
- Make sure you are not using the **default password** which is written on the router – these can be easily found online!
- Apply **strong passwords** and implement **2-factor-authentication** on all devices.



Stay Safe

Methods to keep you secure:

- Report all suspicious emails to the National Cyber Security Centre (NCSC) at report@phishing.gov.uk
- <https://www.ncsc.gov.uk/information/report-suspicious-emails>
- **Do not** be tempted to make short cuts
- **Liaise** with your team members and **share** experiences of suspicious activity



Stay Safe

How can organisations protect themselves from fraud?

- **Awareness** is key. Ensure all colleagues know about these frauds.
- Keep talking with and **listen** to your employees, **understand** and where possible, **support** their challenges.
- If a **suspicion** of fraud has arisen, trust your instincts and develop the next course of action.
- **Notify** your bank immediately if you see any unusual activity on your account or suspect fraud has occurred.



Stay Safe

How can organisations protect themselves from fraud?

- **Verify** all invoices, as well as requests to change bank account details.
- Always **review** financial transactions to check for inconsistencies & errors, such as misspelt names of payees.
- To check if a request is legitimate, contact the supplier **directly** using established contact details you have on file, preferably by phone.



Stay Safe

How can organisations protect themselves from fraud?

- **Access** to sensitive financial information should be carefully controlled.
- Dispose of confidential documents by **cross-shredding** them.
- Perform **background checks** on all new vendors, agents, third parties to reduce the likelihood of fraud.
- Remain **vigilant** whilst working online, do not click on emails or links that you cannot verify.



Thank you

Neil Miller | Founder & CEO
neil.miller@tenintel.com
+44 (0) 7771 764050

Our Intelligence | Your Assurance

Moorgate | Kings Hill | Business Bay

Our Services

Due Diligence
Assurance
Financial Crime Compliance
Strategic Intelligence

Investigations
Corporate Fraud
Litigation Support
Digital Forensics

Protection
Brand Protection
Cyber Security
Data & Privacy



*Together, Reducing
Fraud Worldwide*

