Cyber Resilience COVID-19 Bulletin

ISSUE: 14.05.20

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 through these weekly bulletins. 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.

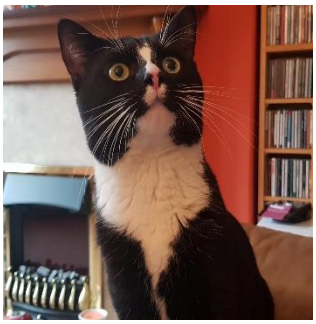
This bulletin is also available online here.

National Cyber Security Centre (NCSC)

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

Trending Topics

Pet Scams



Criminals have been advertising pets online and will ask victims to put down a deposit to secure the purchase. They rarely have any animals to sell in spite of the adorable photos they display. These adverts have been seen on social media, general online selling platforms as well as specific pet-selling platforms. It's estimated that people have lost a combined total of £282,686 in March and April alone.

Be wary when looking at pets advertised online. Trading Standards Scotland have produced a handy guide with top tips if you are thinking of buying a puppy online. Fraudsters are more likely than ever to try to sell animals that may not be healthy or have the right paperwork.

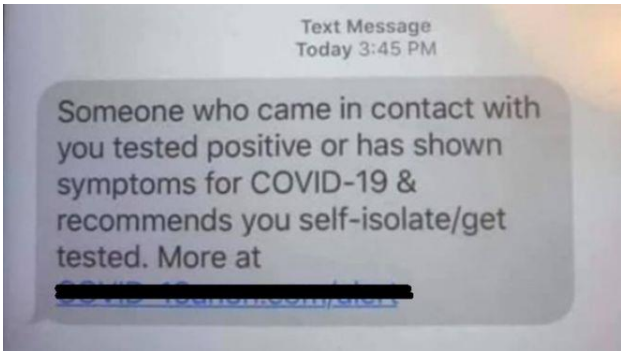
Online Gaming

Children and young people are spending so much more time in the virtual world, chatting, viewing, sharing and gaming. Cyber criminals are upping their game and altering their methods to attack and disrupt all our lives. As parents and carers, we have to remain vigilant and be aware of potential dangers online. Remember, unless you know who you are communicating with people can pretend to be whoever they want to be online. People can easily hide their true identity, so don't just trust anyone you meet online. Make sure you know who they are and, if you're not sure, just stop communicating with them. If anyone makes harmful suggestions or tries to share indecent images, report the incident to Police Scotland on 101, or 999 in an emergency.

Be aware of where you are buying your next gadget from. Consumers should be wary of listings from unfamiliar names – a suspected scam store appearing to offer cheap, hard-to-find gadgets, topped Google search results for days recently.

Contact Tracing Apps Scam

The new NHS app is being trialled in the Isle of Wight this week and scammers have taken advantage of the situation by issuing texts posing as a UK contact tracing solution, telling people they have been in contact with someone showing symptoms of COVID-19.



Bogus text messages seen by the Chartered Trading Standards Institute appear to have been sent from an official source associated with the app, directing recipients to a website where they can learn more information. In fact, the link attempts to gain bank account and other personal identity details. The official NHS app has only been released in a limited testing phase on the Isle of Wight.

This is an example of scammers modifying their campaigns as a situation develops. If you receive this text don't click on any links. You can forward the texts and any other scam texts to 7726 (the numbers spell "SPAM" on your keyboard).

Campaigns

You, Coronavirus and staying safe online.

GetSafeOnline has launched its #SaferOnlineLockdown campaign, inviting individuals to contact its experts for online advice during the pandemic. Experts will be featuring live on the Get Safe Online Facebook page every Thursday at 11am to offer weekly top tips and answer any questions that viewers have. Today's session was hosted by Tim Mitchell, Content Director at Get Safe Online, and focused on passwords. For those unable to look in on the Facebook Live sessions, Get Safe Online has set up an email Coronavirus hotline: covid19@getsafeonline.org, where queries will be answered by online safety experts within 48 hours.

INTERPOL global awareness campaign

INTERPOL has launched a global awareness campaign (running from 4 – 31 May) to keep communities safe from cyber criminals seeking to exploit the outbreak to steal data, commit online fraud or simply disrupt the virtual world. The key message of the campaign, which focuses on alerting the public to the cyber threats linked to the coronavirus pandemic, is to #WashYourCyberHands – to promote good "cyber hygiene".

Newsletters

Trading Standards Scam Share

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

NCSC are publishing detailed information about each of their #CyberAware tips in their weekly cyber security technology newsletter, working with NS Tech. The NS Tech's new weekly cyber security briefing features news, analysis, job opportunities, threat research and the biggest government contracts. NS Tech will also occasionally send you special briefings relating to major cyber incidents. You can sign up here.

Training of The Week

Scottish Businesses Resilience Centre: The challenge to Scotland's rural economy and staying safe in these changing times

Building on their recent cyber workshops across Scotland's Highlands and Islands, SBRC have broadcast a webinar (viewable here), and have another planned for 27th May, to address key cyber related concerns for Scottish SMEs with an ethos of support, signposting and resilience. These webinars are delivered by SBRC on behalf of HIE, with the support of the Scottish Government, Police Scotland, Business Gateway and others. More details here.

ScotlandIS: Cyber Focus, Business Survival as lockdown continues, Wednesday May 20th 11am More details here

SCVO DigiShift : Cyber Security for Third Sector Organisations More details here

National Policing Protect Network has a list of all their cyber security future webinars

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

Case Studies

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

Case Study – Cyber fraud in a care setting/PPE fraud

The manager of a care provider has lost £12,000 due to a cyber fraud while trying to purchase PPE from outside the UK.

Over the past few weeks, the manager had repeated approaches from a number of companies offering to supply PPE quickly. The latest approach seemed to be from a legitimate company, so the owner placed an order for the supply of gowns, masks and gloves, amounting to £12,000.

Without the knowledge of the supplier, a cyber-criminal had compromised the supplier's email account. The criminal then requested that payment be made to an alternative bank account – claiming problems at the supplier's bank.

Having no reason to doubt the authenticity of the email due to previous phone and email interaction, the manager made the payment. The scam was only revealed when the manager contacted the supplier when the PPE failed to arrive. At this point the police were notified.

Police Scotland offer top tips to prevent procurement fraud:

1. Ensure all staff who are able to make or are involved in financial decisions are trained how to identify procurement fraud.

2. Never give in to pressure or threats that it is a time-sensitive issue or an urgent matter. A genuine organisation will have no issues with you verifying a request, however a fraudster will often try to pressurise you into acting immediately.

3. Ensure a three-way match is carried out. Do the amounts documented on the requisition, purchase order and invoice all align?

4. Adopt dual control procedures for authorising payments. Ensure that a senior member of your team reviews your actions and formally authorises the payment.

5. Ensure the procurement process is followed and is enforced. Has an order been placed before the procurement paperwork has been raised? If so, why?

6. Carefully check the sender's email address to identify if it exactly matches your known and trusted records and call your supplier to verify the email is genuine.

7. Be vigilant to any clerical or spelling errors within emails which may indicate the email is fraudulent.

9. If it is a new supplier, carry out internet searches to check if they are genuine, are there any customer reviews and phone any listed landline to check.

10. Be alert to any requests to alter bank details. Carry out an internet search of the new bank account sort code and account details to uncover: Location of the bank (to be checked against the company address) and whether there are any blogs or reports available to indicate the communication is a scam.