Cyber Resilience COVID-19 Bulletin

ISSUE: 18.06.20

A CYBER RESILIENCE STRATEGY FOR SCOTLAND

Scottish Government
Riaghaltas na h-Alba
gov.scot

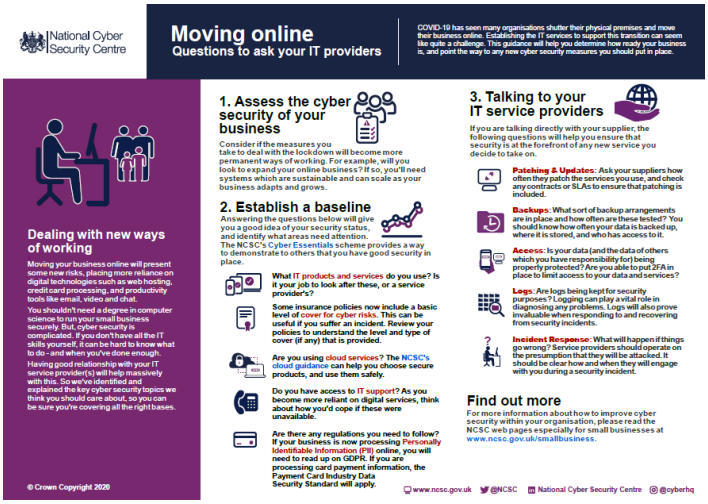
Cyber Resilience COVID-19 Bulletin

As a result of the significant rise in COVID-19 related scams, over the next few month, 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.

We are looking to measure and improve the Bulletin readers' experience and satisfaction. Please answer this short survey to share your thoughts. Survey will close 19/06/2020

National Cyber Security Centre (NCSC)



The National Cyber Security Centre recently produced guidance aimed at helping organisations that are moving their business online. This guidance will help you determine how ready your business is, and point the way to any new cyber security measures you should put in place. Having a good relationship with your IT service provider(s) will help with this. NCSC have identified and explained the key cyber security topics you should be concerned with, so you can be sure you're covering all bases.

Football fans urged to secure their online platform streaming accounts and subscriptions, as Premiere League returns

Millions of football fans are expected to log in to subscriptions to stream behind-closed-door games. NCSC warns online hackers could break into football fans' accounts to carry out 'phishing' scams. The NCSC has urged fans to take some basic steps, which form part of the NCSC's Cyber Aware behaviours, to keep their accounts secure, including setting strong passwords that are made up of three random words and ensuring you download the latest updates for apps on devices.

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, the reports received stand at more than 938,000 with 9,400 individual URLs linked to 3,100 sites being removed.

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

Trending Topics

Returning to work - ICT System Privileges and Access

As businesses and organisations gradually begin to return to work, managers should take time to consider their ICT policies and what they expect from their staff in terms of maintaining business security. Managers could ask themselves: when was the last time you evaluated what level of access employees need to your ICT systems in order to do their job? Who is responsible for regular patching updates or ensuring your system administrator password is protected.

The vulnerability of your system can be managed by providing all users with the reasonable (but minimal) level of system privileges and rights required for their role. This principle is sometimes referred to as 'least privilege'. Businesses and organisations should consider having a policy in place where they allocate minimum system user access to general staff. Increased user system privileges should be allocated to qualified individuals, being carefully reviewed, controlled and managed on a regular basis. By introducing these steps you support staff by raising awareness regarding cyber security, acceptable account usage and their personal responsibility to adhere to corporate security policies.

NCSC have produced guidance to help you manage user privileges as part of their 10 steps to cyber security collection.

Black Lives Matter ransomware

Hackers have been taking advantage of recent events and the popularity of the Black Lives Matter movement. There have been reports of ransomware being spread through phishing emails, targeting those in areas where there have been Black Lives Matter protests. A typical email asks users to fill in a confidential survey to comment on the recent protests, then asks them to download an attachment to fill out a form. The form contains a piece of malware known as "TrickBot" which is a common ransomware program. This will encrypt a user's files and attempt to steal sensitive information such as banking details and passwords that may be saved on the computer/device. Since last Thursday, there has been increase in the number of new domain names registered containing words related to the campaign which may be used in phishing attempts.

Get Safe Online has valuable advice when donating to charities online. Take time to make you sure you are safe to proceed, by checking the web links and charities' official web pages for information. Be cautious of any links asking you to donate. Make sure to verify that your donations are going to a trusted organisation. In Scotland, all charities must be registered, and an online register of charities is maintained by the Office of the Scottish Charity Regulator (OSCR).

Kids at home

As a parent or someone else with responsibility for a child or young person, you'll be all too aware of the dangers they can be exposed to online. Get Safe Online safety experts have put together some expert tips to help you keep the children and young people in your care safe and more aware of these dangers. They also have some simple checklists to help you keep your kids safe online according to their age group.

A command of the National Crime Agency, CEOP explains the dark web, which is part of the World Wide Web that allows users to remain anonymous. This article, written in collaboration with Parent Zone, helps explain the reasons why your child might be using it, and what you need to know about it. Being aware of the basic facts about these parts of the internet can help you to have open and realistic conversations with your child, especially if you are concerned about them using the dark web.

National Scams Awareness

Shut Out Scammers Campaign

Trading Standards Scotland (TSS) are working in partnership with Police Scotland to coordinate the annual Shut Out Scammers campaign, which will run from 15 - 26 June. Shut Out Scammers recognises that as lockdown is now easing, doorstep crime is on the rise again and so too are nuisance calls that can lead to scam visits.

The campaign aims are:

- **To reduce the impact of doorstep crime by providing information and advice on how to prevent falling victim to bogus callers**
- **To raise awareness of the issues surrounding doorstep crime and the organisations that are able to help. Police Scotland share their tips on how to spot a rogue trader**
- **To interact with vulnerable groups most affected by doorstep crime and revisit previous victims (virtually or by telephone), ensuring appropriate crime prevention advice is given**
- **To encourage reporting of doorstep crime**
- **To investigate all instances of doorstep crime and consider using enforcement activities in partnership with other agencies to target offenders**

Scams Awareness Fortnight 2020

Citizens Advice Scotland has welcomed the launch of their 2020 Scams Awareness campaign which runs from 15 - 28 June. The 2020 campaign objective is to reduce the risk and impact of coronavirus scams by raising awareness and encouraging behaviour change amongst the public at a local and national level. For further information, visit Citizens Advice website Scams Awareness Fortnight 2020. (Please note that the material provided by Citizens Advice includes England-only contact information.)

Alongside this campaign, the Advertising Standards Authority (ASA) in partnership with the Internet Advertising Bureau, launched a new scam ad alerting system. This allows internet users to report scam ads appearing in paid-for space online to the ASA. It will then send an alert to advertising platforms and publishers with details of the scam ad. You can report an ad using this form on the ASA website. Use this form to report online scam ads including ads on newspaper websites, paid-for search engine ads or ads appearing on social media.

For more help on spotting scams and how to protect yourself online, Martin Lewis (money saving expert) has some great articles including: 30+ ways to stop scams and 20+ coronavirus scams to watch out for.

Please note that if you wish to participate in the Scam Awareness campaign in **Scotland**, use the provided campaign materials, or reporting a scam ad online – please use and promote the links below. This will help to ensure Scottish consumers are directed to the most appropriate sources of information, advice and/or scams reporting helplines.

- If you feel threatened or unsafe, contact **Police Scotland** on 101 or 999 in an emergency.
- Report scams to **Advice Direct Scotland** on 0808 164 6000.
- Online web-chat **Scams Action Service** Citizens Advice Scotland.
- Suspicious email? Forward it to the National Cyber Security Centre - Suspicious Email Reporting Service (SERS) **reporting@phishing.gov.uk**

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 publish detailed information about each of their #CyberAware tips in their weekly cyber security technology newsletter, working alongside 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

Microsoft has released a set of free cyber security training course for Microsoft 365 (formerly Office 365) subscribers

The courses, produced in partnership with Terranova Security, focus on COVID-19 specific threats. The rate of attack continues to increase and with so many people working from home, hackers see multiple opportunities to breach corporate and personal security. The attack simulator trainings cover mass phishing, protecting home computers and privacy. Microsoft 365 subscribers may access the cyberattack simulator trainings here. There is also a download with more content, including blog posts and infographics to educate your target audience.

The Cyber Academy - New technologies and privacy in times of COVID-19: what are the concerns and how to address them.

Laura Irvine, partner at Davidson Chalmers Stewart and accredited specialist in data protection law, presented a webinar looking at some of the new technologies that she has been experiencing and advising on during lock down, so that we can continue to engage in the work place and socially without being concerned about losing our privacy. View the webinar here.

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

Each week, 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 – Vishing – NHS Scotland's Test and Protect

NHS Scotland's Test and Protect was rolled out across Scotland at the end of May and is extremely important in the fight against coronavirus.

Unfortunately, criminals will exploit every opportunity they can to defraud people of their money, or steal their personal details. Criminals are acting quickly and have started to contact victims pretending to be from the NHS. See below an example transcript of how criminals might try to trick you into handing over your money.

SCAMMER - 'Good morning, I'm calling from the NHS track and trace service. According to our system, you are likely to have been in close proximity to someone who has tested positive for COVID-19. This means that you now need to self-isolate for 7 days and take a COVID-19 test.'

VICTIM - 'OK. Can you tell me who that person was?'

SCAMMER - 'I'm not able to tell you that. That is confidential information.'

VICTIM - 'Right. Um... so ....'

SCAMMER - 'But you do need to be tested within the next 72 hours. So can I just get the best mailing address so that we can send a kit to you?'

VICTIM - 'Ok (gives address)'

SCAMMER - 'Thank you - and I just need to take a payment card so that we can finalise this and send the kit to you.'

VICTIM - 'Sorry - a payment card? I thought this was all free?'

SCAMMER - 'No - I'm afraid not. There is a one-off fee of £50 for the kit, and test results. Could you read off the long card number for me, please, when you're ready.'

VICTIM - 'No - that's not right. This is part of the NHS so there's no charge.'

SCAMMER - 'I'm afraid there is. Can you give me the card number please - this is very important. It ensures that you get the test tomorrow. Also there are penalties for not complying.'

VICTIM - Puts phone down.

VICTIM - Calls Police Scotland on 101 to report the incident.

If you have been a victim of fraud of any kind, report this to Police Scotland by calling 101.

The Scottish Health Secretary has advised what to expect when called by a contact tracer:

An NHS contract tracer will:

- **introduce themselves, state the reason for their call, and will always identify the call recipient by name**
- **ask about your symptoms, where you work and information about your movements**
- **ask for information about the people you have been in close physical proximity to including the names, phone numbers and locations you have been physically close to**
- **they may send a text message or email to provide links to online guidance and support**

An NHS contact tracer will not:

- **ask for personal information like bank accounts, credit card details, passwords or PINs, or medical records**
- **offer services to you, ask you to download anything or try to sell you anything**.

Get information about contact tracing in Scotland from official sources: NHS Scotland, the Scottish Government or Public Health Scotland.