CLEVELAND POLICE

Cyber Crime Newsletter

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

SCAM WARNING

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Coronavirus scam costs victims over £800k in one month

Since February 2020, the National Fraud Intelligence Bureau (NFIB) has identified 21 reports of fraud where Coronavirus was mentioned, with victim losses totalling over £800k. Ten of these reports were made by victims that attempted to purchase protective face masks from fraudulent sellers. One victim reported losing over £15k when they purchased face masks that were never delivered. Reporting numbers are expected to rise as the virus continues to spread across the world. We have also received multiple reports about coronavirus-themed phishing emails attempting to trick people into opening malicious attachments or revealing sensitive personal and financial information.

Watch out for scam messages: Don't click on the links or attachments in suspicious emails, and never respond to unsolicited messages and calls that ask for your personal or financial details

Shopping online: If you're making a purchase from a company or person you don't know and trust, carry out some research first, and ask a friend or family member for advice before completing the purchase. Where possible, use a credit card to make the payment, as most major credit card providers insure online purchases.

Protect your devices from the latest threats: Always install the latest software and app updates to protect your devices from the latest threats.

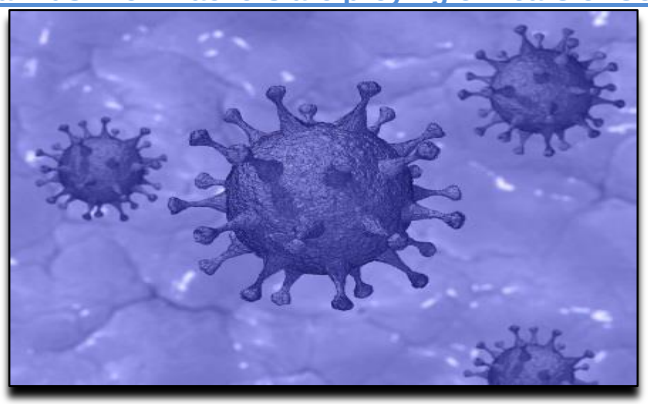
Coronavirus (COVID-19) information: how to stay safe
https://www.nhs.uk/conditions/coronavirus-covid-19/

For details, please visit: https://www.actionfraud.police.uk/alert/coronavirus-scam-costs-victims-over-800k-in-one-month

OTHER NEWS

BBC News

Coronavirus: How hackers are preying on fears of Covid-19



Security experts say a spike in email scams linked to coronavirus is the worst they have seen in years.

Cyber-criminals are targeting individuals as well as industries, including aerospace, transport, manufacturing, hospitality, healthcare and insurance.

Phishing emails written in English, French, Italian, Japanese, and Turkish languages have been found.

The BBC has tracked five of the campaigns.

1. Click here for a cure

Researchers at the cyber-security firm Proofpoint first noticed a strange email being sent to customers in February. The message purported to be from a mysterious doctor claiming to have details about a vaccine being covered up by the Chinese and UK governments.

The firm says people who click on the attached document are taken to a spoof webpage designed to harvest login details. It says up to 200,000 of the emails are being sent at a time.

"We have seen 35-plus consecutive days of malicious coronavirus email campaigns, with many using fear to convince victims to click," says Sherrod DeGrippo from the company's threat research and detection team.

Proofpoint says three to four variations are launched each day.

"It's obvious these campaigns are returning dividends for cyber-criminals," says Ms DeGrippo.

The best way to see where a link will take you is to hover your mouse cursor over it to reveal the true web address. If it looks dodgy, **don't click**.

2. Covid-19 tax refund

Researchers at cyber-security firm Mimecast flagged this scam a few weeks ago. On the morning they detected it, they saw more than 200 examples in just a few hours.

If a member of the public clicked on "access your funds now", it would take them to a fake government webpage, encouraging them to input all their financial and tax information.

"Do not respond to any electronic communication in relation to monies via email," says Carl Wearn, head of e-crime at Mimecast. "And certainly **do not click on any links** in any related message. This is not how HMRC would advise you of a potential tax refund."

3. Little measure that saves

Hackers pretending to represent the World Health Organization (WHO) claim that an attached document details how recipients can prevent the disease's spread.

"This little measure can save you," they claim.

But Proofpoint says the attachment doesn't contain any useful advice, and instead infects computers with malicious software called AgentTesla Keylogger.

This records every keystroke and sends it to the attackers, a tactic that allows them to monitor their victims' every move online.

To avoid this scam, be wary of emails claiming to be from **WHO**, as they are probably fake. Instead visit its official website or social media channels for the latest advice.

4. The virus is now airborne

The subject line reads: Covid-19 - now airborne, increased community transmission.
It is designed to look like it's from the Centres for Disease Control and Prevention (CDC). It uses one of the organisation's legitimate email addresses, but has in fact been sent via a spoofing tool.
Cofense, the cyber-defence provider, first detected the scam and describes it as an example of hackers "weaponising' fear and panic".
It says the link directs victims to a fake Microsoft login page, where people are encouraged to enter their email and password. Then victims are redirected to the real CDC advice page, making it seem even more authentic. Of course, the hackers now have control of the email account.
Cofense says the combination of a "rather good forgery" and a "high stress situation" make for a potent trap.

One way to protect yourself is to **enable two-factor authentication**, so that you have to enter a code texted or otherwise provided to you, to access your email account.

5. Donate here to help the fight

This example was reported to malware experts Kaspersky. The fake CDC email asks for donations to develop a vaccine, and requests payments be made in the cryptocurrency Bitcoin.
The premise is of course ridiculous, but the email address and signature look convincing.
Overall, Kaspersky says it has detected more 513 different files with coronavirus in their title, which contain malware.
"We expect the numbers to grow, of course, as the real virus continues to spread," says David Emm, principal security researcher at the firm.

For details and images of emails mentioned above, please visit: https://www.bbc.co.uk/news/technology-51838468

GET SAFE ONLINE
Get Safe Online
Free expert advice

Coronavirus scams you should be aware of

Globally, the number of infections and, tragically, deaths resulting from COVID-19 (Coronavirus) is increasing daily, and there is almost universal concern amongst people for their own health and that of their loved ones and communities. News bulletins, your email inbox and social media conversations are, understandably dominated by the subject.

Get Safe Online CEO Tony Neate is voicing serious concerns about the threats posed by the current situation online, quite apart from the physical dangers to our health, and widespread disruption caused by business closures, travel bans and enforced and self-imposed isolations. *"Whenever there's a crisis, you can be certain that there will be a rash of scams exploiting the situation. Sadly, Coronavirus is no exception.*

"At Get Safe Online, we've heard about a number of scams, from fake news to people offering vaccines. Even with my long career in cybersecurity, it never fails to amaze me how low some people will sink to exploit innocent people's uncertainty and misery."

In common with most other crisis situations, criminals are using emails, text messages, social media posts, online advertisements and phone calls to defraud their unsuspecting victims. The scams that we have heard about to date include:
- Fake advertisements for protective masks
- Fake advertisements for sanitising gel
- Fake advertisements for vaccines (these *do not* currently exist)

- Links to fake / sensational news, photos and video and unorthodox ways to gain protection, in reality designed purely to spread panic, gain clicks and sell newspapers.
- Appeals from fake charities (either with made-up names, or fraudsters impersonating real charities) for donations

In the case of the fake advertisements, hopeful customers make payments for the items, often by bank transfer, never to see the products they have ordered, nor their money, ever again. The links and email attachments generally lead to fraudulent websites which request your confidential details, or malware infections on the computer or other device you use to view them.

Neate explains why it is so easy for fraudsters to operate under the current circumstances: *"It's a double-whammy: most of us are understandably concerned or at least uncertain about what's going to happen in the short to medium term. This means that we might tend to drop our guard, and exercise less caution than usual when carrying out everyday tasks online."*

Get Safe Online expert advice

- Do not get tempted into ordering Coronavirus-related products online, especially if it calls for payment by any means except credit card (which normally affords additional protection).

- Do not believe in everything you read, but instead get your up-to-date Coronavirus advice from official sources such as:
  - HM Government: https://www.gov.uk/guidance/coronavirus-covid-19-information-for-the-public
  - NHS: https://www.nhs.uk/conditions/coronavirus-covid-19/

- Check the authenticity of charity appeals

- Be wary of approaches from supposed travel agents, tour operators, airlines, cruise companies, insurance companies or compensation firms promising to deal with refunds on travel, accommodation and event entry. If in doubt, call companies you have been dealing with, on the phone number you know to be correct.

Businesses

Many businesses are sending their employees home to work, where possible, and it is anticipated that this will increase as the virus extends its grip. Business owners are urged to provide training and advice on how to work remotely without compromising the safety and security of companies and their networks, data and devices. Tony Neate added this warning: *"Don't assume that your staff are necessarily up to speed on working safely at home ... it's a very different environment from the relatively secure systems and processes to be found in many offices. We have very comprehensive, easy to follow advice at getsafeonline.org/business."*

National Cyber Security Centre

News

Cyber experts step in as criminals seek to exploit Coronavirus fears

The public are being urged to follow online safety advice as evidence emerges that criminals are exploiting the Coronavirus online.
Experts from the National Cyber Security Centre have revealed a range of attacks being perpetrated online as cyber criminals seek to exploit COVID-19.

Techniques seen since the start of the year include bogus emails with links claiming to have important updates, which once clicked on lead to devices being infected.

These ‘phishing’ attempts have been seen in several countries and can lead to loss of money and sensitive data.
The NCSC, a part of GCHQ created to keep the UK safe online, is urging businesses and the public to

consult its online guidance, including how to spot and deal with suspicious emails as well as mitigate and defend against malware and ransomware.

In addition, in recent days the NCSC has taken measures to automatically discover and remove malicious sites which serve phishing and malware. These sites use COVID-19 and Coronavirus as a lure to make victims 'click the link'.

Paul Chichester, Director of Operations at the NCSC, said:
"We know that cyber criminals are opportunistic and will look to exploit people's fears, and this has undoubtedly been the case with the Coronavirus outbreak.
"Our advice to the public is to follow our guidance, which includes everything from password advice to spotting suspect emails.
"In the event that someone does fall victim to a phishing attempt, they should look to report this to Action Fraud as soon as possible."

The NCSC has seen an increase in the registration of webpages relating to the Coronavirus suggesting that cyber criminals are likely to be taking advantage of the outbreak.

These attacks are versatile and can be conducted through various media, adapted to different sectors and monetised via multiple means, including ransomware, credential theft, bitcoin or fraud.

Continued global susceptibility to phishing will probably make this approach a persistent and attractive technique for cyber criminals. Moreover, if the outbreak intensifies, it is highly likely that the volume of such attacks will rise.

There are numerous examples of cyber attacks worldwide since the Coronavirus outbreak.
On 16 February, the World Health Organisation (WHO) warned of fraudulent emails sent by criminals posing as the WHO. This followed a warning from the US Federal Trade Commission about scammers spreading phishing 'clickbait' via email and social media, as well as creating fraudulent websites to sell fake antiviral equipment.

Cyber criminals have also impersonated the US Center for Disease Control (CDC), creating domain names similar to the CDC's web address to request passwords and even bitcoin donations to fund a fake vaccine.

In January, attackers spread the Emotet banking trojan in Japan by posing as a state welfare provider to distribute infected Word documents. Similar operations have been observed in Indonesia, the US and Italy, with attackers attempting to spread the Lokibot infostealer, Remcos RAT and other malware.

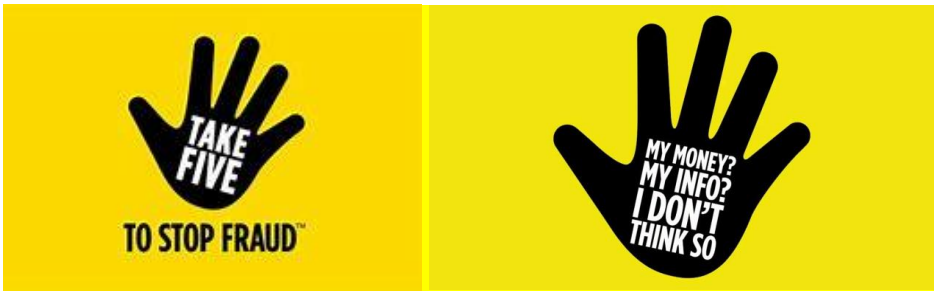
Individuals in the UK have also been targeted by Coronavirus-themed phishing emails with infected attachments containing fictitious 'safety measures.' According to Proofpoint researchers, such attacks have recently become more targeted, with greater numbers focusing on specific sectors like shipping, transport or retail to increase the likelihood of success.

For details, please visit: https://www.ncsc.gov.uk/news/cyber-experts-step-criminals-exploit-coronavirus

---

What is Take Five?

Take Five is a national campaign offering straight-forward, impartial advice that helps prevent email, phone-based and online fraud – particularly where criminals impersonate trusted organisations.



TAKE FIVE TO STOP FRAUD. Criminals are experts at impersonating people, organisations and the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment. Stop and think. It could protect you and your money.

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

TAKE FIVE TOOLKIT
We want organisations, businesses and individuals to be able to spread the message and get involved in the campaign so we can all help protect the nation against financial Fraud. Please support Take Five and make use of the full suite of campaign materials we have on offer.
To view campaign materials please visit https://takefive-stopfraud.org.uk/toolkit/

For further details visit www.takefive-stopfraud.org.uk

Information in this newsletter has been collated from following online sources;
www.getsafeonline.org
www.bbc.co.uk
www.actionfraud.police.uk
www.ncsc.gov.uk
www.takefive-stopfraud.org.uk

Should you become a victim of online crime please contact your local force on **101.** You can also report via **Action Fraud** using their online fraud reporting tool at **www.actionfraud.police.uk.**
Alternatively you can report to **Action Fraud** and get advice by calling **0300 1230 2040.**

If you would like to be added to the mailing list to receive monthly updates or if you have any queries and would like further details on any of the above please contact:

C8648 Adele Dack
Intelligence Researcher
Cyber Crime Unit

Middlesbrough Police Office | Bridge Street West | Middlesbrough | TS2 1AB
Website | Facebook | Twitter | Instagram | LinkedIn

CLEVELAND POLICE

Public Service Transparency Impartiality Integrity

"Delivering outstanding policing for our communities"