Cyber Resilience COVID-19 Bulletin

ISSUE: 11.06.20

A CYBER RESILIENCE STRATEGY FOR SCOTLAND

Scottish Government
Riaghaltas na h-Alba
gov.scot

Cyber Resilience COVID-19 Bulletin

As a result of the significant rise in COVID-19 related scams, the Scottish Government's Cyber Resilience Unit is sharing 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 the contents to suit your audience. 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.

Trending Topics

Man arrested for allegedly selling over 500 fake COVID-19 testing kits

A man in Birmingham has been arrested for allegedly selling fake testing kits for COVID-19 on the dark and open web. The arrest is part of the National Crime Agency's response to criminals attempting to exploit the COVID-19 pandemic.

Furlough, refund and grant fraud

Scams centred on exploiting COVID-19 have become prevalent in recent months. Everything from Government grants, furlough payments, requests for refund of overpayments, to mortgage-holidays, are being targeted by scammers, using ever-more sophisticated methods.

Many scammers use "phishing" to obtain sensitive information such as usernames, passwords and credit card details. They do this by disguising themselves as a trustworthy organisation in an email or text message, perhaps offering refunds or government grants. They often ask recipients to enter personal information into a fake website which matches the look and feel of the legitimate site.

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

you that you have been overpaid a grant or furlough payment, or contains a demand for payback, use trusted contact details for your employer or the relevant government department to find out if the request is genuine -- and never immediately make a payment.

HMRC scam warning

HMRC has warned students to be alert to a fresh wave of cyber frauds aimed at them, offering bogus tax refunds. Last week saw a sudden spike in students reporting suspected scams received at their official university email addresses. Experience shows that when new scams emerge targeting students, they often multiply. We therefore want to warn students to take a moment to think before parting with their personal information.

- Scam emails say that the student is owed a tax refund and invite them to click on a link to 'complete the required form'. They add: 'If you do not complete the refund form now, you will not be able to claim your tax refund online.' Criminals will then use the malicious link to harvest students' personal data.
- The emails include a scam warning, saying: 'If you're unsure an email is from HMRC do not reply to it or click on any links.'

If you suspect you have received such an HMRC Scam email you can **report this directly to HMRC using the email address: phishing@hmrc.gov.uk**

Please forward suspicious emails to the NCSC's Suspicious Email Reporting Service: report@phishing.gov.uk

Forward scam text messages to 7726 (the numbers spell "SPAM" on your keypad).

Visit www.gov.uk/search to find official government services and phone numbers.

HMRC guidance on phishing and scams is available at www.gov.uk/topic/dealing-with-hmrc/phishing-scams

For further advice on how to stay secure online visit NCSC website at www.ncsc.gov.uk and remember if you are the victim of any type of fraud report it immediately to Police Scotland on 101.

Patching and updates: Largest ever Microsoft 'Patch Tuesday' and Zoom update advice

On Tuesday 9th June, Microsoft issued their largest ever monthly 'patch Tuesday' update, which patches 129 vulnerabilities.

Users of Zoom should update their version to the latest 5.0 release, which became available mid-May. This patch addresses many of the security issues previously highlighted in this popular video conferencing platform. Users who have not updated to the latest version are finding issues with access to virtual meeting calls. Organisations that host events using Zoom are asked to encourage their attendees to ensure they have the correct version at the point of sign up.

NCSC guidance on installing the latest software and app updates is available here.

Scam third party sellers on Amazon

Back in February, Amazon banned more than one million product listings related to COVID-19 from third party sellers, where listings were seen to be "price gouging" or selling fake products with misleading health claims. Huffington Post recently revealed that some products may still be slipping through, including counterfeit medical supplies, hand sanitiser, UV lights, supplements and non-expert books on COVID-19.

Consumers who haven't received goods or who have received goods in an unsatisfactory condition can request a refund from the seller and may be eligible for an Amazon 'A-to-Z Guarantee' refund.

Doctor scam

Doctor surgeries have highlighted that some of their patients have been contacted by a bogus doctor. The patients have been asked for their bank details to pay for a prescription under the COVID-19 regulations. This is a scam and you should never give your bank details to someone claiming to be your doctor. If you have been affected, please contact your bank card provider and report this to Police Scotland on 101.

Example Scam Text

;
SCAM ALERT The practice has been made aware that some patients have been contacted by bogus Doctors requesting a sum of money due to COVID-19. Please see the website for more information

Newsletters

Trading Standards Scam Share newsletter

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

Webinar - Fix Home Working Cyber Security Risks

Remote working creates new and complex cyber security challenges for businesses. YUDU's Jim Preen and Richard Stephenson talk to Zobi Founder, Scott Lever, about how to mitigate these risks.

https://www.yudu.com/resources/webinar/fix-home-cyber-security-risks

SASIG: Adapting Through Change: defending the new perimeter – your people

Cyber criminals continue to exploit uncertainty and fear to launch malicious campaigns with one aim in mind – to get your people (staff) to click. These attacks are targeted at people and require "social engineering" to succeed. What's more, the disruption we are all facing today has forced us all to quickly adapt, potentially exposing staff to increased attacks – from phishing to business email compromise attacks.

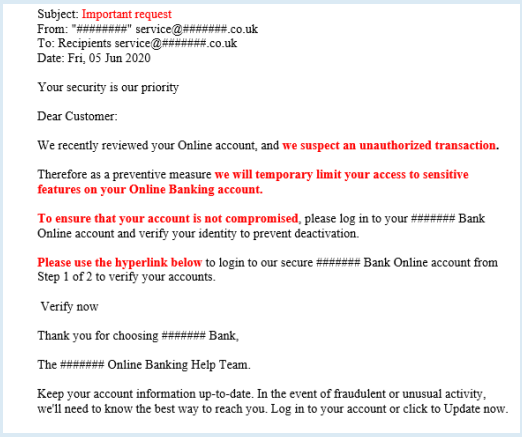
While cyber criminals remain busy in their pursuit of exploiting our employees, the Chief Information Security Officer's (CISO) role has been pushed to new limits. So how must CISOs and their security teams evolve to protect your organisation better this year? SASIG invite you to join this webinar to hear real-life experiences about how CISOs are updating their security programmes to ensure they thrive in this digital-first world: https://www.thesasig.com/calendar/event/adapting-through-change-defending-the-new-perimeter-your-people/

Case Studies

We aim to bring you real-life examples of scams, phishing emails and 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 Banking

Recently we have seen phishing emails that look as if they have come from the banking sector. The email will be marked as being a priority and will often say that your **account has been reviewed and an unauthorised transaction** has been identified – and, as a result, your **account has been temporarily limited to protect it**. The email recipient is then told to **click on a link** and provide personal details to verify their identity, or their account will be deactivated. A phishing email can appear to be from a trusted source, and may ask you to act as matter of urgency and try and scare you into taking action quickly.



Subject: Important request
From: "########" service@########.co.uk
To: Recipients service@########.co.uk
Date: Fri, 05 Jun 2020

Your security is our priority

Dear Customer:

We recently reviewed your Online account, and **we suspect an unauthorized transaction.**

Therefore as a preventive measure **we will temporary limit your access to sensitive features on your Online Banking account.**

To ensure that your account is not compromised, please log in to your ######## Bank Online account and verify your identity to prevent deactivation.

Please use the hyperlink below to login to our secure ######## Bank Online account from Step 1 of 2 to verify your accounts.

Verify now

Thank you for choosing ######## Bank,

The ######## Online Banking Help Team.

Keep your account information up-to-date. In the event of fraudulent or unusual activity, we'll need to know the best way to reach you. Log in to your account or click to Update now.

On pay day, 'Steven' received an e-mail from what appeared to be his bank. Steven did all of his banking online so he wasn't surprised to receive an e-mail from his bank as he was regularly sent updates to check his statements or to inform him when he'd set up new payments. This e-mail, which looked at first glance to be the same as any other e-mail he'd had from the bank told him that there had been unauthorised activity on his account and, as a result, to protect his money, the bank had limited his accounts. Steven panicked as he had bills to pay and all of his wages were in his bank account. Thankfully, rather than click on the link in the e-mail, Steven went onto his online banking app and saw that his accounts all appeared to be active and untouched. To be sure, Steven messaged his bank securely through the app to check that his accounts were uncompromised. The bank was able to confirm that he had been the victim of a phishing attack, one which could have seen him give his details, including his bank account details to cyber criminals.

Things to Remember:

- **Don't respond to any emails or texts asking for personal or financial information.**
- **Banks will never ask for that information via an email.**
- **If you are unsure, always independently verify any email that asks you for personal information.**

- **Please forward suspicious emails to the NCSC's Suspicious Email Reporting Service: report@phishing.gov.uk**
- **For further advice on how to stay secure online visit NCSC website at www.ncsc.gov.uk and remember if you are the victim of any type of fraud report it immediately to Police Scotland on 101.**

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