Cyber Resilience Notice COVID-19 07/05/2020

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

As well emailing this bulletin to our stakeholders we have also made it available online here

National Cyber Security Centre (NCSC)

Joint Advisory issued

The National Cyber Security Centre (NCSC) and Cybersecurity & Infrastructure Security Agency (CISA) continue to see indications that Advanced Persistent Threat (APT) groups are exploiting the COVID-19 pandemic as part of their cyber operations and have issued a second joint advisory**.** The joint NCSC/CISA advisory from 8 April 2020 detailed the exploitation of the COVID-19 pandemic by cyber criminals and APT groups. This joint NCSC-CISA advisory provides an update to ongoing malicious cyber activity relating to both national and international COVID-19 responses. Organisations at risk include healthcare bodies, pharmaceutical companies, academia, medical research organisations, and local government. The document describes some of the methods criminals are using to target organisations and provides mitigation advice.

National Cyber Security Centre

COVID-19 CYBER THREAT EXPLOITATION

The Threat and How to Think About It

The Cybersecurity and Infrastructure Security Agency (CISA) and United Kingdom's National Cyber Security Centre (NCSC) have seen an increase in malicious activity with themes related to Coronavirus Disease 2019 (COVID-19). Malicious cyber actors are targeting individuals, small and medium enterprises, and large organizations worldwide with COVID-19-related scams and phishing campaigns (see figure 1). At the same time, the surge in teleworking has increased the use of potentially vulnerable services.

Additionally, CISA and NCSC are investigating advanced persistent threat (APT) activity targeting healthcare and essential services. This activity includes password spraying—a commonly used style of brute force attack in which the attacker tries a single and commonly used password against many accounts before moving on to try a second password, and so on.

This product provides practical advice for individuals and organizations on how to defend against COVID-19-related malicious cyber activity.

For detailed guidance on these threats, see the CISA-NCSC joint Alert on COVID-19-related malicious cyber activity as well as the CISA-NCSC joint Alert on APT activity targeting healthcare and essential services.

Actions To Take Today

Communication Platform Guidance for Individuals and Organizations[1]

Limit screensharing options

Do not make meetings public.

Ensure users have the most up-to-date version of remote access/meeting applications

Do not share links to meetings on unrestricted, publicly available social media posts.

Ensure telework policies address requirements for physical and information security.

Guidance for Defending Against Password Spraying Attacks

Set up a security monitoring capability so you are collecting the data that will be needed to analyze network intrusions.

Use multi-factor authentication to reduce the impact of password compromises.

Review and refresh your incident management processes.

Protect the management interfaces of your critical systems. Use browse-down architecture to prevent attackers easily gaining privileged access.

Use modern systems and software. These have better security built-in.

[1] FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic, FBI press release, March 30, 2020, https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

Actions To Take Today Continued on next page >

Trending Topics

Communicating online during COVID-19

We all remain separated from loved ones due to physical distancing, and many of us are keeping in contact with each other through online communication; for example, through video chats. We have heard of people lending devices to older relatives, or dropping them in to care homes, for example, to enable this contact.

Please remember that devices should be secured with a password (ideally three random words), and that care should be taken when joining WiFi. WiFi in public settings should be password protected as well.

The NCSC offer a wealth of advice and guidance relating to such matters as the use of passwords and the use of devices such as mobile phones and tablets; and specific guidance relating to common questions (for example, relating to the use of WiFi).

NHS Covid symptom tracker app – NCSC security

Experts from the National Cyber Security Centre have been supporting the development of the NHS COVID-19 contact tracing app, which will be launched on the Isle of Wight this week. The privacy and security of app users' data is a priority and the NCSC has been advising on best practice throughout the app's development. They have published three documents relating to the work, including a technical paper which provides a high-level overview of the security and privacy characteristics of the app. You can read more their website.

NCSC Suspicious Email Reporting Service

As part of the Cyber Aware campaign, the NCSC successfully launched its suspicious email reporting service (SERS), resulting in dozens of malicious web campaigns being shut down in its first day, after a spike in coronavirus phishing scams. In just over two weeks since the NCSC and police launched the service, the public have passed on more than **160,000 suspect emails, with more than 300 bogus sites taken down**. You can view images of some of the removed fake websites on the NCSC website.

Action Fraud have reported that 1,467 victims have lost a combined total of £2,996,252 to coronavirus-related scams with 6,069 reports of coronavirus-related phishing emails – Thursday 7th May, 2020.

By forwarding any dubious emails – including those claiming to offer support related to coronavirus – to report@phishing.gov.uk, the NCSC's automated programme will immediately test the validity of the site. Any sites found to be phishing scams will be removed immediately.

Mandate Fraud

The threat from mandate fraud has increased during the COVID-19 response. This could result in organisations losing substantial amounts of money that will be difficult to recover. Criminals will gather information about a business's suppliers, customers or senior employees, from different sources to make their approaches seem legitimate. They will then request to change a direct debit, standing order or bank transfer mandate in order to divert payments or to create new payments. Criminals have used changes in business practices around COVID-19 as a reason for a change of bank details, or the fact that more people are working from home. Approaches from criminals might be made over the telephone, or by letter or email.

Police Scotland have published an article on what you need to know about mandate fraud as well as on their keep safe pages.

TAKE FIVE TO STOP FRAUD™

Stop – Taking a moment to stop and think before parting with your money or information could keep you safe.
Challenge – Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
Protect – Contact your bank immediately if you think you've fallen for a scam. Report a crime or incident to Police Scotland by calling 101.

https://takefive-stopfraud.org.uk/

Anti-Virus

An anti-virus firewall software provider (Sophos) recently revealed that cyber criminals exploited an SQL injection vulnerability in their management interface to extract user data such as usernames, passwords, and local device administration information. Sophos have released a "hot fix" for devices that have auto-update turned on. All customers should take note of the further advice on remediation, whether they have received the hot fix or not. You can read NCSC statement following this discovery on their website.

Blackmail

A new phishing email has been found in the US and Australia, where fraudsters are blackmailing victims, claiming they will infect their family with the coronavirus if they do not pay a fee. They claim to know everything about the victim, and may even display a password that has been leaked in a data breach, that the recipient would be familiar with. These emails have been compared to popular phishing email tactics like those threatening to expose indecent images of the victim. However, this email attack goes further by threatening the lives of the recipient's family. If you receive an email like this, you should forward it on to the NCSC phishing email account (report@phishing.gov.uk) and contact Police Scotland on 101

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 the 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 relating to major cyber incidents. You can sign up here

Europol new report – Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU. 30th April 2020

Training of the Week

NCSC

- The National Cyber Security Centre Certified Training scheme provides a benchmark for cyber security training by assuring the quality of both content and its delivery. These courses are rigorously quality assessed against exacting standards.
- 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.

Further Training Available

- National Policing Protect Network has a list of all their cyber security future webinars
- 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.
- TechUk have provided a cyber training and skills content repository
- 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 Protecting your business online with Peter Jones

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.

Awareness raising for individuals

World Password Day Thursday 7th May is World Password Day. Passwords protect valuable information held in our emails, mobile phones, online bank accounts and more. Create a strong password by using a sequence of **three random words** you'll remember. You can make it even stronger with special characters. For more advice check out the NCSC's website where there is further information on password strategies that can help your organisation remain secure.

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.

CASE STUDY

In these Notices, 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

Buying COVID-19 related goods online

Organised Criminals are using this national crisis to defraud people online of money, and also selling sub-standard or fake goods online. We want you to be aware and prepared when you see offers online, and to be especially careful when you are interacting with sellers.

The Internet is flooded with adverts aimed at the general public, offering "surgical face masks" and other similar goods for sale. When you see these adverts, take the time to consider those who really need this type of Personal Protective Equipment (PPE). Are you considering the ethical nature of these adverts for alleged specialised products? Are these products of a proper standard? Are they from a reputable seller? Will you actually receive them?

It isn't the case that there is a cyber criminal behind every advert such as these, but if you see or are sent links offering such items for sale, please take care. You could find yourself the victim of a scam where either your personal details are harvested, or where you lose your money or don't receive the goods advertised.

Photo by De an Sun on Unsplash

Top tips to prevent procurement fraud: Police Scotland offer top tips to prevent procurement fraud:

1. Ensure all staff who are able to make or are involved in financial decisions are trained how to identify procurement fraud.

2. Never give in to pressure or threats that it is a time-sensitive issue or an urgent matter. A genuine organisation will have no issues with you verifying a request, however a fraudster will often try to pressurise you into acting immediately.

3. Ensure a three-way match is carried out. Do the amounts documented on the requisition, purchase order and invoice all align?

4. Adopt dual control procedures for authorising payments. Ensure that a senior member of your team reviews your actions and formally authorises the payment.

5. Ensure the procurement process is followed and is enforced. Has an order been placed before the procurement paperwork has been raised? If so, why?

6. Carefully check the sender's email address to identify if it exactly matches your known and trusted records and call your supplier to verify the email is genuine

7. Be vigilant to any clerical or spelling errors within emails which may indicate the email is fraudulent.

8. If it is a new supplier, carry out internet searches to check if they are genuine, are there any customer reviews and phone any listed landline to check.

9. Be alert to any requests to alter bank details. Carry out an internet search of the new bank account sort code and account details to uncover: Location of the bank (to be checked against the company address) and whether there are any blogs or reports available to indicate the communication is a scam.