COVID-19 Fraud

Table of Contents

Key Messages

1. Criminals will use every opportunity they can to defraud innocent people. They will continue to exploit every angle of this national crisis and we want people to be prepared.
2. We are not trying to scare people at a time when they are already anxious. We simply want people to be aware of the very simple steps they can take to protect themselves from handing over their money, or personal details, to criminals.
3. Law enforcement, government and industry are working together to protect people, raise awareness, take down fraudulent websites and email addresses, ultimately bring those responsible to justice.
4. If you think you have fallen for a scam, contact your bank immediately and report it to Action Fraud on 0300 123 2040 or via actionfraud.police.uk. If you are in Scotland, please report it to Scotland Police directly by calling 101.
5. You can report suspicious texts by forwarding the original message to 7726, which spells SPAM on your keyboard. You can report suspicious emails by forwarding the original message to report@phishing.gov.uk. An automated system will scan the email and if malicious links are found, the associated website will be taken down.

Key protection advice for individuals

Criminals are experts a impersonating people, organisations and the police. They spend hours researching you hoping you'll let your guard down just for a moment.

They can contact you by phone, email, text, on social media, or in person. They will try to trick you in parting with your money, personal information, or buying goods or services that don't exist.

If you are approached unexpectedly remember to:

- **Stop**: Taking a moment to think before parting with your money or information could keep you safe.
- **Challenge**: Ask questions like 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 you bank immediately if you think you've fallen victim to a scam and report it to Action Fraud.

Some other points to remember include:

- The police or your bank will never ask you to withdraw money or transfer it to a different account. They will never ask you to reveal your full banking password or PIN.
- Do not click on links or attachments in unexpected or suspicious texts or emails.
- Confirm requests are genuine by using a known number or email address to contact organisations directly.
- To keep yourself secure online, ensure you are using the latest software, apps and operating systems on your phones, tablets, and laptops. Update these regularly or set your devices to automatically update so you don't have to worry.

The Nation Cyber Security Centre (NCSC) has launched the Cyber Aware campaign with six actionable steps to protect yourself. By implementing the six 'Cyber Aware' tips and flagging threats

to the NCSC, you will keep yourself and others secure from the vast majority of threats. To find out more visit CyberAware.gov.uk.

Key protection advice for businesses

Criminals don't change their ability when it comes to businesses. They are still good at what they do and experts at impersonations. Again, in the hope that you will let your guard down for a moment.

Stop: If you receive a request to make an urgent payment, change supplier bank details, or provide financial information, take a moment to stop and think.

Challenge: Could it be fake? Make sure to verify all payments and supplier details directly with the company on a known phone number or in person first.

Protect: Contact your business's bank immediately if you think you have been scammed and report it to Action Fraud.

Keeping your business secure online

Threat actors will try to gain access to your device or network and everything stored on it. They can do this by:

- Sending emails with malicious attachments
- Exploiting vulnerabilities in the operating system if they are not up-to-date
- Trying to get you to click the links or visit malicious websites

Once they have achieved this, you are essentially granting them access to your device and your data on that device, which they may proceed to extract money from you by getting you to pay a ransom after encrypting your data. There are a number of steps you can take in order to protect your device, its operating system, and educate others on your network. Please visit the NCSC's website to find out more.

You can also read the National Cyber Security Centre's Small Business Guide: Cyber Security for more advice on how to keep your business secure online.

Agreed lines on specific issues

Press release

What is happening to fraud levels in general?

While fraud reporting levels into Action Fraud and the Financial Conduct Authority have not increased, we have seen a number of different scams circulating relating to COVID-19. This includes people falling victim to online shopping scams such as believing they are purchasing protective face masks or hand sanitiser that, in reality, do not exist. Criminals are also using Government branding to try to trick people, including using HMRC branding to make spurious offers of financial support through unsolicited emails, phone calls and text messages. We have also seen fake websites and emails purporting to be genuine companies.

This situation is likely to continue, with criminals looking to take advantage of the pandemic such as exploiting people's financial concerns to ask for upfront fees fraudulently applied to bogus loans; offer high-return investment scams; or target pensions.

Huge increases in the number of people working remotely presents an opportunity for criminals to commit computer software service fraud, which involves offers of help to fix devices. As IT systems are under increased pressure, making them work more slowly, such offers of help may seem more believable. In reality, criminals are trying to gain access to your computer or get you to divulge your login details and passwords. Visit the NCSC website for home working guidance and suspicious email advice.
It is also anticipated that there will be new phishing scams or calls claiming to be from government departments offering grants, tax rebates, or compensation.

What do you expect to see in the next few weeks? Months? Next year?

Fraud is incredibly hard to predict and while we are monitoring crime trends carefully, the most important thing is to get the message out there to the general public to be aware, be alert, and think twice before parting with their money or personal details. Always remember to stop, think, and challenge any requests for personal information or financial details.

The government, law enforcement, security agencies, regulators and the private sector are continuing to work together to protect the public and businesses from all types of fraud.

Government smishing

The Government has only sent one text message to the public regarding new rules about staying at home to prevent the spread of COVID-19. Any others claiming to be from UK Government are false.

Criminals are able to use spoofing technology to send texts and emails impersonating organisations that you know and trust. If you receive an unexpected text or email, asking for personal or financial details, do not respond. Remember, don't click on the links or attachments in any texts or emails and instead visit the official website through a known route.

The public can report any type of SMS scams by forwarding the original message to 7726, which spells SPAM on your keypad.

Universal Credit scam

Secretary of State for Work and Pensions Therese Coffey:

"We know cyber criminals and fraudsters are despicably attempting to exploit opportunities around coronavirus. DWP will never text or email asking for your personal information or bank details. Anyone who thinks they have been a victim of fraud should report it to Action Fraud, and notify DWP, as soon as possible."

Additional Information:

- For latest information on Universal Credit go to https://www.understanduniversalcredit.gov.uk/.
- We urge people not to click on the links or attachments in suspicious emails, and never respond to unsolicited messages and calls that ask for personal or financial details.

- We continue to work with Action Fraud and the National Fraud Intelligence Bureau to shut down sites and posts which promote this type of fraud.

UPDATE 21 May 2020

A DWP spokesperson said:

"Our focus is on getting money to those who need it and thanks to the extraordinary efforts of staff, since mid-March we've managed to process more than two million new claims for Universal Credit.

"We continue to monitor benefit fraud very closely and will relentlessly pursue the minority attempting to abuse the system using the full range of available powers, including prosecution through the courts.

"Our detection systems make use of increasingly sophisticated techniques to identify discrepancies and thwart those seeking to rip off taxpayers."

Further briefing:

- DWP has one of the most sophisticated counter fraud capabilities, both in intelligence and investigations, in government, and continues to stamp out organised crime. Our serious organised crime capability has been maintained throughout the current outbreak.

To what extent are the government support schemes vulnerable to abuse by criminals?

A government spokesperson said:

"We take fraud against the public sector seriously.

"Sadly, the government's stimulus packages are at risk of fraud, from those who would seek to take advantage in these circumstances.

"Public servants across government are looking for ways to reduce the instances of fraud, and take action against those who do try and commit fraud. To support this, the Cabinet Office has established a COVID-19 Counter Fraud Response Team. This team is working with departments to identify fraud risks and put in place measures to reduce the impact and harm of fraud against the government.

"The government wants to keep fraud as low as it can to make sure the stimulus funding is as effective as possible.

"The team are also working collaboratively to understand wider threats of fraud, and to take action, with the NECC, NCA, City of London Police and partners."

Please check GOV.UK for information on how to recognise genuine HMRC contact and on how to avoid, and report, scams. Check HMRC-related phishing, or bogus, emails or text messages against examples published on GOV.UK.

Please visit the GOV.UK website for all the information required to seek support at this time and

apply for stimulus packages.

Advice for businesses in regards to people working from home

Many organisations are either moving towards working remotely for the first time or significantly increasing it, which presents a number of cyber security challenges. Advice on how to respond to those challenges is set out in the NCSC's working from home guidance.

There are a number of practical steps an organisation can take to reduce the risk, including:

- Supporting people to use stronger passwords and setup two-factor authentication.
- Ensuring staff know how to report threats, especially those related to security.
- Creating 'How to' guides for new software and tools staff may be using.
- Utilising VPNs to allow users to securely access the organisation's IT services.
- Ensuring devices encrypt data while at rest.

Some organisations may be allowing staff to use their own devices to work remotely. In this case, please refer to the NCSC's Bring Your Own Device (BYOD) guidance.

Additionally, it is worth being aware of phishing emails, which attempt to trick users into clicking a malicious link or an attachment. Once clicked the user will be sent to a malicious website, which could automatically download a program onto your computer without you knowing, or steal you passwords. For attachments, the user could be promoted to enable macros, which again can install malicious software on your computer and steal data and/or passwords. Cybercriminals are opportunistic and will look to take advantage of people's fears, there is evidence that the coronavirus outbreak is being exploited in this way.

Those who do fall victim should not feel bad – these scams can be extremely convincing – but what they should do, as quickly as possible, is report it to their IT department when the incident is work-related or Action Fraud when it is personal. Users can also open their antivirus (AV) software if installed, if it is not you should turn it on, and run a full virus scan and follow any instructions given. If a user has been tricked into giving their password, they should change their password for all their accounts. But hopefully they have not been reusing their passwords.

The NCSC's guidance on suspicious emails provides more tips on this.

As a further resource, the Global Alliance has created a 'Work from Home Community Forum' support group, where subject matter experts are on hand to answer specific questions about security issues related to working from home.

Action Fraud Interview

An Action Fraud spokesperson said:

"Fraudsters will use any opportunity they can to take money from the public. This includes exploiting tragedies and global emergencies.

"While the pandemic has created opportunities for criminals to exploit, reports of fraud to Action Fraud have not increased during the COVID-19 outbreak. Reports of investment fraud have also not

increased. However, it can take some time before an investment scam is spotted by its victims. We are monitoring this, and all crime types, very closely.

"It is likely that criminals will continue to attempt to exploit the impact of COVID-19 on the economy and people's personal finances, as they did after the financial crisis in 2008. This could lead to a rise in fraudulent investment schemes, so we would advise people to remain vigilant at this time. If you are thinking about making an investment, please check the FCA's register to make sure the company is regulated. If you deal with a firm or individual that isn't regulated, you may not be able to get your money back if something goes wrong."

Top tips for spotting an investment scam:

- You're contacted out of the blue by phone, email or social media about an investment opportunity;
- You're pressurised into making a decision with no time to consider the investment;
- You're offered a high return on your investment with apparently little or no risk;
- You're told the investment opportunity is exclusive to you.

If you think you've fallen victim to a scam, please report it to Action Fraud via actionfraud.police.uk or by calling 0300 123 2040.

Suspicious email and reporting service

The National Cyber Security Centre (NCSC) has launched a suspicious email reporting service in partnership with the City of London Police. This service makes it easier than ever to flag suspicious emails – including those claiming to offer services related to coronavirus.

Members of the public can send their suspicious emails to report@phishing.gov.uk and the NCSC#s automated program will immediately test the validity of the address. If there are any issues found within the email that are phishing scams, will be removed.

As well as taking down malicious sites, the service will support the police by providing live time analysis of reports and identifying new patterns in online offending – helping them to stop even more offenders in their tracks.

Phishing/Smishing definitions

Phishing: These are emails that contain a call to action by encouraging the recipient to visit a website that criminals use for various unsolicited activities, such as stealing user credentials and other personal information. They often use a sense of urgency to trick recipients into making a rash decision and not inspecting the email closely.

In the majority of scams, if the recipient clicks on the link, a spoofed login page appears that includes a password entry form, very similar, if not identical, to the legitimate website. These spoofed website login pages may relate to a wide array of online services, such as email services provided by Google or Microsoft, or services accessed via a government websites. If credentials and personal information are entered on these spoofed websites, criminals will be able to access the individual's online accounts, wherever these credentials are used. This can then be utilised to retrieve further

personal information or to further disseminate phishing emails, using the compromised email's address book.

SMS Phishing (Smishing): The term 'smishing' describes a phishing attempt delivered by SMS text message rather than via email. These messages also contain a call to action and encourage the recipient to click on a malicious link. Historically, this type of attack has often used finance incentives, such as including government payments and tax rebates, as the bait to lure you in. Coronavirus-related smishing continues this financial theme, exploiting the economic impact of the pandemic and employment and financial support packages being offered by the government. It is also good to note that these messages can be disseminated through other channels, such as WhatsApp and other in app messaging services.

Phishing for malware deployment

A number of cyber criminals have used Covid-19 related lures to deploy malware. Most cases begin with an email that persuades the recipient to open an attachment or download a file from a linked website. When they do this, malware is executed, which compromises their system.

Fake certification for PPE

Lines issued by the Office for Product Safety and Standards (part of BEIS).

A Government spokesperson said:

"To get PPE to frontline staff as quickly as possible the Government has eased administrative requirements without compromising safety.

"All PPE on the market must meet essential safety requirements, and the Office for Product Safety and Standards is working closely with local authorities, the Health and Safety Executive, Medicines and Healthcare Regulatory Agency and National Crime Agency to prevent unsafe PPE reaching the marketplace and the NHS."

Additional Information:

- The Office for Product Safety and Standards has produced guidance for business on the regulations which outlines the steps the Government has already taken to speed up supply of PPE. OPSS guidance on the legislation that governs PPE can be found here.
- Any manufacturer who can help produce much-needed PPE must ensure it first meets essential safety requirements and register at www.gov.uk/coronavirus-support-from-business.
- On fake certificates, intelligence is being investigated by a combination of authorities, including the NCA. We can't comment on specific cases.

NHS test and trace

If NHS Test and Trace calls you by phone, the service will be using a single phone number 0300 0135 000. The only website the service will ask you to visit is https://contact-tracing.phe.gov.uk.

Contact tracers will never:

- Ask you to dial a premium rate number to speak to us (i.e., those starting 09 or 087).
- Ask you to make any form of payment.
- Ask for any details about your bank account.
- Ask for your social media identities or login details, or those of your contacts.
- Ask you for any passwords or PINs, or ask you to set up any passwords or PINs over the phone.
- Ask you to purchase a product.
- Ask you to download any software to your device or ask you to hand over control of your PC, smartphone or tablet.
- Ask you to access any website that does not belong to the Government or NHS.

Latest update from the NFIB

AS of 23:59hrs on Wednesday 27 May 2020

Total reports to Action Fraud = 2,057
Total losses = £4,690,996
Total reports of phishing to Action Fraud = 11,206
(as of 27/4/20, includes figures from NCSC suspicious email reporting service)

COVID-19 related fraud makes up around 3% of all fraud reports received to Action Fraud at the moment.

What scams are the NFIB seeing?

The majority of reports are still related to online shopping scams where people have ordered protective face masks, hand sanitiser, COVID-19 testing kits, and other products, which have never arrived. In a lot of cases, if they have arrived, they have been sub-standard.

Other frequently reported scams include:

- Suspect advertises a vehicle for sale online but says it can't be viewed in person, due to the lockdown restrictions. The suspect instead arranges for the vehicle to be delivered using a delivery company. The victim pays for the vehicle (or a deposit), but the vehicle is never delivered. The victim is given the option of paying by bank transfer or through PayPal. The PayPal link they're provided with is a spoofed site.

- Suspect advertises a pet online (puppy or kitten) and uses the outbreak as a reason the victim can't come and see the animal. The suspect sends photos and persuades the victim to make a payment in advance. The suspects will often try to get the victim to pay additional unforeseen costs (insurance, vaccinations) after they've made the initial payment but never provide the pet.
  NOTE: Action Fraud have issued a press release on this scam which can be found on their website.

- Victim tried to apply for a government grant to assist their business during the outbreak but was informed their business had already received a grant and were therefore not eligible for

any more financial assistance. The victim did not make this initial application and does not recognise the account the payment was made to.

- Suspects are incorporating the coronavirus pandemic into push payment frauds and using the outbreak to convince victims to speak with the suspect on the phone, saying the banks are closed etc.

Trends

- There have been 3 reports of courier fraud in the last 24 hours and 37 in the previous week. To help in getting protect messaging out, we have uploaded a number of social media assets to the resources section of the Action Fraud website for people to utilise.

- The highest loss reported in the last 24 hours was for £41,616, which related to a bulk order for wall mounted hand gel dispensers which never arrived. These dispensers were ultimately supposed to be for the NHS.

- Other high losses included: a dating fraud in which the suspect claimed to have contracted the coronavirus and needed help with medical bills; and a suspect using the government's furlough scheme to claim for an individual who doesn't work for them.

Phishing/smishing

HMRC phishing emails

Context from HMRC spokesperson.

We continue to see emails purporting to be from HMRC, titled *'Helping you during this covid from government*' and sent from the email address HMRC@hotmail.com. The email offers a grant of between £2,500 and £7,500 to tax payers out of work or working less because of the pandemic. The recipient is told to click on a link to check their eligibility.

We are also seeing emails sent largely from different Hotmail accounts but the sender name is spoofed to read 'HMRevenue & Customs(HMRC)'. The message informs the recipient that they are eligible for a £698.99 tax refund which they need to claim within 24 hours by clicking on a link. The link has been identified as malicious.

Bitcoin investment

We continue to receive a high number of reports about emails advertising investments in Bitcoin platforms that claim to "take advantage of the financial downturn" and can help people recover from bankruptcy. A link is provided in the email which claims to take recipients to a website that explains how Bitcoin trading platforms work. This link has two main threats; one for phishing and one for malware, where the suspect is trying to steal credentials and/or get the recipient to download a virus.
NOTE: Action Fraud have posted an alert about this scam on their Twitter page.

TV Licensing

We continue to see a large number of fake TV Licensing emails but there have been minor changes to the messaging and links, with some including a COVID-19 related hook. The emails now being reported claim that the recipient's direct debit has failed and that they need to pay in order to avoid prosecution.

These emails display the subject header *"We couldn't process the latest payment from your Debit Card - COVID19 Personalized Offer: You are be eligible for a 1 x 6 months of free TVLicence"*. They include a link to set up a new direct debit on a website controlled by the criminals.

At the end of this email to lure recipients in, the fraudsters are also offering six months of free TV licence. Recipients are asked to click on a link to apply for the offer. The link takes them to a sign in page where they are asked to complete an online application form, providing the criminals with an opportunity to steal email logins, passwords, and personal details.
NOTE: Action Fraud have posted an alert about this scam on their Twitter page.

GOV.UK council tax reduction

Fake Government emails are still circulating that claim to help individuals on benefits, or a low income, pay for their council tax. The subject line of the email reads: '*Online application – (COVID-19) – You are getting a Council Tax Reduction (Total amount of benefits: GBP 385.55) Stay at home this weekend'*. The recipient is told that they are eligible for a council tax reduction and are asked to click on a link in order to claim the benefit which will be automatically transferred to their debit/credit card. The sender name has been spoofed to read 'Council Tax – GOV.UK'.
NOTE: Action Fraud have posted an alert about this scam on their Twitter page.

International cash grants and relief funds

There has been a new phishing attempt reported, claiming to be from the World Health Organisation (WHO), offering cash intervention grants to selected individuals for the sum of $950,000 as a result of the outbreak. This is a similar MO to what has been reported before, although there has been some minor changes to the messaging content and the contact email address used by the criminals to deceive recipients. Recipients are told they will receive their funds through an ATM card insurance and are asked to contact the sender via email (manager@swisscard.org) for more information on how to receive these funds. They are told they need to respond within 10 days to ensure they receive these payments.

Another new but similar type of phishing attempt has emerged, purporting to be from the IMF Global Pandemic Relief Fund, informing recipients that they have been awarded a sum of $650,000mil dollars by the fund as a result of the outbreak. Recipients are asked to contact the bursary official to request for further details on how to receive the money.