Cyber Resilience COVID-19 Bulletin

ISSUE: 27.08.20

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 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)

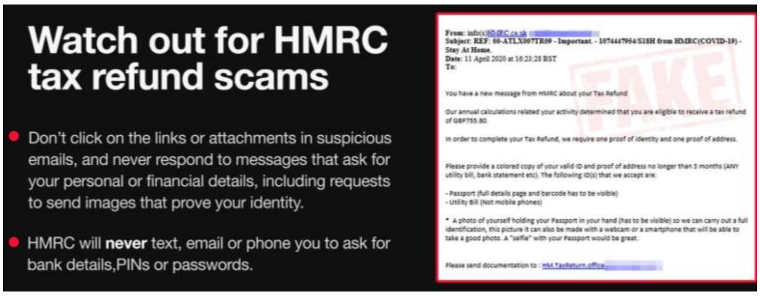
Exercise In A Box

The NCSC have launched two new micro exercises as part of their Exercise In A Box service. This is a free tool that helps organisations test and practise their response to a cyber attack. The micro exercises cover the topics of Phishing and Ransomware take approximately 20 minutes to complete. To use Exercise in a Box you need to register for an account. This enables the NCSC to provide you with a tailored report, helping you identify your next steps and pointing you towards the guidance which is most relevant for your organisation.

The Suspicious Email Reporting Service 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 1.9 million leading to 7,080 sites being removed. 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. View this week's report here. This report noted that more than 10,000 phishing scams are being investigated by Her Majesty's Revenue and Customs (HMRC). In May alone more than 5,000 scams were reported to HMRC by the public, which is three times higher than figures seen in March, when lockdown began. HMRC asked internet service providers to remove 292 scam websites in May to help combat the issue. You can report HMRC phishing emails directly to phishing@hmrc.gov.uk and then delete it.

NCSC have published guidance with top tips to help you stay secure online, how to deal with suspicious messages and ensuring your devices are secure as possible.



Watch out for HMRC tax refund scams

- Don't click on the links or attachments in suspicious emails, and never respond to messages that ask for your personal or financial details, including requests to send images that prove your identity.
- HMRC will **never** text, email or phone you to ask for bank details,PINs or passwords.

From: info(s)HMRC.co.uk [redacted]
Subject: REF: 00-ATLX007TR09 - Important. - 1074447964S18H from HMRC(COVID-19) - Stay At Home.
Date: 11 April 2020 at 16:23:28 BST
To:

You have a new message from HMRC about your Tax Refund

Our annual calculations related your activity determined that you are eligible to receive a tax refund of GBP755.80.

In order to complete your Tax Refund, we require one proof of identity and one proof of address.

Please provide a colored copy of your valid ID and proof of address no longer than 3 months (ANY utility bill, bank statement etc). The following ID(s) that we accept are:

- Passport (full details page and barcode has to be visible)
- Utility Bill (Not mobile phones)

* A photo of yourself holding your Passport in your hand (has to be visible) so we can carry out a full identification, this picture it can also be made with a webcam or a smartphone that will be able to take a good photo. A "selfie" with your Passport would be great.

Please send documentation to : HM.TaxReturn.office[redacted]

Trending Topics

Holiday scams

Police are warning the public to be on their guard amid a rise in "fake online adverts" offering rentals that do not exist. Recent incidents where people have made bookings to rent caravans at an Ayrshire caravan park left victims out of pocket when the caravan in question was found not to be owned by the person posing to be the owner. You should book a holiday direct with the site operators or through a reputable agent in order to ensure the holiday is genuine. Be extra cautious when asked to pay using a money transfer service or cash.

Remote access scams

A remote access scam, also known as a 'computer takeover scam', is when a criminal tells you that you have a problem with your account and that, to "fix the issue", they need to install software on your computer; which, once installed, provides the criminal remote access and control of your computer. At some point, the criminal will try to convince you to log into your Internet banking – perhaps to pay a nominal sum of money for the "fix". Shortly after, the criminal will then take control of your online account and transfer larger amounts of money. In some cases, the screen goes blank so you can't see what's going on.

Look out for unsolicited telephone calls by scammers claiming to be from a telecommunications or technology company claiming to be able to fix your computer or WiFi router. Never share your PIN, banking login details or passwords with anyone, even if they claim to be from your bank. If you think you're a victim of a remote scam, turn off your computer, seek help from a qualified computer technician. Contact your bank immediately and report the incident Police Scotland on 101.

Safe Student

Young people are generally familiar at using technology, however, this confidence can result in them taking more risks online that could adversely affect their finances or their reputation. Action Fraud reported that nearly a quarter of shopping fraud victims were aged between 18 to 26.

A common tactic used by criminals is to promote "investment" opportunities on social media accounts, promising large returns from a small up-front payments. During June 2020, 164 reports of individuals falling victim to fraudulent investment schemes resulted in a financial loss of £358,809. This fraud targets a younger demographic, typically aged between 20 and 30.

All the advice you need to talk to your young student about online safety and digital responsibility.
GET SAFE ONLINE
#safestudentonline
www.getsafeonline.org/safestudentonline

Get Safe Online's campaign this month is #SafeStudent and their experts have put together some tips to help advise students on a range of cyber security topics, before they go to university or college.

Keeping Children Safe Online

The internet is a fantastic place for children to learn, create and have fun, but they may occasionally have to deal with a variety of sometimes challenging issues. These might include cyberbullying, the pressure to take part in sexting, encouragement to self-harm, along with various others. But there are positive things you can do to equip yourself and your child to support them in resolving any issue they may face.

As a Parent/Carer, you can find support to enhance your children or young people's safety, security and awareness at a time when they will be spending more time online. Please have a look at the links below which are very informative, easy to follow and will provide the opportunity to start the discussion about online safety.

- **ThinkUKnow activity packs - an online safety education programme from National Crime Agency**
- **NCPCC, CEOP and Internet Matters have created a number of advice hubs**
- **Guides to help you set up parental controls**
- **Toolkits for young people and parents to help talk about data protection and privacy online**

Fake News

False information online costs lives. The World Health Organisation (WHO) previously said that the "infodemic" surrounding COVID-19 spread just as quickly as the virus itself, with conspiracy theories, rumours and cultural stigma all contributing to deaths and injuries.

World Health Organization
PROTECT YOURSELF AND OTHERS BY REPORTING MISINFORMATION

Scottish Government have posted a video on twitter, sharing tips for recognising false information, encouraging people to find the latest official information from trusted sources such as the Government, NHS or the World Health Organisation. Learn about inaccurate information on the WHO myth busters page.

If you see content online that you believe to be false or misleading, you can report it to the hosting social media platform on which it appears. Guides on how to do this are available on the WHO website as well as information on cyber criminals pretending to be WHO.

Citizen Advice Scotland Online Scams Helper

After issuing High Court proceedings against Facebook, Martin Lewis (Money Saving Expert) agreed to settle his case out of court, in return for Facebook making a binding commitment to donate £3 million to set up the Citizens Advice Scam Action (CASA) service across the UK, to provide one-to-one support. Facebook also agreed to create a scam ads reporting tool, unique to Facebook in the UK.

Scams Action

online web-chat service

Specialist one-on-one help for people who are worried they're being scammed, and those who have already lost money

citizens advice scotland

In Scotland, the service is provided by Citizens Advice Scotland's dedicated online scams webchat service giving specialist one-to one help to people who are worried they're being scammed, and those who have already lost money. Launched in July 2019, the service also undertakes scams prevention work to identity, tackle and raise awareness of online scams. The service is available on their website and runs from Monday to Friday, 9am- to 5pm. Their online scams helper tool will help you check if something might be a scam and what to do if you become a victim.

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

SBRC: Cybercrime through the pandemic then and now, 27th August, 12pm

The pandemic has fostered an online boom and working practices have now changed forever. This webinar will explore the "then and now" including presentations from international experts from the Cyber Defence Alliance, Adarma, CyberConnect Scotland and the Scottish Business Resilience Centre. You can view a recording of this webinar on the SBRC YouTube Channel after the event.

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 – Tea at the Ritz

The Ritz restaurant in London was a recent target for a convincing scam aiming to steal customer payment card details. Scammers managed to obtain the details of customers who had reservations booked at the restaurant. They called up the customers asking them to confirm their booking by providing payment card details. The scam was convincing as it appeared to have come from the hotels real phone number and the scammers knew when and where the reservation was.

The scammers told the victim that their card details had been “declined” and asked for a second bank card. Once they had these details, the scammer would attempt to make several transactions in excess of £1,000.

When one victim’s bank spotted the suspicious transactions, the scammer phoned again - this time pretending to be from the victims bank. The scammer told the victim that somebody was trying to use their credit card, and in order to cancel the transaction they should read out a security code sent to their mobile phone. In reality, this would have authorised the transactions made. The Chartered Trading Standards Institute have seen similar reports on a scam involving callers pretending to be from a bank security team.

This incident was alerted to the Information Commissioner’s Office (ICO) as a potential data breach within their food and beverage reservation system and is continuing to be investigated.

Advice

- **Verify each caller before revealing any credit card details over the phone. Numbers can be easily spoofed on caller ID, if you are unsure it’s best to call the venue back later, or from a different phone, using the number on their official website.**
- **If a bank believes a transaction has been fraudulent, they will not ask for security codes in order to cancel these. You can call your bank about suspicious activity using the number on the back of your payment card.**
- **If you become a victim of fraud, report this to Police Scotland by calling 101 or visiting your local Police station.**

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.**