Cyber Resilience COVID-19 Bulletin

ISSUE: 04.06.20

Scottish Government
Riaghaltas na h-Alba
gov.scot

As a result of the significant rise in COVID-19 related scams, over the next few months, the Scottish Government Cyber Resilience Unit will share important information on current cyber resilience issues. We aim to update the Bulletin on a weekly basis and ask that you consider circulating the information to your networks, adapting where you see fit. Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from trusted sources.

This Bulletin is also available online here.

We are looking to measure and improve the Bulletin readers' experience and satisfaction. Please answer this short survey to share your thoughts.

National Cyber Security Centre (NCSC)

NCSC produce weekly threat reports drawn from recent open source reporting. View this week's report here.

Scotland's Serious Organised Crime Taskforce

Organised crime gangs are targeting vulnerable people at home and in the care sector during the Covid-19 crisis, the Scottish government has warned. Justice Secretary Humza Yousaf described the tactics as "abhorrent, but not unexpected". Mr Yousaf, who chairs Scotland's Serious Organised Crime Taskforce, has urged the public and businesses to be alert to gangs looking to "exploit their fears and concerns". The government and police taskforce has now issued official guidelines on how to spot and report suspicious activities. Details within these Bulletins will help protect you against COVID related online scams.

If you've been a victim of coronavirus-related or any other fraud**, report it to Police Scotland by calling 101** (not Action Fraud).

- **If you have received an email you're not quite sure about, forward it to NCSC's Suspicious Email Reporting Service (report@phishing.gov.uk) then delete it. The service has received over 687,000 reports in the six weeks since it launched. To date these reports have enabled to removal of 1,472 malicious websites.**
- **Forward scam texts to 7726 (the numbers spell "SPAM" on your keypad).**

Returning to work

Over the coming weeks many people will be returning to work from furlough and switching on computers and opening email inboxes for the first time in months. But as we do that, what are some of the cyber security considerations we should be thinking about? Police Scotland recommend that you:

- **Install updates - consider running an update to see what patches, or updates, are available for your system as these may contain vital security improvements. Make sure to have an up-to-date back-up of your system in case you need it.**
- **Phishing Emails - Be on the lookout for any phishing emails. Do not click on any links in a suspicious email, report it to your IT department or provider and remember to forward it to the NCSC's Suspicious Email Reporting Service – report@phishing.gov.uk.**
- **Mandate fraud - You may also find some "urgent" invoices requesting immediate payment in your inbox. Using social engineering cyber, criminals can learn who you do business with and then send you fake invoices in that company's name. We call this "mandate fraud" and some of the tell-tale signs are an urgency with the request and also a request to change bank details. If you are unsure then never immediately pay and use a trusted telephone number to contact the company and confirm the request.**

Another issue to be aware of as we all continue to work much more with technology is "crypto-jacking". This is the unauthorised use of a computer, tablet, mobile phone, or connected home device by cybercriminals to steal cryptocurrency like Bitcoin. Hackers trick victims into downloading a malicious file that forces their computers to mine for this money which can be turned it into mainstream cash. Victims may receive a legitimate looking email that encourages them to click on a link, or visits a website infected with malware, or when an infected advert pops up malicious code automatically runs.

After installing malware on compromised devices, criminals will use the processing power of the device to run a malicious script in the background. There have been at least a dozen supercomputers across Europe shut down after hackers targeted them with crypto-jacking attacks. As with any other malware infections, there are some signs your device is used for crypto-jacking. These include:

- **High processor usage on your device**
- **Sluggish or unusually slow response times**
- **Overheating of your device**

For more advice and information on crypto-jacking malware access the NCSC website. There is a range of useful information and guidance available for businesses on the National Cyber Security Centre Website and remember if you are the victim of any type of fraud report it immediately to **Police Scotland on 101**.

Trending Topics

Google Scam Spotter

Google has launched a new website called Scam Spotter. Google has partnered with the Cybercrime Support Network and says this will help people identify and avoid common scams on the internet. The

website teaches the three golden rules of scam spotting: '**Slow it down, Spot check and Stop! Don't send'**. This encourages individuals to:

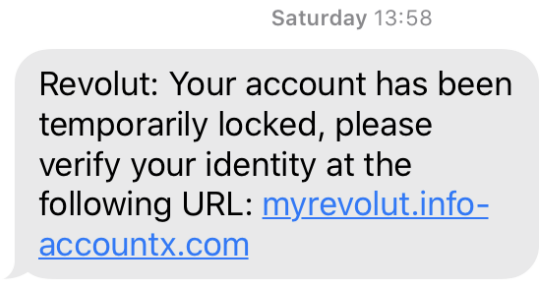
- **Slow it Down: Take the time to read over the suspected scam, and ignore the sense of urgency;**
- **Spot Check: Do their research in proving the authenticity of the suspected scam;**
- **Stop! Don't Send: Not to pay any money on the spot. No reputable person or agency would ask this of you.**

There is also a quiz on the website where users can test their knowledge with real-life examples to see if they can spot the scam.

Revolut Card Scam

Revolut customers targeted with scam texts and malicious Google ads. Consumer rights organisation Which? first reported a malicious Revolut ad in March, but this attack has recently resurfaced, leading to one victim losing almost £8,000. Fraudsters paid for a Google ad posing as digital bank to trick victims into giving away personal details or transferring money. There has also been an increase in phishing texts – all sent to Revolut customers last week – that invite the recipient to click on a link to a scam website.

If you bank with Revolut, watch out for similar texts and never click on links within messages. You should contact Revolut via the in-app chat function. If you think you've been scammed, you should contact your card provider immediately and report this crime to Police Scotland on 101. Forward scam texts to 7726.



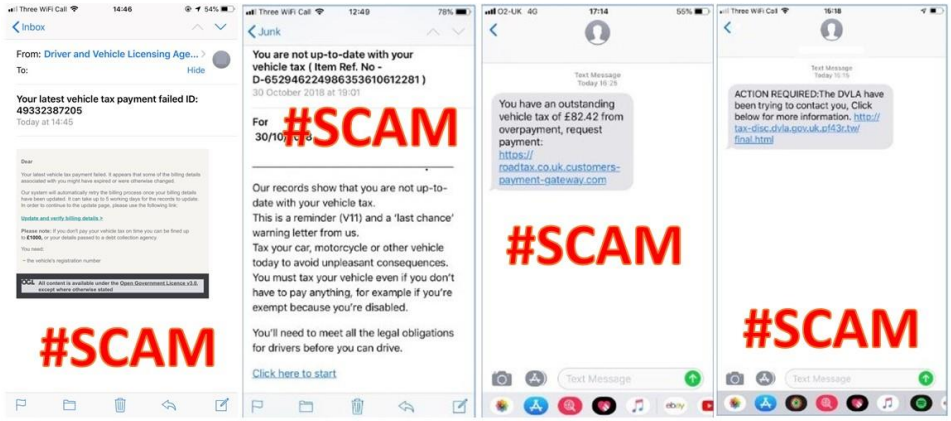
WHO Impersonators

Google has noticed an increase in spoofed accounts impersonating the World Health Organisation. These accounts, often made by hack-for-hire criminal organisations, are being used to target businesses and healthcare organisations in the US and UK. The scams are similar to those seen before where the email poses as a way to get up-to-date information on the pandemic. However many of these sites now contain logins to attempt to phish user credentials. NCSC have guidance to help you spot the most obvious signs of scam emails and what to do if you've already clicked.

DVLA & TV Licence

DVLA scam text messages are sent to thousands of motorists with officials warning customers not to click on any links or share any personal information. DVLA do not send texts or emails about vehicle tax

refunds nor would they ask you to confirm your personal details or payment information. DVLA is reminding customers that the only official place to find their services and information is on GOV.UK. Cyber scams are common so they have put together some helpful tips online to help customers to spot fraudulent activity.



Following on from last week's Bulletin, the public are being warned about a fake TV Licence email. 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, instead visit the website directly.

Newsletters

Trading Standards Scam Share

Other scams to be aware of are identified in this week's Trading Standards Scotland Scam Share newsletter. You can sign up for their newsletter here.

NCSC are publishing detailed information about each of their #CyberAware tips in their weekly cyber security technology newsletter, working with NS Tech. The NS Tech's new weekly cyber security briefing features news, analysis, job opportunities, threat research and the biggest government contracts. NS Tech will also occasionally send you special briefings relating to major cyber incidents. You can sign up here.

Training of The Week

SCVO Cyber Resilience for the Third Sector

Got burning questions about cyber security and don't know who to ask? Join us for a question and answer session on Friday 5th June 2020 at 11am and quiz our experts from British Red Cross, Police Scotland, Scottish Government and SCVO. Please feel free to submit questions in advance to alison.stone@scvo.org.uk Register Here

Case Studies

We aim to bring you real-life examples of scams, phishing emails and redacted case studies. If you have had an issue and would like to share your experience and learning with others, please contact us to discuss: CyberFeedback@gov.scot. We are happy to anonymise the case study.

Case Study – Online Security for Live Streaming, Video Conferencing and Charity Donations

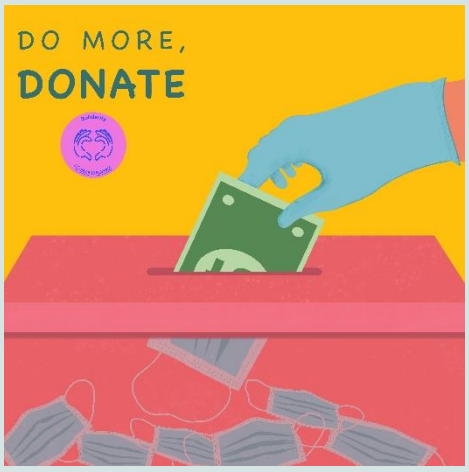
Authoritative Sources:

- National Cyber Security Centre (NCSC)
- Police Scotland
- Trading Standards Scotland
- Europol
- Coronavirus in Scotland
- Health advice NHS Inform

To **report a crime** call Police Scotland on **101** or in an emergency **999.**
We are constantly seeking to improve. Please send any feedback to CyberFeedback@gov.scot

Due to the enforced lockdown because of COVID-19 our use of online services like live streaming/video conferencing and donating to charities has increased. Several artists are offering live concert streams to keep us entertained at home. During some performances there might be an opportunity to support and raise money for a particular subject, for example, a nominated charity. Cyber criminals are taking this opportunity to exploit the links to streaming/video conferencing sites with links to charities and re-directing them to fake websites.

'Kevin' saw an event promoted on Facebook early in the week that was due to be streamed live the following Saturday night. Kevin signed up to attend this free event that was raising money, via text donations and Facebook link, for charity. Kevin clicked the link to stream the free event just before it was due to start and he was redirected to a website that was asking for credit card details to "pay to view", Kevin was sure this was to be a free event so he contacted the organisers to let them know. Further investigation by the event technical team established that the web links had been re-directed by cyber criminals eager to cash in and divert funds.



Very quickly, the organisers were able to stop the divert to that site and they also changed the method of donation to text only and stopped the attempts to steal donations. Many people could have lost a lot of money, but thanks to Kevin and others who contacted the organisers, the concert ended up raising over £140,000.00 for the charity.

We can learn a lot from the actions that Kevin took. Whilst it's wonderful that we can access this online content it's very important to pause for thought and exercise common sense when asked for money online. As this event had been heavily promoted well in advance, the cyber criminals had time to plan and deploy spoofed links.

Things to think about are:

- **Be cautious of any links asking you to donate throughout or after the performance.**
- **Take time to make you sure you are safe to proceed, by checking the web links and checking the streaming/video conferencing/charities official web pages for information.**
- **If an event has been advertised as "free to view" and you are re-directed to a payment page – act with caution. Maybe even drop the organisers a line and check this is a bona fide link. They too, may not even be aware that they have been compromised.**
- **The National Cyber Security Centre has issued the following advice on video conferencing and streaming. Get Safe Online has valuable advice when donating to charities online.**
- **Make sure to verify that the worthy causes that your donations are going towards are a trusted organisation. In Scotland, all charities must be registered and an online register of charities is maintained by the Office of the Scottish Charity Regulator (OSCR).**