Cyber Resilience Notice COVID-19 09/04/2020

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.**

Trending

A joint advisory issued by National Cyber Security Centre (NCSC) and CISA regarding COVID-19 being exploited by malicious cyber actors. It includes a non-exhaustive list of indicators of compromise (IOCs) for detection as well as mitigation advice

- https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory

The Europol report provides an overview of how criminals adapt their misdeeds to the COVID-19 pandemic. It is based on information Europol receives from the EU Member States on a 24/7 basis and intends to support Member States' law enforcement authorities in their work.

- How cyber criminals are exploiting the crisis
- Catching the virus cybercrime, disinformation and the COVID-19 pandemic

The International Police Association INTERPOL have produced a number of Covid related reports

- Interpol Covid 19 Cyber threats
- Interpol Covid Stay Safe
- Interpol Covid Financial Crime

The Scottish Business Resilience Centre along with experts including NCSC CEO Ciaran Martin, discuss the latest cyber scams which have been circulating since the start of the pandemic. View the webinar here https://youtu.be/tqhleM1pqQc

Smishing / Phishing

Fake texts messages and emails appearing to be from a trusted source.
Latest scam text messages to look out for include those that:

- Claim to link you to a GOV.UK website to claim COVID-19 relief payments, council tax or business rate 'holidays' or free school dinner funds or similar.
- HM Government asking for donations to the NHS during the COVID-19 outbreak.
- Suggest you have been seen leaving your home on multiple occasions in breach of lock-down laws and levying 'fines'.
- Offering "health supplements" or Personal Protective Equipment supplies that falsely claim to prevent you becoming infected with COVID-19.
- Appear to come from your bank and relate to mortgage holidays or other financial support (business or consumer).

Advice: Be wary of any texts you receive, even if it appears to come from an organisation you know and trust. Don't follow links in text messages or phone any numbers provided. If you believe a text message is genuine and require more information, contact the organisation via their website by typing their genuine web address into your browser.

Home Working

The **National Cyber Security Centre (NCSC)** have produced advice and guidance to help individuals and businesses who are working from home to stay safe online.

- How to make sure your organisation is prepared for an increase in home working, and advice on spotting coronavirus (COVID-19) scam emails https://www.ncsc.gov.uk/guidance/home-working

Web conferencing:

Communications platforms (such as Zoom and Microsoft Teams) for online meetings are becoming popular given the need for home based working. Malicious cyber actors are taking advantage of this and are hijacking online meetings that are not secured with passwords or that use unpatched software. Organisations will have their own preferences based on their risk appetite. Tips from the NCSC Covid 19 Advisory for defending against online meeting hijacking include;

- Do not make meetings public. Instead, require a meeting password or use the waiting room feature and control the admittance of guests.
- Do not share a link to meeting on an unrestricted publicly available social media post. Provide the link directly to specific people.
- Manage screen sharing options. Change screen sharing to "Host Only."
- Ensure users are using the updated version of remote access/meeting applications.
- Ensure telework policies address requirements for physical and information security. Make sure to update your software and applications regularly. This will install the latest security improvements.

Zoom application has gained significant prominence and some criticism over security concerns. Zoom describes how they are improving their privacy and security settings. https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/ Zoom has enabled the Waiting Room feature and require **additional password settings** for all Basic users on free accounts and accounts with a single licensed user.

National Cyber Security Centre will produce guidance on using web conferencing securely. This will follow in a future Cyber Resilience Notice.

Police Scotland

Cyber Griffin Unit at the City of London Police have created videos specifically look at some of the cybersecurity risks associated with working from home.
The videos are all available on YouTube and can be found here or by searching for "City of London Police" on YouTube.
If you've been a victim of coronavirus related or any other fraud, report it to **Police Scotland by calling 101** (not Action Fraud).

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 the way that we distribute this notice. Please send any feedback to CyberFeedback@gov.scot

Scottish Government
Riaghaltas na h-Alba
gov.scot