Cyber Resilience Notice COVID-19 30/04/2020

As a result of the significant rise in COVID-19 related scams, the Scottish Government's Cyber Resilience Unit will share important information on a weekly basis. **Please 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.**

Video Conferencing Update

In relation to Zoom, important issues have been raised about encryption, and who keeps records or can listen in to calls. To help meet privacy obligations for their customers, Zoom report that they are introducing a new encryption method and the ability to report users. They have also increased the minimum password length for meetings. You can read more about Zoom 5.0 and how to start updating your version today.

Our advice is that you follow the National Cyber Security Centre's guidelines on using video conferencing software and platforms.

NCSC Guidance on Video Conferencing

- Video Conferencing services: using them securely – guidance for **individuals and families** about the use of video conferencing software.
- Video conferencing services: guidance for organisations – advice about how **businesses** can use video conferencing safely and securely.
- Video conferencing: new guidance for individuals and organisations (BLOG POST) – content introducing the two new pieces of guidance above. Refers to schools and National Crime Agency advice.

SBRC's team of ethical hackers has produced guidance on using Zoom for video conferencing. You can download 'Zoom: etiquette and security' from their website: https://www.sbrcentre.co.uk/resources/

Warning – Fake Zoom "HR Meetings" emails phishing for passwords.
Threat researchers at Sophos Labs have uncovered a new phishing campaign that seeks to ensnare victims by luring them with bogus Zoom invites. When receiving a Zoom link or logging in to your Zoom account, ensure that the URL is **zoom.us** - Zoom's official domain name.

Schools and online learning

NCSC guidance for schools and colleges (online/remote learning and teaching).
Now, more than ever, schools are relying on online technologies for learning and teaching as well as admin tasks. All staff can play a role in keeping online services (and the information they access) secure, safe and available.

NCSC have produced some Practical Tips for school and college staff to help them understand what cyber security is, how it's relevant and what steps they can take to improve their school's resilience when faced with cyber threats. The Blog that sits alongside this is also very helpful.

Further advice can be found here:

- Supporting Pupils, Parents and Teachers – Learning During Term 4 - guidance for home learning (Scottish Government)
- Engaging online: A guide for teachers (GTCS)
- Home working guidance, for school IT Teams or providers, which is also helpful for staff (NCSC)
- 10 steps to cyber security - key guidance (NCSC)
- Cyber Aware hub – an area for the new Cyber Aware campaign (NCSC)

Information and guidance for young people

- Young Scot DigiAye – Tips for young people on how to be more cyber resilient

- Young Scot DigiKnow – Want to start a career in cyber security? This guide is filled with fun ways to learn digital skills and alternative ways to get into the industry, as well as info on how to stay safe online
- https://youngscot.net/learning-resources Learning resources for anyone working with young people, including resources relating to staying safe online.

More information can be found on their dedicated Covid-19 landing page or on their Twitter page.

Community learning and development (CLD) resources

YouthLink Scotland worked with CLD partners to produce Safe Secured and Empowered, a set of resources, information and insights for people working in non-formal learning settings about being secure online.

Newsletters

Trading Standards Scam Share

Other scams to be aware of are detailed 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 the 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 for major cyber incidents. You can sign up here: https://tech.newstatesman.com/cyber-security-newsletter-sign-up

Get Safe Online

On Friday 1st May, Get Safe Online's **'Safe email'** campaign will go live. The campaign focuses on advice specific to the COVID-19 (Coronavirus) outbreak, including identifying phishing emails and safe home working. https://www.getsafeonline.org/safeemail/

Trending Topics

Fake NHS website

A hoax copy of the NHS website has been discovered. The website includes harmful links to COVID-19-related health tips. Once these links are clicked on, a pop-up box appears asking visitors to save a file called 'COVID19'. If saved, the malware it contains can steal passwords, credit card data, cookies from browsers, crypto wallets, files and screenshots.

COVID-19 Testing scam

Reports are being received from the US of a new SMS scam claiming 'someone who came into contact with you has tested positive for COVID-19'. Attackers have deployed a phishing campaign against remote workers using Skype, luring them with phishing emails with fake notifications from the service. The social engineering in this campaign is refined enough to make many people access the fraudulent login page and provide their credentials. Furthermore, the username is automatically filled in, which only helps reduce suspicion. All the victim has to do is type in their password and the attacker gets it automatically.

Retailers

Police have issued warnings of ongoing phishing emails and WhatsApp messages claiming to be from well-known retailers (such as Morrisons, Tesco and Heineken) offering free goods or vouchers. If you get a message like this, don't click on the links and don't share any personal or financial information.

You can report any suspicious emails directly to NCSC using their new suspicious reporting service.

- Public urged to flag coronavirus related email scams as new online campaign launches (PRESS RELEASE)

- Suspicious Email Reporting Service (SERS) – a webpage and email inbox which gives people an opportunity to report suspicious messages to the NCSC.

Training of the Week

The Cyber Griffin Unit at the City of London Police have created videos specifically looking at some of the cyber security risks associated with working from home. These videos are available on YouTube and can be found here or by searching for "City of London Police" on YouTube.

National Policing Protect Network has a list of all future webinars

Awareness raising for individuals

NCSC: E-learning Stay Safe Online: Top tips for staff - https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available . They have produced e-learning for staff, introducing why cyber security is important and how attacks happen.

BT
It is great to see an increase in cyber awareness campaigns from organisations within the financial services industry and others. The BT Tech Tips advert which runs in association with STV during the early Evening News provides really accessible messages for anyone using digital technologies for the first time:

- How to stay safe online with Angelica Bell
- How to keep your kids safe online, with Marvin & Rochelle

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.

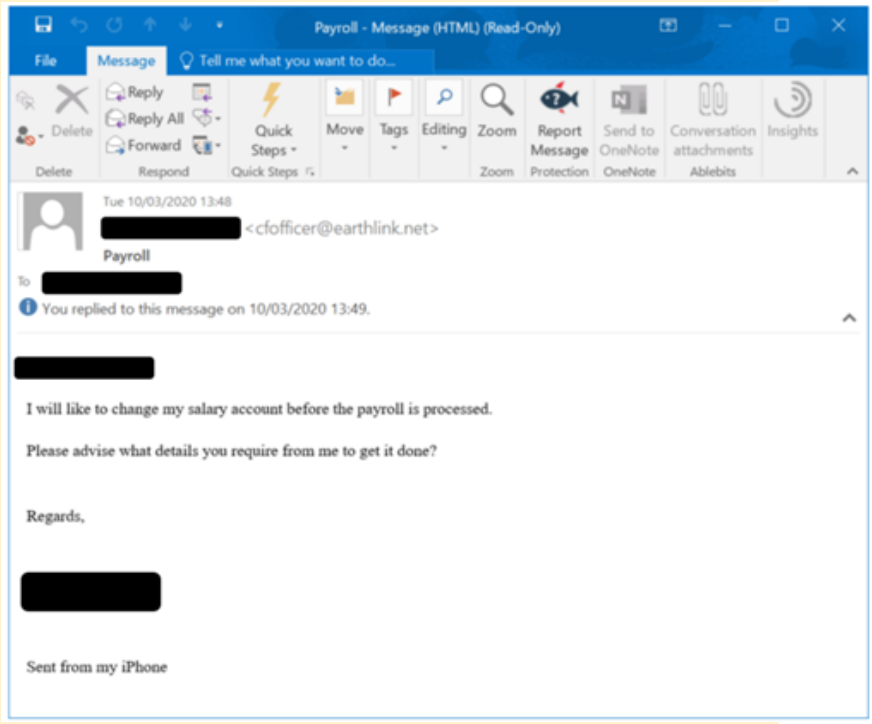
We are constantly seeking to improve. Please send any feedback to CyberFeedback@gov.scot

CASE STUDIES

From this week we will 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

Case Study – HR Phishing Scam

'Kath', a new member of an HR team working remotely due to the Covid 19 pandemic has received an email from someone she assumes is a legitimate member of staff and who is asking for his bank details to be changed for payroll purposes. Kath replies to the email, requesting information so that she can make the change.



The fake staff member then emails Kath with his fraudulent bank account details. Kath, believing the request to be authentic, changes a legitimate staff member's bank account details to the one of the criminal.

On payroll day the criminal sends another email asking for a copy of 'his' payslip. The criminal may have done this in order to provide his bank with the required information to secure a new bank account. At this point, fortunately Kath, phones the genuine staff member to confirm the request – only to find out that the staff member knows nothing about it.

Management have used this incident as an opportunity to highlight to all staff the importance of recognising phishing scams, what digital identity means, and how criminals can piece together information from multiple sources (Facebook, LinkedIn, Twitter etc.) to gain intelligence on a target. The incident also inspired an in-house email phishing campaign to raise awareness of how easy it is to fall for such an attack.

In light of lockdown restrictions, reviews have also been undertaken of similar business processes to ensure that correct checks and balances are in place.