Cyber Resilience COVID-19 Bulletin

ISSUE: 16.07.20

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, 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 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.

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. Since the launch of this service, the reports received stand at more than 1,417,000 with 13,350 individual URLs linked to 5,200 sites being removed.

Earlier this week the NCSC introduced a 'home and remote working' exercise to its *Exercise in a Box* toolkit. The exercise is intended to help small and medium sized businesses to test their cyber resilience whilst staff work remotely.

The exercise follows a range of products developed by the NCSC – which is a part of GCHQ – to support remote working during the coronavirus pandemic, including advice on working from home and securely setting up video conferencing.

The NCSC produces weekly threat reports drawn from recent open source reporting. View this week's report here which contains information on a vulnerability affecting F5 BIG-IP devices (CVE-2020-5902).

Trending Topics

Scammers continue to exploit COVID-19

Scams centred on exploiting COVID-19 have become prevalent in recent months. Everything from government grants and furlough payments, to mortgage holidays and demands for payment of fines, are being targeted by scammers utilising ever more sophisticated methods.

Many scammers are using "phishing" and "smishing" (the term for phishing by SMS/text message) techniques 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, then by offering refunds or demanding payments, then direct the recipients to enter personal information on a fake website which matches the look and feel of the legitimate site.

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 message, and never immediately make a payment.

Use trusted contact information to make enquiries with the organisation that the communication appears to be from -- and do not reply to the initial email or text message.

Fake HMRC emails

There have been reports of fake HMRC emails saying that your recent Coronavirus Job Retention Scheme application has been rejected or recalled and asking you to open an attached document. If you have received a similar email, don't download any attachments or click on any links. You can view HMRC Guidance on recognising scams if you're not sure.

You'll never get an email, text message or phone call from HMRC which:

- tells you about a tax rebate or penalty
- asks for your personal or payment information

You can report suspicious messages from someone claiming to be HMRC to HMRC's phishing team, for example:

- a text message (forward it to 60599 - you'll be charged at your network rate)
- an email (forward this to phishing@hmrc.gov.uk)
- details of a phone call asking for personal information or threatening a lawsuit

Updated guidance from Information Commissioner's Office (ICO) on holding data for Test and Protect

With lockdown easing and hospitality venues re-opening, there is a requirement within the Test and Protect programme for places we visit to collect our personal data, to assist in tracing should there be an outbreak of the virus. The Information Commissioner's Office (ICO) has updated its Data Protection and Coronavirus Information Hub with guidance for people who are concerned about what their personal information is being used for, including what you should expect to be collected by staff at a venue you visit, how it should be stored and for how long it should be retained. Further information on this is available on the ICO Data Protection and Coronavirus Information Hub and within Scottish Government guidance for the hospitality sector on collecting contact details.

Venues collecting data should have updated their privacy policies to reflect the requirement to collect your personal information. Should you be contacted by someone who may be using personal data you submitted at a venue for their own purposes, this would constitute a data breach and you would be within your rights to report the organisation to the Information Commissioner's Office for further investigation.

Bounce Back Loan Scam

Bounce Back Loans are a government scheme to assist genuine businesses through COVID-19 but the scheme has also been a target for criminals. Not only are the lenders being targeted for fraudulent applications, but businesses are also being targeted and phished for their business data to be used in fraudulent Bounce Back Loan applications.

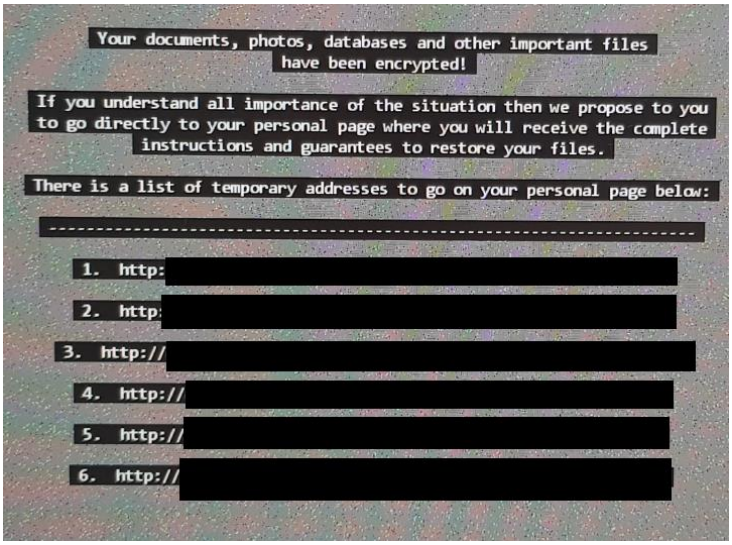
The Daily Record and Automotive Management Online have reported that a fraudster tried to scam a Scottish car dealer by taking out a UK Government-supported business loan in their name and claiming it was a payment for a car. Information on the Bounce Back Loan scheme can be found on the UK Government website.

Returning to work – phishing emails

@CheckPointSW has noted in a recent blog post that many organisations are asking employees to complete some online training before they return to work. Ensure that the emails you receive from your employer are genuine, especially any that ask you to put in log in details, as it could be someone malicious seeking to harvest information.

A reminder about the threat of ransomware

What would you do if you logged into your computer network and instead of seeing all your files you saw the threatening message on the right? This is exactly what happened to a company when they discovered that their system had been infected with ransomware and all their files were unavailable. No matter how many times the company employees restarted their networked computers, all users were met with the same message.



Ransomware is a type of malicious software which will stop you from accessing the files on your computer. Police Scotland's Cybercrime Prevention Unit have created a handy guide to help your organisation protect your system from a Ransomware attack and there is also a great deal of helpful advice on the National Cyber Security Centre website.

TECHNICAL GUIDANCE: Windows DNS Server Vulnerability: CVE-2020-1350 (aka SigRed)

As part of the July 2020 security updates Microsoft have included an update for a critical remote code execution (RCE) vulnerability in Windows DNS Server. This vulnerability is 'wormable' and can be exploited by an unauthenticated attacker remotely over a network without any user interaction.

Currently there are no known exploits for the vulnerability. Malicious actors and security researchers will be in the process of reverse engineering the updates and an exploit code will likely be released soon. Further information can be found in a Microsoft blog post.

Bitcoin Investment Scams

There have been reports of a number of US-based Twitter accounts being compromised yesterday (15 July), and used to promote a scam enticing people to "send $1,000 worth of bitcoin and receive $2,000 back". Whilst the use of high profile accounts is new, double-your-money scams have been happening for years. If something seems too good to be true, it probably is.

Source: Action Fraud UK

The NCSC report that this appears to be an attack on the company rather than on individual users, and urge people to treat requests for money or sensitive information on social media with extreme caution.

The NCSC has recently produced guidance for organisations on protecting what they publish on social media, and more widely we would remind people of our advice on staying secure through measures such as strong passwords and turning on two-factor authentication (2FA).

Newsletters

Trading Standards Scam Share

Other scams to be aware of are identified in last week's and 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

Learn about the latest phone scams in under 7 minutes – Bitesized Lunch

BITESIZED LUNCH

PC Bryan MacKie
Safer Communities Department
Forth Valley Police Division

Stirling Carers Centre

Stirling Carers Centre have published a 'bitesized lunch' video on their Facebook page where PC Bryan MacKie from Police Scotland's Forth Valley Police Division offers advice on telephone scams and what to do if you suspect you've received a call from a scammer. You can view it on Facebook without an account.

How to de-risk cyber in mid-market Scotland - SBRC Webinar

The cyber security landscape has changed and not for the better. High profile incidents at companies like Yahoo, TalkTalk and Tesco Bank mean large corporates in high-risk sectors are investing heavily to defend against new risks. But what about mid-market firms – how should they respond? Sign up for the online event on 22 July.

Staying safe on social media during COVID-19 - Scottish Union Learning workshops

How can workers protect themselves and their families when using social media? Based on advice from the National Cyber Security Centre, we will highlight some of the current social engineering cyber-attacks related to COVID-19 and show you the steps to take to protect yourself.

- An overview of the main social media platforms and their security/privacy settings
- How to spot phishing attacks and how to report them to NCSC (Suspicious Email Reporting Service)

- “Dos and Don’ts” of social media – thinking about their digital footprint and the impact on employment and future employment
- Keeping your personal and financial information safe online when using social media
- Understanding privacy and confidentiality when using social media

The workshops take place at 11am, 2pm and 6pm on Thursday 16 July but resources will be available online afterwards for one month.

Digital security following Covid-19 and keeping your business secure online – HM Government

Join a free webinar on Wednesday 22 July at 11am to find out more about the most common cyber threats faced by businesses and how to mitigate being the victim of a cyber incident. A representative from the National Cyber Security Centre (NCSC) will provide an overview of the cyber security risks facing businesses during and after COVID-19, as well as a look at the range of resources freely available from the NCSC for businesses. Please register here.

Top Tips For Staff – National Cyber Security Centre

NCSC have an e-learning training package: 'Stay Safe Online: Top Tips for Staff'. It’s totally free, easy-to-use and takes less than 30 minutes to complete. The training introduces why cyber security is important and how attacks happen, and then covers four key areas:

- defending yourself against phishing
- using strong passwords
- securing your devices
- reporting incidents ('if in doubt, call it out')

The training is primarily aimed at SMEs, charities and the voluntary sector, but can be applied to any organisation, regardless of size or sector. It's been deliberately designed for a non-technical audience (who may have little or no knowledge of cyber security), with tips that complement any existing policies and procedures. More information is available here.

Case Studies

We aim to bring you real-life case studies of scams, phishing attacks and other similar incidents. 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 any case study.

Case Study – Elderly shielding couple left distraught after losing £4,000 in Amazon phone scam

A disabled elderly couple lost thousands of pounds of savings after they were targeted by scammer posing as an Amazon staff member. The couple, in their late seventies, had been shielding because of COVID-19. They were cold-called on the phone by scammers who tricked into giving them access to their computer and bank accounts.

The scammers seemed initially pleasant and plausible, and the conversation was not un-welcomed by the couple, who'd had limited contact with others during the pandemic. The scammers persuaded the couple to give them remote access to their computer and their online bank accounts, transferring £4,000 in the form of a loan. Having hooked the couple, they put them under pressure to go the branch and transfer an additional £4,000 to an account of scammers' choosing. When the couple said that they were unable to do so, the scammers pestered them with further calls and became aggressive.

Police Scotland confirmed the crime had been reported to them and was one of a number of similar scams that they had been contacted about. Police Scotland urged the public to be vigilant to such calls and has provided information on how people can prevent themselves from being defrauded as part of their Shut Out Scammers campaign.

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.**