Cyber Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

November - December 2024

INTRODUCTION

For the period 1st November - 31st December

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 suspicious 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 26,400 suspicious emails. In November and December 2024, we received 2,721 suspicious emails.

SUSPICIOUS EMAILS

2721 REPORTED

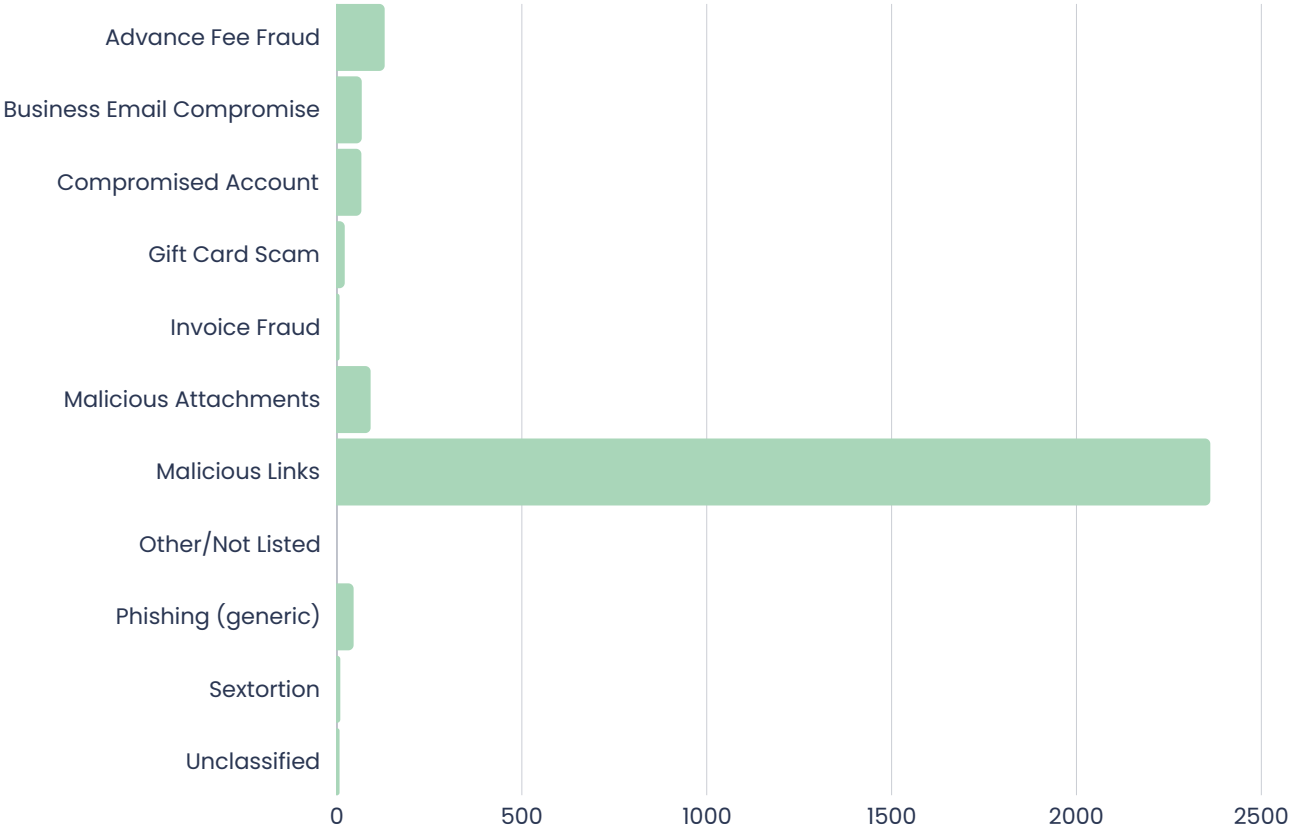
in November and December

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. Romance and dating
3. Microsoft
4. Parcel Delivery
5. Wise



CYBER CONCERNS

68 REPORTED

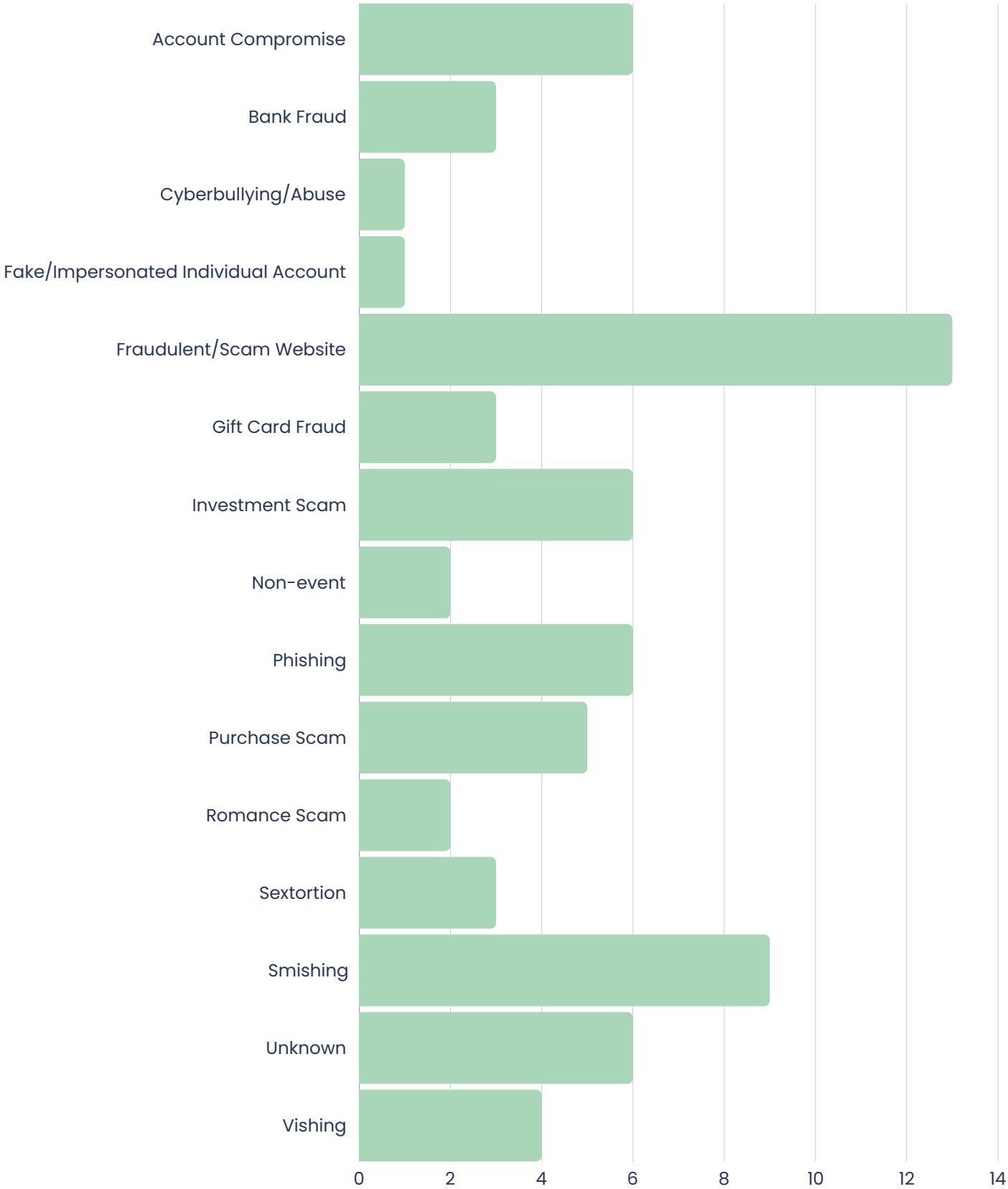
in November and December

Detail

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

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 November and December

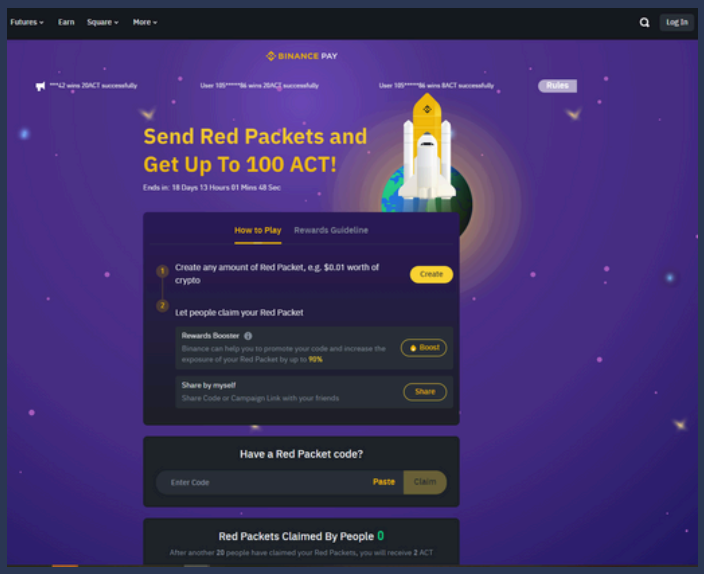


ISLE OF MAN THREAT COMMENTARY

FRAUDULENT/SCAM WEBSITE

FAKE BINANCE WEBSITE

Binance, established in 2017, is a global cryptocurrency trading website, serving millions of users. Its prominence makes it a common target for cybercriminals. The Cyber Security Centre received a report from Doppel SOC Team about a phishing site using the .im domain, which was mimicking Binance's official website (http://binance.com) to steal sensitive information and payments.



Liaising with Doppel who are authorised to act on Binance's behalf, we confirmed the report's accuracy. The Cyber Security Centre submitted a takedown request to the domain registrar, detailing the phishing activity, risks to users, and Doppel's authority. The registrar verified the claims and quickly suspended the domain, stopping the malicious activity. Effective communication and detailed documentation expedited this process.

Whilst the website has now moved domains, it is important that the Island's domain space is seen to be a well managed and legitimate environment. By working withcybersecurity teams, registrars, and organisations like Binance we can ensure that scams are not facilitated from the Isle of Man.

ISLE OF MAN TRANSPORT - FAKE GO CARDS

We were made aware of a Facebook page named 'Public Transport Isle of Man' alongside numerous other variations. The page, featuring stock images of Isle of Man buses as well as official logos, ran Facebook adverts offering 6 months free travel for £2.

These adverts contained a link to an external site which then asked a series of generic questions. Irrespective of the answers given you would then be directed to click on a number of gift boxes. A visitor would then be directed to click the gift boxes of which the second would grant the user the 'prize' of cheap travel. After that a new page would open to enter personal and card details and an initial payment of €2 (euros) was taken from the card.

Following on from this, victims reported other attempted charges to the card, as well as multiple emails encouraging users to sign up for services. We received several reports from victims of the scam, all of which were encouraged to contact their banks and have cards cancelled or frozen.

Despite the clear misuse of official branding and fraudulent activity, it has proven near impossible to have these scam adverts removed swiftly. Facebook's lack of robust safeguards and the often cumbersome reporting processes leave victims vulnerable and allow scams to continue.

There were several signs that should have been a 'red-flag' for potential victims. First, the page itself had very few followers and was set up recently. Secondly, a promotion such as this would have been covered in a legitimate news outlet, thirdly taking payment in euros. These factors, alongside the unlikely nature of the promotion signalled this was a scam.

Fundamentally individuals must understand that not all content on social media can be trusted, even when it appears legitimate. Users should not rush into any decisions and carefully consider any offers they are tempted by.

VISHING

IOM BANK IMPERSONATION

An individual encountered problems with their bank card issued by Isle of Man bank and visited the bank's branch in Ramsey to resolve the issue. While there, they were informed that the bank's fraud team would contact them. Approximately one month later, the victim received a phone call on their landline from a man claiming to represent the IOM Bank Fraud Team. The caller alleged that fraudulent activity had been detected on the victim's accounts in Manchester and Douglas and further suggested that staff at the bank's Douglas branch might be involved.

The fraudster convinced the victim to assist with the supposed investigation by purchasing £20,000 worth of gold and sending it to a specified address in London. Trusting the caller, the victim purchased the gold from a local dealer in Douglas and mailed it in a shoebox via recorded delivery to the address provided.

Over time, the fraudsters maintained regular contact with the victim, claiming the investigation was ongoing and requesting additional assistance. They persuaded the victim to purchase another £150,000 worth of gold. Following the same process, the victim ordered the gold from the same dealer, paid via bank transfer, collected it, and sent it to the same address in London.

The fraud came to light when the victim travelled to the UK to visit family. Upon learning of the significant financial transactions and gold shipments, the victim's family immediately contacted authorities to report the situation.

Scammers often strike when people are caught off guard, and happen to act at a time that 'makes sense' to a victim. This highlights the importance of education about common fraud schemes, the need for independent verification of claims, and the value of open communication about financial matters within families. Additionally, it serves as a reminder to report suspicious activity promptly to prevent further losses and aid in the investigation of such crimes.

PURCHASE SCAMS

FACEBOOK PURCHASE SCAMS

Online marketplaces like Facebook offer convenience and variety, but they also present opportunities for fraudsters to exploit unsuspecting buyers. Two recent experiences highlight the risks associated with these platforms and the tactics scammers commonly use.

In one case, a buyer attempted to purchase garden furniture advertised on Facebook Marketplace for £200. The seller requested a £30 delivery fee, which was sent via PayPal. When the payment was made using PayPal's 'goods and services' option, the seller claimed it hadn't been received because it wasn't sent as 'friends and family' which is an option that gives more protection to those sending money. Realising it was likely a scam, the buyer blocked the seller on Facebook Messenger and WhatsApp.

Days later, an unexplained deposit of £115 from a stranger named Joel Price appeared in the buyer's bank account. Concerned about both the scam and the mysterious deposit, they contacted their bank, which reversed the deposit, cancelled their card, and secured the account.

In another instance, a buyer ordered a neon sign from a seller advertising on Facebook. They made three payments totalling £34 via PayPal's "friends and family" option, only to discover the seller had no intention of delivering the item. Because "friends and family" payments lack buyer protection, the victim was unable to dispute the transactions despite retaining evidence of chats and payment records.

These cases underscore the importance of vigilance when buying through online marketplaces. To avoid falling victim to similar scams, always use payment methods with buyer protection, verify the seller's legitimacy, and report suspicious activity promptly. Additionally, saving all transaction records can help if disputes arise. By taking these precautions, buyers can navigate platforms like Facebook more safely.

INVESTMENT SCAMS

IMPERSONATION OF ISLAND FINANCIAL BUSINESS

In early 2024, an individual fell victim to a cryptocurrency scam, transferring approximately £200,000—their life savings—to a fraudulent platform promising high returns. After the transfer, the scammers ceased communication, leaving the victim financially devastated.

The situation escalated when the victim received a partial repayment of £8,262 from a client account linked to a legitimate financial services provider based in the Isle of Man. This repayment, likely orchestrated by the scammers to lend credibility to their scheme, led the victim to reinvest the funds, resulting in further losses.

While the Isle of Man-based firm was likely unaware of its involvement, its legitimate identity was exploited by the fraudsters to build trust with the victim. Despite investigations by law enforcement and the victim's bank, the scammers remained untraceable.

This case highlights how scammers misuse trusted business identities to enhance the credibility of their schemes, creating challenges for both victims and implicated firms. It underscores the importance of robust due diligence measures by businesses, transparency in responding to fraud-related inquiries, and collaboration between international authorities to combat financial crime.

Greater public awareness about these tactics and stronger safeguards can help mitigate the risks of such schemes and protect both individuals and businesses from similar exploitation in the future.

THE ONGOING MANX.NET SCAMS...

Over 60 accounts were recently compromised in a targeted phishing attack that exploited impersonation tactics using Manx Telecom and Manx.net branding. The cause of the compromises was where the victims received emails in the account's main inbox urging them to update their account details on the threat of having their email account closed. These emails all contained links that led to phishing pages designed to capture login credentials.

Once attackers gained access, they changed passwords to lock users out or remained undetected, redirecting emails to gather intelligence and sending fraudulent messages under the guise of the legitimate account holders.

These compromised accounts were primarily used for gift card scams. As the scammers had access to a person's email correspondence, they were able to send emails to a person's prior correspondents by looking an old email exchanges. As the emails were coming from a friend's or family member's email account, the emails looked genuine. The scammers then added urgent to the scam by claiming that they could not buy the cards owing to illness. The victim's of these scams were pressured to buy gift cards, which were purchased at locals shop or online, and then told to give the scammer the PINs or codes on the back of the cards, allowing the scammer to strip the funds off the cards.

In response to these compromises, we take immediate action by liaising with Manx Telecom to have the accounts suspended. Where friends and family members have reported gift card scam emails, we have encouraged them to contact the victim of the scam by a telephone call to warn them about their account having been compromised. The absence of multi-factor authentication (MFA) was identified as a key vulnerability that allowed the attackers to bypass security measures. To prevent future incidents, we have advised members of the public on the importance of having adequate security on the email accounts with the use of strong passwords and by enabling MFA

This incident highlights the ongoing threat of social engineering attacks and the importance of robust, multi-layered security measures. It underscores the need for continuous monitoring, user awareness, and proactive measures to address emerging cyber threats.

EXTERNAL THREAT COMMENTARY

ALDER HEY AND LIVERPOOL HOSPITALS TARGETED IN RANSOMWARE ATTACK

A cyber-attack has impacted Alder Hey Children's Hospital, Liverpool Heart and Chest Hospital, and Royal Liverpool University Hospital, with hackers claiming to have accessed sensitive data via a shared digital gateway. INC Ransom, a ransomware group linked to previous attacks on NHS organisations, has published samples of allegedly stolen data, including patient and donor details, financial records, and medical reports, spanning 2018 to 2024.

Alder Hey confirmed the breach but emphasised that its services remain fully operational. Investigations indicate no data published so far pertains to children or young people. The hospitals are collaborating with the National Crime Agency (NCA) and other partners to secure systems and assess the extent of the breach.

The attack follows another unrelated cyber-incident earlier in the week at Wirral University Teaching Hospital NHS Trust, highlighting the growing risk to NHS infrastructure. INC Ransom has previously targeted NHS Dumfries and Galloway, stealing data from 150,000 individuals.

The hospitals have initiated forensic investigations and are preparing to notify affected individuals if necessary. While the stolen data could be published before investigations conclude, authorities are focused on mitigating the impact and strengthening cyber-security measures.

HACKNEY COUNCIL CYBER-ATTACK FALLOUT COSTS SOAR, BBC REPORTS

According to a report by the BBC on 21 December, 2024, Hackney Council is facing substantial financial pressures as it continues to recover from a 2020 cyber-attack. The council's accounts indicate an additional £757,000 in costs this year, contributing to a total overspend of approximately £37 million for the accounting year.

The BBC reports that £344,000 has been allocated to agency staff to manage backlogs created by the attack, while £413,000 is being spent on cyber-security consultants. Councillor Robert Chapman reportedly described the borough's financial situation as 'serious,' citing the cyber-attack's ongoing impact alongside broader budgetary challenges.

The 2020 ransomware attack resulted in sensitive data about staff and residents being leaked on the dark web. The Information Commissioner's Office (ICO) rebuked the council earlier this year, with Deputy Commissioner Stephen Bonner labelling the breach a 'clear and avoidable error.' The ICO identified inadequate security measures, such as dormant accounts with default credentials, as contributing factors.

In response, Hackney Council told the BBC it disagreed with the ICO's findings, asserting compliance with its security obligations. The BBC also reported that the council is adopting a new housing system to address lingering technical issues from the hack.

The BBC noted that Hackney's financial recovery is further strained by a real-terms funding cut of nearly 40% since 2010, exacerbating the borough's challenges in dealing with the attack's fallout. This shows how the ongoing costs of recovery can really add up and makes it clear that taking a few simple steps early on—like having solid cybersecurity measures and regular training—can save a lot of money and hassle down the line.

UK: 16% RISE IN CYBER INCIDENTS IN 2024

The UK's National Cyber Security Centre (NCSC) has reported a significant rise in cyber incidents, marking a 16% increase in cases handled in 2024 compared to the previous year. Richard Horne, NCSC CEO, highlighted the growing frequency, sophistication, and intensity of hostile activities targeting the nation's cyberspace.

"Actors are increasingly using our technology dependence against us, seeking to cause maximum disruption and destruction," Horne stated.

The NCSC's incident management team responded to 430 incidents this year, up from 371 in 2023. Alarmingly, 347 of these cases involved data exfiltration, a covert and unauthorised transfer of sensitive information, while 20 incidents were ransomware-related. To address these threats, the agency issued 542 tailored notifications to affected organisations, offering mitigation guidance—more than double the 258 issued last year.

Ransomware remains the most immediate and disruptive threat to critical infrastructure, including energy, water, transportation, healthcare, and telecommunications sectors. The NCSC's annual review also underscored the emerging danger of hackers leveraging artificial intelligence to develop increasingly sophisticated attacks.

"We believe the severity of the risk facing the UK is being widely underestimated," warned Horne. "There is no room for complacency about the severity of state-led threats or the volume of the threat posed by cybercriminals."

As the UK strengthens its cyber defenses, the need for vigilance and proactive measures has never been more critical. The NCSC's findings underscore the importance of addressing these challenges head-on to safeguard the nation's digital future.

NOKIA CONFIRMS THIRD-PARTY DATA BREACH AMID HACKER CLAIMS

Nokia has confirmed a data breach involving a third-party vendor, following claims from a hacker who is selling stolen data for $20,000 on a dark web forum. The Finnish tech giant has stated that the breach does not involve its internal systems or sensitive customer information, asserting there is 'no evidence' of any impact on its operations.

The hacker, using the alias 'DataIntruder,' has reportedly offered a database containing nearly 30GB of information allegedly linked to Nokia. The seller claims this data includes customer records, internal documents, and operational details. However, Nokia has refuted these allegations, saying the information originates from an attack on an external partner, not its internal infrastructure.

The breach came to light in late October, with cyber-security experts expressing concerns over the potential misuse of the data. While Nokia maintains that the stolen data does not compromise its core operations, experts warn that such breaches highlight vulnerabilities in supply chain security.

Nokia stated it is actively monitoring the situation and collaborating with the affected vendor to address the issue. A spokesperson said: 'Nokia's own systems remain secure, and we are taking all necessary measures to mitigate risks related to this incident.'

The breach has reignited debates around the cyber-security challenges posed by third-party partnerships. Experts recommend robust oversight and security measures for vendors to prevent sensitive information from being exposed, particularly as hackers increasingly target supply chain weaknesses.

RUSSIAN HACKERS EXPLOIT NEARBY WI-FI NETWORKS IN 'NEAREST NEIGHBOUR' ATTACK

Researchers have uncovered a sophisticated cyber-espionage method dubbed the ‘Nearest Neighbour’ attack, deployed by the Russian hacking group Fancy Bear (also known as APT28). According to reports from cyber-security firm Volexity and multiple other sources, the group leveraged weak Wi-Fi security to infiltrate networks of organisations in Washington, D.C., while operating remotely from thousands of miles away.

The attack was first identified ahead of Russia’s invasion of Ukraine in 2022. Fancy Bear reportedly used compromised credentials to breach Wi-Fi networks near their intended target, ‘Organisation A.’ By daisy-chaining through other organisations in close physical proximity, they circumvented stronger security measures, including multi-factor authentication (MFA).

Researchers revealed that Fancy Bear employed password-spraying techniques and exploited Wi-Fi networks unprotected by MFA. The attackers gained access to Organisation A's systems by first infiltrating the networks of ‘Organisation B’ and ‘Organisation C.’ A dual-homed device within Organisation B, connected to both Ethernet and Wi-Fi, provided the bridge for the hackers to move laterally.

The campaign highlights the vulnerabilities of poorly secured Wi-Fi networks. ‘Proximity and valid credentials were the only requirements to connect,’ said Volexity. The hackers reportedly used standard Windows tools like Cipher.exe and netsh to avoid detection while exfiltrating data.

Experts recommend separating Wi-Fi from sensitive wired networks, implementing MFA for Wi-Fi access, and monitoring anomalous network activity. The incident underscores the evolving threats posed by resourceful cyber adversaries capable of exploiting everyday technologies for high-stakes espionage.

RUSSIA CAN TURN THE LIGHTS OFF: UK PREPARING FOR CYBERWAR

The UK faces an escalating cyber threat from state actors like Russia and China, with risks to national security being "widely underestimated," warns Pat McFadden, whose role includes responsibility for national security. This comes as the NCSC reports a significant rise in serious cyber incidents over the past year.

Experts caution that while the UK's energy grid is designed to withstand disruptions, Russia's advanced cyber capabilities could still cause significant damage. Former NCSC head Ciaran Martin stresses the need for organisations to prepare for infrastructure failures, noting that the speed of recovery can mean the difference between manageable disruptions and prolonged crises.

Russia's cyber aggression has intensified alongside its war in Ukraine, with intelligence revealing campaigns targeting critical infrastructure and government systems worldwide. These include ransomware attacks by criminal groups linked to the Russian state, which disrupt organisations and demand payments to restore stolen data.

Lessons from countries like Sweden and Norway highlight the importance of strong cybersecurity habits and individual preparedness. The UK government similarly advises steps to protect against emergencies, urging calm and resilience. Jamie MacColl of RUSI emphasises that panic only amplifies the impact of attacks, urging a collective focus on preparation and psychological resilience to counter these growing threats.

Pat McFadden (image BBC News)

CYBER GLOSSARY

2-step verification (2SV): Sometimes called 2FA or MFA is a second way to confirm your identity to help keep your personal and financial information from being compromised or stolen.

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).

ABOUT US

TThe Cyber Security Centre for the Isle of Man (CSC) is dedicated to enhancing the cyber resilience of organisations and individuals across the island. As a public-facing entity, the CSC provides comprehensive advice, guidance, and practical support to both residents and businesses.

The CSC is committed to bolstering cyber defences by offering tailored solutions, resources, and educational programmes. Its primary focus lies in empowering Island-based entities and individuals with the necessary knowledge and tools to effectively safeguard against cyber threats.

Through proactive initiatives, including targeted advisory notices, vulnerability scanning, and awareness campaigns, the CSC aims to elevate the overall cyber awareness and preparedness of the Isle of Man community. By fostering a culture of vigilance and best practices, the CSC aims to fortify the cyber resilience of organisations and individuals, ensuring a safer digital environment for all.

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