Cyber Resilience Notice COVID-19 23/04/2020

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 share these updates weekly. **We ask that you consider circulating this information through your networks**, adapting 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 weeks' notice will be showing examples of COVID-19 scam emails that have been observed in Scotland and steps you can take to spot them.

National Cyber Security Centre (NCSC)

NCSC have launched the new Cyber Aware campaign promoting behaviours to mitigate cyber threat. The cross-governmental 'Cyber Aware' campaign, offers actionable advice for people to protect passwords, accounts and devices. You can find out more about what NCSC have launched recently here. This includes new guidance for individuals and organisations using online video conferencing.

Phishing – How to report it to NCSC https://www.ncsc.gov.uk/information/report-suspicious-emails

As part of NCSC's Cyber Aware campaign, NCSC launched their new Suspicious Email Reporting Service which has been co-developed with the City of London Police. The new *Suspicious Email Reporting Service* will offer an automated service for people to highlight what they think to be a suspicious email. This will build on the organisation's existing takedown services, which have already removed more than 2,000 online scams related to coronavirus in the last month.

Please forward any dubious emails – including those claiming to offer support related to COVID-19 – to report@phishing.gov.uk, the NCSC's automated programme will immediately test the validity of the site. You will receive an email acknowledging your report. Any sites found to be phishing scams will be removed immediately.

If people have lost money, they should tell their bank and report it as a crime to **Police Scotland**.

Tips for spotting telltale signs of phishing (fake emails) -

Spotting a phishing email is becoming increasingly difficult, and many scams will even trick computer experts. However, there are some common signs to look out for:

- **Authority** - Is the sender claiming to be from someone official (like your bank, doctor, a solicitor, government department)? Criminals often pretend to be important people or organisations to trick you into doing what they want.
- **Urgency** - Are you told you have a limited time to respond (like in 24 hours or immediately)? Criminals often threaten you with fines or other negative consequences.
- **Emotion** - Does the message make you panic, fearful, hopeful or curious? Criminals often use threatening language, make false claims of support, or tease you into wanting to find out more.
- **Scarcity** - Is the message offering something in short supply (like concert tickets, money or a cure for medical conditions)? Fear of missing out on a good deal or opportunity can make you respond quickly.
- **Current events** - Are you expecting to see a message like this? Criminals often exploit current news stories, big events or specific times of year (like tax reporting) to make their scam seem more relevant to you.

Your bank (or any other official source) should never ask you to supply personal information from an email. If you have any doubts about a message , call them directly. Don't use the numbers/emails in the email, but visit the official website instead.

Scottish Government
Riaghaltas na h-Alba
gov.scot

Cyber Resilience Notice COVID-19 23/04/2020

Training Of The Week

Scottish Businesses Care: COVID-19 and counterfeit goods:

In this webinar, the panel discuss the rise of counterfeit goods during the COVID-19 pandemic, hosted by Rachel Jones of SnapDragon Monitoring. https://youtu.be/z6GWudEa8Qo

For further reading, Europol have published a report on Counterfeits, substandard goods and intellectual property crime in the COVID-19 pandemic

New Scottish Government Guidance For Home Learning

This new guidance is aimed at pupils, parents and teachers, which makes reference to digital learning, with a focus on safety, security, privacy and safeguarding. This complements earlier guidance published by the General Teaching Council Scotland relating to online engagement by education professionals.

Trading Standards Scam Share

Other scams to be aware of are available in this weeks' Trading Standards Scotland Scam Share newsletter. You can sign up for their newsletter here.

Trending Topics

WHICH, a well-known provider of product and services reviews are running a **very** informative page on COVID-19 scams and how to spot and prevent them. Their page contains some excellent information and advice on the current scams. WHICH also cover wider COVID-19 related concerns.

HMRC

Criminals preying on our financial worries as they spoof government websites to take our money.

Emails or texts supposedly from HMRC or our local council offering a tax refund or financial help (for example, Coronavirus Job retention scheme) during the COVID-19 pandemic have started appearing. The Government has an up-to-date list of common HMRC scams on their website and all similar scams should be reported to them directly. Even if you get the same or similar phishing email or text message often, email it to phishing@hmrc.gov.uk and then delete it.

HMRC has also warned that returning NHS workers are being targeted by promoters of tax avoidance. Read more on their website.
https://www.gov.uk/topic/dealing-with-hmrc/phishing-scams


GOV.UK ALERT
CORONAVIRUS

It has come to our attention that you have been out of the house more than once. Due to this irresponsible behaviour, we are issuing you a formal warning and £250 fine. If this continues, the fine could increase to a maximum of £5000 and/or an arrest. Payment will be taken automatically out of your account. Call 0800 345 9999 for any enquiries or to appeal.

Please remember: New rules in force now: you must stay at home. More info and exemptions at gov.uk/coronavirus
Stay at home. Protect the NHS. Save lives

Google

The BBC have reported that scammers are sending 18 million hoax emails about COVID-19 to Gmail users every day, according to Google. The tech giant says the pandemic has led to an explosion of phishing attacks in which criminals try to trick users into revealing personal data.

Out of approximately 100 million phishing emails a day and over the past week, almost a fifth were scam emails related to coronavirus. This means that COVID-19 may now be the biggest phishing topic ever.

Tesco Vouchers

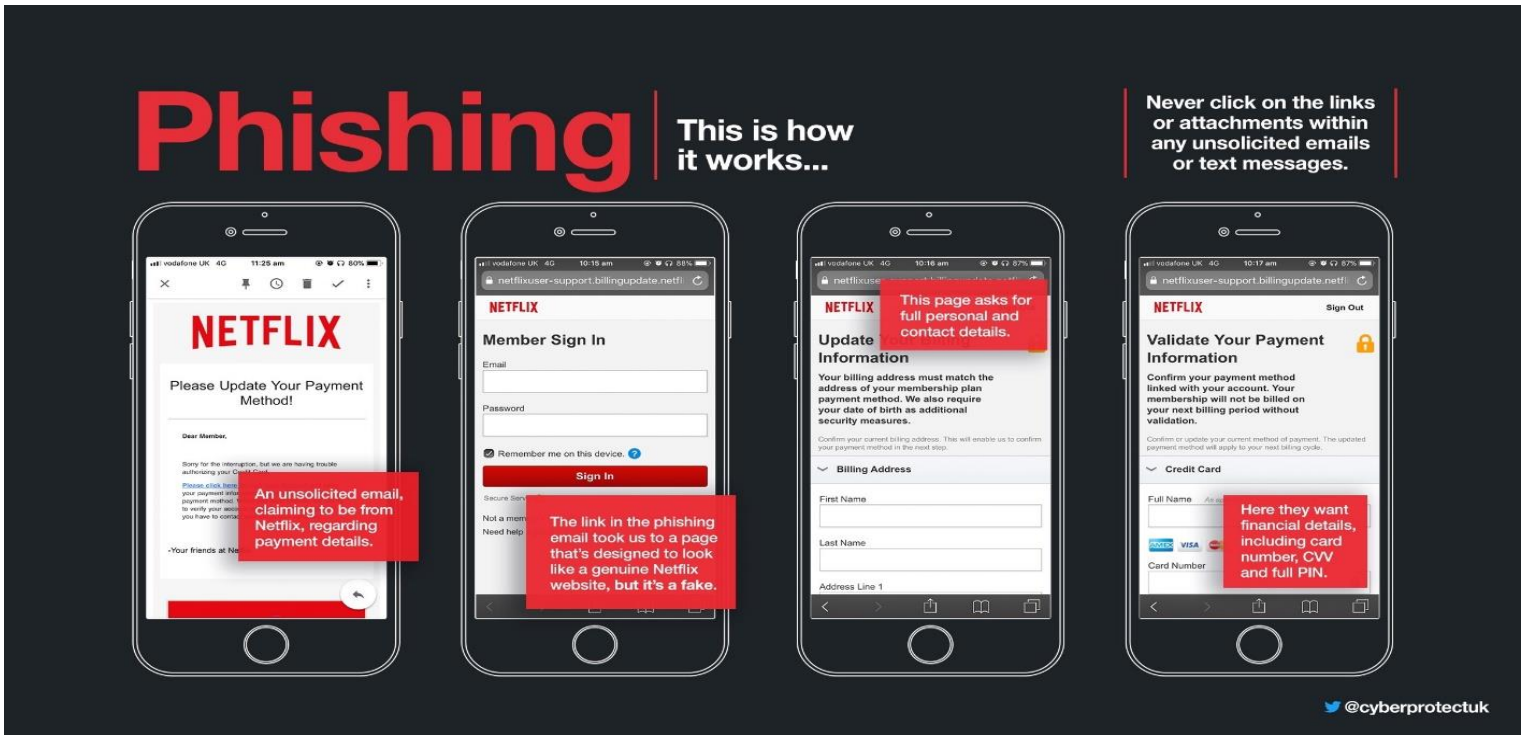
There have been reports about fake emails that appear to be from Tesco. The email states that the supermarket is offering free vouchers. The link in the email leads to a phishing website that looks like the genuine website that is designed to steal login credentials as well as personal and financial information.

Cyber Resilience Notice COVID-19 23/04/2020

Netflix Scam

As lockdown continues, usage for online streaming services has skyrocketed. Scammers have caught onto this, and so there has been an influx of Netflix related phishing emails circulating.

The cybersecurity firm BrandShield have noted that since January 2020, 639 fake domains containing the word "Netflix" have been registered. These are being used to steal users credentials, money, or even to spread malware onto users devices. Users should be cautious and only enter credentials into the legitimate Netflix website.



Sextortion Scam

Police Scotland is asking people to be aware of an email scam currently circulating where fraudsters are threatening to publish online footage of victims. Sixteen reports were made to Police Scotland overnight on Thursday 9 April 2020, with the latest number rising to 96 reports by Tuesday 14 April 2020. The reports have been from people across every police division in Scotland.

The scam involves emails being sent to people with the suspect claiming to have video footage of the recipient visiting an adult website. The suspect is then demanding payment in bitcoin, threatening that failure to do so will result in the video being published. This is known as sextortion, an example of a phishing attack.

NCSC advice:

- Don't communicate with the criminal
- Don't pay the ransom
- Check if your account has been compromised - https://haveibeenpwned.com/
- Change any passwords mentioned
- Report any losses to your local police force

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

Scottish Government
Riaghaltas na h-Alba
gov.scot