Cyber Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

May - June 2024

This page is intentionally left blank

INTRODUCTION

For the period 1st May - 30th June

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

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

CONTENTS

SUSPICIOUS EMAIL REPORTING SERVICE (SERS)

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

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

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

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

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

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

Since the launch of SERS, we have received over 20,037 suspicious emails. In May and June 2024, we received 694 suspicious emails.

SUSPICIOUS EMAILS

694 REPORTED

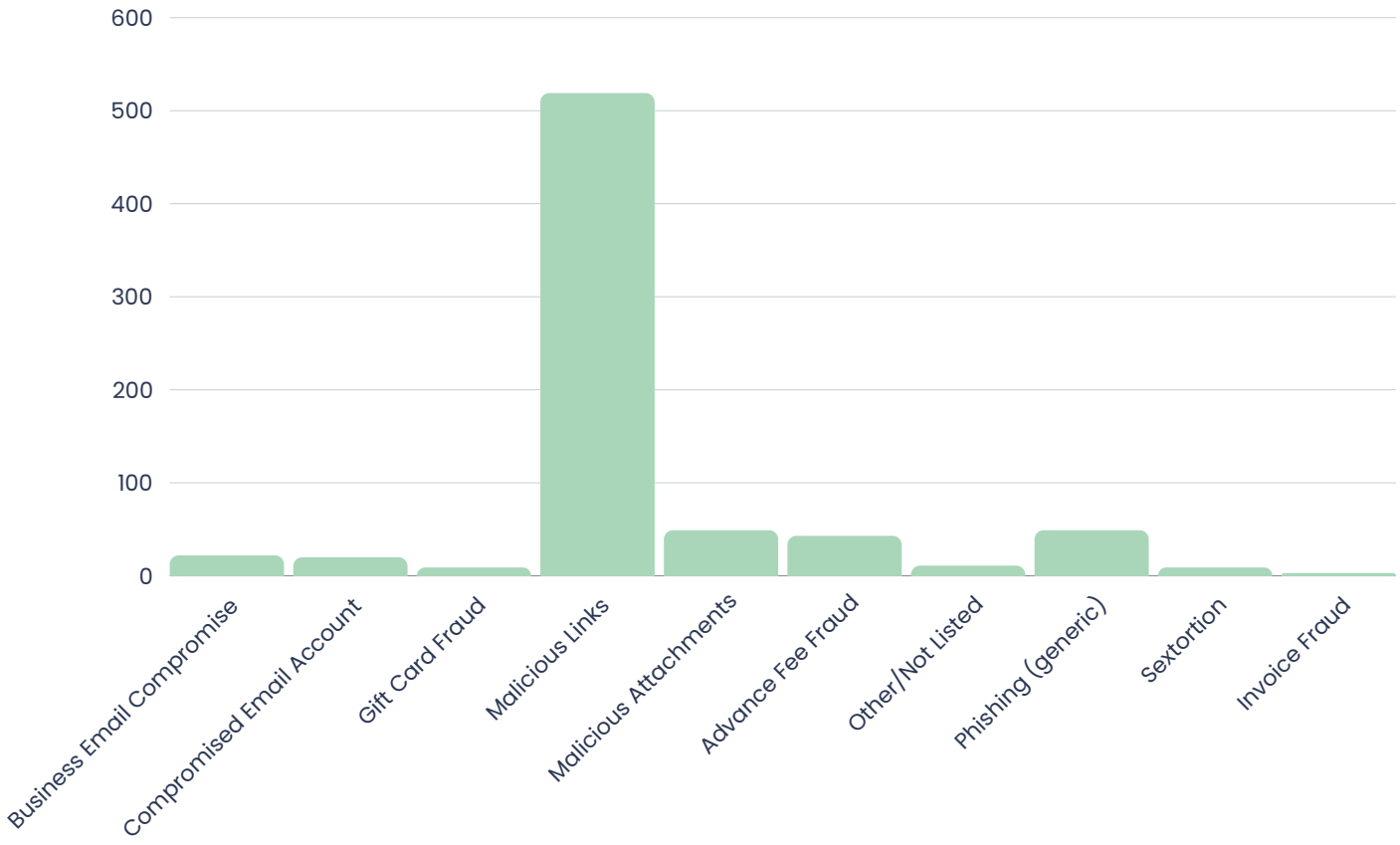
in May and June

Detail

The chart (below) details the type of emails sent by cybercriminals that have been reported to our SERS for the months of May and June. Whilst the infographic (right) showcases the top five most impersonated companies and services.

Top 5 Phishing Scams Imitating Popular Services:

1. Manx.net
2. Parcel Delivery
3. Amazon
4. Anti-malware software
5. Competition and Rewards



CYBER CONCERNS

47 REPORTED

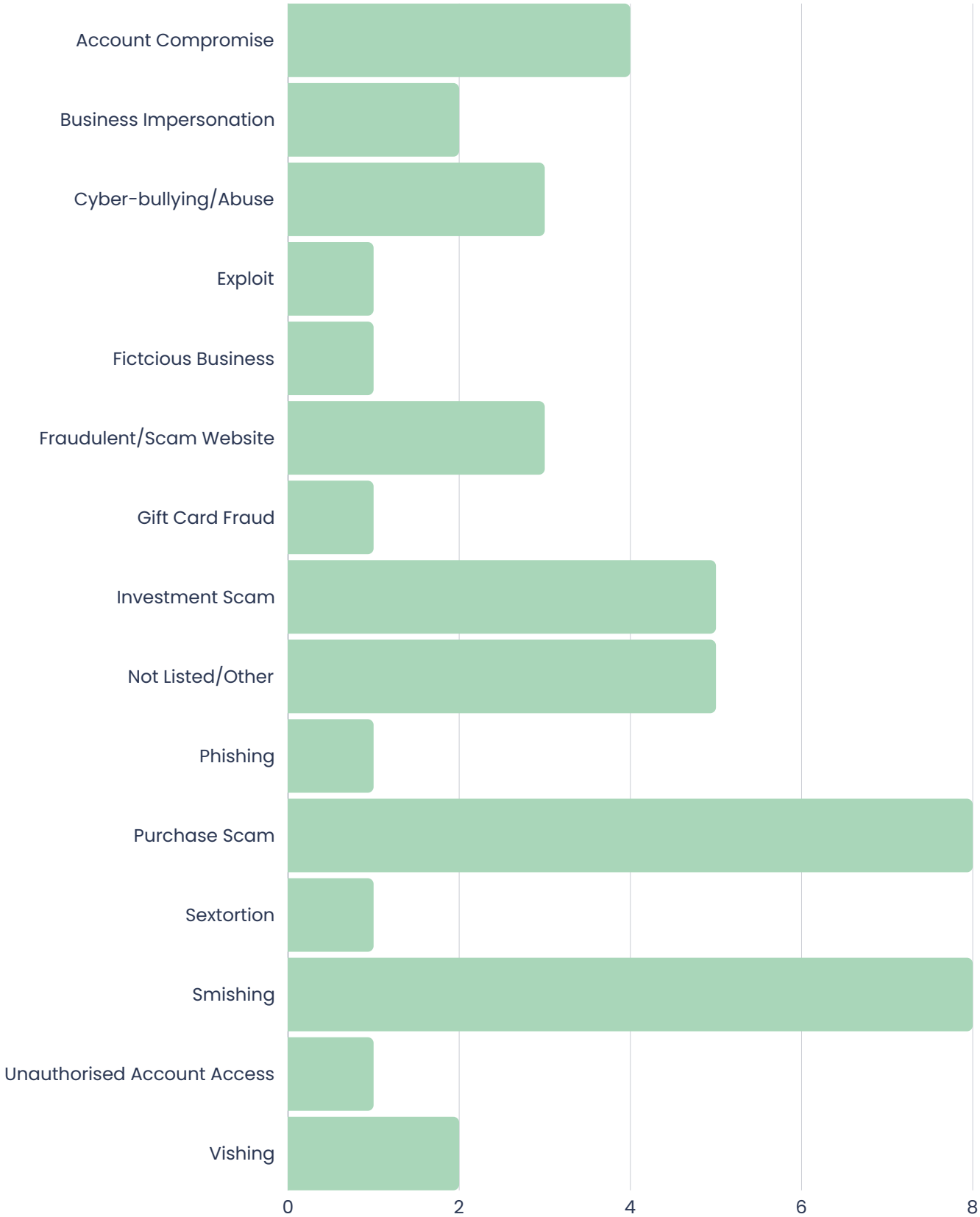
in May and June

Detail

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

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 May and June



ISLE OF MAN THREAT COMMENTARY

PURCHASE SCAMS

FACEBOOK SELLER PURCHASE SCAM

In the period, we were contacted by a local illustrator (the Reporter) who was selling a painting on Facebook. The illustrator then received a message by a fake profile asking the purchase and providing a fake paypal email.

The illustrator was then asked if the scammer could send an additional £300 for the painting to which the illustrator refused. The scammer then got angry and dismissive, further evidencing that this was a scam.

If the illustrator was to accept this offer, it is likely that there would have been an attempt to deceive them by a fake email 'confirming' that the funds had been sent. This would have then been requested to be 'returned' leaving the seller £300 out-of-pocket.

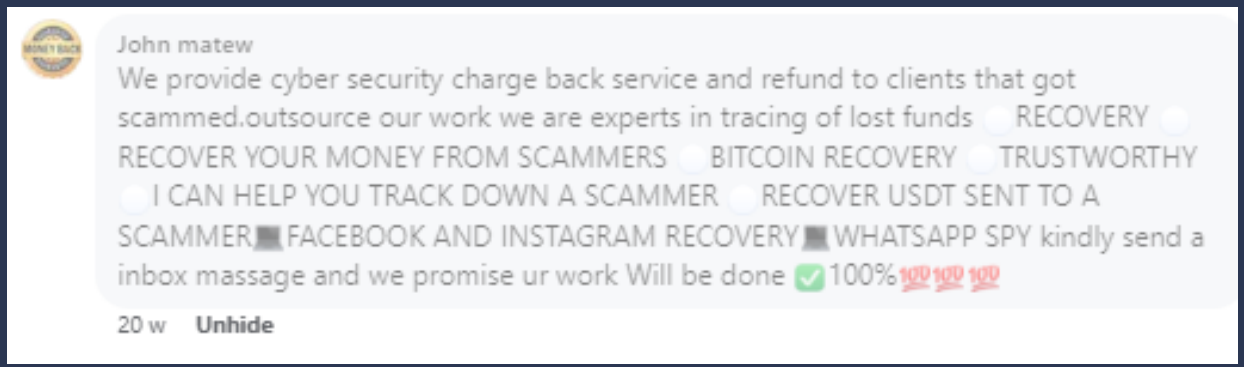
This case shows us that Facebook purchase scams aren't exclusive to buyers, and the criminals have adapted to targeting sellers. By following the old mantra, 'if it sounds too good to be true, it probably is', the Reporter saved themselves the hassle of further dealing with a scammer.

CRYPTOCURRENCY RECOVERY SCAM

In May, a victim of an investment scam communicated with a company that claimed to have recovered the funds that he had lost in the scam.. The company requested that the victim to pay a fee to facilitate the return of these funds. Trusting their claims, the victim made the payments via the Kraken Cryptocurrency platform. Initially, the victim had a balance of $1,600 in his cryptocurrency account and subsequently added two payments of $680 and $300.

In an unfortunate turn of events, the victim unwittingly allowed criminals to have access to his cryptocurrency account, resulting in the loss of all of his funds and his inability to pay anything more. Despite recognising the possibility of being scammed again, the victim of this theft continued to hold out hope that the company was legitimate and could recover his funds upon payment of the fee.

This case highlights the vulnerability of fraud victims to recovery scams, especially when the promise of recovering lost funds is involved. It underscores the importance of scepticism and thorough verification when dealing with entities claiming to offer financial recovery services. Check out our recent piece on recovery scams here.



Facebook Comment advertising fake recovery services

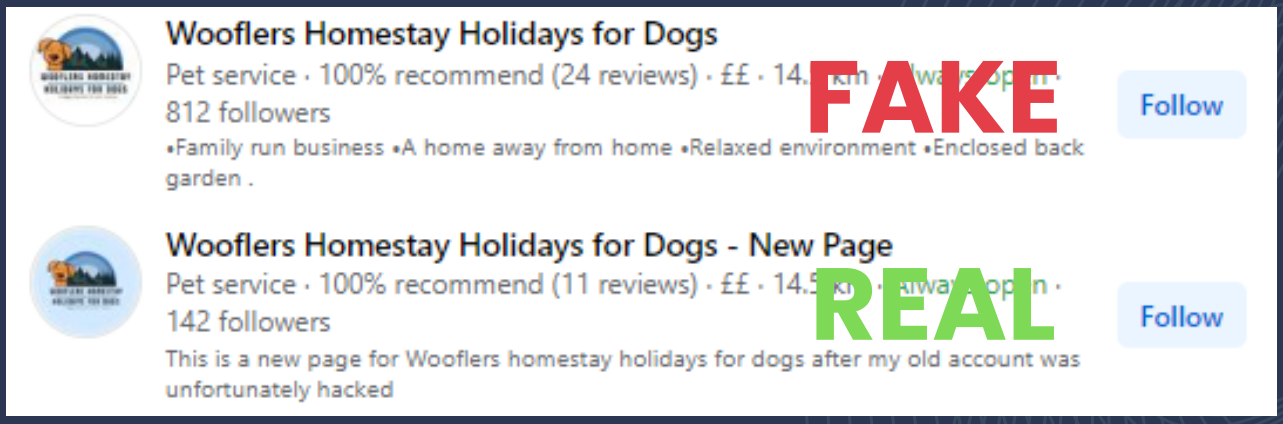
BUSINESS IMPERSONATION

WOOFLERS HOMESTAY FOR DOGS

A member of the public responded to a local Facebook page advertising 'Wooflers Homestay For Dogs', a dog-sitting service. Unbeknownst to him, the page had been compromised, and the legitimate owners had been unable to recover the account or have the page taken down. The victim visited the page, sent a private message expressing interest, and was then invited to pay £60 to a PayPal account that closely resembled the genuine PayPal account (i.e., wooflershomestay.ltd01@gmail.com, whereas the real email address did not have the '01'). The payment was made, resulting in the victim falling prey to the scam.

Wooflers has made a new page, however, Facebook has so far not taken any action to remove the compromised page. Furthermore, the compromise of this page has received media coverage, yet despite the media warning, we are still receiving reports of new victims.

This highlights the importance of doing research before parting with money as googling the company would have returned news articles and their legitimate website. Furthermore, its important for businesses to spread the word of any compromise as much as possible, adding warnings on uncompromised communication channels.



ACCOUNT COMPROMISE

LEAKED PASSWORD LEADS TO MULTIPLE ACCOUNT COMPROMISES

In May, a multi-platform hacking incident occurred involving the unauthorised access to an individual's email, Facebook, and eBay accounts. Prompt actions enabled the recovery of the email and eBay accounts; however, the Facebook account remains compromised. The hacker continues to exploit this account by sending scam messages to the individual's Facebook friends, promoting fraudulent cryptocurrency investments.

The eBay account breach led to unauthorised purchases using a stolen PayPal account. The hacker altered the delivery address to an American location and bought several items. Although eBay intervened to secure the account, a notification from eBay indicated that the fraudulent orders were dispatched, highlighting ongoing issues with the recovery process. The payment for these items was made using a combination of a hijacked PayPal account and a gift card.

Upon regaining control of the email, the individual discovered an alarming message from the hacker. The email confirming the hack, which was sent from the individual's own account, included an old password in the body of the email and it also demanded a ransom payment in Bitcoin to prevent the release of personal details. Refusing to comply with the demand, the individual immediately changed all passwords and implemented two-factor authentication across the accounts.

Despite these measures, frequent alerts from the authenticator app indicate global attempts to access the email account. However, enabling multifactor authentication has allowed the individual to retain control of their accounts.

It appears that the initial compromise was due to passwords obtained through a data breach. These are passwords which have been sold on the Dark Web by criminals who have stolen them from a business the victim was registered for. This highlights the need to change passwords frequently and use multiple passwords across accounts. You can check if your data has been stolen in a breach by using https://haveibeenpwned.com.

FRAUDULENT BUSINESS

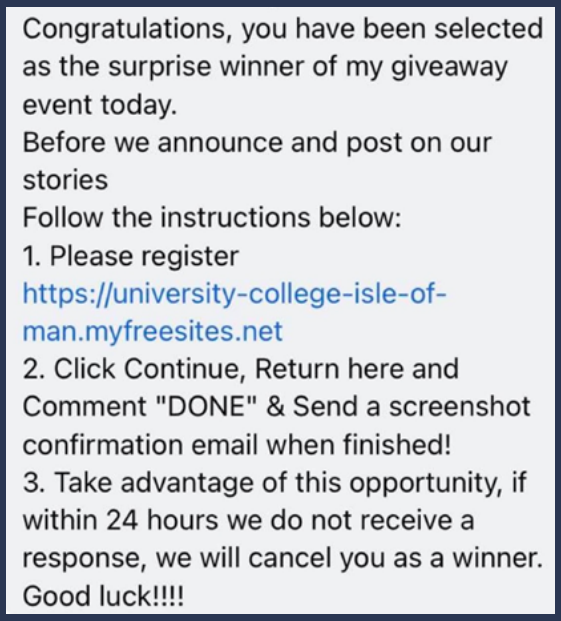
FACEBOOK COMPETITION SCAM

As mentioned in previous threat reports, Facebook competition scams continue to be a problem. During the period, Visit Isle of Man hosted a competition that was 'hijacked' by malicious actors.

On the original post that encouraged users to comment, a fake page was set up that commented under public entries. This comment included a link to a newly set up website, which encouraged users to hand over details in order to 'enter' the competition. These details would have then been used by criminals to take money off potential victims.

It's important to note that these fake pages can be distinguished from the genuine ones through various indicators, such as the absence of an 'author' tag on posts and significantly lower follower counts, post frequency, and creation dates compared to legitimate pages.

Upon receipt of this report, the CSC contacted the website host and had the phishing page taken down.


Congratulations, you have been selected as the surprise winner of my giveaway event today.
Before we announce and post on our stories
Follow the instructions below:
1. Please register
https://university-college-isle-of-man.myfreesites.net
2. Click Continue, Return here and Comment "DONE" & Send a screenshot confirmation email when finished!
3. Take advantage of this opportunity, if within 24 hours we do not receive a response, we will cancel you as a winner.
Good luck!!!!

A similar Facebook competition scam

EXTERNAL THREAT COMMENTARY

RANSOMWARE ATTACK ON CHRISTIES AUCTION HOUSE

A criminal organisation known as RansomHub claimed responsibility for a cyberattack on Christie's, the prominent British auction house. This group posted samples of stolen data on its darknet extortion site, asserting it had obtained sensitive information from Christie's network. This incident targets the world's largest auction house by revenue, serving some of the wealthiest art collectors globally.

Earlier this month, Christie's CEO, Guillaume Cerutti, reported that the company had taken its website offline due to a ‘technology security incident’. Cerutti later confirmed that an unauthorised third-party had accessed parts of Christie's network and exfiltrated some personal data of clients. However, he emphasised that there was no evidence of financial or transactional data being compromised.

Despite these reassurances, RansomHub threatened to publish the stolen data unless a ransom was paid, claiming this would result in fines under data protection laws. Christie's, adhering to regulatory obligations, has refused to negotiate with the criminals and has notified privacy regulators accordingly.

This attack is part of a growing trend of ransomware incidents in the UK, which saw a record number of such attacks reported in 2023. The situation has been exacerbated by delays in government responses due to the recent general election, hindering efforts to reform the approach to ransomware threats. The UK’s national security committee has warned of potential cyber threats to electoral processes, indicating a broader risk to national security from such international cybercriminal activities.

TICKETMASTER AND LIVENATION DATA BREACH

The notorious hacking group ShinyHunters claims to have stolen 1.3 terabytes of customer data from entertainment giants Ticketmaster and Live Nation. This incident has drawn the attention of the Australian Home Affairs, which is currently investigating the breach. ShinyHunters has listed the stolen data for sale on a popular hacking forum for US$500,000.

The compromised data reportedly includes details of 560 million Ticketmaster customers, organised into 16 folders and files, each containing dozens of gigabytes of information. Samples of the data shared by ShinyHunters include hashed credit card numbers, the last four digits of credit cards, expiration dates, fraud details, and personal information such as customer names, addresses, and emails.

A separate hacker on a Russian forum has posted identical data, raising questions about potential connections between the two groups. ShinyHunters has a history of large-scale data breaches, dating back to May 2022, involving companies such as Indonesian e-commerce giant Tokopedia, Microsoft, Wishbone, and AT&T. The group’s leader also administers the BreachForums hacking community, which was recently resurrected after being seized by the FBI and international law enforcement, including the Australian Federal Police.

The group's actions represent a significant international threat, with their activities spanning multiple countries and industries, underscoring the global impact and reach of such cybercriminal enterprises.

MINISTRY OF DEFENCE CYBER ATTACK

A recent cyberattack on a third-party payroll system used by the UK Ministry of Defence (MoD) has had severe repercussions. The attack exposed the personal data of approximately 270,000 serving personnel, reservists, and veterans from all three branches of the British Armed Forces. This incident has sparked significant political outrage and underscored the critical importance of third-party cybersecurity.

Suspected Nation State actors targeted the British Armed Forces in this three-week-long cyber espionage campaign, which aligns with broader patterns of state-sponsored cyber activities. Our detailed timeline document chronicles the attack and provides context on the persistent cyber threats from Nation State actors linked to this data breach. This document includes statements from government officials and critiques from opposition parties, offering a comprehensive overview of the incident.

The breach exposed sensitive information such as identities, bank details, addresses, and national insurance numbers. The prolonged duration of the compromise before detection has raised serious concerns about the security protocols safeguarding military data and the potential for further exploitation.

In response, the MoD took the affected network offline and is advising those impacted on how to monitor their accounts for suspicious activity. Prime Minister Rishi Sunak and other officials have highlighted the gravity of the situation, suggesting that a 'malign actor' is behind the attack. This breach is part of a larger trend of increasing cyber threats against the UK, with over six million attacks recorded on military networks last year alone. The incident emphasises the urgent need for organisations and government bodies to enhance the security of their third-party vendors and supply chains.

CYBER ATTACK AT UK SCHOOL

The Billericay School in Essex experienced a significant cyber-attack during the half-term holiday, potentially exposing the names, addresses, and medical notes of children to criminal access. In a letter to parents, Head Teacher Patrick Berry reported that the contact details of parents and carers might also have been compromised.

While the specific data accessed or exported remains uncertain, Mr Berry assured parents that the school is taking all necessary measures to strengthen its defences against cyber-crime. The school, which had to shut for several year groups on Monday, reopened to all pupils on Tuesday.

The school is collaborating with Action Fraud to investigate the incident. This attack is part of a worrying trend in the education sector, which saw 347 cyber incidents reported in 2023, a 55% increase from the previous year. Government data indicates that most schools and colleges have encountered a cyber-security breach in the past year, often resulting in temporary closures and extended disruption.

This incident highlights the growing international threat of cyber-attacks on educational institutions, emphasising the urgent need for robust cyber-security measures to protect sensitive information

HACKERS TARGET NEW MOVEIT TRANSFER CRITICAL AUTH BYPASS BUG

Threat actors have begun exploiting a critical authentication bypass flaw in Progress MOVEit Transfer, less than a day after its disclosure by the vendor.

The security issue, identified as CVE-2024-5806, allows attackers to bypass authentication in the Secure File Transfer Protocol (SFTP) module, potentially enabling unauthorized access to sensitive data on the MOVEit Transfer server. This vulnerability could allow attackers to upload, download, delete, or modify files and intercept or tamper with file transfers.

Shortly after the bulletin on CVE-2024-5806 was published, the Shadowserver Foundation, a threat monitoring platform, reported seeing exploitation attempts. Network scans by Censys revealed around 2,700 internet-exposed MOVEit Transfer instances, predominantly in the US, UK, Germany, Canada, and the Netherlands.

Progress has released patches for affected versions of MOVEit Transfer:

2023.0.0 before 2023.0.11
2023.1.0 before 2023.1.6
2024.0.0 before 2024.0.2

These fixes are available on the Progress Community portal. MOVEit Cloud customers do not need to take any action as patches have been automatically deployed. Progress has also advised system administrators to block Remote Desktop Protocol (RDP) access to MOVEit Transfer servers and restrict outbound connections to trusted endpoints to mitigate risks until a fix from the third-party vendor is available.

Additionally, Progress disclosed a separate vulnerability, CVE-2024-5805, impacting MOVEit Gateway 2024.0.0, which further elevates the risks associated with CVE-2024-5806. This incident underscores the critical importance of promptly applying security updates and mitigations to protect against rapidly evolving cyber threats.

MOVEit is widely used in enterprise environments, making it a prime target for hackers. Last year, Clop ransomware exploited a zero-day vulnerability in MOVEit to breach and extort thousands of organisations, highlighting the ongoing risks associated with software vulnerabilities in widely deployed enterprise solutions.

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

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

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

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

Disclaimer

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

Open Government Licence

Cyber Security Centre for the Isle of Man

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

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

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

T: +44 1624 685557

Isle of Man Government

Reiltys Ellan Vannin