Cyber Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

July - August 2024

INTRODUCTION

For the period 1st July - 31st August

Welcome to the latest edition of the Cyber Threat Update brought to you by the Cyber Security Centre for the Isle of Man (CSC), a part of OCSIA. This document provides an overview of cyber threats using data collected from our reporting points as well as intelligence obtained from partner agencies and open-source services.

We can only offer advice and guidance based on the information we have. Therefore, if you have any information that you believe should be considered for this document, please reach out to us at cyber@gov.im or submit it via our online cyber concerns form.

CONTENTS

SUSPICIOUS EMAIL REPORTING SERVICE (SERS)

As part of the Isle of Man Government's Cyber Security Strategy, the Cyber Security Centre for the Isle of Man (CSC) operates a Suspicious Email Reporting Service (SERS), allowing residents to forward suspicious emails for analysis.

If you have received an email which you're not quite sure about, forward it to SERS@ocsia.im. The message might be from a company that you don't normally receive communications from or from someone that you do not know. You may just have a hunch. If you are suspicious about an email, you should report it.

Your report of a phishing email will help us to act quickly, protecting many more people from being affected. In a small number of cases, an email may not reach our service due to it already being widely recognised by spam detection services.

By sending your suspicious emails to us we can better understand the threats on our Island and provide relevant advice and warnings. Your email will also be analysed by the UK's National Cyber Security Centre (NCSC), assisting in the disruption of malicious phishing campaigns and take down of websites.

The National Cyber Security Centre (NCSC) has the power to investigate and remove scam email addresses and websites. By reporting phishing attempts you can:

- reduce the amount of scam emails you receive
- make yourself a harder target for scammers
- protect others from cyber crime online

Since the launch of SERS, we have received over 22,032 suspicious emails. In July and August 2024, we received 1995 suspicious emails.

SUSPICIOUS EMAILS

1995 REPORTED

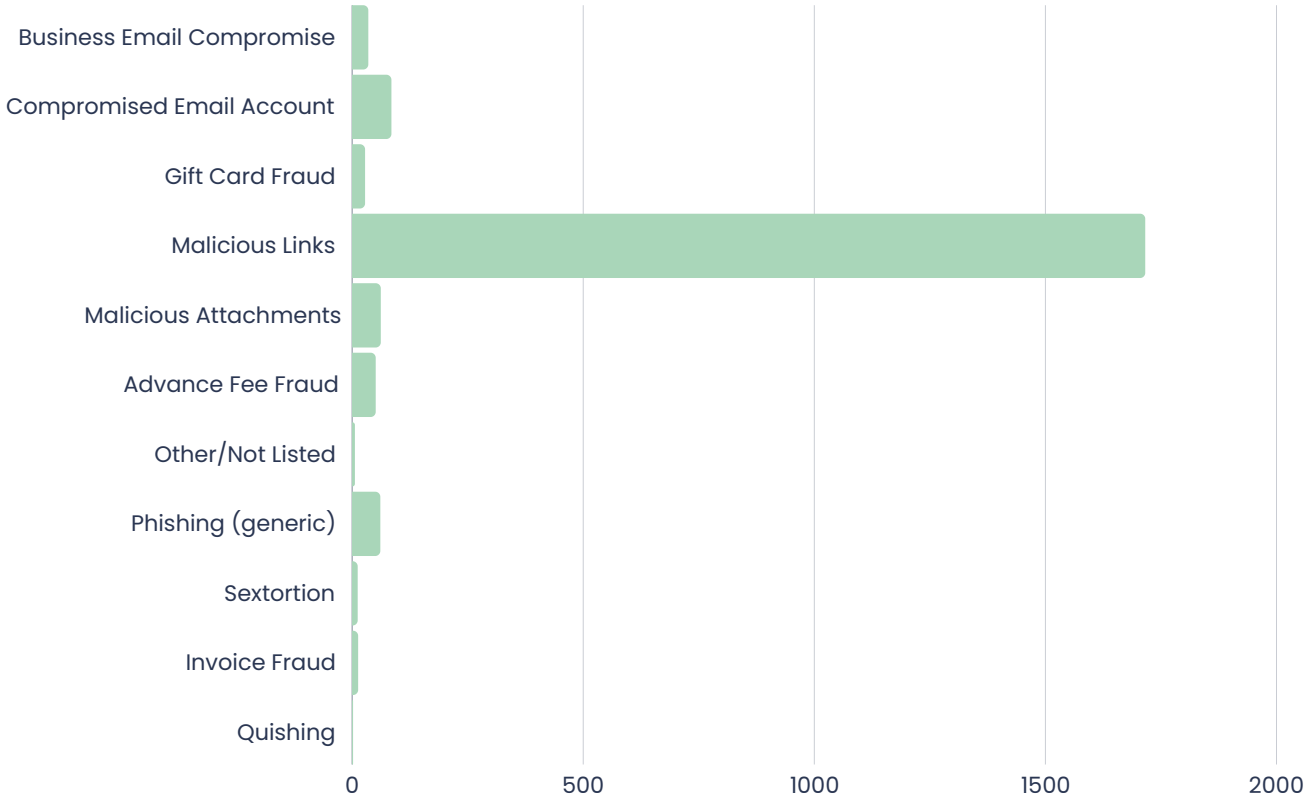
in July and August

Detail

The graph below shows the frequency of specific characteristics identified in submitted SERS emails. Please note that some emails have more than one recorded characteristic

Top 5 Phishing Scams Imitating Popular Services:

1. Manx.net
2. Parcel Delivery
3. Wise (money services business)
4. Anti-malware software
5. Apple



CYBER CONCERNS

101 REPORTED

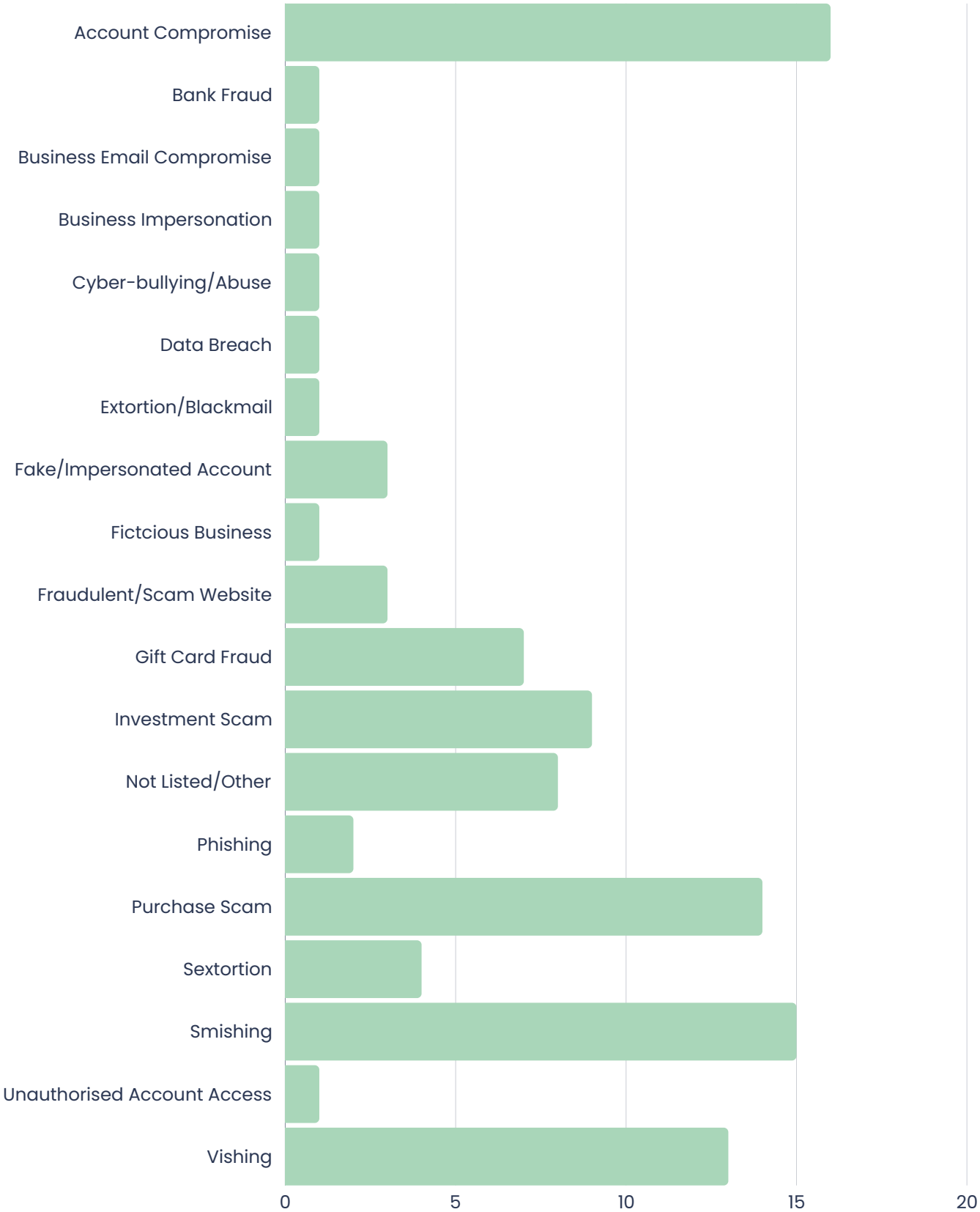
in July and August

Detail

The chart (on page 4) shows a breakdown of cyber concerns reported to us over July and August.

As mentioned previously, we can only provide the right advice and guidance to the public and local businesses from the information that is shared and reported to us. It is, therefore, important that we receive reports from the public and from organisations. If anyone has any information that they wish to put forward for consideration that could contribute to this document, please contact us at cyber@gov.im or report it using our online cyber concerns form.

Cyber Concerns July and August



ISLE OF MAN THREAT COMMENTARY

BUSINESS EMAIL COMPROMISE

EMPLOYEE BUYS GIFT CARDS FOLLOWING FAKE REQUEST FROM COLLEAGUE

A report that we received in July demonstrates the threat that can arise from correspondence that impersonates other colleagues.

An email was sent to several members of staff in a Douglas business that appeared to be from a senior executive: the email address was different, but the name matched. The first email, from an unrecognised email account, was very brief and asked for some assistance with a confidential task but also provided a new telephone number to be used for WhatsApp correspondence. Upon replying by WhatsApp chat, a member of staff was told to purchase gift cards as a present for other colleagues. Owing to the confidentiality and assurance of being reimbursed, the employee used their own personal bank account card, rather than any company payment card, to purchase multiple gift cards. The photographs of the cards were then provided to the scammer who redeemed the gift to collect the money.

BEC emails are a threat to businesses and workers, as it is easy to send a targeted email to multiple staff using email addresses freely available on company websites and provided by employees on LinkedIn. Because BEC often exploits the authority of senior staff, it can lead to someone (especially newer staff) dismissing concerns about the nature of a scammer's requests, e.g. the use of WhatsApp and the use of personal finances for business purchases. Raising awareness of BEC emails and what constitutes appropriate and inappropriate communication in the workplace can help in their quick identification

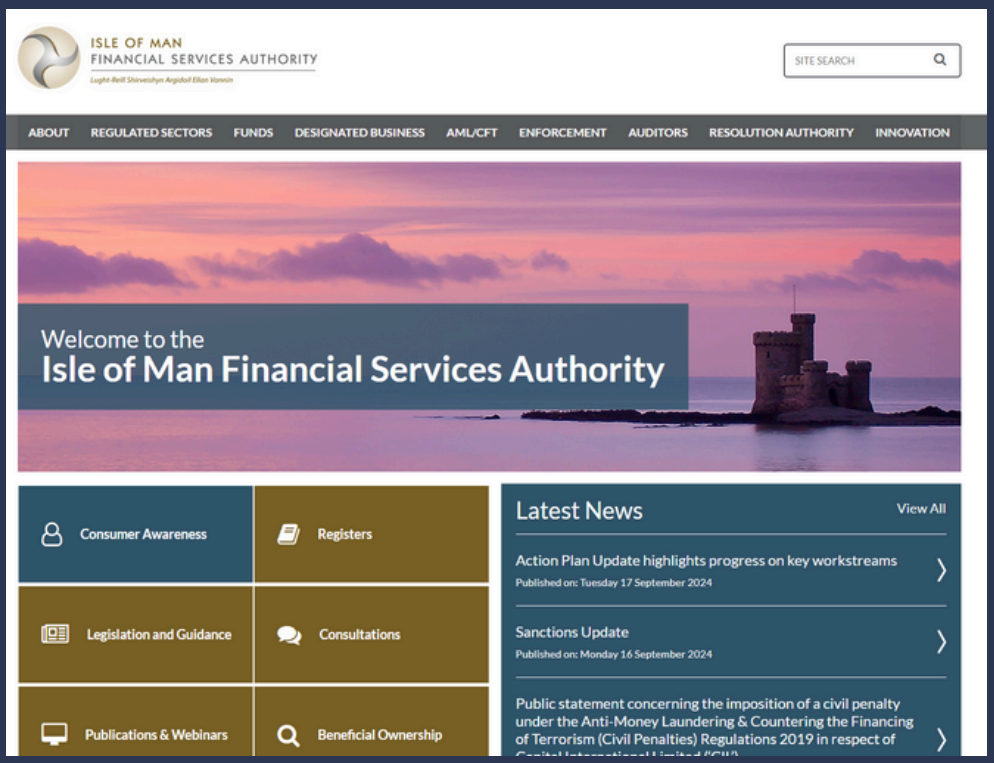
DOMAIN SQUATTING

FAKE ISLE OF MAN FINANCIAL SERVICES AUTHORITY WEBSITE

In August, the Cyber Security Centre (CSC) was made aware of a website that had been imitating the website of the Isle of Man Financial Services Authority (IOM FSA). The IOM FSA had published a warning notice about a bogus invoice requesting payment of a 'notarization of agreement' and which was apparently sent by 'Joan C Hudson'. The invoice provided a telephone number, email address and also a fake website that had been very recently created.

This website was created to add legitimacy to the invoice and was a direct copy of the legitimate site, potentially misleading recipients and adding a sense of legitimacy to the scam.

Having been notified of the fake website, the CSC made a report to the website host and worked with the UK's National Cyber Security Centre to close down the website. If you come across a fake website, government or otherwise please report it to the Cyber Security Centre using our online reporting form.



The offending website was a near-identical copy of the legitimate website.

ACCOUNT COMPROMISE

DISABILITY AWARENESS

In August, the Cyber Security Centre was contacted by the National Crime Agency (NCA) regarding a company, Disability Awareness, as the company's data was advertised sale on a crime-forum called Breach Forums. The Police asked whether the CSC could make contact with the company.

Disability Awareness was made aware that there had likely been an attack and subsequent breach. Disability Awareness were contacted by the CSC and provided with a number of recommendations. It was discovered that the website itself had been compromised owing to a vulnerability and attacks had been focused on the 'Register' account on the website through which there had been 232,000 new account sign-ups. The security of the website was subsequently reviewed and improved.

The Owner of the company has provided the following testimony regarding his experiences: *The cyber-attack was initially very disconcerting. As a business that requires authenticity, to have the store section of my website compromised was a particular concern in regard to my reputation. My main concern however was that the people who had nefarious accounts set up would be vulnerable to further cyber-attacks themselves. With the quick response and help from my website designer we were able to pinpoint the vulnerable area of my website and rectify the situation.*

Both my website designer and I have learnt from this experience, particularly in terms of making sure that you have all the protective tools and measures in place to prevent attacks such as these happening. If I could offer any advice to others, it would be to review your website security at your earliest convenience. One small omission in our store set up caused a very difficult issue which it took a lot of effort to resolve. And a lot of anxiety that stemmed from having to deal with it. Check your websites and make sure they're secure!

I am extremely grateful to the help given from the Isle of Man Office of Cyber Security. Their support and advice throughout the process was really invaluable in helping to rectify the issue quickly, and I am very grateful. Thank you

SMISHING

WHATSAPP FAMILY MEMBER MONEY REQUESTS

In July, a member of the public received a text from his son briefly mentioning that he had changed his telephone number and, the following day, his son sent another message asking whether his father had saved the number. The third message, however, asked for money to cover the payment of an urgent bill that could not be paid yet owing to the change of details (i.e. the telephone number). Despite trying to telephone his son to clarify this request, the phone was not answered so a transfer of money was made to the bank details provided in the texts. Shortly after, it was discovered that these text messages were from a scammer.

To keep safe, unexpected text messages from unrecognised numbers should always be treated with caution and even ignored if they are vague or strange. Scammers often trying to create feelings of worry by pretending the message is from a family member and is urgent. Scammers also try to be vague to provoke a response. If a message seems to be important and the Sender is known to you, it is wiser to make a telephone call using their normal telephone number to ask whether they had sent the message.

Please read our guidance on 'Scam texts and WhatsApp messages: How to Stay Safe' for further advice and tips about dealing with unexpected text messages.

FAKE/IMPERSONATED ACCOUNT OR PROFILE

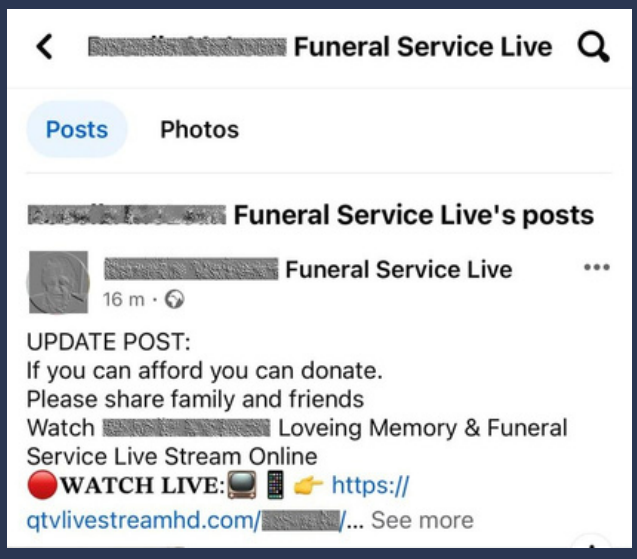
FACEBOOK FUNERAL LIVESTREAM

The Cyber Security Centre received a report about a fake Facebook page that was exploiting the recent death of a local resident to steal money. The page offered a URL to allow people to live-stream the funeral which leads to a phishing page designed to steal login credentials, in other instances this page also encourages a sign up to 'subsciption' which charges victims for a bogus service. In other cases we've seen another (identical) link was offered for donations.

The cybercriminals are good at making these Facebook posts look real. They often copy and paste real photographs of the deceased person taken from a funeral director's site or a genuine tribute site. But they are fake and could turn out very costly for those that fall for them.

The page was reported to the Isle of Man Police and the Cyber Security Centre reported the scam URL to the website host, NameCheap, which quickly closed it down.

This scam amply demonstrates how low scammers will stoop to trick people in giving them money. With this scam repeated internationally. Furthermore, it also serves to show how easy it is for scams to appear on Facebook and how the social media content cannot be assumed to be true. If a page or post appears to be a scam, it is best to report it to Facebook first and, if relevant, the admin of the page or group.



An example of the scam Facebook post

EXTERNAL THREAT COMMENTARY

TICKETMASTER FACES ESCALATING CYBERATTACK AS HACKERS LEAK THOUSANDS OF EVENT TICKETS

A cyber extortion campaign against Ticketmaster has escalated, with hackers leaking nearly 39,000 print-at-home tickets for upcoming concerts. The threat actors, known as 'Sp1derHunters,' stole data from Ticketmaster's Snowflake accounts and have been selling it on hacking forums. The attack began in April when stolen credentials allowed cybercriminals to access the Snowflake databases of at least 165 organisations. In May, the hacking group ShinyHunters claimed to have stolen the personal data of 560 million Ticketmaster customers, demanding $500,000 to prevent its release.

Despite Ticketmaster's assurances that its SafeTix technology prevents ticket fraud by frequently refreshing barcodes, the hackers have retaliated by leaking barcodes from non-refreshable print-at-home tickets. The breach affects tickets for major events featuring artists such as Pearl Jam, Foo Fighters, and Bruce Springsteen. A recent leak also revealed 166,000 Taylor Swift tickets, with the hackers raising their extortion demand to $2 million.

In response, Ticketmaster has stated that stolen data is largely unusable due to its security measures, but the hackers claim that non-digital tickets, such as those printed at home, remain vulnerable. The situation has intensified as ShinyHunters has begun selling massive datasets, including customers' personal and payment information, for a one-time fee of $500,000.

ShinyHunters is notorious for large-scale data breaches, including those affecting companies like Microsoft and AT&T. With multiple hackers now offering the stolen data, the breach highlights the growing threats to data security and the need for stronger protection against cyberattacks, as hackers continue to target high-profile companies like Ticketmaster and Live Nation.

CROATIA'S LARGEST HOSPITAL HIT BY RANSOMWARE ATTACK, LOCKBIT 3.0 CLAIMS RESPONSIBILITY

Croatia's largest hospital, the University Hospital Centre Zagreb (KBC Zagreb), was severely impacted by a ransomware attack on 27 June 2024. The LockBit 3.0 ransomware group claimed responsibility, forcing the hospital to shut down its IT systems to prevent further damage. The attack disrupted digital operations, pushing the hospital back '50 years – to paper and pencil,' according to Milivoj Novak, assistant director of healthcare quality and supervision.

More than 100 specialists worked to restore the hospital's systems, which were offline for 24 hours. During this period, medical reports had to be handwritten, and emergency patients were diverted to other hospitals in Zagreb. LockBit claims to have stolen sensitive data, including medical records, patient exams, surgery data, and employee information, though this has not yet been confirmed by the hospital. Health Minister Vili Beros emphasised that the government would not negotiate with the hackers. Authorities have launched a criminal investigation to determine the extent of the data breach.

This attack is part of a broader surge in cyberattacks on Croatian institutions, which began after Russia's invasion of Ukraine in 2022. Before the hospital attack, several government websites were targeted by distributed denial-of-service (DDoS) attacks, claimed by Russia-linked hacker group NoName057(16). However, NoName denied any involvement in the hospital incident, stating that they do not target medical facilities.

UK GOVT LINKS 2021 ELECTORAL COMMISSION BREACH TO EXCHANGE SERVER

The United Kingdom's Electoral Commission was reprimanded after a major data breach in August 2021, which exposed the personal information of 40 million voters. The breach occurred because the Commission failed to update its Microsoft Exchange Server with essential security patches, leaving it vulnerable to ProxyShell attacks. These vulnerabilities, identified as CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207, were exploited by Chinese state-backed hackers, according to the UK's National Cyber Security Centre (NCSC). The attackers gained access to the Commission's systems by installing web shells and backdoors, allowing them to persist in the network undetected.

The Information Commissioner's Office (ICO) criticised the Electoral Commission for failing to implement basic security measures like password management and timely updates. ICO Deputy Commissioner Stephen Bonner emphasised that the breach could have been prevented with proper security practices. Despite this, there is no evidence that the compromised data has been misused or caused direct harm to voters.

The breach was part of a broader wave of cyberattacks attributed to China, which also targeted organisations in the U.S. and other countries. Beijing has denied these accusations. Since the attack, the Electoral Commission has taken steps to improve its security, including modernising infrastructure, introducing multi-factor authentication, and enforcing stricter password policies. The incident has renewed calls for stronger cybersecurity measures across the UK. This reprimand serves to offer two critical lessons for organisations regarding the consequences of improper cybersecurity practices, such as poor password management policies and poor patch management.

MASSIVE PHISHING CAMPAIGN EXPLOITS MICROSOFT SWAY: BUSINESSES URGED TO STRENGTHEN MOBILE DEVICE SECURITY

In July 2024, cybersecurity researchers at Netskope Threat Labs uncovered a massive phishing campaign exploiting Microsoft Sway, a cloud-based presentation tool, to deceive Microsoft 365 users. This sophisticated attack, primarily targeting victims in Asia and North America, led to a 2,000-fold increase in malicious activity compared to the year's first half, marking a significant surge in attacks aimed at stealing Microsoft 365 credentials.

The phishing campaign, often referred to as 'quishing', involves sending QR codes that redirect users to fake login pages designed to harvest sensitive information. These phishing pages are hosted on Microsoft's Sway platform, making them appear more legitimate. By tricking users into scanning QR codes with their mobile devices, attackers exploit weaker security measures typically found on personal devices compared to corporate-issued ones. This technique increases the likelihood of bypassing security controls, providing unrestricted access to phishing sites.

Netskope's researchers noted that the attackers employed several advanced tactics to increase the effectiveness of their campaign. These included the use of 'transparent phishing', where the malicious pages closely mimicked legitimate Microsoft login pages, and the deployment of Cloudflare Turnstile, which helped the attackers evade detection by security scanners. Victims would enter their credentials, which were then sent to compromised websites, while they were seamlessly redirected to legitimate domains to avoid suspicion.

This isn't the first time Microsoft Sway has been abused in phishing attacks. A similar campaign five years ago, known as PerSwaysion, targeted high-ranking executives across various industries.

To counter phishing campaigns targeting Microsoft Sway and employing QR codes, businesses should enforce strong Mobile Device Management policies and mobile-specific security measures, such as anti-phishing tools and secure browsing apps, and educate employees on better recognition phishing attempts.

QNAP ADDS NAS RANSOMWARE PROTECTION TO LATEST QTS VERSION

Taiwanese hardware vendor QNAP has launched its QTS 5.2 operating system for network-attached storage (NAS) devices, introducing a Security Centre to bolster ransomware protection. This update, released on 21st August 2024, aims to address the rising threat of ransomware, which increasingly targets NAS devices due to their valuable stored data and frequent misconfigurations.

As reported by the website CUJOAI in their 2023 cybersecurity report, NAS devices attract a disproportionate number of attacks compared to other consumer devices. Despite accounting for just 0.02% of devices globally, NAS systems are the focus of over 10% of all cybersecurity threats. An average NAS device is attacked hundreds of times more often than a typical computer or smartphone, making the new protections in QTS 5.2 particularly relevant.

One reason NAS devices are so vulnerable is their configuration, often requiring open ports (such as 8080 and 443) for remote access. These open ports make NAS devices easy targets for attackers. Additionally, users often delay firmware upgrades, leaving security vulnerabilities unpatched for extended periods. QNAP's NAS devices have been a common target, with significant security issues reported as recently as February 2023.

The new Security Centre in QTS 5.2 actively monitors file activity to detect and block ransomware threats. If suspicious behaviour is identified, protective measures are automatically triggered, including setting volumes to read-only mode or creating snapshots for data restoration. These features are designed to mitigate risks and prevent data loss.

QTS 5.2 also improves security by supporting TCG-Ruby self-encrypting drives (SED), accelerating NAS performance, and enhancing backup processes. For the latest security patches and advisories, QNAP users are encouraged to visit the company's security advisory page.

CYBER GLOSSARY

Anti-virus software: Designed to identify and remove computer viruses, other malware and spyware on a device or IT system. To be effective, it should be kept up-to-date with the latest anti-virus signatures and definitions.

Backdoor: A backdoor is a method of avoiding normal authentication on a device. They are often used for securing remote access to a computer, or obtaining access to plaintext in cryptographic systems

Common Vulnerabilities and Exposures (CVE): The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures.

Cryptocurrency: A cryptocurrency is a digital asset that is designed to act as an exchange medium. They use cryptography to verify and secure transactions, control the creation of new assets and protect the identity of asset holders.

Dark web: A collection of thousands of websites which are not indexed by conventional search engines. They often use anonymity tools, like the Tor network, to hide their IP address and preserve the anonymity of the creators and visitors.

Encryption: A method to scramble a message, file or other data and turn it into a secret code using an algorithm (complex mathematical formula). The code can only be read using a key or other piece of information (such as a password) which can decrypt the code.

Firewall: A security system that monitors and controls traffic between an internal network (trusted to be secure) and an external network (not trusted). It is generally considered insufficient against modern cyber threats.

General Data Protection Regulation - GDPR: The General Data Protection Regulation (GDPR) 2016/679 is a European Union regulation covering data protection and individual privacy rights. It was introduced in April 2018 and enforced on May 25 2018.

Hacker: A hacker is a computer and networking attacker who systematically attempts to penetrate a computer system or network using tools and attack methods to find and exploit security vulnerabilities.

IP address: An IP address (Internet Protocol Address) is a label assigned to computer devices. An IP address is essential for Internet Protocol communication.

Keylogging: Keylogging, also known as keystroke logging or keyboard capture, is the action of recording, often secretly, the keys struck on a keyboard.

Malware: Malware is malicious or hostile software used to disrupt, damage or compromise a computer system or network

Patch management: Patch management covers acquiring, testing and installing multiple patches (manufacturer released code changes) to a computer system or application. Firmware and software vendors release patches to fix defects, change functionality and to address known security vulnerabilities.

Phishing: Phishing is a type of fraud in which the attacker attempts to steal sensitive data such as passwords or credit card numbers, via social engineering.

Ransomware: A type of malware that prevents access to the target's computer system or data until a ransom is paid to the attacker.

Smishing: A type of phishing attack that uses text messages (or other types instead of mobile messaging such as MMS or IM services) instead of email messages.

Social engineering: An attack method that tricks people into breaking normal security procedures by masquerading as a reputable entity or person in email, IM or other communication channels.

Vulnerability: A vulnerability is a weakness that allows an attacker to compromise security (integrity, confidentiality or availability).

CLICK HERE OR SCAN TO VIEW OUR FULL CYBER GLOSSARY

CYBERISLE 2024

Residents are encouraged to take up an “invaluable opportunity” and attend the Isle of Man’s premier cybersecurity conference at the Comis Hotel in Santon next month. CYBERISLE 2024 will give people the chance to listen to industry experts from across the British Isles about critical cyber threats and how to stay safe on 10 October.

Key speakers from global leaders like Microsoft, Sophos, and Mimecast, will all take the stage to share their cutting-edge insights on the ever-evolving threats.

Throughout the conference, attendees will delve into pressing topics such as supply chain security, and the vital role every individual plays as part of the "human firewall," with real-world case studies, insider knowledge, and practical advice on tap.

Minister for Justice and Home Affairs, Jane Poole-Wilson MHK, said: “CYBERISLE will equip people with the tools and knowledge to safeguard themselves and their organisations.

“I encourage people to get a free ticket and take up the opportunity to learn from the assembled guest speakers from our neighbours in the British Isles. What people take away will be invaluable in helping to keep our island safe from rising threats.

“Don't miss this opportunity.”

Key sessions include:

- Emerging Cyber Threats: Highlighting the latest trends in cybercrime.
- Supply Chain Security: Critical insights on mitigating third-party risks
- The Human Firewall: Emphasising the role of employees in cyber defence
- Incident Response: Teaching effective strategies for responding to attacks.

CYBERISLE will take place on Thursday 10 October and free tickets can are available here.

ABOUT US

The Cyber Security Centre for the Isle of Man (CSC) was launched as a branch of the Office of Cyber Security and Information Assurance (OCSIA) in October 2023, to increase our presence in the public sphere. The CSC is responsible for providing targeted advice and guidance to individuals and businesses, while OCSIA remains for Information Assurance within Government.

Our objective is to improve cyber resilience of everyone who lives or operates in the Isle of Man. Our commitment to supporting individuals, businesses and the private sector is at the heart of what we do, and we are devoted to maintaining partnerships with everyone who needs us, while raising awareness about the rapidly changing cybersecurity threat landscape.

Established in 2019, our annual one-day cybersecurity conference CYBERISLE takes place in autumn, and acts as a focal point event in the field on Island. We bring together leading experts, students, charities and individuals, to share ideas and allow everyone to gain a deeper understanding of current cyber threats to our Island, and the best mitigation tactics available for increasing nationwide cyber resilience.

Disclaimer

The material in this document is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances. OCSIA accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Open Government Licence

Cyber Security Centre for the Isle of Man

a part of the Office of Cyber-Security & Information Assurance

csc.gov.im
cyber@gov.im
01624 685557

Office of Cyber-Security & Information Assurance
2nd Floor
Former Lower Douglas Police Station
Fort Street
Douglas
Isle of Man
IM1 2SR

T: +44 1624 685557

Isle of Man Government
Reiltys Ellan Vannin