Cyber Resilience COVID-19 Bulletin

ISSUE: 10.09.20

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 Cyber Resilience Unit will share important information. We aim to update the Bulletin on a regular basis and ask that you consider circulating the information to your networks, adapting it 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. If there are any cyber terms you do not understand, you can look them up in the NCSC Glossary.

The Cyber Resilience COVID-19 Bulletin was set up to provide guidance relating to scams during the pandemic. Moving forward, we plan to adapt the Bulletin to cover a greater scope of cyber security and cyber resilience topics. We will continue to provide you with information about the latest threats, scams, news and updates. We hope you continue to feel you benefit from this resource and ask that you continue to circulate this information to your networks, adapting where you see fit.

Please subscribe to our CyberScotland mailing list to receive these updates directly.

Our next CyberScotland Bulletin will be available to view online from the 1st October 2020. A viewing link will be sent via our mailing list.

National Cyber Security Centre (NCSC)

The Suspicious Email Reporting Tool was launched by the NCSC to allow members of the public to report suspicious emails. As of 8th September, the reports received stand at more than **2,486,000** with the removal of **10,400 scams** and **24,100 URLs**. Timely alerts from the general public help the NCSC to act quickly and protect many more people from being affected. Please forward any suspicious emails to: **report@phishing.gov.uk**, suspicious text messages should be forwarded to **7726.**

The NCSC produces weekly threat reports drawn from recent open source reporting. This week's threat report included information on the Anti-Phishing Working Group report findings, that an average sum of $80,000 is requested by cyber criminals through the form of business email compromise (BEC). BEC scams usually begin with a phishing attempt in which a scam email is sent to a company's employee, to try and trick them into paying a fake invoice or paying money into the attacker's account.

Putting defences in place to ensure employees are supported in the event of a phishing attack should be high on any organisation's agenda. The NCSC have published guidance for organisations looking to protect themselves against phishing attacks. There's also specific guidance for more targeted attacks against senior executives which is often called 'whaling'.

Trending Topics

Exercise In A Box

Scottish Business Resilience Centre (SBRC) has won a competitive tender from the Scottish Government to deliver a programme of work aimed at increasing the uptake of the NCSC's Exercise in a Box toolkit to businesses across Scotland. Over the next nine months, up to 250 Scottish Businesses will learn how prepared they are to defend against the most common cyber attacks through scenario based exercising.

This includes setting up, planning, delivery, and post-exercise activity, and the resource is available for free from the NCSC website.

SBRC are encouraging organisations from all across Scotland to register for their taster session which will give you an overview of what you can expect from one of their full Exercise in a Box training sessions. For more information about this programme and to register visit the SBRC website.

Protect Scotland - NHS Scotland's COVID Tracing App

A new app called Protect Scotland has been launched to support proximity contact tracing and help suppress the spread of COVID-19. The free app which is entirely voluntary to download will monitor the spread of the virus by tracing people's movements via their smartphones. It will not store details on an individual or their location but uses encrypted anonymised codes exchanged between smart phones to determine all close contacts. Close contacts are defined as people who have been within two metres of someone who has tested positive for at least 15 minutes.

Further information on the app is available at**:** **https://protect.scot/** and you can view an explainer video here.

NHS SCOTLAND TEST&PROTECT
PROTECT SCOTLAND
Help reduce the spread of coronavirus in Scotland
NHS SCOTLAND TEST&PROTECT
PROTECT SCOTLAND

- **Information on how to avoid Contact Tracing Scams**
- **Only download apps from official and trusted app stores like the Apple App Store or Google Play Store.**
- **Read the privacy policy for an app before you download it.**
- **Check permissions during installation and watch out for any changes that might be made to terms and conditions when apps are updated.**
- **The Information Commissioners Office (ICO) is the UK's independent body set up to uphold information rights. Resources to help you understand your rights with regards to your online data.**

Pension Scams

Scammers are continuing to target pension pots of all sizes during the pandemic. A total of £30,857,329 has been reportedly lost to pension scammers since 2017 according to complaints filed with Action Fraud, say the Financial Conduct Authority and The Pensions Regulator. Scammers targeted pension pots big and small, with reported losses ranging from under £1,000 to as much as £500,000 and the average victim being a man in his 50s. But the true number of victims is likely to be much higher as savers fail to spot the signs of a scam and don't know how much is in their pots.

Scammers design attractive offers to persuade you to transfer your pension pot to them, often setting 'time-limited offers' or deadlines to pressure you into releasing your money.

- **Information about pension scams and investment scams and how to avoid them.**
- **Use the Financial Service Register and Warning List to check who you are dealing with.**
- **ScamSmart campaign increases consumer awareness of investment scams and the common tactics fraudsters use.**
- **How fraudsters claim to be from the FCA and what you can do to spot and avoid these scams.**

Vehicle Fraud Awareness

When selling, never release the vehicle until you have cleared payment.
GET SAFE ONLINE
www.getsafeonline.org/safevehicle
GB
VSTAG

The vast majority of second-hand cars, vans, trucks, motorcycles and other vehicles are bought and sold online. This activity can be very popular with fraudsters who try and trick you into paying deposits or transportation fees for vehicles that don't exist. How can you tell what ads, vehicles, buyers and sellers and genuine? Get Safe Online are running an auto fraud awareness campaign this month, sharing tips on buying and selling a vehicle safely.

Cyber Security Month – October 2020

European Cyber Security Month (ECSM) is the EU's annual awareness campaign that takes place each **October** across Europe. The aim is to raise awareness of cyber security threats, promote cyber security among citizens and organisations; and provide resources to protect themselves online, through education and sharing of good practices. Find out how you can get involved by visiting their website.

2020 ECSM Themes

- **Week 1 & 2: (October 1 – 16) – Digital Skills: educational activities that inform the general public on internet security. It conveys the importance of cyber hygiene and establishing good practices online.**
- **Week 3 & 4: (October 17-31) – Cyber Scams: provides insights on current and potential cyber threats to the public and business minimise risks. The key message encourages users to have heightened awareness of cyber scams when conducting business and personal transactions online.**

Newsletters

Trading Standards Scam Share

Other scams to be aware of are identified in last week's scam share. Check out this week's Trading Standards Scotland Scam Share newsletter. You can sign up for the weekly newsletter here.

Neighbourhood Watch Scotland

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.

Training and Webinars

SCAM YOU – Videos

The Intellectual Property Office (IPO), is the official UK government body responsible for intellectual property (IP) rights including patents, designs, trademarks and copyright. They have created a series of online videos based on real stories of people who have fallen victim to online scams after unknowingly buying fake goods. You can view them on their YouTube Channel.

Fighting Fraud and Cyber-Crime in the Third Sector – 23rd September 10.30-11.30am

Join this informative seminar, hosted by SCVO and The Royal Bank of Scotland, will provide an overview of the current cyber and fraud threats to the third sector and what simple actions can be undertaken to protect both individuals and the organisations they work for. Find out more information and booking link here.

Case Studies

Each issue, 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 learnings with others, please contact us to discuss: CyberFeedback@gov.scot We are happy to anonymise the case study.

Case Study – Facebook Messenger

‘Mark’ received a message from someone who appeared to be his friend ‘Chris’ through Facebook Messenger. Mark hadn’t heard from Chris since they were at university together. Chris explained that he wasn’t able to pay his bills and lost his job due to COVID. The criminal pretending to be Chris, asked Mark if he could help him out with his bills by transferring him some funds.

Mark immediately thought this was strange behaviour as he hadn’t heard from Chris for a number of months. Mark encouraged him to speak to his bank about his problems but Chris insisted that he needed to have this money now or he would lose his house and proceeded to share the banking details across.

Mark didn’t transfer any money and decided to give Chris a call to speak to his friend directly. This confirmed that this was in fact a cloned, fake profile set up to look like his friends account, which they were able to report to Facebook.

Action Fraud have reported similar scams where victims have received messages through Facebook Messenger from friends and family requesting to use their PayPal account to receive funds from the sale of items on eBay. Between 1st June and 31st July 2020, a total of 95 reports have been made with the total losses amounting to £44,035.

Advice

- **Be wary of unusual messages asking for assistance with financial transactions, even if it appears to be from a friend or family member. Verify with the person directly by calling using a number you know is really theirs or speaking in person.**
- **Secure your social media accounts by using strong separate passwords and where possible turn on two factor authentication (2FA).**
- **Check out the NCSC guidance on how to use social media safely.**
- **How to report a Facebook account.**

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.**