Cyber Resilience COVID-19 Bulletin

ISSUE: 13.08.20

A CYBER RESILIENCE STRATEGY FOR SCOTLAND

Scottish Government
Riaghaltas na h-Alba
gov.scot

Cyber Resilience COVID-19 Bulletin

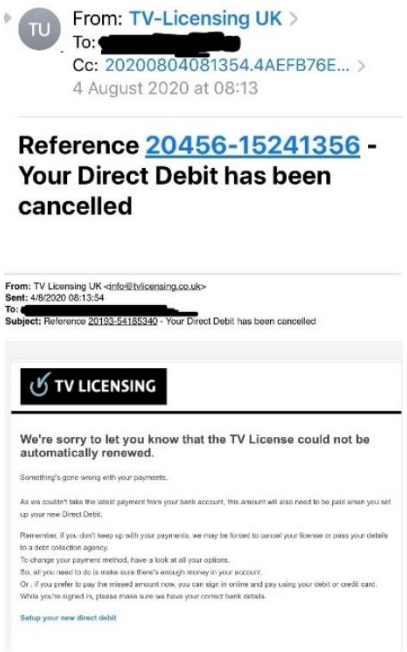
As a result of the significant rise in COVID-19 related scams, over the next few months the Scottish Government Cyber Resilience Unit will share important information. We aim to update the Bulletin on a regular basis and ask that you consider circulating the information in it to your networks, adapting it 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. If there are any cyber terms you do not understand, you can look them up in the NCSC Glossary.

National Cyber Security Centre (NCSC)

NCSC have released their first ever guidance on taking out cyber insurance. The new cyber insurance guidance published online urges businesses to consider seven key questions to help them make informed decisions about cover. The advice encourages organisations of all sizes to think about how insurance might help in the wake of a cyber attack and contribute to existing risk management strategies. Questions range from what levels of defence are already in place to whether the insurance covers the aftermath of an incident. Before considering taking out any cyber insurance, you can help protect your organisation by ensuring you have fundamental cyber security safeguards in place, such as those certified by Cyber Essentials, or Cyber Essentials Plus. Some organisations that achieve Cyber Essentials are provided with cyber liability insurance offered as part of this certification through the IASME Consortium.

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 1,929,000 with 18,100 individual URLs linked to 7,080 sites being removed. Please forward any suspicious emails to: **report@phishing.gov.uk,** suspicious text messages should be forwarded to **7726.**



The NCSC produces weekly threat reports drawn from recent open source reporting. This week's report highlights that cyber criminals have exploited recent changes to TV licence requirements for the over 75s and used these changes to target vulnerable users. TV Licensing have put up a page on their website with FAQ on TV Licensing during COVID-19, including advice for managing your licence and viewing your payment plan online. TV Licensing have email security and scam advice on their website, including four quick ways to spot a scam.

Always question unsolicited requests for your personal or financial information in case it's a scam. Never automatically click on a link in an unexpected email or text, instead visit the website directly.

Trending Topics

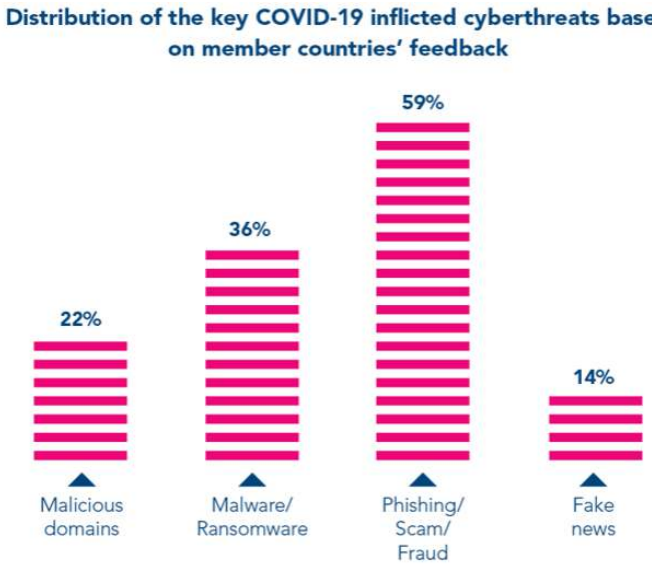
Unexpected delivery

The public are being warned that some Amazon and Facebook sellers are setting up accounts in strangers' names, then sending their products to unsuspecting recipients. Scammers mail lightweight (inexpensive to ship) packages, such as rings, face mask and seeds, to people who did not order the merchandise. They do this in order to create fake customer profiles with real names on e-commerce sites, and then create false positive reviews for their products and/or company. You should report the incident to the retailer that your package has come from. You can check if your personal details have been part of a data breach on haveibeenpwned.com and change any passwords connected to your account. Police Scotland provide further information on identify theft and how to protect yourself.

Significant numbers of Scottish households have been receiving unsolicited packets of seeds in the post from China/Singapore as part of a likely scam. The advice is not to open the packet or handle the seeds. Don't plant or compost the seeds as it could pose a threat to agriculture and the environment. Science and Advice for Scottish Agriculture (SASA) is collecting these unsolicited packets of seeds for analysis. It is asking for your co-operation to send these seeds to SASA and further details are available on their website.

INTERPOL Report

An INTERPOL assessment of the impact of COVID-19 on cyber crime has shown a significant target shift from individuals and small businesses to major corporations, governments and critical infrastructure. With organisations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption.



Future primary areas of concern highlighted by the INTERPOL report include the following:

- **A further increase in cybercrime is highly likely in the near future. Vulnerabilities related to working from home and the potential for increased financial benefit will see cybercriminals continue to ramp up their activities and develop more advanced and sophisticated modes of operation.**
- **Threat actors are likely to continue proliferating COVID-19-themed online scams and phishing campaigns to exploit public concern about the pandemic.**

- **Business Email Compromise schemes will also likely surge due to the economic downturn and shift in the business landscape, generating new opportunities for criminal activities.**
- **When a COVID-19 vaccination is available, it is highly probable that there will be another spike in phishing related to these medical products as well as network intrusion and cyber attacks to steal data.**

Test and Trace – Protecting customer and visitor details

Businesses serving customers who remain on the premises, for example those in the tourism and hospitality sector, have been asked to gather minimal contact customer details to help support the NHS Scotland's Test and Protect service. From **Friday (14 August)**, it will be mandatory to collect contact details of customers in a range of hospitality and other public settings.

It is important that this information is collected, stored and deleted securely and businesses should consider the principles of data protection law. That means you must make sure the information you collect is adequate, relevant and limited to what you need. It must be accurate and not used for any other purposes, such as marketing. You should also keep it secure, so you minimise the risk of accidentally losing or destroying it. After 21 days, data must be disposed of securely. More details are noted in the links below.

- **The Information Commissioners Office (ICO) have created five simple steps to help ensure that you protect customer data.**
- **The ICO have published further detailed guidance on this topic and information on processing children's data is available here.**
- **Scottish Government guidance is available to read here.**
- **Digital Skills Education's blog lists some tools available to make it easy to abide by the rules.**

Top 10 COVID-19 Scams

UK Finance has warned that scammers are preying on consumers' financial fears and have named ten COVID-19 scams the public should be wary of. Citizens Advice Scotland have an online scams helper to check whether something might be a scam and give you advice that's specific to your situation.

Financial support scams

1. **Fake government emails offering grants of up to £7,500. Clicking on the links allows scammers to steal personal and financial information.**
2. **Scam emails offering access to "COVID-19 relief funds".**
3. **Official-looking emails offering a "council tax reduction".**

4 **Benefit recipients are offered help in applying for universal credit, but fraudsters grab some of the payment as an advance for their "services".**

Health scams

5 **Phishing emails claiming that the recipient has been in contact with someone diagnosed with COVID-19. They lead to fake websites that are used to steal personal and financial information or infect devices with malware.**

6 **Fake adverts for non-existent COVID-19-related products, such as hand sanitizer and face masks, which simply take the victim's cash and send them nothing.**

Lockdown scams

7 **Fake emails and texts claiming to be from TV Licensing, telling people they are eligible for six months' viewing free but ask people to update their payment information.**

8 **Emails asking people to update their TV subscription services payment details by clicking on a link which is then used to steal credit card information.**

9 **Fake profiles on social media sites are used to manipulate victims into handing over their money. Criminals will often use the identities of real people to strike up conversation with their targets.**

10 **Fake investment opportunities are advertised on social media sites, encouraging victims to "take advantage of the financial downturn".**

Newsletters

Trading Standards Scam Share

Other scams to be aware of are identified in last week's scam share, where reports are detailed of cold calls purporting to be from Citizens Advice Scotland and scams linked to the UK Government's Green Homes Grant scheme (which is only available in England). Check out this week's Trading Standards Scotland Scam Share newsletter for more. You can sign up for the weekly newsletter here.

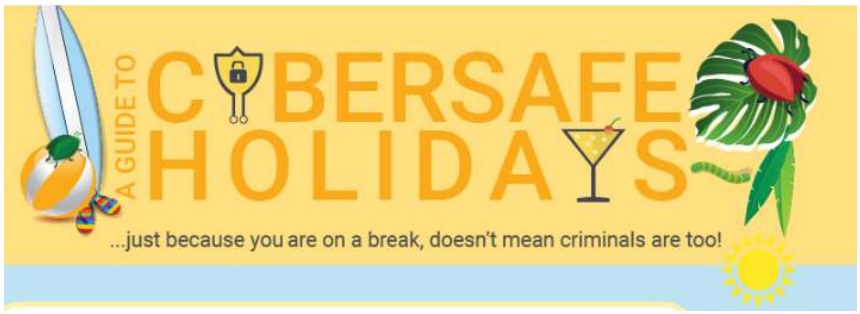
Neighbourhood Watch Scotland

Sign up to the Neighbourhood Watch Alert system to receive timely alerts about local crime prevention and safety issues from partners such as Police Scotland.

Training and Webinars

EUROPOL (European Cybercrime Centre)

Europol's crime-prevention guides contain information that can help citizens protect themselves and their property. The guides cover a range of topics from how to keep your home cyber secure to staying cyber safe on holiday. You can view all the public prevention and awareness guides on their website. These guides are available in multiple languages. Follow them on twitter (@EC3Europol) for more tips and great infographics



EUROPOL: Full infographic available here

Case Studies

Each week, we 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 We are happy to anonymise the case study.

Case Study – Scammers call dentist surgery

A dental surgery received a phone call from someone with an American accent purporting to be from the NHS, who was insistent that their list of dental practices need to be updated urgently. They said they would call back in 15 minutes to confirm completion.

Only when the 'urgent' paperwork arrived by e-mail did the sharp-eyed recipient realise it was in fact a two-year contract for an entry in a City Maps directory costing £35 per month.

Replying as the caller insisted would have resulted in an unexpected invoice a month later with the practice stamp on a contract, with the misleading statements made in the preceding telephone conversation long forgotten.

Trading Standards Scotland have previously reported similar email scams targeting large retailers, restaurant and cafe chains, all stating that their Head Office is closed or that they have staff shortages and asking for information about business accounts for various sites. Businesses of all sizes should be wary of these scams and should ensure that anything they agree to sign not only comes from a trusted source, but that the details/terms are fully understood before they commit.

In other news, the British Dental Association (BDA) has announced that a major cyberattack has put the private data of its members at risk. Hackers have apparently gained access to names, contact details, transaction histories, bank details, logs of correspondence and case notes, giving them the opportunity to carry out identity theft scams.

Advice:

- **Question unexpected emails which request private business information or payments, even if they appear to come from someone within your company**
- **Think about what you are being asked to do – if in doubt about financial transactions or changes to Direct Debits get a second opinion from a colleague or manager**
- **Confirm requests for payment or sensitive information with the person or company who has supposedly sent them, using contact information that you know to be correct**
- **Remember that scam emails and texts can look genuine and can appear to come from Government agencies, people within your organisation and trusted companies**
- **Report scam business emails to the National Cyber Security Centre**

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.**