Cyber Resilience Notice COVID-19

ISSUE: 30.07.20

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 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.

National Cyber Security Centre (NCSC)

NCSC this week announced that Lindy Cameron will become its new Chief Executive Officer. Her role will include overseeing the organisation's response to hundreds of cyber incidents each year, improving the cyber resilience of the UK's Critical National Infrastructure (CNI), identifying the risks and opportunities for the UK in emerging technologies and leading the NCSC's ongoing response to the coronavirus pandemic. Lindy Cameron will formally become CEO in October following a handover period with her predecessor, Ciaran Martin.

The NCSC have urged the sport sector to tighten its cyber security after experts revealed a range of attacks by hackers including an attempt to sabotage a Premier League transfer deal. Their first ever report on threats to the sports industry has revealed it to be a high-value target – at least 70% of institutions suffer a cyber incident every 12 months, more than double the average for UK businesses. The report highlights the cyber threats faced by the sports sector and suggests how to stop or lessen their impact on organisations. All sports organisations, from local clubs to national federations, will find this guide useful.

The Suspicious Email Reporting Tool

This 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 1,645,000 with 15,150 individual URLs linked to 6,300 sites being removed.

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

Trending Topics

Ransomware

Ransomware is a type of malware. It lets hackers take control of a company's systems and encrypt their data, demanding payment to release it. It is often sent via a malicious email link to employees. This type of cyber attack is not uncommon.

Blackbaud - In May of 2020, US based company Blackbaud, discovered and stopped a ransomware attack. Blackbaud is one of the world's largest providers of education administration, fundraising, and financial management software. At least 10 universities and over 125 charity organisations have been impacted as a result of this attack. Organisations impacted are now reaching out to their stakeholders to inform them of a potential data breach, in line with Data Protection regulations. A statement on their website confirms that they 'paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed.' Although paying the ransom is not illegal, it goes against the advice of numerous law enforcement agencies, including the FBI, National Crime Agency and Europol, as there is no guarantee that you will get access to your device (or data).

Garmin Fitness Tracker - Garmin fitness devices have been left disconnected for nearly a day after the company suffered a major outage, possibly caused by a ransomware attack. Customers were not able to log into Garmin Connect to record and analyse their health and fitness data. This outage also affected their call centres and were unable to receive any calls, emails or online chats. Garmin has not officially confirmed the cause of this cyber-attack and has released an official statement about their recent outage.

No More Ransom is an initiative by Europol's European Cybercrime Centre, is celebrating its fourth anniversary this month. The decryption tool repository site is designed to help define the type of ransomware affecting your device and check whether a decryption solution is available. Since its launch in July 2016, over 4.2 million visitors from 188 countries and has stopped an estimated $632 million in ransom demands from ending up in criminals' pockets. You should take precautions before running unknown tools on your devices.

The National Cyber Security Centre has guidance how to defend your organisation against malware and ransomware attacks, including steps to take if your organisation is already infected. Police Scotland's Cybercrime Prevention Unit have created a handy guide to help your organisation protect your system from a Ransomware attack.

Rise in telephone scams as call centres reopen

National Trading Standards is predicting a rise in scam telephone calls as illegitimate call centres around the world get back to work. One company was found to have made more than 680,000 automated scam calls over a four-week period, urging people to purchase face masks and hand sanitisers at a cost of £29.99 to £49.99 by falsely claiming that the PPE was a government requirement.

Another common scam is victims receiving an automatic phone call, which claims that they've just been charged for an Amazon Prime subscription. The recipient is told that fraudsters have used their details to subscribe to Amazon Prime and that they can cancel the transaction by simply pressing 1. One variation of the scam claims that doing so will provide the recipient with more information, whilst a slightly different call promises to connect victims with an 'account manager' - who is in fact a fraudster.

Scottish consumers continue to be hassled by a variety of nuisance calls. Trading Standards Scotland have listed in their newsletter the Top 10 Scottish phone scams that have been reported between April-June 2020.

There are steps you can take to help stop nuisance calls on the Scottish Government website, including information about the Telephone Preference Service (TPS) which allows people and businesses to opt out of unsolicited live sales and marketing calls.

Fake Government helpline

The Crown Prosecution Service has warned the public to beware of fraudsters exploiting the COVID-19 pandemic after a man was today jailed for 30 weeks for offering fake Government refunds. He obtained 191 sets of personal details and used 49 for fraud. The total loss to his victims was £10,019.17

One text message read: *'UKGOV: You are eligible for a Tax Refund as a result of the COVID-19 pandemic. Please fill out the following form so that we can process your refund.'*

You can report suspicious HMRC emails to HMRC's phishing team directly by forwarding them to phishing@hmrc.gov.uk. You can report suspicious HMRC text messages by forwarding the message to 60599 - you'll be charged at your standard network rate.

You've got Zoom mail

Trading Standards have warned that scammers are sending fake zoom / conference call invitations. The email asks you to click link to "REVIEW INVITATION" which then redirects you to a fake login page for you to input your username and password.

Similarly, another email claiming that you have been sent "Zoom Mail' tell you a 'Zoom Voicemail' has been received and you should ring the given number. This number is a premium rate with high charges. Be extra cautious when receiving these emails and if you are not sure, don't click on the links.

Scam Emails

Action Fraud received over 1,000 reports in a 24 hour period about fake

PayPal emails and text messages. They lead to genuine-looking sites that steal your personal information.

Similarly, fake amazon emails have been noted being sent to try to convince you to review your billing information.

UK Finance reveal their Top 10 Scams to be wary of that aim to trick people for money.

If you receive any scam emails, you can report it by forwarding the email to the National Cyber Security Centre's Suspicious Email Reporting Service (SERS): Report@phishing.gov.uk

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

Staying Safe and Secure when using Personal Equipment and Working from Home during COVID-19, Scottish Union Learning workshops

With more workers having to "work from home", what steps should they take to keep themselves cyber safe. This webinar will help manage the cyber security challenges of increased home working. Based on advice from the National Cyber Security Centre, we will show you how to reduce the risk of cyber-attacks on laptops, mobiles and tablets, and tips to help you spot typical signs of phishing scams.

- **How to make your "personal/working from home" set up cyber resilient**
- **Cyber tips for reducing the risk of cyber attacks**
- **Protecting laptops, mobiles and tablets**
- **Keeping personal data safe and company data safe**
- **Business Resumption - looking ahead to go back to work - steps to reduce risk (potential malware on people's home/work machines, sanitising laptops both physically and digitally) adapting to the next stages in the pandemic)**

The workshops take place at 11am, 2.30pm and 6pm on Thursday 30 July but resources will be available online afterwards for one month. Tickets for future webinars (**August 13th**) will be made available soon.

Police Scotland and The Digital and Data Skills Academy (DDSA)

Police Scotland are delighted to present the offering of introductory digital skills courses to communities across Scotland. The industry standard courses available within the academy are provided for free through the Cisco Academy and contains training and qualifications in Networking, Cyber Security and Programming Languages. These courses provide a starting point for adults and children to understand

concepts such as computer basics and cybersecurity. Further information and self-enrolment is available on the DDSA Website.

Case Studies

Each week, 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 – Travel Compensation Scams

Like many Scots, 'Kate' was looking forward to her holiday abroad this summer but unfortunately this trip was cancelled as a result of the pandemic.

A few weeks ago, Kate received an email from a group of criminals impersonating as a service company that deals with compensation claims. The scammer set up a fake compensation company website which offered a variety of services including estimating how much money she would receive due to her recent flight being cancelled. The criminals promised a 'no win, no-fee' service'.

Kate proceeded to fill out an online web form to check her eligibility for a pay-out, on the fake company website. The results came back to show that she was due £200 compensation.

Having filled in the form online, unwittingly she revealed personal details to the fraudsters. Kate was pursued by the criminals as they tried to charge her a fee for the use of this 'free' service, despite choosing not to engage with the firm after she received the results online. She did not she receive any refund from her quoted compensation.

UK Finance is warning that fraudsters are impersonating airlines, travel companies and banks in order to steal personal information and money. Look out for fake emails and copycat websites, as well as fake messages and adverts on social media. Some companies are out to directly defraud consumers of their refunds, others are charging a fee for a service consumers can get themselves for free.

Be wary of:

- **Cold calls, unsolicited emails or fake posts on social media advertising holiday refunds. You may be asked to pay an upfront fee as payment for handling a refund claim;**
- **Fake websites advertising cheap holiday deals. These can look similar to genuine websites, with similar URLs and ask for deposits for holidays which often don't exist.**

What to Do:

- **Never give any personal or financial details to a cold caller and don't click on links in unexpected emails;**
- **If in doubt about an unexpected message which appears to be from your holiday provider, contact the provider via their official phone number or website.**
- **If you have been affected by any travel/accommodation cancellations and are unsure about your consumer rights, contact Advice Direct Scotland on 0808 164 6000 or check their regularly updated COVID-19 consumer website for advice and guidance.**

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.**