Cyber Resilience COVID-19 Bulletin

ISSUE: 25.06.20

A CYBER RESILIENCE STRATEGY FOR SCOTLAND

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's 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. Thanks to all who shared feedback via our survey. Your suggestions will be helpful in making improvements to future editions of the Bulletin. We are pleased to see how many people are finding the Bulletins useful.

National Cyber Security Centre (NCSC)

Over one million reports of scam emails

The Suspicious Email Reporting Tool was launched by the NCSC to allow members of the public to report suspicious emails. Just two months after the launch of this service, the reports received stand at more than 1 million. Latest figures show that 10% of the scams were removed within an hour of an email being reported, and 40% were down within a day of a report. 10,200 malicious URLs linked to 3,485 individual sites have been removed thanks to the 1 million reports received.

NCSC thank the public for their contribution and encouraged you to stay vigilant as cyber criminals continue to seek out opportunities. If you have received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS): **report@phishing.gov.uk**

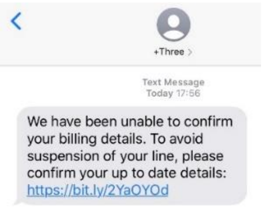
The NCSC produce weekly threat reports drawn from recent open source reporting. View this week's report here. This week's report highlights the continued investigation of an automated, ongoing, widespread credential-harvesting phishing campaign currently affecting the UK.

Trending Topics

Text and Private Messages Scams

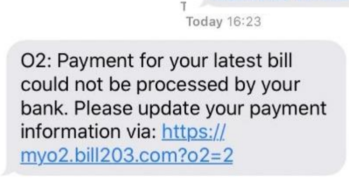
The consumer rights organisation Which has drawn attention to a credible direct message pretending to be from Instagram's help centre. The message is sent to private inboxes on the photo-sharing app, and warns the user that one of their posts has infringed copyright law. It threatens to close the user's account within 24 hours. The message is a phishing scam, encouraging you to click on the link to dispute the claim and to disclose personal information. Instagram contacts its users about account information over email, so the advice is to delete the message if you receive one.

Text scams supposedly coming from the phone companies like Three and o2 have been reported to Citizens Advice Scotland. Consumers noted that texts appear to have come from the phone company. The texts state that the recipient's latest bill has not been paid and that they need to verify their payment details via a link. The companies have a range of helpful advice on the Three and O2 websites to help users spot SMS phishing attempts.



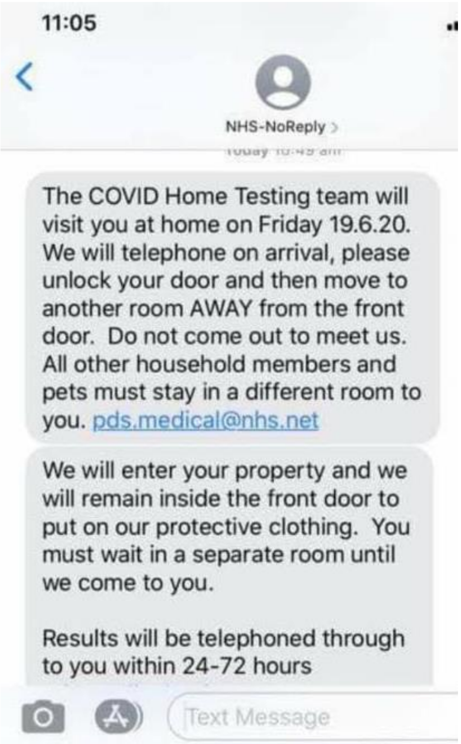
Text Message
Today 17:56

We have been unable to confirm your billing details. To avoid suspension of your line, please confirm your up to date details: https://bit.ly/2YaOYOd


Today 16:23

O2: Payment for your latest bill could not be processed by your bank. Please update your payment information via: https://myo2.bill203.com?o2=2

Fake COVID-19 home testing appointment texts targets public



The COVID Home Testing team will visit you at home on Friday 19.6.20. We will telephone on arrival, please unlock your door and then move to another room AWAY from the front door. Do not come out to meet us. All other household members and pets must stay in a different room to you. pds.medical@nhs.net

We will enter your property and we will remain inside the front door to put on our protective clothing. You must wait in a separate room until we come to you.

Results will be telephoned through to you within 24-72 hours

The Chartered Trading Standards Institute (CTSI) has witnessed evidence of bogus texts informing members of the public that a "COVID Home Testing Team" will soon visit their homes. The text specifies a date and time for the visit and that the "team" will telephone the recipient upon arrival. The text becomes suspicious where it states that the team "will enter your property and we will remain inside the front door to put on our protective clothing. You must wait in a separate room before we come to you." This is an attempt by thieves to gain access to people's homes under cover of COVID-19 measures. NHS Test and Trace will never ask you for financial details, PINs or passwords. They will also never visit your home. There is more information on NHS Scotland's Test and Trace in last week's bulletin and check out this video for advice on what to expect from a genuine contact tracer call.

Sign up to the Neighbourhood Watch Alert system to receive timely alerts about local crime prevention and safety issues from partners such as Police Scotland. For example, if there are known doorstep scammers going around your area, you will be alerted.

Call Blocking Devices

As part of the #ShutOutScammers campaign, Trading Standards Scotland are launching the roll out of free call blocking devices to vulnerable Scottish consumers who are most at risk from scammers and rogue traders. The Scottish Government has provided £15,000 in match funding to Trading Standards Scotland to procure 280 trueCall call blocking devices which are available free of charge. Find out more information on the Trading Standards website.

Dealing with suspicious emails, phone calls and text messages:

- **The NCSC have guidance on how to spot the most obvious signs of a scam, and what to do if you've already responded: https://www.ncsc.gov.uk/guidance/suspicious-email-actions**
- **Closely inspect URLs you are not sure about, and don't click on any links you believe to be a scam**
- **Report SMS (text) scams by forwarding the original message to 7726 (spells SPAM on the keypad)**
- **Suspicious email? Forward it to the National Cyber Security Centre - Suspicious Email Reporting Service (SERS) reporting@phishing.gov.uk**
- **Report to Police Scotland by calling 101**

ThinkUKnow

ThinkUKnow is an education programme from National Crime Agency (CEOP) which protects children both online and offline. They have created a range of guidance to support parents during COVID-19 and the closure of schools. Every fortnight, they aim to release a new presentation for parents and carers to help with online safety at home. Regrettably amongst our children and young people there is a common trend of sharing sexual imagery of themselves on messaging apps. This is a concerning issue which can put young people at risk of embarrassment, bullying and increased vulnerability to sexual exploitation. CEOP links to range of hot topics which cover internet safety advice on the dangers of sending nude pics, sexting and more to help provide support on these topics. A report published by Europol shines a light on the increased sharing of child sexual exploitation images online and how to confront this serious threat to children's safety. See useful presentation from Police Scotland linked below.

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

Police Scotland Cybercrime Harm Prevention Unit

Police Scotland recently delivered a presentation to provide guidance and support for parents and carers on how to keep children and young people safe online. View this online here.

SBRC – How to deduce the cyber risk for Scotland's mid-market businesses

Mid-market firms are highly diverse: vulnerabilities and assets requiring protection vary. While the mid-market is a dynamic, high growth part of the economy, organisations rarely have the scale and financial resource to employ full-time cyber security teams. Directors are faced with complex investment decisions surrounding security versus growth-driving initiatives. Hear from a range of speakers on how organisations can be more effective in this area, and if incidents do arise, how to respond.

Sign up for this webinar below:

- **8th July 12pm**
- **15th July 12pm**

SASIG – A business approach to cyber security – 25th June

The Security Awareness Special Interest Group (SASIG) frequently hold webinars on a range of security topics. This week's webinar highlighted the value of cyber security during the ongoing COVID-19 Pandemic. View their upcoming webinars here.

Scotland: The smart and secure location for Cyber Security – 7th July 2020

This webinar, hosted by Scottish Development International, will be of interest to anyone involved in or with an interest in cyber security. It will highlight the many cyber security developments taking place in Scotland and will demonstrate why Scotland is the best location in which to locate and grow your cyber business or division. More detail and information to book can be found here.

Authoritative Sources:

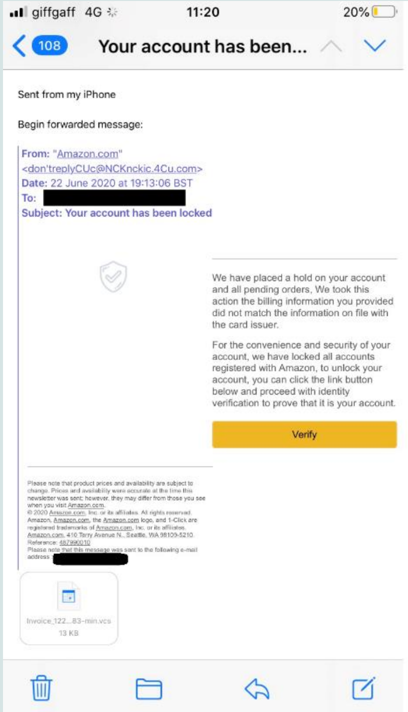
- **National Cyber Security Centre (NCSC)**
- **Police Scotland**
- **Trading Standards Scotland**
- **Europol**
- **Coronavirus in Scotland**
- **Health advice NHS Inform**

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

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 – Amazon Phishing Scam



Sent from my iPhone

Begin forwarded message:

From: "Amazon.com"
<don'treplyCUc@NCKnckic.4Cu.com>
Date: 22 June 2020 at 19:13:06 BST
To: [redacted]
Subject: Your account has been locked

We have placed a hold on your account and all pending orders, We took this action the billing information you provided did not match the information on file with the card issuer.

For the convenience and security of your account, we have locked all accounts registered with Amazon, to unlock your account, you can click the link button below and proceed with identity verification to prove that it is your account.

Verify

Please note that product prices and availability are subject to change. Prices and availability were accurate at the time this newsletter was sent; however, they may differ from those you see when you visit Amazon.com.
© 2020 Amazon.com, Inc. or its affiliates. All rights reserved. Amazon, Amazon.com, the Amazon.com logo, and 1-Click are registered trademarks of Amazon.com, Inc. or its affiliates. Amazon.com, 410 Terry Avenue N., Seattle, WA 98109-5210.
Reference: 487990010
Please note that this message was sent to the following e-mail address: [redacted]

Invoice_122...83-min.vcs
13 KB

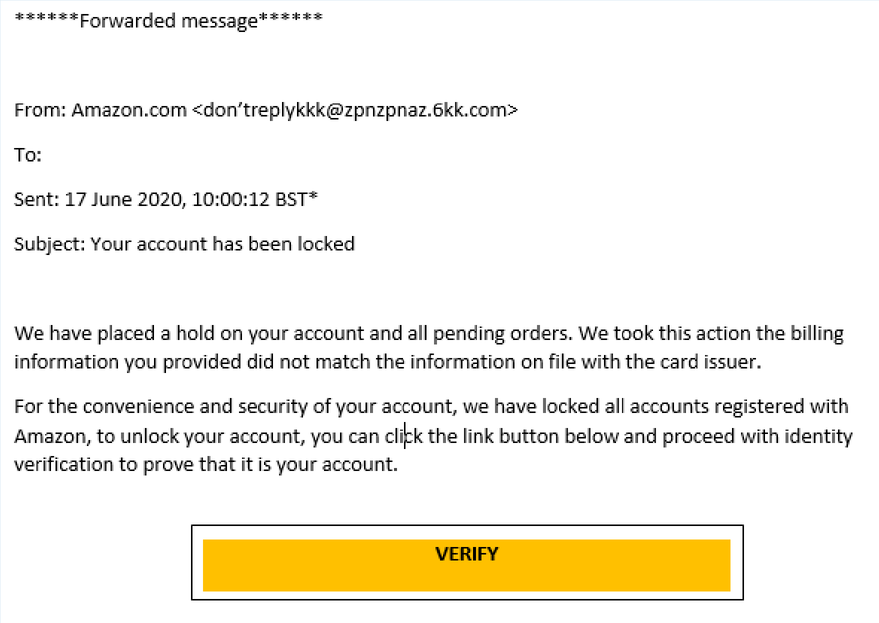
During lock-down 'Jennifer' had been doing a lot of online shopping. In preparation for a family birthday she had ordered some items from Amazon which she was waiting to arrive. During this time she received an e-mail that looked to be from Amazon advising her that her account had been locked and her order placed on hold due to a discrepancy with the payment method. The email said that to protect the security of the account, all aspects of her account were locked.

The e-mail asked that Jennifer click on the link to verify her account to allow it be unlocked. Under the circumstances you could understand why Jennifer would be tempted to click on that link, especially as she keen to receive the items she had ordered but thankfully she did not click the link.

Instead she clicked on the 'From:Amazon.com' line of the e-mail and discovered that the e-mail address that came up was not from Amazon but from a strange looking 'no-reply' e-mail address. Jennifer became more suspicious and logged on to her Amazon account to find that there was indeed no lock on her account and everything seemed normal. Jennifer reported the email to amazon and to the Suspicious Email Reporting Service (SERS): **report@phishing.gov.uk.**

It's important to remember that often phishing e-mails will not be personalised, may have grammatical errors, and will often require you to click on a link to make some kind of verification. There is also often a sense of scaremongering and urgency on the part of the recipient to take a course of action they would not normally take.

Example Fake Email



******Forwarded message******

From: Amazon.com <don'treplykkk@zpnzpnaz.6kk.com>

To:

Sent: 17 June 2020, 10:00:12 BST*

Subject: Your account has been locked

We have placed a hold on your account and all pending orders. We took this action the billing information you provided did not match the information on file with the card issuer.

For the convenience and security of your account, we have locked all accounts registered with Amazon, to unlock your account, you can click the link button below and proceed with identity verification to prove that it is your account.

Tips for spotting signs of phishing (fake emails)

Spotting a phishing email is becoming increasingly difficult, and many scams will even trick computer experts. However, there are some common signs to look out for:

- **Authority - Is the sender claiming to be from someone official (like your bank, doctor, a solicitor, government department)? Criminals often pretend to be important people or organisations to trick you into doing what they want.**
- **Urgency - Are you told you have a limited time to respond (like in 24 hours or immediately)? Criminals often threaten you with fines or other negative consequences.**
- **Emotion - Does the message make you panic, or feel fearful, hopeful or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more.**
- **Scarcity - Is the message offering something in short supply (like concert tickets, money or a cure for medical conditions)? Fear of missing out on a good deal or opportunity can make you respond quickly.**
- **Current events - Are you expecting to see a message like this? Criminals often exploit current news stories, big events or specific times of year (like tax reporting) to make their scam seem more relevant to you.**

Your bank (or any other official source) should never ask you to supply personal information from an email. If you have any doubts about a message, call your bank (or the supposed official source of the email) directly. Don't use the numbers/emails in the suspicious email, but visit the official website instead. Please forward any dubious emails – including those claiming to offer support related to COVID-19 – to report@phishing.gov.uk