Cyber Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

September - October 2024

INTRODUCTION

For the period 1st September - 31st October

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 23,820 suspicious emails. In September and October 2024, we received 1,564 suspicious emails.

SUSPICIOUS EMAILS

1564 REPORTED

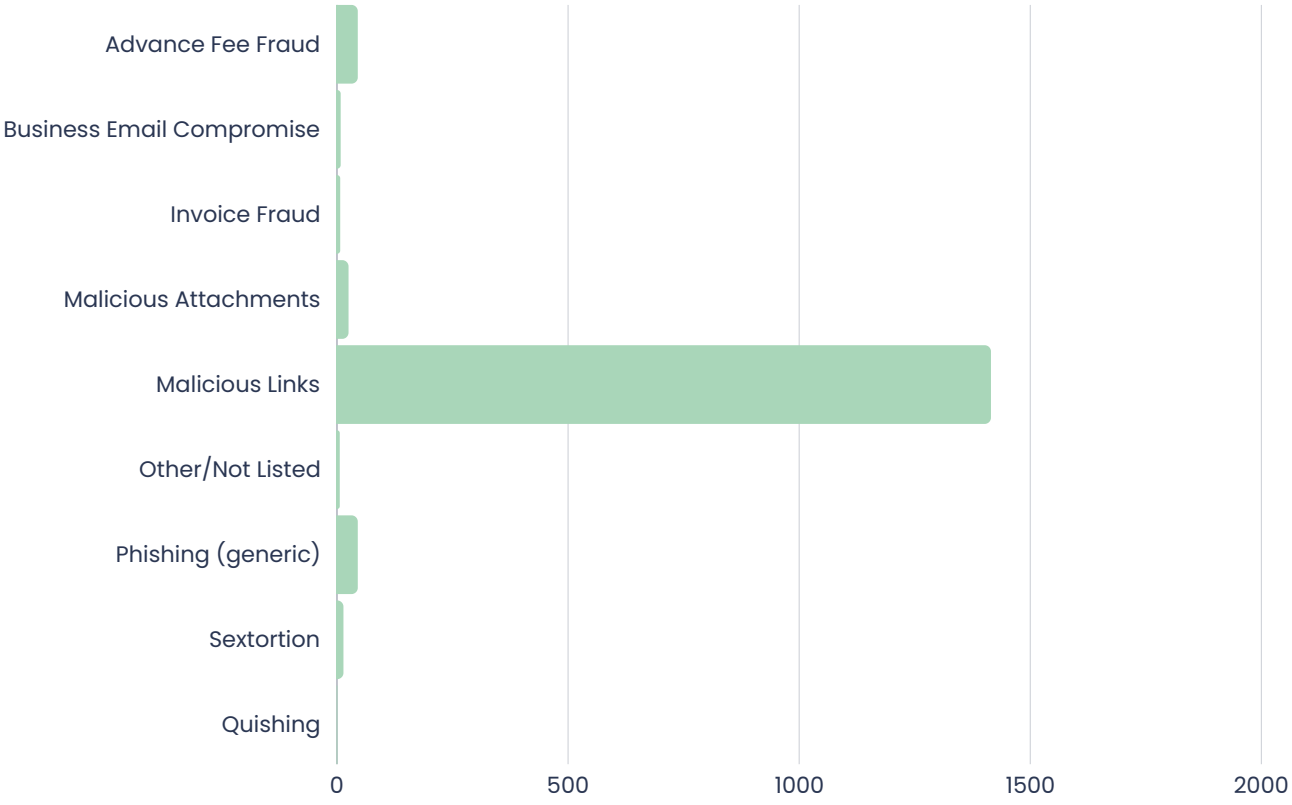
in September and October

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. Anti-malware software
4. AAA (American Automobile Association)
5. Competitions and Awards



CYBER CONCERNS

95 REPORTED

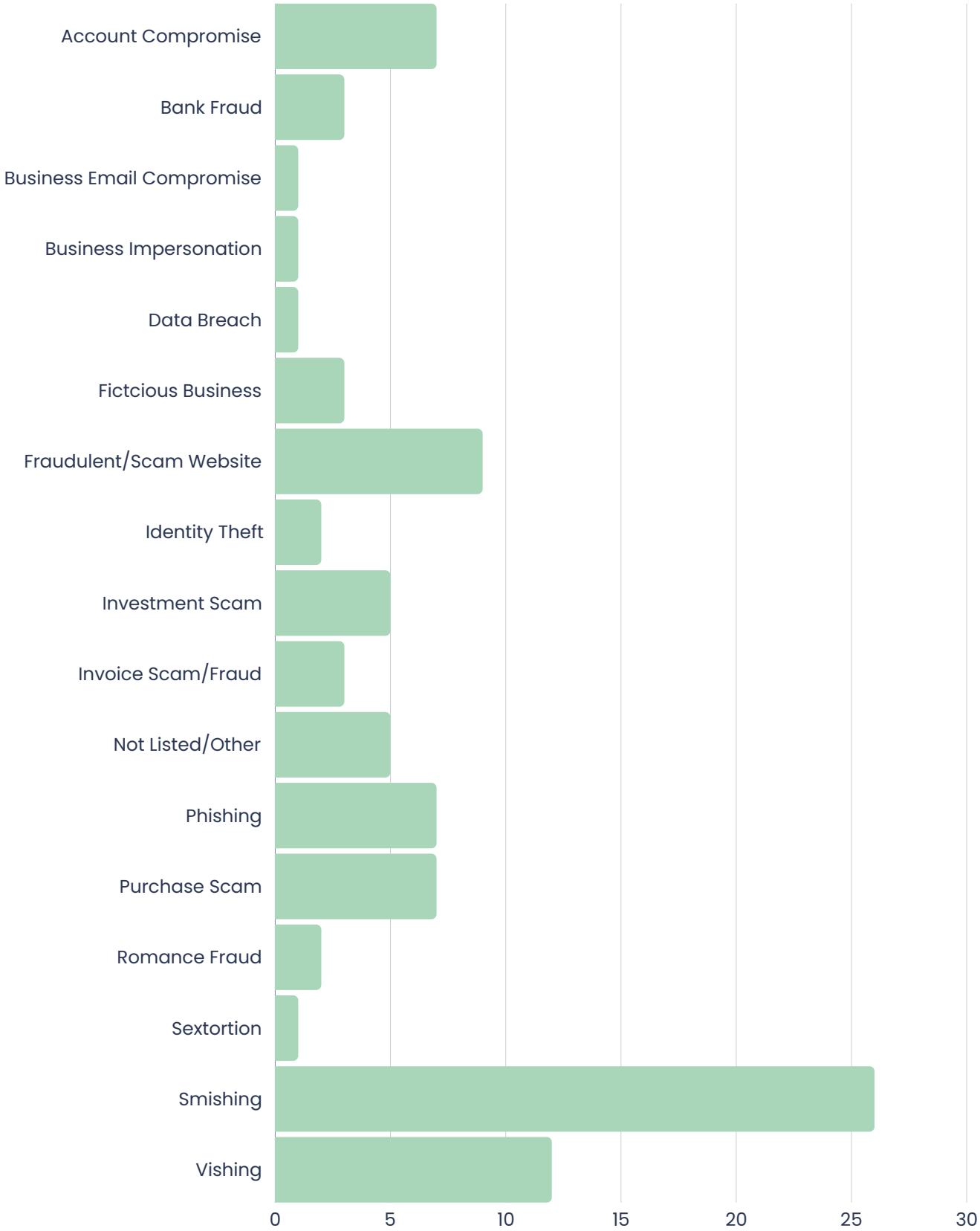
in September and October

Detail

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

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 September and October



ISLE OF MAN THREAT COMMENTARY

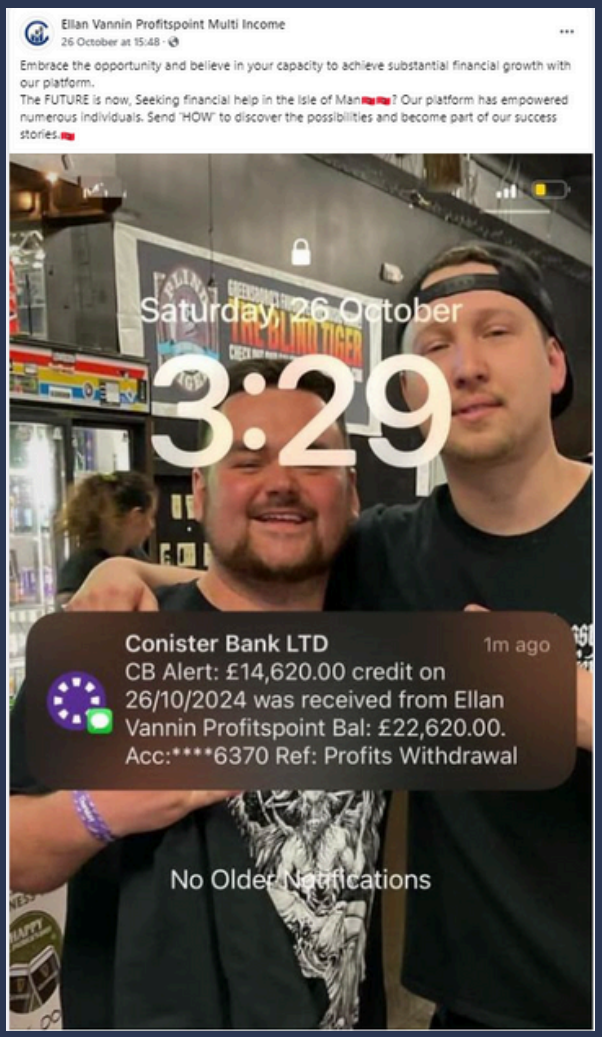
INVESTMENT SCAMS

TAILORED ISLE OF MAN INVESTMENT SCAMS

We were made aware of a Facebook page 'Ellan Vannin Profitspoint Multi Income' [sic] offering a fraudulent platform to help victims receive financial growth.

The page posts use screenshots from iPhone home screens with a notification from Conister Bank showing significant amounts of money being received into an account under the reference 'Profits Withdrawal'. These posts are then shared through Facebook Ads through another page and have been set to target Manx residents. The scam domains were quickly taken down however the Facebook page remains up.

This was a typical investment scam that would have left victims handing over money to a fake platform with no hope of returns. However, what makes this story notable is how tailored towards to the Isle of Man. This shows how criminals are adapting their techniques, putting more time into research and are highly aware of Isle of Man residents as viable targets.



Scam post using the Conister name

ACCOUNT COMPROMISE

WOOFLERS FEELING THE LONG-TERM EFFECTS OF A COMPROMISE

Wooflers Homestay for Dogs, a local dog-sitting business, has been grappling with the ongoing impact of a Facebook account compromise. Initially, the legitimate Wooflers page was hacked, and scammers took control. They then used a nearly identical PayPal address to deceive potential customers into sending payments. Despite the creation of a new, legitimate page and media coverage warning the public, new victims continued to fall prey to the fraud.

The situation worsened recently when the hackers escalated their activity. They stole images from another dog-sitting business, Paw Patrol, and used personal photos of the owner's family, including images of her sister, nephew, and their family dog, as well as pictures taken inside the owner's home, to create another fraudulent page. This has added a personal, emotional toll, as her family's images have been misused without consent.

The police have been informed of the ongoing issue, as the scammers managed to take money from another unsuspecting family just this week. We have also been involved, working to notify authorities and assist with legal steps for takedown requests. Although Facebook has provided a reporting point for legal action, the process has been slow, and the fraudulent pages remain active. This highlights the challenges businesses face when attempting to recover from an online security breach, as the response from platforms like Facebook can be frustratingly delayed.

This case illustrates the critical need for businesses to verify their online communications, spread awareness of any security breaches, and ensure they have appropriate security controls. It also highlights the importance of being cautious when sharing personal images online, especially with wider audiences. Once shared, these images can be misused to impersonate or harm you, as seen in this case. By limiting the exposure of personal content and carefully managing privacy settings, individuals can reduce the risk of their photos being exploited. The emotional and financial toll on business owners affected by online fraud cannot be overstated, and this case serves as a stark reminder of the long-term consequences of a compromised online presence.

FRAUDULENT BUSINESS

COLLABORATION TO REMOVE SCAM BUSINESSES

In September 2024, the Isle of Man Financial Services Authority (FSA) sought assistance from the ourselves to address three fraudulent financial services websites falsely claiming to operate from the Isle of Man. The websites, felicitycu.org, securehavenbnk.com, and paradisevalleybnk.com, represented fictitious entities named Felicity Credit Union, Secure Haven Bank, and Paradise Valley Bank. These websites appeared to replicate the branding and content of a legitimate U.S.-based credit union, Alliance Bank.

The IOM FSA and OCSIA promptly reported the fraudulent websites to various stakeholders, including NameCheap, the UK National Cyber Security Centre (NCSC), and Google, to initiate takedown actions. While Cloudflare identified NameCheap as the host, NameCheap denied this, complicating initial efforts to take the websites offline.

Further escalation involved reporting the matter to the Public Domain Registry, a Registrar with potential authority over the domain names. By September 19, 2024, the Public Domain Registry successfully took down all three fraudulent websites. This case underscores the challenges of navigating multi-party collaborations in addressing online fraud, particularly when conflicting information about domain hosting arises. It highlights the importance of persistent reporting as well as clear and quick communication between stakeholders.

INVOICE SCAM/FRAUD

LOCAL ORGANISATION LOSES £37,640

In September 2024, a local organisation fell victim to an authorised push payment (APP) scam following the compromise of an employee email account. The attack led to fraudulent payments totalling £37,640.

The incident began when an attacker, posing as a trusted entity, sent an urgent email requesting payment for software, including a copy of a fake invoice. After the initial payment was processed, a follow-up email claimed an additional invoice had been overlooked. This second invoice was also paid. The scam went undetected for several weeks, until a routine review identified a breach of in-house payment procedures.

A subsequent investigation revealed the attacker gained access to the employee's email account through a phishing attack. An email impersonating a Business Gateway tricked the employee into entering login credentials and a two-factor authentication (2FA) code on a malicious site. This allowed the attacker full access to the email account, enabling them to carry out the scam.

The organisation's technical team took steps to secure the compromised account, including resetting the password, terminating all open sessions, and reviewing account rules for unauthorised changes. They also implemented email security for all staff to provide better protection against phishing and malware. To enhance future resilience, the organisation has initiated Security Awareness Training (SAT) to educate employees on recognising cyber threats and deployed Managed Detection and Response (MDR) for Microsoft 365 to monitor for ongoing attacks.

This case underscores the critical need for robust security practices, including phishing awareness, strict adherence to internal procedures, and multi-layered technical defences. Whilst a compromised account automatically adds a level of legitimacy to the email, it is important that staff and organisations have the appropriate policies and procedures in place.

ROMANCE FRAUD

MEETISLEOFMANSINGLES.CO.UK, LOCAL RESIDENTS TARGETED

Two separate incidents on the Isle of Man highlight the threat of romance scams targeting vulnerable individuals. In the first case, a scammer posing as 'Alice Wellberk' purportedly a local woman, connected with an individual through the website *Meetisleofmansingles.co.uk.* Using the phone number +44 7908 922293, the scammer communicated via WhatsApp, building trust by sending explicit images and videos. Over time, they attempted to obtain the victim's bank account details to request money. Fortunately, no payments were made, and the individual, unaware of such scams, reported the matter to the police and blocked the scammer.

In the second incident, another individual was approached by a scammer claiming to be 'Chery Jenny Bryce', a U.S. Army soldier. The scammer, using the phone number +1 (920) 939-9442, also communicated via WhatsApp and sought to extract personal details, including the victim's name, address, and contact information. They arranged for a fake parcel delivery and sent a payment link for tracking fees, applying persistent pressure to compel payment. Although no financial loss occurred, the victim, similarly unaware of such scams, reported the incident to the police and blocked the scammer.

For loved ones of vulnerable individuals, it is essential to remain vigilant and supportive. Signs of manipulation may include secretive behaviour about online relationships, sudden requests for financial help, or emotional distress when discussing the online connection. Encourage open conversations about online interactions and help them understand the common tactics scammers use, such as urgent financial requests, excessive flattery, or fabricated stories designed to elicit sympathy or trust. If you suspect a loved one is being manipulated, approach the subject with care and understanding, offering to review communications together and providing resources for reporting scams. Awareness, patience, and consistent support are critical in protecting vulnerable individuals from falling victim to these schemes.

Read our article about protecting a loved one involved in a romance scam here.

SEASONAL THREATS

As the holiday shopping season approaches, including Black Friday and Cyber Monday, shoppers eagerly hunt for bargains. With thousands of fake e-commerce sites being created, scammers have created the perfect environment to catch-out bargain hunters and Christmas shoppers. Staying vigilant is essential to protecting your finances and personal information during this busy time. Here are practical tips to stay safe while shopping online or navigating holiday scams.

Shop with Reputable Retailers and Verify Websites

Stick to trusted brands and avoid clicking on links in ads or emails. Always visit official websites directly, using bookmarks if possible. Look for secure URLs with 'https://' and a padlock icon. Be cautious on online marketplaces like Facebook Marketplace or Etsy; meet sellers in person when possible and check profiles for inconsistencies.

Use Strong Passwords and Secure Accounts

Create strong, unique passwords using random words, numbers, and special characters. Don't reuse passwords, especially for email accounts. Use a password manager and enable multi-factor authentication for added security.

Protect Your Payment Information

Credit cards offer better fraud protection than debit cards, which can drain your account. Avoid saving card details on retailer websites and use services like PayPal for extra security.

Be Sceptical of Amazing Deals

If a deal seems too good to be true, it likely is. Verify discounts on the retailer's official website instead of clicking on ads.

Stay Alert for Delivery and Fake Website Scams

Beware of SMS delivery scams. Don't click on links in texts, check for physical notices instead. Research unfamiliar websites and ensure they use HTTPS for secure transactions.

Beware of Scam Emails and Social Media Ads

Check email sender addresses for errors and avoid clicking on unexpected links. Be cautious with social media ads and report suspicious activity. Regularly run antivirus scans to detect threats.

Monitor Your Accounts and Act Quickly if Scammed

Regularly check your bank and credit card statements. If you notice suspicious transactions, contact your bank immediately to stop further fraud.

Additional Holiday Shopping Safety Tips

Use guest checkout for occasional shopping to limit personal data exposure. Be cautious of strange buyer or seller requests, like fake payment receipts. Run antivirus scans if you suspect visiting malicious websites.

With the holiday season approaching, be extra vigilant. Scammers take advantage of the rush of Black Friday and Cyber Monday shopping. Stay cautious and follow these tips to protect your money and enjoy a secure shopping experience.

EXTERNAL THREAT COMMENTARY

LANCASHIRE SCHOOLS DISRUPTED BY CYBER ATTACK AS FYLDE COAST ACADEMY TRUST GRAPPLES WITH RANSOMWARE

In late September, schools across Lancashire, managed by the Fylde Coast Academy Trust, have been hit by a cyber-attack, disrupting access to the majority of their computer systems. Dean Logan, CEO of the Trust, confirmed that a ransomware attack affected their IT infrastructure, leaving staff and students with limited system accessibility. It remains unclear if the attackers are demanding a ransom payment from the trust.

The Trust oversees 10 academies, including Blackpool's Aspire, Montgomery, and Unity high schools, as well as several primary schools, all of which have been forced to revert to manual, non-IT-based processes. Phone lines were also affected, prompting Mr Logan to urge parents and carers to contact them 'only when necessary'.

Responding swiftly, the Trust received support from the Department for Education and a cybersecurity team within hours of the incident. Logan expects that essential services will resume next week, though full restoration of IT systems could take several weeks as they work to remove the ransomware completely.

Mr Logan expressed appreciation for the resilience shown by students, teachers, and support staff during this challenging period. The Trust is drawing on lessons from the pandemic to manage the disruption effectively, with support from the local authority, other school trusts, and the community.

This incident demonstrates the critical importance of having an effective incident response and business continuity plans that include knowing who to telephone at the first sign of an attack. The swift coordination with cybersecurity professionals and government agencies showcases the Trust's ability to mitigate the immediate effects of the attack and prioritise the continuity of the service.

CYBERATTACK DISRUPTS TRANSPORT FOR LONDON OPERATIONS, CUSTOMER DATA COMPROMISED

Transport for London (TfL) was the target of a severe cyberattack that has caused significant operational disruptions and affected thousands of customers. First detected on September 1, the attack has been described by TfL's Chief Technology Officer, Shashi Verma, as "sophisticated" and "aggressive." Initial investigations revealed unauthorised access to personal data, including names, addresses, contact information, and sensitive bank details.

Approximately 5,000 customers have been notified that their data was compromised. In letters sent to affected individuals, TfL acknowledged the potential exposure of bank account numbers, sort codes, and Oyster refund information. Customers have been unable to apply for new concession cards, access their contactless data, or process refunds for nearly three weeks following the breach.

The cyberattack has also disrupted various TfL services. While public transport operations remained intact, key applications such as live Tube arrival information and the photocard portal for travel concessions have been impacted. Additionally, the Dial-a-Ride booking system has faced disruptions, and customers have reported issues processing payments through the Oyster and contactless app, although payments are still possible on-site.

Furthermore, while the impact on customers is the most evident affect, staff were also impacted. Following the cyber-attack, TfL required all of its approximately 30,000 employees to attend in-person appointments for password resets. This time consuming process was to validate the authenticity of staff and was required in order to regain access to TfL applications and data.

In response to the incident, TfL is collaborating with the National Crime Agency and the National Cyber Security Centre to investigate the breach and restore services. Security measures have been heightened, with increased physical security at TfL offices and new protocols for staff accessing the IT network.

The National Crime Agency has emphasised that such cyberattacks are ‘hugely disruptive’ and have severe implications for local communities. has TfL apologised for the inconvenience caused and is committed to keeping customers informed as the situation evolves. While the duration of service disruptions remains uncertain, TfL is focused on quickly restoring full functionality.

A 17 year-old suspect was arrested in Walsall in connection with the attack and on suspicion of Computer Misuse Act offences.

RISE OF SEXTORTION SCAMS USING GOOGLE STREET VIEW IMAGES

A disturbing surge in sextortion scams has emerged, using Google Street View images to manipulate and intimidate victims. Reports indicate that cybercriminals are using these publicly accessible images to create personalised threats, claiming to possess incriminating material and threatening to share it unless a ransom is paid, often in cryptocurrencies like Bitcoin.

The South Wales Cyber Crime Unit has highlighted this tactic, warning victims that attackers may even address them by name and reference their local area, making the threats seem more credible. Victims receive emails containing explicit threats that they will be publicly shamed if they do not comply.

The SWCRC's campaign, titled 'Hello Pervert', aims to raise awareness of these scams, urging individuals not to panic but to report such incidents to authorities immediately.

Experts from cybersecurity firms like Avast emphasise the evolving nature of these scams. By incorporating geographical data, scammers instil a sense of dread and urgency, making it crucial for potential targets to remain vigilant

Many individuals may feel overwhelmed and ashamed, often leading them to comply with the demands out of fear of exposure.

CLICK HERE OR SCAN TO VIEW OUR SEXTORTION ADVISORY

NCSC WARNS OF GROWING CYBERSECURITY GAP

Speaking at Singapore International Cyber Week, Dr Richard Horne, the newly appointed head of The National Cyber Security Centre (NCSC) has raised alarms about a significant and widening gap between the increasing sophistication of cyber threats and the defensive capabilities of organisations across the UK. In a recent report, the NCSC outlines how cyber-attacks are not only escalating in frequency but are also evolving in complexity, making it more challenging for businesses and institutions to defend themselves effectively.

The report indicates that cybercriminals are adopting advanced techniques, employing artificial intelligence and other technologies to launch more targeted and damaging attacks. This shift highlights the necessity for organisations to enhance their cybersecurity measures, including updating their security protocols and investing in cutting-edge technologies to better protect sensitive information.

Moreover, the NCSC emphasises the need for collaboration among government bodies, private sectors, and cybersecurity experts to develop robust strategies that address these emerging threats. The agency calls for increased investment in training and resources to equip personnel with the skills necessary to counteract cyber threats effectively.

In addition, the NCSC points out that many organisations still operate under outdated security frameworks, leaving them vulnerable to exploitation. The centre urges businesses to prioritise cybersecurity as an integral component of their operational strategies, advocating for regular assessments and updates to their security systems.

As the threat landscape continues to evolve, the NCSC's report serves as a crucial reminder that proactive measures and collaboration are essential to bridging the gap between current threats and defence capabilities. The agency encourages organisations to take immediate steps to bolster their cybersecurity posture and remain vigilant against potential breaches.

MICROSOFT DIGITAL DEFENSE REPORT 2024: COMPREHENSIVE INSIGHTS AND STRATEGIC RECOMMENDATIONS

The 2024 Microsoft Digital Defense Report sheds light on the rapidly evolving cyber threat landscape, highlighting the increasing complexity of attacks and the dual role of artificial intelligence (AI) in both enabling defences and empowering attackers.

Threat Trends

Surge in Ransomware Attacks
The frequency of human-operated ransomware attacks has skyrocketed, with incidents nearly tripling over the past year. Attackers are exploiting unmanaged devices, vulnerabilities in IT systems, and social engineering techniques such as phishing to gain entry. These threats disproportionately affect organisations with insufficient device management and outdated security policies.

Evolving Phishing Techniques
Phishing attacks continue to grow in sophistication. Newer tactics include using malicious QR codes to direct users to credential-stealing sites, bypassing traditional email security measures. Business Email Compromise (BEC) remains pervasive, with attackers manipulating inbox rules to obscure fraudulent communications. Microsoft also flagged a notable rise in deepfake technologies, which cybercriminals are using for high-stakes fraud schemes.

Identity Compromises
Password-based security remains a critical vulnerability, with Microsoft detecting over 600 million password attacks daily. Cybercriminals are increasingly bypassing multifactor authentication (MFA) with techniques like Adversary-in-the-Middle (AiTM) phishing, which intercepts sensitive authentication details in real-time.

AI in Cybercrime and Defence
While AI offers transformative capabilities for threat detection and mitigation, cybercriminals are also employing AI for highly targeted social engineering and advanced attacks. Deepfake technology poses a growing threat, particularly in financial fraud and misinformation campaigns, raising alarms about the robustness of existing authentication systems.

AI-Powered Defence Mechanisms
Microsoft's adoption of AI in cybersecurity accelerates the identification and resolution of threats. AI-driven tools automate risk assessments, analyse historical attack data, and streamline incident response. This allows organisations to drastically reduce the time required to detect and mitigate breaches, while optimising resources.

AI-Powered Defence Mechanisms
Microsoft's adoption of AI in cybersecurity accelerates the identification and resolution of threats. AI-driven tools automate risk assessments, analyse historical attack data, and streamline incident response. This allows organisations to drastically reduce the time required to detect and mitigate breaches, while optimising resources.

Recommendations for Organisations

Adopt a Zero Trust Security Model
Embrace a 'never trust, always verify' mindset by continuously validating access permissions and assuming breach possibilities. Limit user privileges and enforce stringent verification protocols.

Shift to Password-less Authentication
Replace traditional passwords with advanced methods such as passkeys, biometrics, or hardware tokens to eliminate common vulnerabilities.

Security by Design
Build cybersecurity into products and services from the outset. Ensure that default configurations prioritise security and provide end-users with clear guidance on best practices.

Phishing Prevention and Education
Train employees to recognise the latest phishing strategies. Combine this training with real-time monitoring tools to pre-emptively detect and neutralise threats.

Strengthen Incident Response
Invest in AI-powered detection systems to respond to breaches faster. Organisations should also establish regular drills and audits to test their preparedness.

Microsoft's Secure Future Initiative

Microsoft's Secure Future Initiative aims to amplify global cybersecurity readiness by integrating security-by-default approaches and expanding its workforce with specialists in cyber defence. Education and collaboration are key pillars, with the initiative prioritising partnerships between private and public sectors to tackle cyber threats at scale.

As the digital landscape becomes increasingly hostile, Microsoft stresses that resilience hinges on collaboration, innovation, and proactive strategies. By adopting the outlined measures, organisations can better protect sensitive data, minimise operational disruptions, and adapt to a future where cyber threats are ever-changing.

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

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