Cyber Resilience Notice COVID-19 16/04/2020

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, so please ensure you only take information from trusted sources.

Training of the Week

Scottish Business Cares: The dos and don'ts of video conferencing
This webinar recording looks into video conferencing and how to do it securely. Learn how easy it is to protect your meetings with ethical hackers; Declan Doyle, Jess Amery **and Moe Keir**. https://youtu.be/LlTHJZypIpA

'ZOOM Bombings'

There have been cases globally of video conferencing broadcasts and meetings being hijacked by malicious users including a recent incident where obscene content was broadcast during an online swimming workout aimed at children in Scotland. This event, along with other events that are open by design are vulnerable to being hijacked as anyone can join them.

There are steps which can be taken to minimise the risk of intrusion which include using a unique meeting ID for each meeting and enabling a 'waiting room' feature so meeting hosts can add guests manually. Using Zoom securely is one of the topics covered in the webinar mentioned above and in a recent blog by Alison Stone at SCVO.

Each platform has security features and it's recommended that you take the time to familiarise yourself with configuring security settings to meet the needs of your organisation.

Zoom Security Skype Security Microsoft Teams Security Cisco Webex

There are numerous platforms out there, the list above is far from exhaustive and we recommend that you research and select a platform that meets your needs and has appropriate security functions.

Is your video conferencing password for sale online?

It is reported in Forbes and other trusted sources that up to 500,000 hacked Zoom account passwords are available on the dark web. Whilst the passwords appear to be quite old, the aim from the cyber criminals perspective is to take advantage of the fact that many users have the same password over multiple accounts. **If your password for video conferencing is the same as a password for any other service that has been leaked then there is the risk that your account could be comprised. Use a unique password.**

As ever, NCSC guidance for strong passwords applies – choose 3 random words and consider the use of a password manager to ensure that each online account has its own discreet passphrase.
Further guidance is available in the password section of the NCSC's Small Business Guide.

Cyber Resilience Notice COVID-19 16/04/2020

A quiz too far?

This week we are hearing details of online COVID-19 focused quizzes being used to harvest personal details for participants which could be used for fraudulent activity.
Taking advantage of the desire for information about the disease, these quizzes appear to be checking our knowledge but are also asking for details such as maiden names, family information, telephone and email addresses – even pet names. This may appear harmless, but this information allows scammers to build up a picture of a target which could be used subsequently for identity theft.

As always, be mindful of the information you share online. Further details on this and other scams are available in this weeks' Trading Standards Scotland Scam Share newsletter. You can sign up for their newsletter here.

Patching and security updates

Research carried out by Cyber Security Firm, FireEye has revealed that 12% of vulnerabilities were exploited within one week of patch issuance and 27% within one month. This makes the impact of these exploits entirely preventable by patching. You are in a race to patch against someone wishing to exploit the vulnerabilities.

Whilst some vulnerabilities are exploited and can cause havoc before patches come out, much like a vaccine, patching can prevent known vulnerabilities from being exploited in the future.

This applies to your own personal devices too, including your mobile phone and apps. Where possible, enable automatic software and security updates.

Guidance on patching can be found in the NCSC's Small Business Guide,
Advice on software updates for individuals can be found at Get Safe Online

PPE and Procurement Scams

In the US, the FBI have issued a warning after becoming aware of multiple incidents where state government agencies have transferred pre-payment funds to fraudsters in the hope of securing PPE which is in short supply globally.

Similarly, Europol have reported that a 39 year old man was arrested in Singapore thanks to international cooperation after he defrauded a French pharmaceutical company out of €6.64 million by pretending to be a legitimate company and advertising fast delivery of FFP2 surgical masks and hand sanitisers.

Europol, also reported that a number of EU member states have experienced similar frauds. Given the challenges in securing PPE from established conventional and trusted suppliers, all organisations large and small urgently seeking PPE are potentially at risk of exploitation by cyber criminals when seeking novel sources of supply. The importance of due diligence and process in procurement is paramount as the loss in addition to financial includes valuable time to secure supplies as victims may not know that they've been scammed until a delivery has failed to materialise. If it seems too good to be true, it probably is!

Europol are also aware of a manifold increase in the selling counterfeit PPE, healthcare and pharmaceutical products since the outbreak of the crisis.

If you've been a victim of coronavirus related or any other fraud, report it to Police Scotland by calling 101 (not Action Fraud).

Cyber Resilience Notice COVID-19 16/04/2020

Child Online Sexual Abuse

Children and young people are spending a lot more time online for learning and socialising during the Covid-19 Pandemic, and with parents, carers and guardians working from home, children are allowed more screen time than usual.

The UK National Crime Agency (NCA) released a figure in early April that shows that there are at least 300,000 people in the UK posing a sexual threat to children and that the NCA knows from online chat that offenders are discussing opportunities to target children and vulnerable users online during the Covid-19 Pandemic. Europol have also seen an increase in the number of attempts to access illegal websites featuring child sexual exploitation material.

Police Scotland have launched their online child sexual abuse campaign **#GetHelpOrGetCaught** on the 14th April 2020. The campaign is targeting perpetrators of online child grooming and encouraging them to seek help by contacting *Stop it Now!* as well as educating parents about the warning signs that their child may be a victim.
You can find out more about the campaign, the warning signs and how to report it here.

Child Protection Committees Scotland is also undertaking their '*eyes and ears open campaign*' urging everyone to be alert to signs of children being at risk of neglect and abuse during the coronavirus outbreak and enforcing online safety messaging. **#KeepingKidsSafeC-19**

Young Scot is stepping up efforts to promote their vast range of resources and materials to support young people to be more resilient online through their communications channels on Twitter, Facebook, Snapchat, Instagram and TikTok. https://young.scot/get-informed/national/how-is-covid-19-changing-how-we-interact-digitally

The Scottish Government is developing a Parent Club campaign on channels including TV, radio, digital and social media, offering practical advice and support across the breadth of challenges parents are facing during this time, including online safety.

Next 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.

AUTHORITATIVE SOURCES

- National Cyber Security Centre (NCSC) https://www.ncsc.gov.uk/
- Police Scotland https://www.scotland.police.uk/keep-safe/
- Trading Standards Scotland https://www.tsscot.co.uk/coronavirus-covid-19/
- Europol https://www.europol.europa.eu/
- Coronavirus in Scotland https://www.gov.scot/coronavirus-covid-19/
- Health advice NHS Inform https://www.nhsinform.scot/coronavirus

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