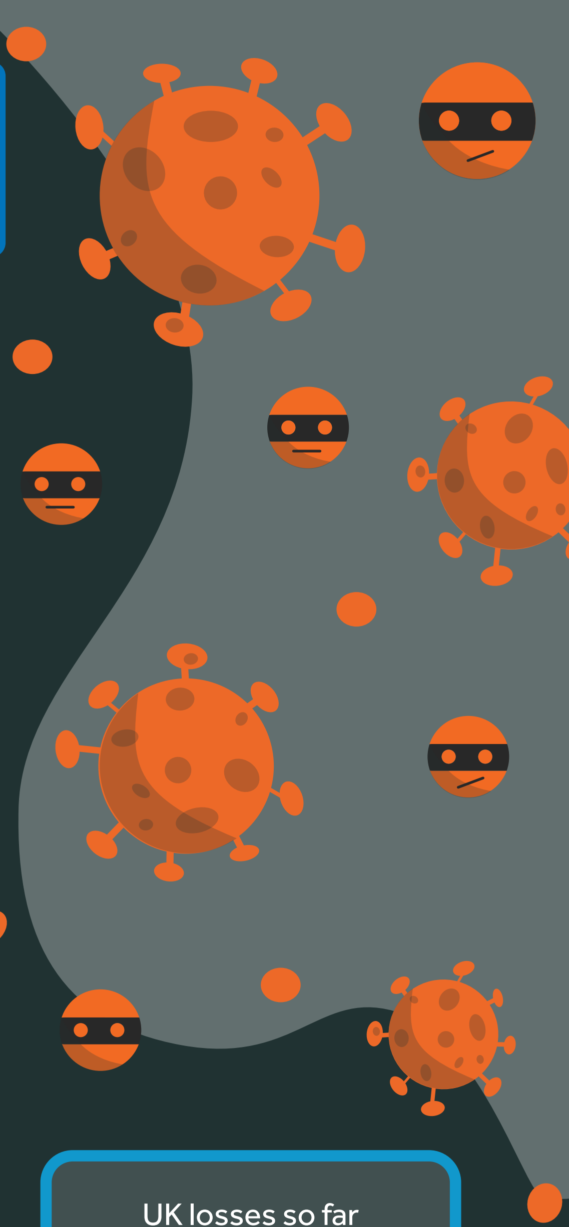
Fraud-watch:
COVID-19 and cybercriminals



IT is helping us work remotely, connect with colleagues and remain safe during the COVID-19 pandemic. But cybercriminals are exploiting the crisis – and the very technology that is helping us to retain business operations while socially distancing – to target companies and consumers with fraudulent communications.

Capitalising on an increased used of remote working technologies including personal devices, domestic WiFi, eBanking and email, sweeping changes to the way we work have presented a huge opportunity for criminals.
With the public urged by the NCSC to flag suspicious coronavirus comms, we wanted to share the most prevalent and high-risk scams and how you can increase your vigilance.

The COVID-19 scam numbers

At present,
3%
of all global spam
is now estimated to be
COVID-19 related

Google blocked
126 million
COVID-19 phishing
emails during one week
in April alone

UK losses so far
among those targeted
are estimated to be
£1.6m

There are at least
832 advance-fee
COVID-19 scams
where a large sum of money
is promised in return for a
set-up payment

More than
500 different
coronavirus-related scams
have been reported to UK
investigators

Don't fall for these fraud attempts

The most common scams in circulation are cruelly and immorally capitalising on the public's generosity, financial distress and sometimes confusion. We're seeing a trend for scams that:

- **Falsely represent health organisations and the NHS**
- **Pose as government sources, including HMRC**
- **Make fraudulent financial offers or debt collection requests**
- **Falsify charitable donation requests**

NHS medical supplies

Countless reports are logged daily regarding a scam email asking for donations to buy "medical preparations and supplies" for the NHS. Other NHS-related fraud includes a fake NHS 111 website that captures sensitive details and charges £5 to "talk to a doctor".

Lockdown fines

Scams purporting to be official messages from the Government include texts telling people they have been fined £250 for leaving their home more than once during lockdown. These emerged following the UK's "stay at home order" and still continue.

Financial support grants

Criminals are using UK Government branding to trick businesses and consumers using with HMRC branded emails and text messages that make spurious offers of financial support. These may reference coronavirus business interruption loans.

WHO health advice

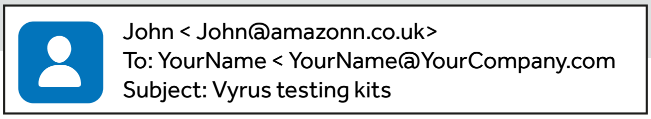
A spam campaign impersonating the WHO asks recipients to enter their details to receive personalised health advice. The communication intends to obtain personal information to sell on the dark web, use to commit identify theft or steal funds.

Goodwill groceries

A phishing email falsely claiming to be from the supermarket Asda states you can claim a £500 voucher. However, hackers are instead trying to obtain banking details. A similar WhatsApp scam is circulating purporting to be from Morrisons.

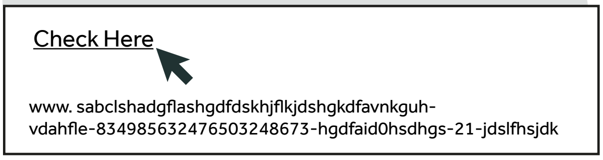
How to combat COVID-19 scams

1 Beware of emails with generic introductions, look out for **poor grammar and spelling**, and **check that the sender's email matches the domain of the organisation**



John < John@amazonn.co.uk>
To: YourName < YourName@YourCompany.com
Subject: Vyrus testing kits

2 **Double check links and email addresses** before clicking – hover over or long press the text



Check Here

www. sabclshadgflashgdfdskhjflkjdshgkdfavnkguh-vdahfle-834985632476503248673-hgdfaid0hsdhgs-21-jdslfhsjdk

3 Only access secure https websites and **visit authoritative websites** such as gov.uk or NHS.uk directly

4 **Do not download attachments** from suspicious emails or unexpected attachments – especially zipped files

5 No matter who you think it could be from, always be **suspicious** of an email that **asks for your personal or financial information**

🔒 ***** ?

6 **Do not open emails from untrusted sources** or give strangers the benefit of the doubt. Contact your IT department if you're unsure

7 Search online to see if **a scam resembling your email has been reported**. And report it yourself once the scam is verified by IT

8 Ask your IT team if business-grade **firewalls, email filtering and anti-malware** are in place on all remote devices

9 But most importantly, request **IT security training.** These attacks change constantly, so be aware of threats and appropriate responses

Email, text and website scams leading with COVID-19 are here to stay. Experts are predicting a new deluge of fraud focused on panicked money movement, money laundering via cryptocurrencies, and exploitation around business loans. With vigilance though, we can protect against theft and disruption. For more about internet-based cyber threats, visit **k3msp.com.**