Cyber Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

March - April 2025

INTRODUCTION

For the period 1st March - 30th April

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 28,100 suspicious emails. In March and April 2025, we received 716 suspicious emails.

SUSPICIOUS EMAILS

716 REPORTED

in March and April

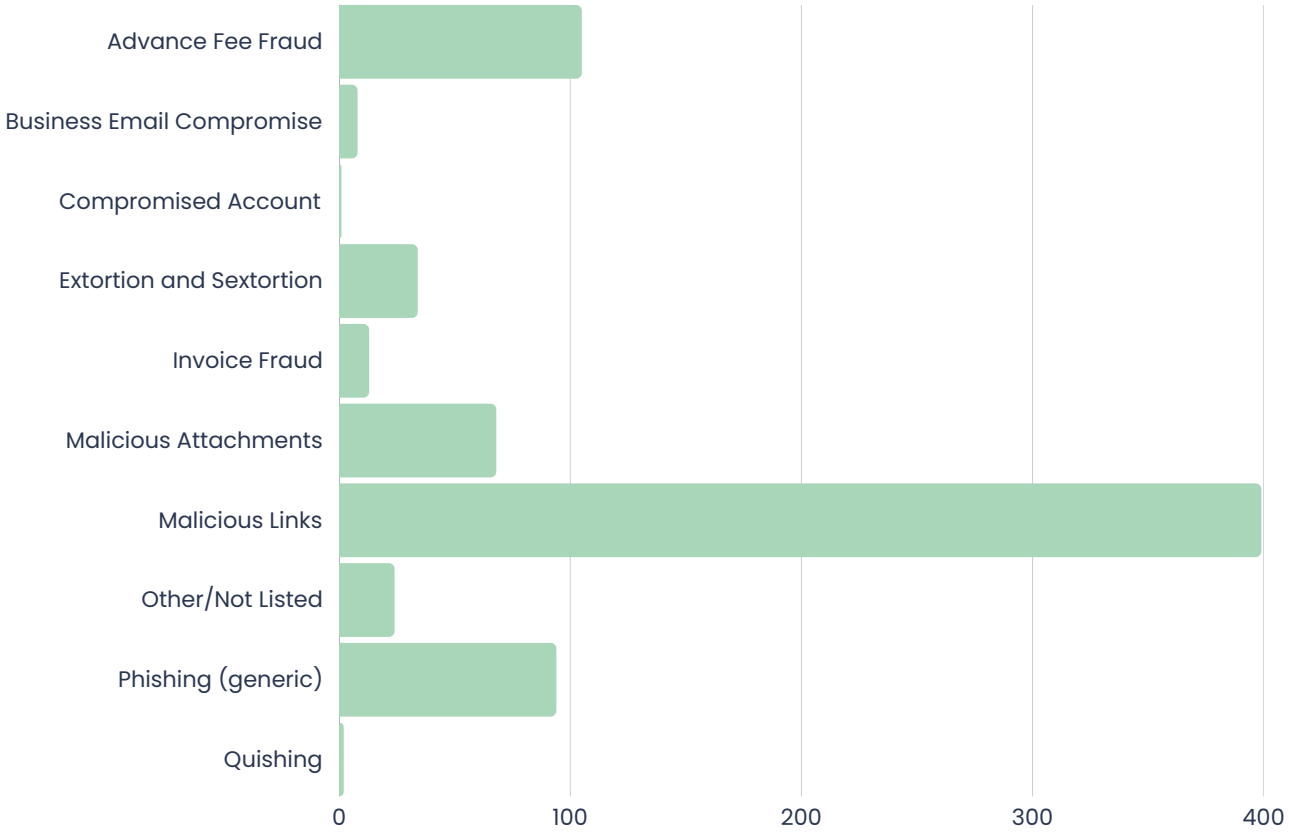
Detail

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.

Whilst malicious links do make the bulk of submissions as usual, this period is notable for the increased prevalence of advance fee fraud.

Top 5 Phishing Scams Imitating Popular Services:

1. Manx.net
2. Romance and dating
3. Trump/Musk Spam
4. Parcel Delivery
5. Anti-malware Software



CYBER CONCERNS

100 REPORTED

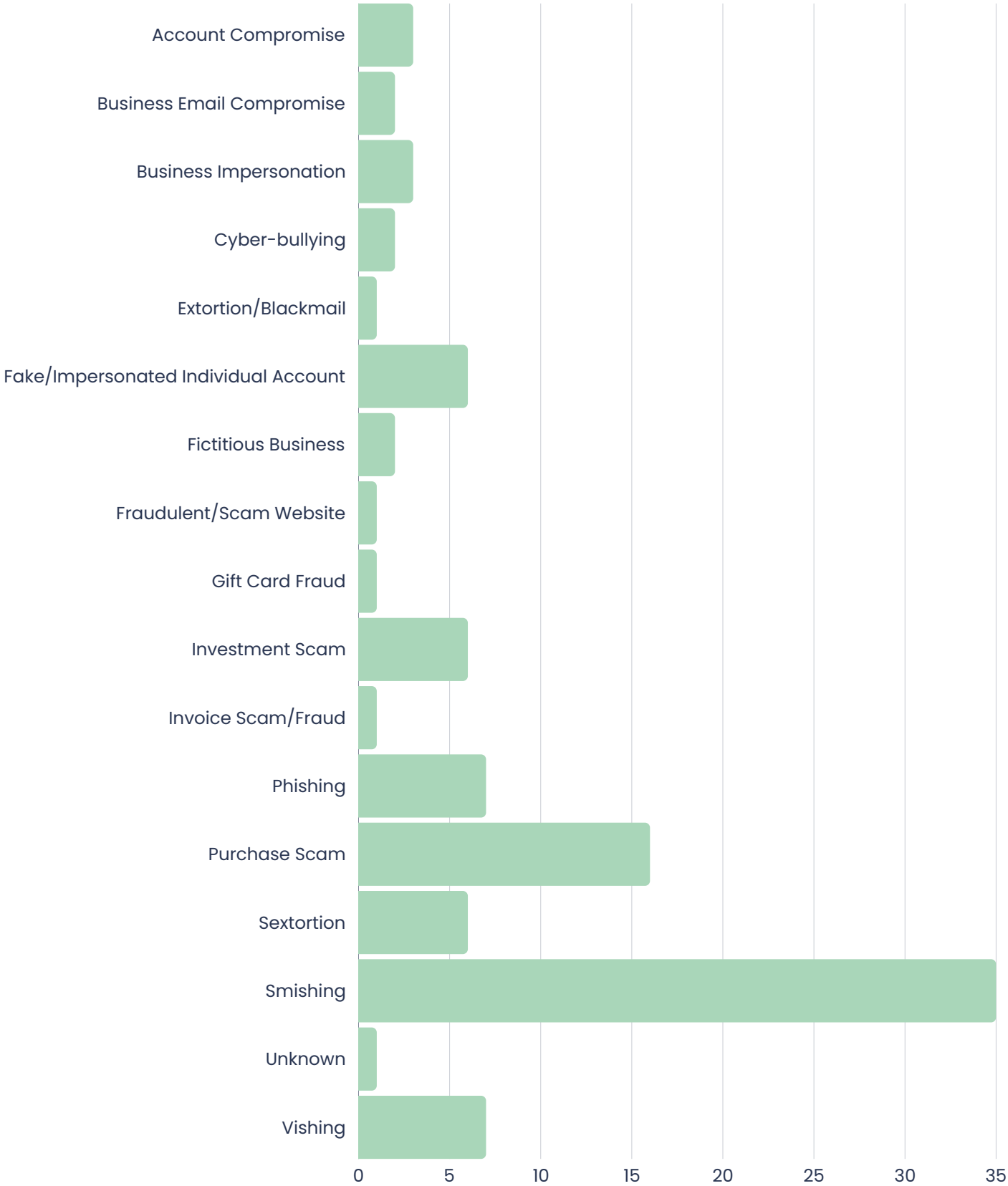
in March and April

Detail

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

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 March and April



ISLE OF MAN THREAT COMMENTARY

BUSINESS IMPERSONATION

SCAM WEBSITES MIMICKING GOVERNMENT AND LAW FIRMS

We received two new reports highlighting the persistent threat posed by imitation or 'copycat' websites, often created by cyber-criminals to deceive the public and exploit legitimate organisations.

In one case, a fraudulent website, falsely claimed to represent an Isle of Man-based law firm while using the address of a property unconnected to it. The CSC investigated and confirmed the site was bogus.

A second report came from the Financial Services Authority (FSA) after a fraudulent website, https://fsa-lom/uk, was found to be an exact replica of a legitimate government website.

The third case involved an almost-identical copy of a local bank's website that used a similar domain to mislead users.

In response to all three cases, the CSC took coordinated action. Reports were submitted to the UK's National Cyber Security Centre (NCSC), Google's Safe Browsing service, and the respective domain registrars or website hosts. Additional direct complaints were made by affected parties, such as the FSA and Conister Bank.

Copycat websites pose serious risks including identity theft, financial fraud, and erosion of public trust. When they imitate government or business websites, they can mislead users into sharing sensitive information or making payments to criminals. The CSC urges the public to stay vigilant and report suspicious websites to help combat this ongoing threat.

FAKE DOGGY HOMESTAY PAGES EXPLOIT TRUST

A local dog-sitting service, No Worries Doggy Homestay, has become the latest victim of a scam involving imitation Facebook pages designed to defraud pet owners. The business discovered that a bogus Facebook page was using their name and impersonating their service — directing users to a suspicious link and displaying photos stolen from other businesses, including Wooflers Doggy Homestay and a private family website previously linked to a hacking incident.

The fraudulent page, believed to have originally been created in 2018 under false pretences, has undergone at least four name changes since 2024, likely in an effort to evade detection and reporting. The photos on the fake profile are not affiliated with No Worries, and include misleading 'awards' and images of other local homestay businesses, all designed to build false credibility and trick pet owners into placing deposits.

'No Worries' has stressed to its community that it never requests a deposit before clients have visited, met the team, and discussed their needs — a message they've had to repeat often due to ongoing impersonation.

Despite efforts to report the fake page, response times from Facebook remain slow, leaving affected businesses exposed and potential customers at risk.

Cyber impersonation can have lasting effects on small businesses, both emotionally and financially. Businesses could consider relying more on their own websites rather than social media platforms, where impersonation is easier and harder to control. Your website can serve as the definitive source of information and booking processes. Another protective measure could be to add discreet watermarks to any images you post online. This can deter scammers from using your content and helps identify your original media.

GIFT CARD FRAUD

FACEBOOK 'SOLDIER' TRICKS VICTIM OUT OF £1,500 IN GIFT CARDS

A report regarding romance fraud was received by the CSC in which an Isle of Man resident was manipulated into sending £1,500 in Apple gift cards to a scammer posing as a member of the military. The scam began when the scammer made contact with the victim via Facebook Messenger in early March.

Over time, he claimed he was serving in the military and needed gift cards to pay his commander in order to be discharged. The victim, believing the story, purchased and sent the gift cards in mid-March. As is typical in these types of scams, the fraudster soon asked for more money. Realising the situation was fraudulent, the victim cut off contact around mid-April and blocked the scammer.

However, the scammer later resumed contact through the encrypted messaging app Telegram, using the handle @cote-de-pablo5, and began blackmailing the victim by threatening to post intimate photos online unless a further £4,000 was paid.

This case highlights two key warning signs of romance scams: requests for payment using gift cards and a sudden escalation to emotional manipulation or threats. Gift cards are a favourite tool of scammers because they are difficult to trace and nearly impossible to recover once sent.

INVESTMENT SCAMS

DEEPFAKES OF LOCAL POLITICIANS USED IN ONLINE SCAMS

In April, the CSC issued a public warning after detecting a rise in sophisticated scams on Facebook involving deepfake videos and doctored images used to impersonate public figures and celebrities in fraudulent investment schemes.

In this advisory, the CSC outlined how scammers are using artificial intelligence to create highly realistic deepfake videos that falsely appear to show local politicians endorsing bogus financial platforms, particularly cryptocurrency investments.

Sponsored ads circulating online have included fabricated videos of the Chief Minister and the Minister for the Treasury, both seemingly encouraging the public to invest in what appear to be official or government-backed opportunities.

Other similar reports in the period have used digitally altered photographs to falsely associate former MHK Chris Robertshaw and television personality Jeremy Clarkson with similar investment promotions.

In response, the CSC urges members of the public to remain sceptical of investment advice seen on social media or video platforms—especially if it appears to come from a familiar face. The recommendation is to verify any claims through official sources, and never rush into financial decisions based on a video alone.

The full advisory, including examples and guidance on how to spot deepfakes, is available on the CSC website. The public is encouraged to report any suspicious content to help prevent further scams.

INVOICE FRAUD

TRUSTED SUPPLIER IMPERSONATED IN 9K FRAUD

The CSC wishes to warn businesses about remaining vigilant after a recent case of invoice fraud resulted in a £9,000 financial loss, likely linked to email account compromise or spoofing.

The victim, a regular customer of a UK-based company, was targeted in a scam that began in February 2025. Over the course of a month, a convincing email exchange took place, ultimately leading to an order being placed. In the final messages in March 2025, the fraudster, posing as the legitimate supplier, sent an invoice that appeared genuine but included updated bank details. The customer, assuming the change was legitimate, transferred £9,000 using their internet-banking app to the provided bank account Although the payment system flagged that the account name didn't match, the customer proceeded, later explaining that such mismatches are not unusual with some transfers.

Only after contacting the genuine supplier to confirm payment was the fraud uncovered. The company confirmed that their banking details had not changed, exposing the transaction as fraudulent.

The CSC advises all organisations to implement strong email security measures, including two-factor authentication and staff awareness training. It's also recommended to verify any change in payment instructions through a known phone number or separate communication channel, not email alone. Where possible, use bank account name-checking services and never ignore mismatched results.

PURCHASE SCAMS

RENTAL SCAM ON FACEBOOK COSTS LOCAL RESIDENT £850

This scam involved a fake listing titled 'Studio for rent' with a photo of a bed, advertised at $550. The advertisement, posted by a Facebook profile under the name 'Tom Walsh', claimed the property was located near Douglas Promenade. The victim initially messaged the poster on Facebook Messenger in April 2025 and was instructed to continue the conversation via WhatsApp.

Believing the listing to be legitimate, the complainant sent a total of £850 to two individuals to secure the rental. It was later discovered that the property did not exist, and the entire listing was fraudulent. The Police had already issued a warning on social media regarding similar scams, which the CSC shared to help raise awareness.

Fake rental and sales listings are a persistent issue on platforms like Facebook Marketplace, where scammers often use real addresses and attractive prices to lure victims. These scams typically involve pressure to act quickly and send money without in-person viewings or proper documentation. A clear, tell-tale sign of such scams is the scammer's request to move the conversation off Facebook and onto WhatsApp. This tactic allows scammers to hide their messages behind WhatsApp's end-to-end encryption, making it harder for app administrators to see the content of messages. It also protects the scammer's Facebook account from being suspended or flagged.

The CSC strongly advises never to transfer funds or personal details for properties or goods without first verifying the legitimacy of the seller and seeing the property in person.

FAKE EBAY EMAILS LEAD TO PARCEL SCAM

In the period, a member of the public sold an item on eBay for £965.00 and received what appeared to be official confirmation emails from 'paymentscheckout@post.com'.

The first message falsely stated that the buyer's payment had been deducted and would be credited to Seller once tracking information was supplied. Two follow-up emails continued the deception, with one reiterating that the transaction was 'pending' and the other falsely claiming that shipment confirmation had been received, and funds would be released once delivery was completed. The victim of this fraud had already sent the parcel by the time they realised the sale was a scam.

The scammer had cleverly created an email specifically related to the selling of the item that was designed to look like it had come from eBay.

To stay safe, never trust payment confirmation emails alone, as scammers often use fake emails that mimic eBay's branding and language. Always log into your official eBay account to verify that payment has been received. Legitimate eBay emails will come from @ebay.com or related verified domains. Emails from generic addresses like paymentscheckout@post.com are a major red flag. Stick to official channels for all communication and transactions. Using eBay's built-in messaging system ensures that interactions are monitored, and using eBay's payment system (such as PayPal or eBay Payments) provides better buyer/seller protection.

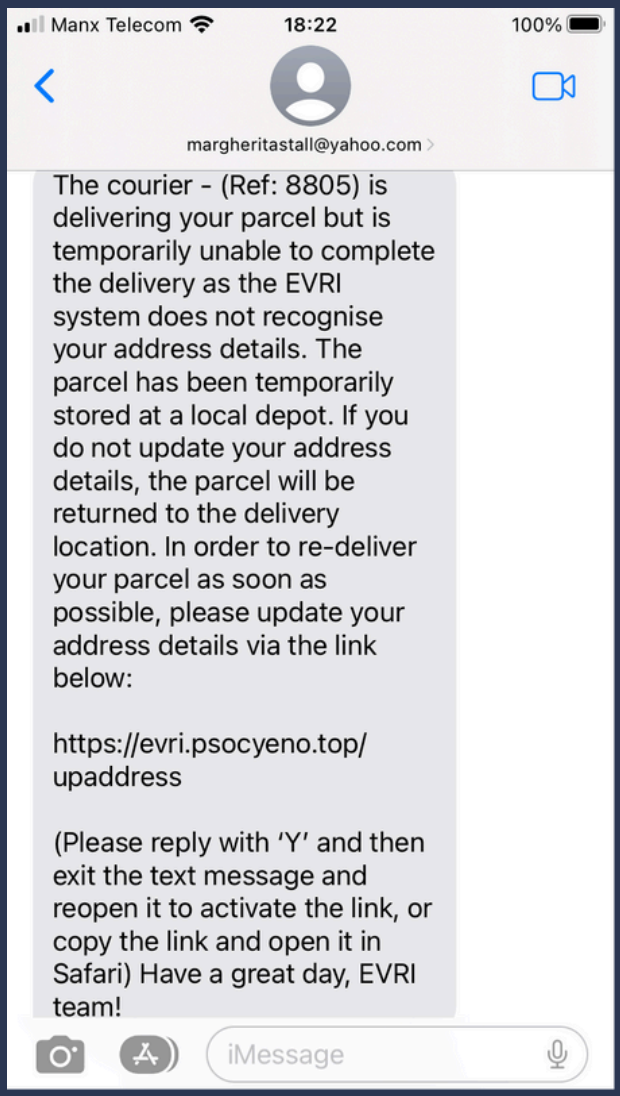
SMISHING

SCAM PARCEL DELIVERY MESSAGES CLAIM TO BE FROM EVRI

The CSC received reports of parcel delivery scams involving fake text messages and most claimed to be from courier company Evri. Individuals were tricked into clicking fraudulent links after being told their parcel could not be delivered due to 'missing or damaged address information'.

One report involved a scam text message from an iCloud address that appeared while the individual was expecting an Amazon delivery via Evri. The message included a suspicious link and instructions to 'reply Y, then exit the SMS and open it again' to activate the link. This tactic is used by criminals to bypass the protections built into messaging applications. Whereby a link from a unknown sender if often not clickable, but reply to the message makes the conversation 'legitimate'.

The website later asked for card details to pay a small redelivery fee of €0.23. Another person received an almost identical message from a Hotmail address and again posing as Evri, with similar content and tactics. Despite having placed a recent order, they recognised the scam and refrained from sharing their details.



These scams exploit the high volume of online shopping and delivery services to target unsuspecting victims, using urgency and realism to trick people into handing over sensitive personal or financial information. Official parcel tracking should always be done through verified websites. For Evri deliveries, customers should visit the official Evri Track Your Parcel page, https://www.evri.com/track-a-parcel, to confirm the status of their shipment.

SPEAR PHISHING

PHISHING ATTACK POSES AS UNIVERSITY OF CHESTER

Two local students reported phishing emails to the CSC and to the Isle of Man Constabulary that falsely claiming to be from the University of Chester. These emails stated that an outstanding balance of £1,250 was due and instructed recipients to transfer the amount within two to three days via bank transfer. The emails included convincing contact details and reply-to addresses that appeared legitimate at first glance, making the scam difficult to spot, particularly when viewed on mobile devices.

In one case, a student unwittingly forwarded a letter containing personal information, including student awards details, to the scammer before realising the email was fraudulent. It was only upon reviewing the sender's full email address on a laptop that the scam was detected.

University College Isle of Man (UCM) had issued a warning on social media days before, advising students not to engage with any unexpected emails about fees. The CSC shared information about the Cifas Protection Registration scheme with the affected student. This UK-based service helps protect individuals who are at risk of identity fraud. By registering, Cifas places a warning flag on their credit file, alerting financial service providers to take extra steps when verifying any future applications in the student's name. This added layer of protection helps reduce the likelihood of fraudsters opening accounts or taking credit in the victim's name.

Phishing scams remain one of the most common cyber threats, especially when they involve trusted institutions. The CSC advises individuals to verify any requests for payment through official channels and avoid responding to emails that demand urgent financial action. Always double-check sender addresses and never click links or share personal information unless you're certain the request is genuine.

EXTERNAL THREAT COMMENTARY

COINBASE TARGETED IN GITHUB ACTIONS SUPPLY CHAIN ATTACK; 218 REPOSITORIES AFFECTED

A sophisticated supply chain attack targeting GitHub Actions has been uncovered, with cryptocurrency exchange Coinbase identified as the primary focus. The breach exploited vulnerabilities in widely used GitHub Actions, leading to the exposure of continuous integration and deployment (CI/CD) secrets across numerous repositories.

The attack commenced with the compromise of the reviewdog/action-setup@v1 GitHub Action. Threat actors injected malicious code into this action, which, when executed, leaked sensitive information such as CI/CD secrets and authentication tokens into GitHub Actions logs. This initial breach facilitated further exploitation of the tj-actions/changed-files GitHub Action, used by over 20,000 projects, including Coinbase's agentkit repository—a framework enabling AI agents to interact with blockchains.

This incident underscores the critical importance of securing CI/CD pipelines and the dependencies they utilise. Organisations are advised to audit their use of third-party GitHub Actions, pin dependencies to specific commit hashes, and monitor workflow logs for unauthorised access. Implementing incident response plans and maintaining vigilance in supply chain security are essential measures to mitigate such threats.

X (FORMERLY TWITTER) EXPERIENCES WIDESPREAD OUTAGES DUE TO MASSIVE DDOS ATTACK

On 10 March 2025, social media platform X (formerly Twitter) suffered significant service disruptions, attributed to a large-scale distributed denial-of-service (DDoS) attack. Elon Musk, CEO of X, confirmed the incident, stating that the platform was under a 'massive cyberattack' involving substantial resources, possibly from a coordinated group or nation-state. He noted that the attack originated from IP addresses in the Ukraine region.

The attack led to intermittent outages, with users experiencing difficulties accessing the platform. Alp Toker, director of internet monitor NetBlocks, observed a cycle of outages over several hours, consistent with a DDoS attack targeting X's infrastructure. Latency remained high, and while services began returning to normal, it was unclear if the issue had been fully mitigated.

A hacker group known as Dark Storm Team claimed responsibility for the attack, stating that it was politically motivated. However, experts caution that attributing attacks based solely on IP addresses can be misleading, as attackers often use compromised devices and proxy networks to conceal their true location.

In response to the incident, X has taken steps to enhance its security measures, including securing vulnerable origin servers that were previously exposed. The company continues to monitor the situation and is working to prevent future attacks.

FACEBOOK IS WORST PLACE FOR SCAMS AFTER BRITS LOSE £214,000,000 IN SOCIAL MEDIA RIP-OFFS

According to a report by Metro, Facebook has been identified as the primary platform for social media scams in the UK, with British users losing a staggering £214 million to online fraud. Metro shared a warning post on Facebook that was published by the Island’s Cyber Security Centre, highlighting a recent scam where the electronics store, Currys, was supposedly claiming to offer laptops for only £2.

The UK’s National Fraud Intelligence Bureau (NFIB) has stated that fraud cases linked to social media have risen dramatically in recent years. In 2024 alone, reports to Action Fraud, the UK’s national reporting centre for fraud and cybercrime, suggested that tens of thousands of people were deceived by posts, messages, and even paid advertisements on platforms like Facebook, Instagram, and WhatsApp.

The Cyber Security Centre's warning advises members of the public to avoid clicking links, making payments and avoid giving out their personal information.

RETAIL UNDER SIEGE: CYBERATTACKS EXPOSE VULNERABILITIES IN UK HIGH STREET GIANTS

A coordinated wave of cyberattacks has disrupted major UK retailers, including Marks & Spencer (M&S), Harrods, and the Co-op, highlighting the growing threat posed by sophisticated hacker groups like Scattered Spider.

The National Crime Agency (NCA) has identified Scattered Spider as a primary suspect in these attacks. This group, known for its English-speaking members operating across platforms like Discord and Telegram, employs ransomware tactics, notably using the 'DragonForce' tool to encrypt systems and demand cryptocurrency ransoms. The group's members are often young individuals who use social engineering tactics to infiltrate IT systems.

At M&S, the breach is believed to have originated through its IT helpdesk contractor, Tata Consultancy Services (TCS), where hackers impersonated staff to obtain passwords. The attack, discovered over the Easter weekend, led to significant operational disruptions, including halted online orders and affected store stock levels. M&S estimates potential losses up to £300 million in profit and has confirmed the theft of some customer data.

The Co-op faced similar challenges, with empty shelves and disrupted supply chains following a cyberattack that decimated its supply systems. Harrods also reported pulling computer systems offline due to an attempted cyberattack.
Experts warn that the retail sector's lack of investment in IT protection and the vast amount of consumer data it holds make it a prime target for cybercriminals. The ongoing incidents serve as a stark reminder of the vulnerabilities in today's digital landscape, emphasising the need for retailers to treat cybersecurity as a strategic business priority.

As investigations continue, the NCA and cybersecurity experts stress the importance of proactive measures to safeguard against such threats, urging retailers to integrate cybersecurity into their core operational strategies.

ICO FINES HEALTHCARE IT FIRM AND LAW FIRM FOR CYBERSECURITY FAILURES EXPOSING SENSITIVE DATA

The UK Information Commissioner's Office (ICO) has taken decisive action against two organisations following serious cybersecurity breaches that exposed sensitive personal data and disrupted critical public services.

Advanced, a major IT services provider for healthcare organisations, was fined £3.1 million after a ransomware attack in August 2022 compromised the data of over 79,000 individuals. The attack, attributed to the LockBit cybercrime group, exploited a customer account that lacked multi-factor authentication (MFA). Among the affected data were access details for 890 home care patients. The incident caused significant operational disruption, including the temporary shutdown of NHS 111 services, forcing healthcare staff to rely on manual systems.

An ICO investigation concluded that Advanced had failed to implement adequate security protections for external connections. Information Commissioner John Edwards criticised the company for not meeting expected standards, stressing the importance of robust cybersecurity practices in sectors handling sensitive data.

In a separate case, DPP Law Ltd, a Liverpool-based law firm, was fined £60,000 after a 2021 cyberattack compromised the personal data of nearly 1,000 individuals, including information related to criminal proceedings. The ICO found that DPP Law had not encrypted personal data or provided adequate employee training. In both instances, the watchdog determined that preventative measures were either absent or significantly lacking.

These penalties highlight the ICO's growing intolerance for lax cybersecurity, particularly among organisations entrusted with sensitive information. Commissioner Edwards reiterated that protecting personal data is a legal requirement, not a choice, and urged all data controllers to prioritise strong digital defences, including the mandatory use of MFA.

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
Second Floor
27-29 Prospect Hill
Douglas
Isle of Man
IM1 1ET

T: +44 1624 685557

Isle of Man Government
Reiltys Ellan Vannin