Cyber Resilience COVID-19 Bulletin

ISSUE: 28.05.20

A CYBER RESILIENCE STRATEGY FOR SCOTLAND

Scottish Government
Riaghaltas na h-Alba
gov.scot

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 weekly basis and ask that you consider circulating the information to 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.

We are looking to measure and improve the Bulletin readers' experience and satisfaction. Please answer this short survey to share your thoughts.

National Cyber Security Centre (NCSC)

Due to the COVID-19 pandemic and the temporary closing down of high streets stores and offices, businesses are adapting the way they operate. Many are moving to an online model, including online shopping, working from home and conferencing software to keep in touch with staff.

Cyber criminals are aware of these changes in working practices and are trying to take advantage of any possible cyber security weaknesses. Businesses transitioning from high street to online or expanding their online presence should not only consider how they make this change to online trading, but also consider the cyber security measures they need to implement to protect themselves.

The National Cyber Security Centre (NCSC) has issued the following advice for these businesses who have seen their physical premises closed and have moved their operations online. 'Moving business form physical to digital'.

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 4 weeks ago, the public have passed on more than 600,000 suspect emails, with more than 4,500 URLS being removed.

Trending Topics

EasyJet Data Breach

Last week's Bulletin contained information following EasyJet's notification of a data breach. If you have been affected, you should have been contacted this week, most likely by email. If affected you should consider following the advice set out by NCSC.

Regardless of the company you've booked with, individuals should be aware of fake websites and emails purporting to offer refunds for holidays cancelled due to COVID-19.

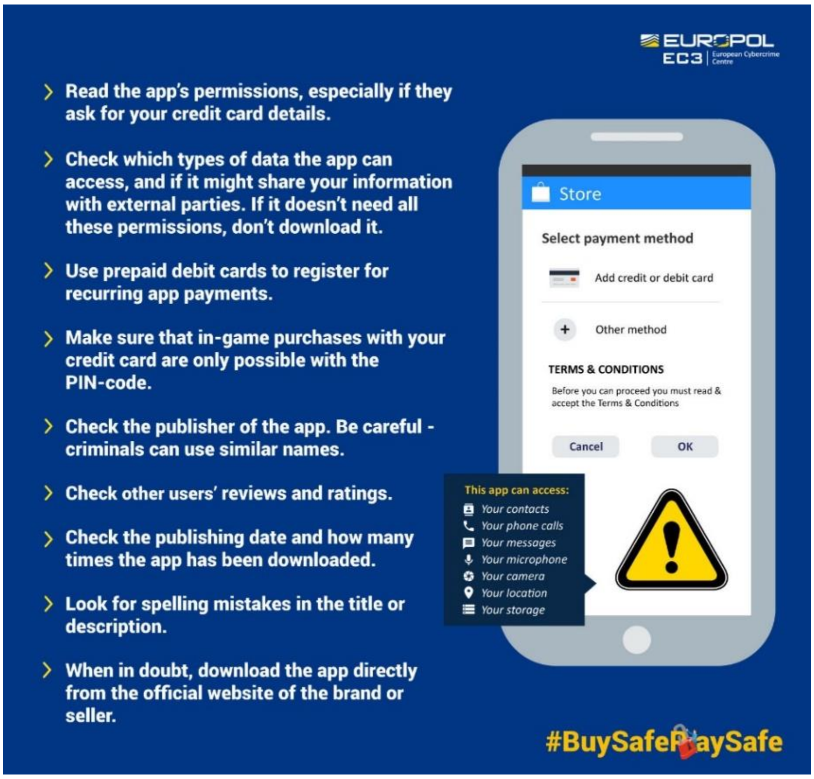
CPNI – Staying secure during COVID-19

The Centre for the Protection of National Infrastructure (CPNI) have created a resource page to help organisations to stay secure during COVID-19. This includes guidance from CPNI and NCSC as well as a 'living' campaign which can be adapted by workplaces to aid them in opening and operating as safely and securely as possible in the coming weeks and months. There is also guidance on protective security and managing risks as well as guidance on personnel security during a pandemic and on insider threats.

Downloading apps

There are millions of apps available to download onto smartphones and tablets that can range from location-based discovery tools and smart search, to games and exercise tracking. Almost all smartphones come with a location-sharing app like Find My Friends that lets you connect with other people's phones, or location tagging on social media apps like Facebook, Instagram, Snapchat and Twitter. By posting where you are, anyone can track your movements.

Downloading a new #app? 📲Do not rush 🔎 take a moment to review the security, privacy and financial implications. #BuySafePaySafe



- Read the app's permissions, especially if they ask for your credit card details.
- Check which types of data the app can access, and if it might share your information with external parties. If it doesn't need all these permissions, don't download it.
- Use prepaid debit cards to register for recurring app payments.
- Make sure that in-game purchases with your credit card are only possible with the PIN-code.
- Check the publisher of the app. Be careful - criminals can use similar names.
- Check other users' reviews and ratings.
- Check the publishing date and how many times the app has been downloaded.
- Look for spelling mistakes in the title or description.
- When in doubt, download the app directly from the official website of the brand or seller.

#BuySafePaySafe

Top Tips

- **Only download apps from official and trusted app stores like the Apple App Store or Google Play Store.**
- **Read the privacy policy for an app before you download it.**
- **Check permissions during installation and watch out for any changes that might be made to terms and conditions when apps are updated.**
- **Turn on automatic lock and password protect features on your mobile device.**
- **Check your privacy settings. Consider making your profile private and disabling functions you don't need, such as your location, third party cookies, advertising and interest preferences and profile visibility to other users of the app.**

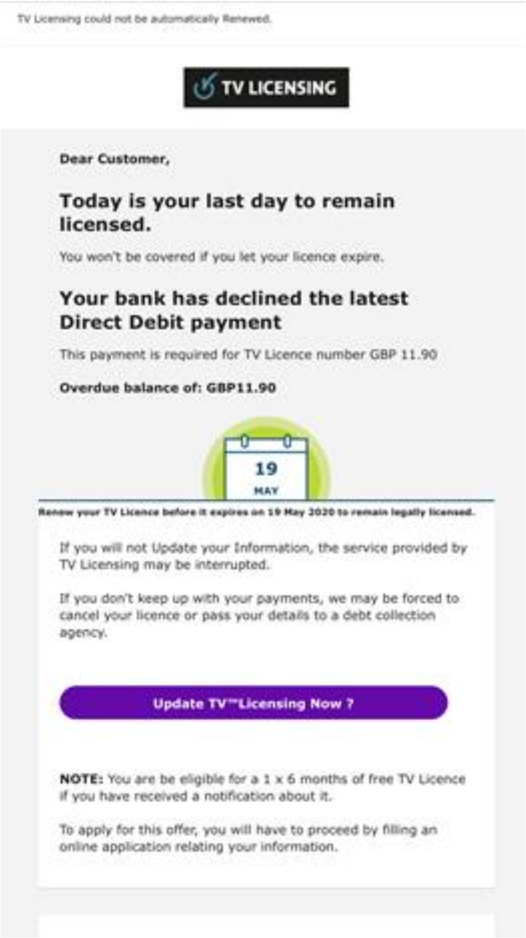
- **Keep your apps up to date and regularly clear out apps you no longer use.**
- **Turn off location sharing when not in use.**
- **Before you sell your device ensure you reset your device to factory settings to make sure all apps and personal information has been deleted from it.**

The Information Commissioners Office (ICO) is the UK's independent body set up to uphold information rights. The ICO have created a number of resources to help you understand your rights with regards to your online data. They provide guidance on social media privacy settings and factsheets on some of the most popular social media platforms (Facebook, Twitter, Snapchat, LinkedIn and Google) to assist you in taking control over how your personal information is used.

TV Licensing Scam

Police forces across the UK have warned of a new scam around TV licensing. The scam impersonates the TV Licensing company, demanding that users give their bank details to make a payment or face prosecution. The scammer also suggests that the user may be entitled to a discount or partial refund due to the coronavirus. The official TV Licensing Company has released a statement saying they will never email individuals with refund or discount offers. Further, they have put a up a page with FAQ on TV Licensing during COVID-19 which states that they are currently not writing to people behind on their license fee payments during the pandemic.

TV Licensing have email security and scam advice on their website, including four quick ways to spot a scam. You can also view your licence or payment plan online.


TV Licensing could not be automatically Renewed.

Dear Customer,

Today is your last day to remain licensed.

You won't be covered if you let your licence expire.

Your bank has declined the latest Direct Debit payment

This payment is required for TV Licence number GBP 11.90

Overdue balance of: GBP11.90

Renew your TV Licence before it expires on 19 May 2020 to remain legally licensed.

If you will not Update your Information, the service provided by TV Licensing may be interrupted.

If you don't keep up with your payments, we may be forced to cancel your licence or pass your details to a debt collection agency.

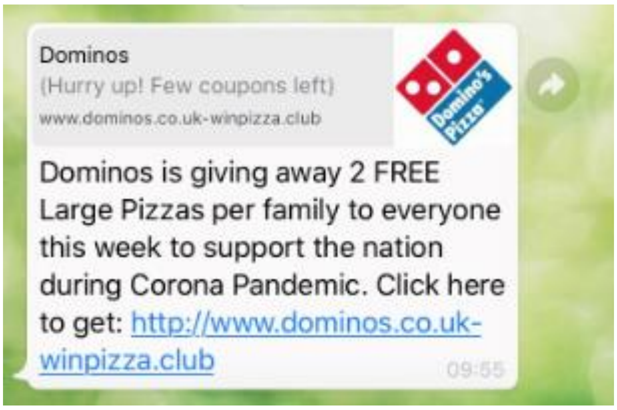
NOTE: You are be eligible for a 1 x 6 months of free TV Licence if you have received a notification about it.

To apply for this offer, you will have to proceed by filling an online application relating your information.

Voucher Scams

There are a range of ‘offers’ circulating online.

North Wales police have warned of a scam WhatsApp message circulating where scammers are impersonating Domino’s Pizza. The scam contains a malicious link that users click to allegedly receive free pizzas. Domino’s Pizza do not offer vouchers through links and only offer voucher codes. 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).


Dominos
(Hurry up! Few coupons left)
www.dominos.co.uk-winpizza.club

Dominos is giving away 2 FREE Large Pizzas per family to everyone this week to support the nation during Corona Pandemic. Click here to get: http://www.dominos.co.uk-winpizza.club

09:55

Reports are still circulating that scammers are emailing fake vouchers, supposedly from supermarkets. In one scam, consumers are being encouraged to click a link on social media to fill out a survey in order to win £175 of Lidl vouchers.

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

ScotlandIS: Cyber Focus – Business survival as lockdown continues

How can our businesses establish and successfully implement our new cyber security processes in the current situation, and ensure future resilience? On Wednesday 3rd June ScotlandIs will host a webinar to explore topics such as optimising cyber budgets during the current climate, maintaining a security culture in the workplace, future resilience, as well as the importance of major incident planning. The panel will be made up of leading experts in the cyber security community. For more details and to book visit their website.

SCVO Cyber Resilience for the Third Sector

Got burning questions about cyber security and don't know who to ask? Want to pick the brains of a number of knowledgeable sources with third sector focused experience?
Join us for a question and answer session on Friday 5th June 2020 at 11am and quiz our experts from British Red Cross, Police Scotland, Scottish Government and SCVO. Please feel free to submit questions in advance to alison.stone@scvo.org.uk Register Here

SBRC recordings of recent webinars:

- **Cyber Resilience for Care Homes**
- **The COVID-19 Response in Highlands and Islands**
- **Business Resumption – All webinars can be viewed on SBRC YouTube Channel**

Authoritative Sources:

- **National Cyber Security Centre (NCSC)**
- **Police Scotland**
- **Trading Standards Scotland**
- **Europol**
- **Coronavirus in Scotland**
- **Health advice NHS Inform**

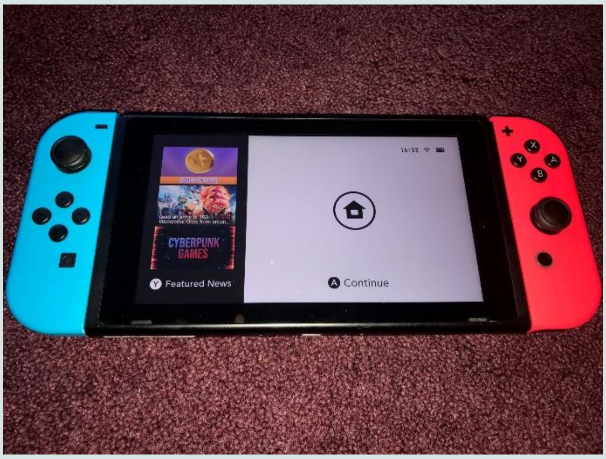
To **report a crime** call Police Scotland on **101** or in an emergency **999.**
We are constantly seeking to improve. Please send any feedback to CyberFeedback@gov.scot

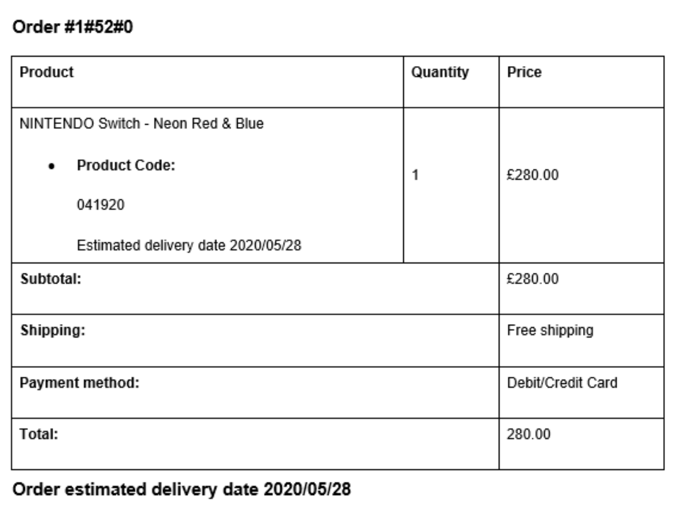
Case Studies

We aim to bring you real-life examples of scams, phishing emails, and 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 – Confirm before you click

Sharon wanted to purchase a Nintendo Switch for her son during lockdown. These devices had been so hard to come by that, after weeks of looking, she couldn't believe her luck when she found a company selling them at a reduced price. It looked like her hopes would be dashed though … because when she tried to enter her card details she couldn't get any further. Sharon was so worried that once again she would miss out, especially given how good a deal it was, she decided to contact the company through their online chat -- after all, the company had a UK website address so it looked genuine.



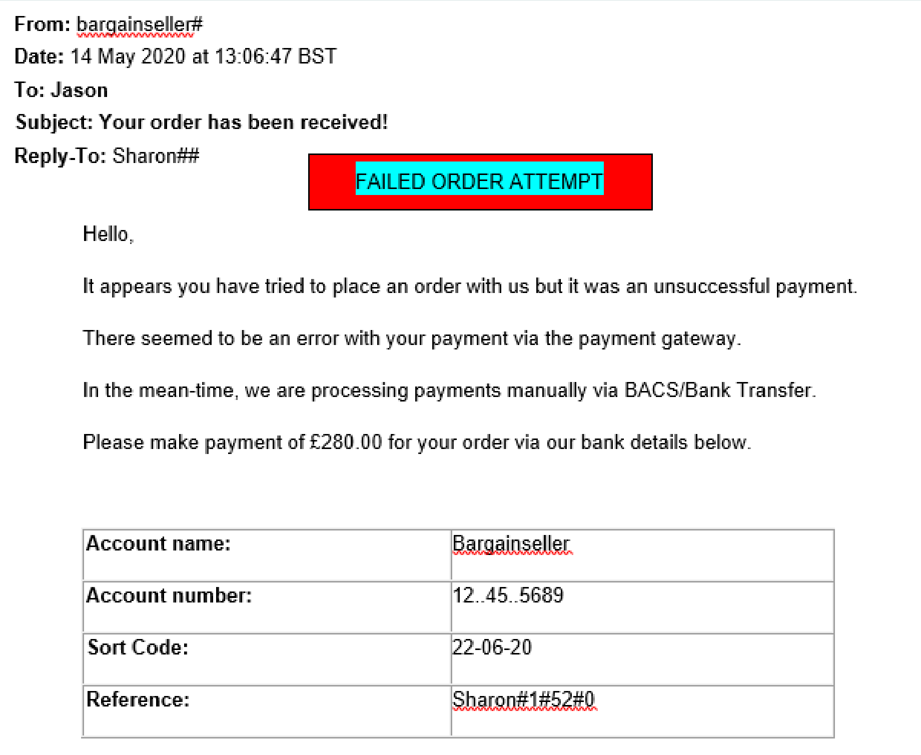


Order #1#52#0

Product	**Quantity**	**Price**
NINTENDO Switch - Neon Red & Blue • **Product Code:** 041920 Estimated delivery date 2020/05/28	1	£280.00
Subtotal:		£280.00
Shipping:		Free shipping
Payment method:		Debit/Credit Card
Total:		280.00

Order estimated delivery date 2020/05/28

The company replied on the chatbot straight away, advising Sharon that with so many people trying to purchase this great deal at the same time their website was having issues, but that she wasn't to worry as they could email an invoice and she could pay directly by BACS transfer. Sharon had her doubts, but the company seemed so helpful, and she felt she had to act quickly, so she agreed to receive the emailed invoice. Deciding to trust her gut instinct, Sharon searched the bank account details she'd been sent by the company online. Sharon's search revealed a bank she'd never heard of, which set alarm bells ringing for her. As hard as it was and given how desperately her son wanted the Nintendo Switch, Sharon resisted taking a chance and relied on her intuition -- which inevitably protected her from losing a lot of money to this online fraud.



From: bargainseller#
Date: 14 May 2020 at 13:06:47 BST
To: Jason
Subject: Your order has been received!
Reply-To: Sharon##

FAILED ORDER ATTEMPT

Hello,

It appears you have tried to place an order with us but it was an unsuccessful payment.

There seemed to be an error with your payment via the payment gateway.

In the mean-time, we are processing payments manually via BACS/Bank Transfer.

Please make payment of £280.00 for your order via our bank details below.

Account name:	Bargainseller
Account number:	12..45..5689
Sort Code:	22-06-20
Reference:	Sharon#1#52#0

The World Wide Web is what it says it is, world-wide. There are no geographical boundaries and cyber criminals operate in all corners of it. In any dealings you carry out online, please make sure you know exactly who you are communicating with and make sure you are absolutely clear before you part with any of your personal information and, as nearly happened in this case, banking details.