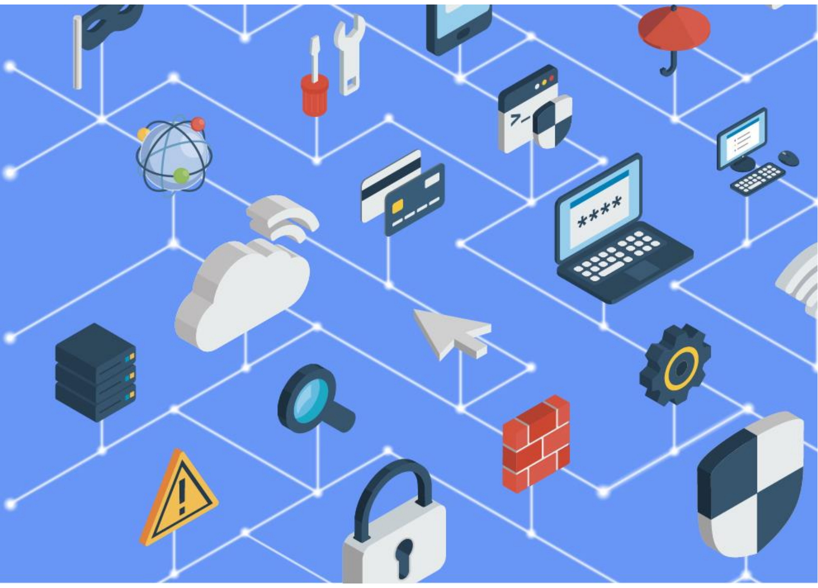
# Cyber Scotland Bulletin



The CyberScotland Bulletin is set up to provide you with information about the latest threats, scams, news and updates covering cyber security and cyber resilience topics. Due to current circumstances we are continuing to circulate a much wider range of scams. We hope you continue to benefit from this resource and we ask that you circulate this information to your networks, adapting where you see fit. Please ensure you take advice and information from **trusted sources**. **Please note, we will no longer be circulating this bulletin with a PDF attachment. This information will be online only and can be viewed at bulletin.cyberscotland.com**

**If there are any cyber terms you do not understand, you can look them up in the NCSC Glossary.**

## National Cyber Security Centre (NCSC)

### The Vulnerability Disclosure Toolkit

Security vulnerabilities are discovered all the time and people want to be able to report them directly to the organisation responsible. These reports can provide you with valuable information that you can use to improve the security of your systems. It really is in your best interest to encourage vulnerability disclosure. The NCSC have created a Vulnerability Disclosure Toolkit which contains the essential components you need to set up your own vulnerability disclosure process. Read more about it here.

### Remote Working

A study conducted by Trend Micro has highlighted that 39% of workers use their personal devices to access corporate data. Research shows that personal devices such as smartphones, tablets, and laptops are not configured to the same level of security when compared with corporate devices. The NCSC has guidance on how to safely use personal devices for work purposes. The recent pandemic has increased the need for remote working and highlighted the need to improve online security outside of the office. The NCSC has published guidance on working from home and detailed advice on how to connect smart devices securely.

**The Suspicious Email Reporting Tool** was launched by the NCSC to allow members of the public to report suspicious emails. As of 29th September, the reports received stand at more than **2,903,000** with the removal of 13,300 scams and 29,800 URLs. 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. View this week's report here.

## Trending Topics

### The Dark Web

The dark web is part of the internet that isn't visible to search engines and requires the use of an anonymizing browser called Tor, which masks a user's identity when accessing it. Through the dark web, private commuter networks can communicate and conduct business anonymously without divulging identifying information, like location. Many dark websites are set up by scammers, who constantly move around to avoid the wrath of their victims.

Law enforcement officials are getting better at finding and prosecuting owners of sites that sell illicit goods and services. An article featured on Europol stated that a coalition of law enforcements agencies across the world worked together to arrest 179 vendors, who engaged in tens of thousands of sales of illicit good across Europe and the United States. This co-ordinated approach resulted in over $6.5 million being seized in both cash and virtual currencies.

### Get Smart About PLAY

The UK Interactive Entertainment Association (UKIE) has launched the Get Smart About P.L.A.Y campaign, which includes easy guides for parents and carers to set controls on most of the popular gaming consoles. View their advice on askaboutgames.

The Get Smart About P.L.A.Y campaign provides parents and care-givers with a four-step process to help set parameters around play:

- **P - Play with your kids. Discover amazing games and understand what they play and why.**
- **L - Learn about family controls for your console.**
- **A - Ask what your kids think. Discuss ground rules before setting restrictions.**
- **Y - You're in charge. Set restrictions that work for your family.**

By protecting your online gaming accounts, you can be free to focus on enjoying the game. Your gaming account (or accounts) should be well protected with a strong password, ideally one which you don't re-use on other accounts. You should also turn on two factor authentication, if available, which will provide you with an extra layer of protection to prevent someone hacking into your account. Read NCSC's guidance on how to enjoy online gaming securely and how to manage passwords for your online services.

## Scammers exploit consumers

Fake protective equipment is among the products touted by con-artists, and National Trading Standards have warned further exploitation is on the way. It has listed the seven likely scams to watch out for in the coming weeks.

Consumer rights group Which? are warning consumers of scam adverts on Google that sit above genuine search results. Fraudsters are taking advantage of the 'pay-per click' (PPC) adverts, which allow advertisers to pay Google to appear first when we search for particular terms. This option is used legitimately by many law-abiding advertisers. But there is widespread concern that it's being routinely exploited by scammers and rogue operators across a range of financial services.

Be wary when clicking on 'paid for' advertising links. Unless you are 100% sure that the advertised website is providing the services or good you're looking for; then consider scrolling down the page to find more organic results to your search. As a consumer you really have no way of knowing who is behind the website you're being taken or to its legitimacy.

## Scammers targeting students

Students studying in a higher education institution have been scammed out of hundreds of pounds in their first week back at university. The students are all studying in a small, specialist department, with close and trusting relationships not only between students in particular years, but across years as well. One student's Facebook account was hacked and the criminal then messaged other students in the department, asking for urgent help to pay bills. The requests were very specific, and for amounts of hundreds of pounds. The victims thought their friend was in serious distress and four helped immediately, sending amounts of money totalling nearly £2000.

The university has warned all students about this scam and the police have been informed.

## Newsletters / Campaigns

### Get Safe Online Global24

The world's longest non-stop cyber event will be held on the **15th October,** as part of Get Safe Online (GSO) week which commences on the 12th October. GSO will be suggesting simple but effective ways, in which individuals and businesses can spread the word on online safety in their communities, and welcoming suggestions for activities from around the world. Find out how you can get involved on their website.

### Cyber Security Month

European Cyber Security Month (ECSM) is the EU's annual awareness campaign that takes place each **October** across Europe. The aim is to raise awareness of cyber security threats, promote cyber security among citizens and organisations; and to provide resources to protect themselves online, through education and sharing of good practices. Find out how you can get involved this month by visiting their website.

### CyberScotland Week

CyberScotland Week, Scotland's annual week-long festival of events on cyber awareness, cyber careers, and innovation in cyber security, is to return next year. Taking place from **22-28 February 2021**, the week will bring together influencers, experts, and the next generation of talent for the third consecutive year to increase awareness of staying safe and secure online.

### Trading Standards Scam Share

Other scams to be aware of are identified in last week's scam share. Check out this week's Trading Standards Scotland Scam Share newsletter. 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

### Police Scotland – Digital and Data Skills Academy

Police Scotland are delighted to present the offering of introductory digital skills courses to communities across Scotland. The industry standard courses available within the academy are provided for free through the Cisco Academy and contains training and qualifications in Networking, Cyber Security and Programming Languages. These courses provide a starting point for adults and children to understand concepts such as computer basics and cyber security. Further information and self-enrolment is available on their website.

### Scottish Business Resilience Centre (SBRC) – Protecting Scotland from a large scale cyber incident – Wednesday 7th October, 10am

As part of European Cyber Security month, SBRC are delighted to welcome Ciaran Martin, founding chief executive of National Cyber Security Centre, part of GCHQ, to lead their discussion. Ciaran is now Professor of Practice in the Management of Public Organisations at Blavatnik School of Government, University of Oxford. To find out more and register visit the SBRC website.

### Staff Training

Sharp UK released new findings identifying cyber security training as a cause for concern amongst UK businesses, as a third of SME owners admit to providing no training or resources for employees.

NCSC have an e-learning training package: 'Stay Safe Online: Top Tips for Staff'. It’s totally free, easy-to-use and takes less than 30 minutes to complete. The training introduces why cyber security is important and how attacks happen, and then covers four key areas:

- **defending yourself against phishing**
- **using strong passwords**
- **securing your devices**
- **reporting incidents ('if in doubt, call it out')**

The training is primarily aimed at SMEs, charities and the voluntary sector, but can be applied to any organisation, regardless of size or sector. It's been deliberately designed for a non-technical audience (who may have little or no knowledge of cyber security), with tips that complement any existing policies and procedures. More information is available here.

## Case Studies

Each issue, 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 – Vishing- NHS Scotland's Test and Protect

NHS Scotland's Test and Protect was rolled out across Scotland at the end of May and most recently a new app called Protect Scotland has been launched to support proximity contact tracing and help suppress the spread of COVID-19. Both are 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.**
- **Information on how to avoid Contact Tracing Scams**
- **More information on the Protect Scotland app can be found on our previous cyber bulletin.**

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.

## 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.**

# Technical Annex

## CVE-2020-1472 MS Windows Netlogon Elevation of Privilege Vulnerability

The vulnerability, dubbed “Zerologon”, enables an elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC). An attacker who successfully exploited the vulnerability could run a specially crafted application on a device on the network, and take over Windows Servers running as Domain Controllers.

This exploit has a  CVSS score of 10 as such Microsoft have urged users to patch CVE-2020-1472 immediately as a Phase 1 approach. Phase 2, planned for the first quarter of 20201, will be an enforcement phase.

It is our understanding that the patching mitigation to this vulnerability may be challenging for some organisations and exploitation may have very serious consequences.

- **More information can be found on Microsoft's website: https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/2020-aug**

- **Specific information regarding CVE-2020-1472 is available on the MSRC website: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472**

- **After installing the August 2020 security updates, Domain Controller (DC) enforcement mode can be deployed. For more information, see: https://support.microsoft.com/en-gb/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc**

## Vulnerabilities Affecting MobileIron Products (CVE-2020-15505)

The NCSC is aware of multiple vulnerabilities affecting MobileIron products. Specifically, a remote code execution vulnerability (CVE-2020-15505) affects MobileIron Core & Connector versions 10.3.0.3 and earlier, 10.4.0.0, 10.4.0.1, 10.4.0.2, 10.4.0.3, 10.5.1.0, 10.5.2.0 and 10.6.0.0; Sentry versions 9.7.2 and earlier, and 9.8.0; and Monitor and Reporting Database (RDB) version 2.0.0.1 and earlier.

The NCSC recommends following vendor best practice advice in the mitigation of vulnerabilities. In this case, the most important aspect is to install the latest version as soon as practicable.

More information is available at:

- https://www.mobileiron.com/en/blog/mobileiron-security-updates-available

A Proof of Concept and other analysis for this vulnerability have also been released:

- https://blog.orange.tw/2020/09/how-i-hacked-facebook-again-mobileiron-mdm-rce.html
- https://github.com/iamnoooob/CVE-Reverse/tree/master/CVE-2020-15505
- https://attackerkb.com/topics/nPl8YRkKRb/cve-2020-15506