


FRAUD *Insight*

auditone
assurance . counter fraud . advisory

ISSUE 10 – MAY 2020

ALERT: BEWARE OF FRAUD SCAMS DURING COVID-19

Criminals are seeking to capitalise on the COVID-19 pandemic. At 15 May 2020, ActionFraud reported that 1,713 people had lost a combined total of over £3.6m to coronavirus-related scams. 7,796 reports have been received about coronavirus-related phishing emails.

Take Five to Stop Fraud is a national campaign that offers advice to help everyone protect themselves from preventable financial fraud. Everyone is encouraged to be more vigilant against fraud, particularly about sharing financial and personal information. People are asked to consider 4 things:

TAKE FIVE TO STOP FRAUD™

STOP Take a moment to stop and think before parting with your money or information.

CHALLENGE Could it be fake? It's okay to reject, refuse or ignore any requests. Be cautious and listen to your instincts.

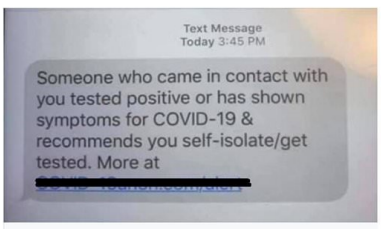
PROTECT Contact your bank immediately if you think you've fallen for a scam. Protect your financial information, especially from people you don't know. Your bank, the police or NHS will never ask for your bank details.

REPORT If you notice anything suspicious contact the police by calling 101 or 999 in an emergency. If you think you have been a victim of fraud or cybercrime, report it to ActionFraud (contact details below).

Further information on Take Five to Stop Fraud can be found at **https://takefive-stopfraud.org.uk/**

PUBLICITY: SCAMMERS TARGET NHS CONTACT TRACING APP BEFORE NATIONAL ROLLOUT

Example of fake text message



Scammers are sending text messages that impersonate the NHS's new contact tracing app before it has even been released. Deceptive texts seen by the Chartered Trading Standards Institute tell people they have been in contact with someone who has tested positive for the virus.

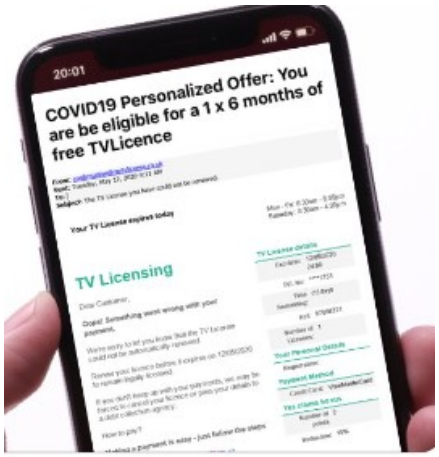
The scam text (shown left) reads: 'Someone who came in contact with you tested positive or has shown symptoms for COVID-19 & recommends you self-isolate/get tested.' The text provides a fake link which will ask for your personal information.

Anyone who receives texts or other similar messages (WhatsApp, etc.) asking for personal information should not click on any accompanying links and report them to ActionFraud.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk
0300 123 2040

ACTIONFRAUD: NEW VERSION OF FAKE TV LICENSING EMAILS

ActionFraud have seen a large volume of TV Licensing phishing emails circulating, but in the last week, have received 70 reports of a new version of this common scam.



These emails, purporting to be from TV Licensing, claim that the recipient's direct debit has failed and that they need to pay to avoid prosecution. Recipients are told that they are eligible for a "COVID19 Personalized Offer" of six months free.

The messages contain links to genuine-looking websites that are designed to steal personal and financial information.

Always question unsolicited requests for your personal or financial information in case it's a scam. Never automatically click on a link in an unexpected email or text.

Go to actionfraud.police.uk/covid19 for up to date information on common COVID-19 scams. They also have information on how to protect yourself when shopping online or using auction sites at actionfraud.police.uk/covid19-shopping.

NON NHS CASE: ANIMAL LOVERS DEFRAUDED OF ALMOST £300K IN TWO MONTHS

ActionFraud have received over 1000 reports of criminals taking advantage of the lockdown to commit fraud involving the purchase of pets, such as puppies and kittens. So far, 669 people have lost a combined total of £282,686 in March and April, after putting down deposits for pets they have seen advertised online. The adverts that victims have responded to were posted on social media, general online selling platforms and also specific pet selling platforms. The criminals posting these adverts never have any animals to sell and will ask victims to put down a deposit for the pet to secure the purchase. After the initial payment more and more funds will be requested to cover insurance, vaccinations and even delivery of the pet which is never delivered. To help protect yourself from scams like this they provide the following advice:

- **Do your research** - before purchasing anything online, including pets, look up reviews for the site, or person, you are buying from. If you're still not sure, ask a trusted friend or family member for their advice
- **Trust your instinct** - If you can't physically go to see the animal in person, ask for a video call. If the seller declines, challenge them on why. If you have any suspicions, don't go ahead with the purchase
- **Choose your payment method wisely** – If you decide to go ahead with the purchase, avoid paying by bank transfer as that offers you little protection if you become a victim of fraud. Instead, use a credit card or a payment service such as PayPal

> "Anyone who is concerned about a breeder or seller should walk away and contact the local council and RSPCA on 0300 1234 999."
>
> RSPCA Spokesperson

ZOOM: VIDEO CONFERENCING SECURITY

Zoom is a video conferencing platform, currently being used by 300 million users on a daily basis. Security and privacy issues have been recently publicised, including "Zoom bombing" where uninvited guests crash your meeting or chat, often sharing offensive content. One of the most effective ways to increase your security is by accessing Zoom via the web interface, rather than accessing it via the app.

The following guidance is intended for both home and business use, to help keep users secure:

Zoom—What to do:

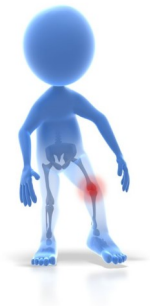
- Make sure you have the latest version of the Zoom software. Click your user icon and select 'Check for Updates'. Version 5 was recently released and has provided increased security features
- Running anti-virus software or a firewall on your computer and keeping software up-to-date will improve your security
- If you are holding public meetings, where anyone can join the conversation, be sure to configure screen-sharing settings
- Go to 'In Meeting (Basic)' and select 'host alone can share' or turn off screen sharing entirely. This can also be controlled by the host during a meeting
- Finally, turn off 'Annotation', if you are worried about how people might annotate your shared slide show

Stop uninvited guests:

- Setting up a Zoom meeting now creates an 9 digit ID. Anyone with this ID can join the conversation—don't advertise it publicly by posting it on social media
- Go to the 'Options Panel' when setting up a meeting and add an access password too. Would-be trolls now need an ID and password to crash your meeting
- Waiting rooms are now enabled by default—people are put in a holding area before you grant or deny their access
- Organisers can lock the meeting once everyone, who needs to has joined. Click Manage Participants>More>Lock Meeting

Remember to stay private—turn off video and mute yourself unless needed.

NON NHS CASE: MAN DELIBERATELY INJURES HIMSELF IN INSURANCE FRAUD



A man has been sentenced to a 2-year community order after CCTV caught him purposely banging his knee on a paving stone in order claim over £6k for a fake injury. Despite being shown the CCTV footage several times in interview, which clearly showed his claim was fraudulent, he continued to deny any wrongdoing and told police they were misinterpreting the footage. Eventually he pleaded guilty before his trial began.

He submitted an injury claim stating that a paving stone had cracked underfoot as he jogged back to his block of flats, causing him to fall over and injure his knee. However, CCTV footage supplied to police by the housing association clearly showed that this is not what happened. The CCTV showed him step on the paving stone to break it and proceed to deliberately bang his knee on a nearby paving stone. He eventually spots the CCTV camera, and at this point, starts to hop on one leg to try and show that he had been injured. When shown the footage, he initially said he tripped and fell just out of shot of the CCTV and claimed that the footage showed him testing the other paving stones [with his knee] to prevent injury to other people. The CCTV footage used by the police as evidence can be viewed at **https://youtu.be/LKBpvk47xno**.

COVID-19 CASE: MAN CHARGED WITH MAKING COUNTERFEIT COVID-19 KITS

A man charged with making counterfeit treatment kits for COVID-19, and sending them across the world, has appeared in court.

Officers from the City of London Police's Intellectual Property Crime Unit (PIPCU) arrested the 59 year old in a post office near to his home address. He was charged with one count of fraud by false representation, one count of possession of articles for use in fraud, and one count of unlawfully manufacturing a medicinal product. The man's arrest follows a joint investigation by PIPCU, the UK's Medicines and Healthcare products Regulatory Agency (MHRA) and the U.S. Food and Drug Administration (FDA).

One of the fake kits (© City of London Police)

The case originated when the U.S. Customs and Border Protection Agency in Los Angeles intercepted a package on 18 March, containing 60 separate COVID-19 treatment kits labelled as 'Anti-Pathogenic treatment', which were sent from the UK. The FDA determined the product to be an unapproved drug based on the labelling and directions for use and alerted the MHRA in the UK. The case was passed to PIPCU and the man was arrested by police officers in a post office attempting to send 60 more fake treatment kits to France, the U.S., and other parts of the UK.

The kits are thought to contain potassium thiocyanate and hydrogen peroxide, both of which are extremely harmful chemicals when the user is instructed to wash and rinse their mouth with them.

During a search of the suspects home, 300 more treatment kits and an estimated 20 litres of chemicals used in the production of the fake kits, were discovered. The case is ongoing.

MEET THE COUNTER FRAUD TEAM

Terry Smith

Head of Service

T: 0191 441 5939

E: terry.smith@audit-one.co.uk

Rebecca Napper

Counter Fraud Manager

T: 0191 441 5941

E: rebecca.napper@audit-one.co.uk

Michelle Watson

Counter Fraud Manager

T: 0191 333 3074

E: michelle.watson@audit-one.co.uk

Paul Bevan

Counter Fraud Specialist

T: 0191 441 5918

E: paul.bevan@audit-one.co.uk

Gemma Collin

Counter Fraud Support

T: 0191 333 3011

E: gemma.collin@audit-one.co.uk

Martyn Tait

Counter Fraud Specialist

T: 0191 333 6218

E: martyn.tait@audit-one.co.uk

Iain Flinn

Counter Fraud Specialist

T: 0191 441 5935

E: iain.flinn@audit-one.co.uk

Nikki Cooper

Counter Fraud Specialist

T: 01482 866 800

E: nikki.cooper@audit-one.co.uk

Stephen Veitch

Counter Fraud Specialist

T: 0191 333 3012

E: stephen.veitch@audit-one.co.uk

Kathryn Wilson

Counter Fraud Specialist

T: 0191 441 5933

E: kathryn.wilson@audit-one.co.uk

Simon Clarkson

Counter Fraud Specialist

T: 01228 635 597

E: simon.clarkson@audit-one.co.uk

Gary Ross

Security Management Specialist

T: 0191 333 3011

E: gary.ross@audit-one.co.uk

David Wearmouth

Counter Fraud Specialist

T: 0191 333 3011

E: dave.wearmouth@audit-one.co.uk

James Paxton

Counter Fraud Specialist

T: 0191 333 3011

E: james.paxton@audit-one.co.uk

FRAUD REPORTING HOTLINE

0191 441 5936

NATIONAL FRAUD REPORTING HOTLINE

0800 028 4060