Cyber Resilience COVID-19 Bulletin

ISSUE: 21.05.20

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, over the next few months, the Scottish Government 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.

National Cyber Security Centre (NCSC)

COVID-19: Moving your business from the physical to the digital

COVID-19 has seen many organisations shutter their physical premises and move their business online. Establishing the IT services to support this transition can seem like quite a challenge.

NCSC have launched new guidance this week to help you determine how ready your business is, and point the way to any new cyber security measures you should put in place.

- **Home Working: Preparing Your Organisation and Staff (published March 2020)**
- **Video Conferencing: Security Guidance for Organisations (published April 2020)**
- **Moving Your Business from the Physical to the Digital – NEW guidance launched this week**

The NCSC website also has hubs for the self-employed and sole traders and for small businesses. These are good entry points into the world of cyber security.

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

Trending Topics

Easy Jet

EasyJet confirmed this week that it had suffered a cyber attack and is in the process of contacting affected customers following the incident. It said email addresses and travel details had been stolen and that 2,208 customers had also had their credit card details "accessed". You can read NCSC statement on the EasyJet incident on their website.

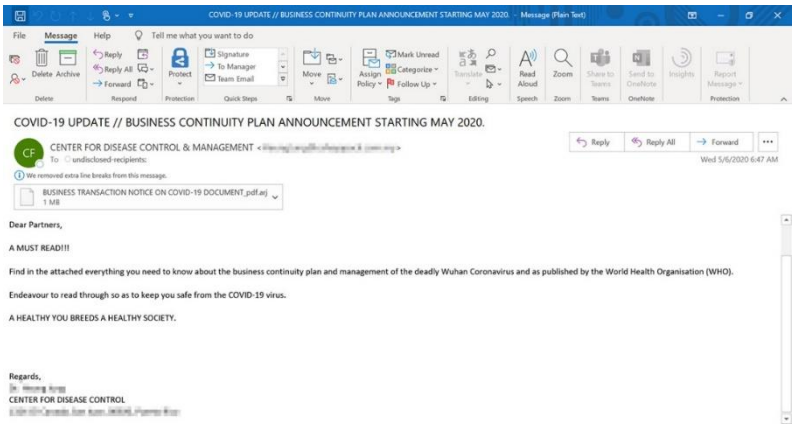
If you're an EasyJet customer, we recommend you:

- **Change your password on your EasyJet account – and if you know you've used that password anywhere else, change it there too. The best way to make your password long and strong is by using a sequence of three random words you'll remember. Avoid recycling old passwords.**

- **Check if your account has appeared in any other public data breaches. Visit https://haveibeenpwned.com and change your password.**
- **Use Two-factor authentication (2FA) - a free security feature that gives you an extra layer of protection online and can stop cyber criminals getting into your accounts - even if they have your password.**
- **Monitor your accounts, including credit monitoring accounts, for any unusual activity and look out for any phishing emails. There is more information on the NCSC website.**

Microsoft warns of COVID-19 phishing attacks spreading info-stealing malware

According to Microsoft, new phishing campaigns are using COVID-19 lures to trick recipients into opening malicious attachments. Threat actors pretend to be from, for example, the Centres for Disease Control (CDC) offering the latest information on the virus and a new "BUSINESS CONTINUITY PLAN ANNOUNCEMENT STARTING MAY 2020". Other, more common COVID-19 lures pretend to be from a vendor asking for updated banking information to process payments.



We continue to see a range of fake emails from retailers, government department: further details on these can be read in our previous bulletins.

If you have received an email you're not quite sure about, forward it to NCSC's Suspicious Email Reporting Service (report@phishing.gov.uk) and help protect the UK from email scams. Since the launch of this service 4 weeks ago, the public have passed on more than 454,828 suspect emails, with more than 3,444 bogus sites taken down.

Bitcoin Scam

Reports are coming in about emails promoting Bitcoin investment scams, claiming to take advantage of the financial downturn and helping people recover from bankruptcy. Fraudsters are using images of celebrities to make the emails seem authentic, but in reality the celebrity has no knowledge of the scam and does not endorse it. Always question unsolicited requests for your personal or financial information.

Romance Scams

Organised criminals will be exploiting loneliness during lockdown to take money from romance scam victims. Cyber criminals "meet" people on dating sites, then take the conversation onto private messaging, build up a picture of their victim, then take any opportunity to steal money from them. Criminals who commit romance fraud trawl through profiles and piece together information such as wealth and lifestyle, in order to manipulate their victims. Never send money to someone online that you have never met. BBC have a consumer series programme focusing on online dating scams that every day see unsuspecting victims conned out of tens of thousands of pounds. You can catch this on BBC iPlayer (For Love or Money).

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 successful 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.

Cyber Advice for the care home industry

SBRC has hosted a webinar around cyber and safe communications online, for those working in the care industry, as well as tips to help residents using their own devices to communicate with relatives. A recording of this webinar will be made available here.

SCVO: DigiShift - Cyber Security for Third Sector Organisations

On May 20th SCVO hosted a cyber security webinar for third sector organisations which consisted of a presentation from Derek Gordon, Director of Cyber Security at PwC. The focus of this session was on the foundations of cyber resilience for third and private sector organisations. A recording of this session can be viewed online.

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.**

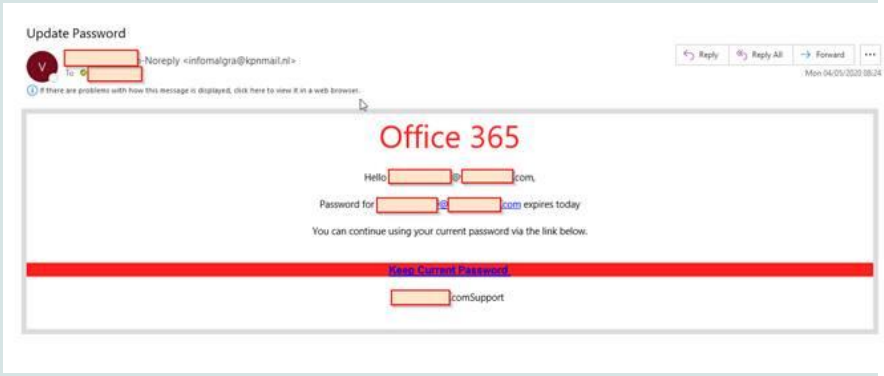
We are constantly seeking to improve. Please send any feedback to CyberFeedback@gov.scot

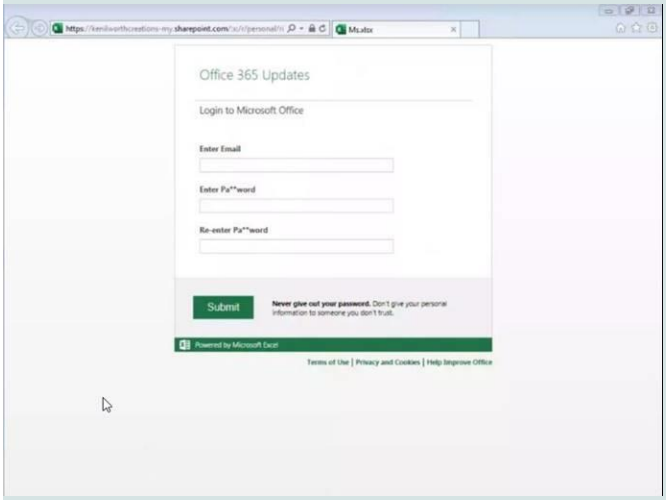
Case Studies

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 – Phishing

'Peter' was sent what turned out to be a phishing e-mail asking him to update his password. He then used the link in this e-mail to update his password taking him to what looked the genuine 'Office 365 Updates' page (The images below show the initial Phishing email and the website that was used to harvest the credentials.)





A few days later, a hacker then tried to use Peter's details to log in, and the multi factor authentication (MFA) was activated.

Peter was woken very early on a Monday morning with a call from Microsoft's MFA service and in his tired state he pressed the wrong button and authorised the login.

Peter realised his mistake and tried to call his IT department at 06:30, the desk wasn't operational yet, so Peter submitted an enquiry online to the IT service desk. At 08:00 IT logged in and saw there was an alert stating that an external forward was setup, which was against company policy. IT investigated this and saw that Peter's e-mails in finance were being forwarded to a strange Gmail address. IT spoke to Peter who explained what had happened. Peter had his password changed and IT took other measures to contain the incident and investigated whether there had been suspicious activity on Peter's account during the time he had given access by mistake. Thankfully no data had been accessed or files changed by the compromised account.

There have been lessons learned as a result of this incident:

- **Set- up out of hours alerting for a quicker reaction to any type of alert with a high or critical status.**
- **Change the MFA response mechanism to force users to enter a one-time password. This mitigates allowing of access by mistake.**
- **Align IT security and Data Protection teams' processes for this type of breach.**
- **Improve internal communication between teams working on different aspects of the incident (Data and IT Security)**
- **Immediately start a phishing awareness campaign and improve staff visibility of cyber security awareness materials and other security guides**
- **Encourage staff to check all links and URLS**
- **Encourage staff to report any suspicious activity on their accounts.**