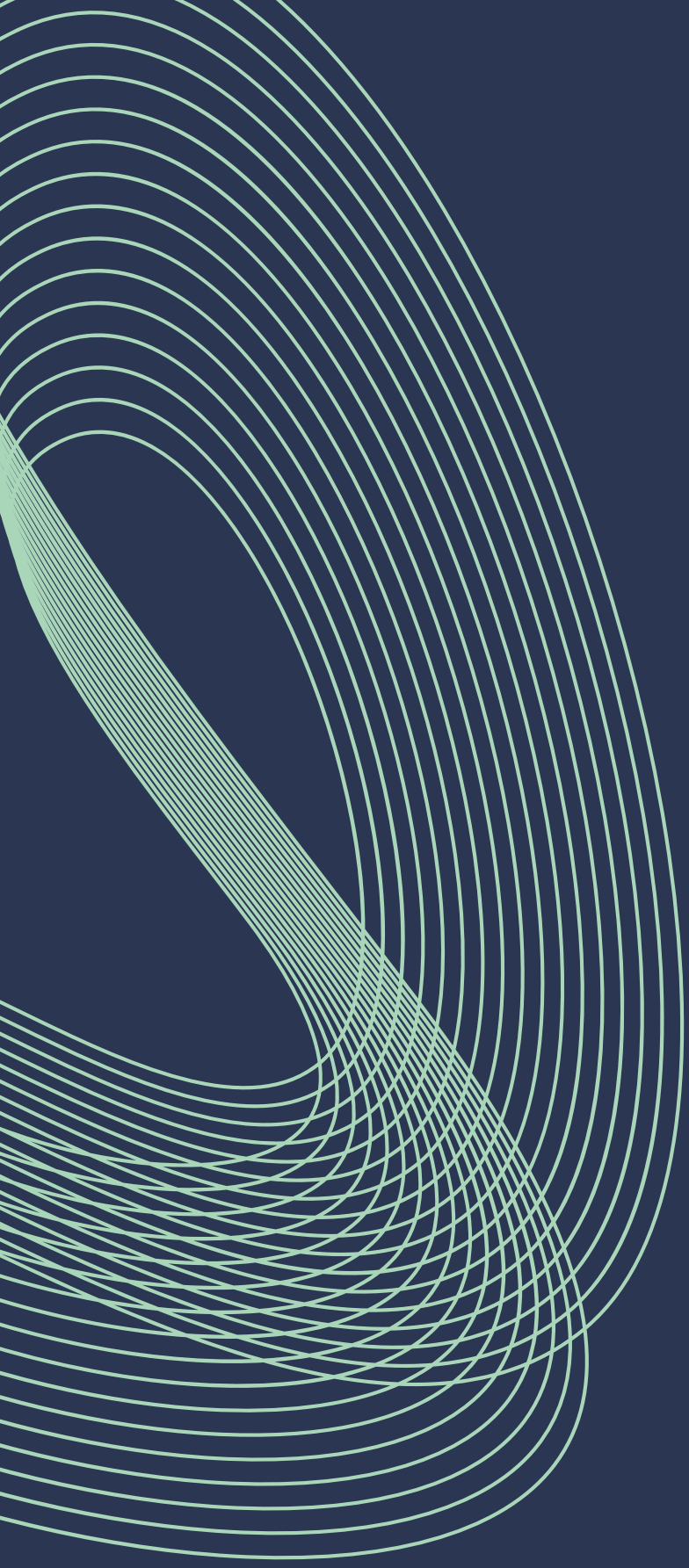
Cyber Security Centre for the Isle of Man

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

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

January - February 2023



INTRODUCTION

For period 1st January - 28th February

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 our own data collected from our reporting points as well as our own intelligence sharing with the private sector.

If anyone has any information they wish to put forward to be considered for this document, please contact the CSC on cyber@gov.im or report it using our online cyber concerns form.

CONTENTS

SUSPICIOUS EMAIL REPORTING SERVICE (SERS)

As part of the Isle of Man Government's Cyber Security Strategy, the Office of Cyber-Security & Information Assurance (OCSIA) introduced the Suspicious Email Reporting Service (SERS) an automated system used to gather intelligence and take down malicious URLs on 23 October 2020.

If you have received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS) 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 11,800 suspicious emails. In January and February 2023 we received 1,154 suspicious emails.

SUSPICIOUS EMAILS

1,154 REPORTED

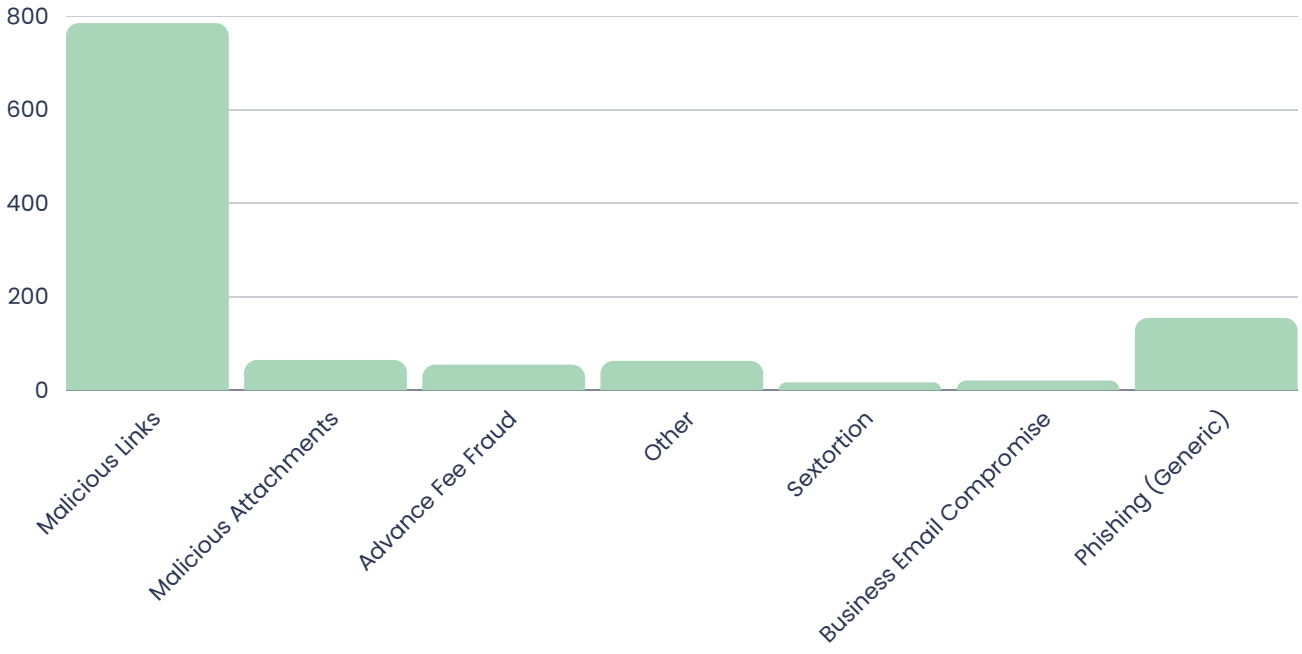
in January & February

Detail

The chart (below) details the type of emails sent by cybercriminals that have been reported to our SERS for the months of January and February. Whilst the infographic (right) showcases the top 5 most impersonated companies and services.

Top 5 Phishing Scams Imitating Popular Services:

1. Manx.net
2. Parcel Delivery
3. Police/Interpol
4. Romance/dating, etc.
5. Antimalware Software



CYBER CONCERNS

99 REPORTED

in January & February

Detail

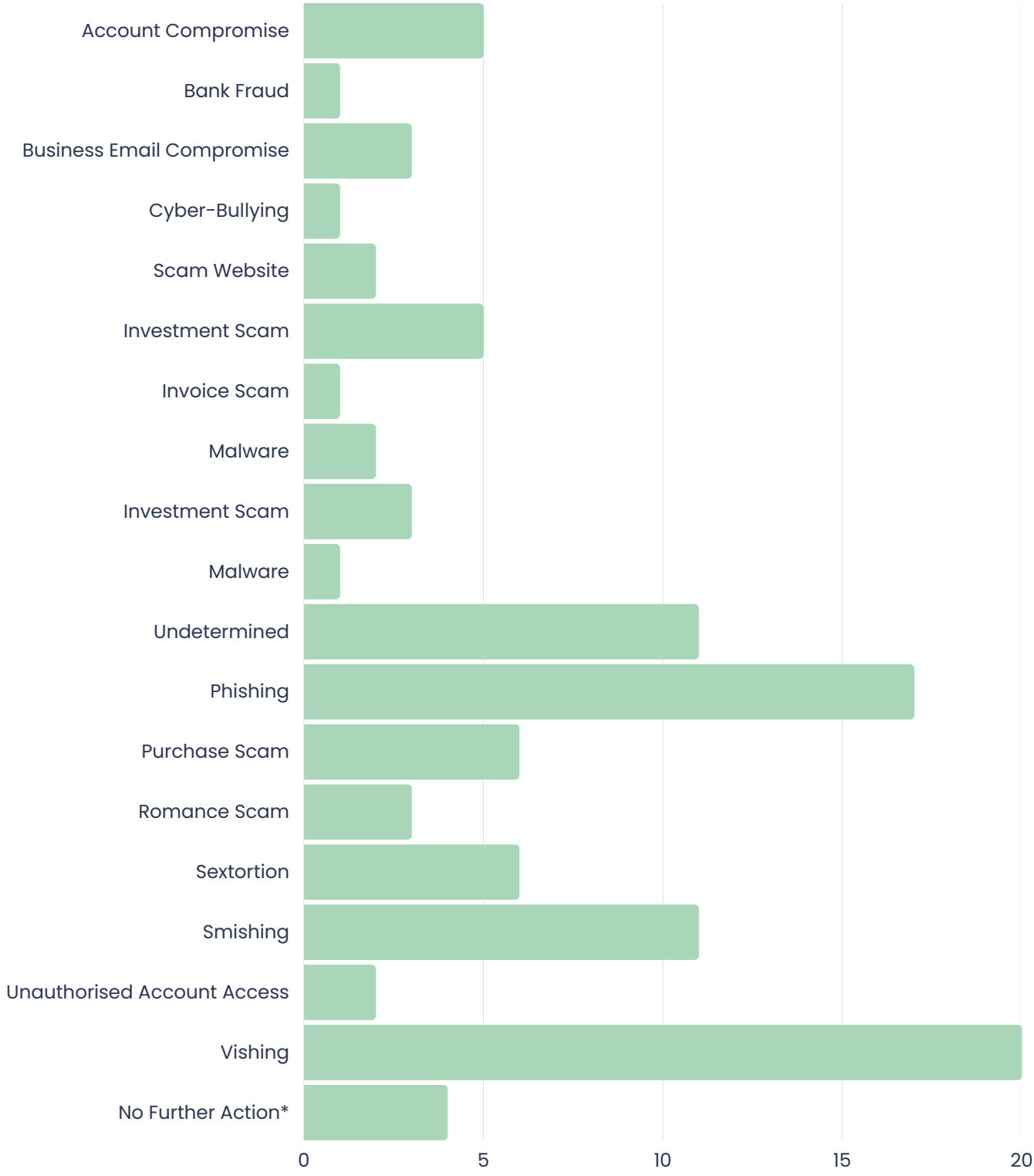
The chart (on page 4) shows a breakdown of cyber concerns reported to us over January and February.

We define a Cyber Concern as a cyber-related issue involving the Internet, email, telephone communications or any other matter involving electronic communications that may or may not have already caused a negative impact.

We use this data from both the public and private sector to build into our threat intelligence and external communications. Where requested, we work with the Constabulary to investigate and provide advice to victims.

Cyber Concerns differ from our Suspicious Email Reporting Service as the primary reporting point for any cyber concern that is not a phishing email. Often cyber concerns involve an already-affected victim or those seeking advice.

Cyber Concerns January & February



***No Further Action:** submitted with good intentions but after further investigation was found to be a non-cyber concern or communication was found to be legitimate.

ISLE OF MAN THREAT COMMENTARY

In order to gain a more detailed understanding of the types of incidents that are contributing to trends, this section presents case studies of specific threats outlined on pages 3 and 4. These case studies, all taken from our cyber concerns reporting tool, provide insight into the methods and motivations of attackers, as well as the impact that these attacks have had on the affected parties.

PHISHING (EMAIL)

INTERPOL-CONSTABULARY

Over the period we received 96 reports (through both SERS and Cyber Concerns) regarding Interpol-Constabulary impersonation. The emails contained a PDF bearing the Constabulary badge and 'signed' by a member of the Constabulary. The person named is an actual serving officer and his name was mentioned to make the email seem legitimate.

The email told the recipient that they had committed crimes involving sexual assault, including that of minors, and invited recipients to get in touch with a provided number.

The Isle of Man was not unique being targeted, with other jurisdictions being hit at roughly the same time.

What is particularly concerning is the use of an existing officer's name and the Isle of Man Constabulary badge. This combined with classic techniques of social engineering, such as creating urgency and panic, led both ourselves and the Constabulary to be worried about the number of potential victims.

Targeted phishing campaigns are not uncommon but the nature of this meant both ourselves and the Constabulary quickly issued warnings on our social media sites.

PHISHING (SOCIAL MEDIA)

Whilst phishing is commonly-associated with email it can occur through other media. Over the period we received multiple reports of phishing occurring on Facebook, whereby a question or quiz was posted on popular local groups and members invited to respond. Once a member responded they were invited to talk over messenger to then provide details to claim a prize.

In some cases, details were requested for their Facebook account which then allowed the scammers to take over the victim's account. In others PayPal details were requested in order to take money out of their PayPal account. Some victims reported that they were asked to transfer money (usually in the hundred's of pounds) to an account from which details would be 'verified' before receiving their prize money.

ROMANCE FRAUD

Valentine's day did not generate the volume of reports that might have been expected with only 3 issues reported.

Despite this, romance scams are reported regularly throughout the year and can have both a serious emotional and financial impact on victims. We are aware of instances where victims have sent over £10,000 in the hope of their online partner visiting the Island. All romance scams involve manipulating the victim and preying on any potential vulnerabilities they may have. Social engineering is used to gain the victim's trust and to make them lower their guard to the reality they're being scammed.

Often it takes a significant period of time (and financial loss) for a victim to finally recognise that their online partner doesn't exist. We sometimes receive reports from concerned family or friends who are struggling to get their loved one to accept that they're a victim.

CLICK HERE TO READ 'HELPING A LOVED ONE CAUGHT IN AN ONLINE ROMANCE SCAM'

BUSINESS EMAIL COMPROMISE

INVOICE SCAMS

We were made aware of a local financial services company with a number of clients, one of whom had their email account compromised.

The scammers sent an email to the Island-based company with a modified email requesting an amount in the hundreds of thousands of pounds. This was paid and only upon later correspondence with the client was it revealed that the communication was illegitimate.

Whilst there is no fault on the business' side, this instance is a reminder to remain sceptical even when liaising with trusted partners. Whilst you or your business's cybersecurity may be resilient and trusted, that same level of trust should not apply to third-parties regardless of the existing relationship. It is important to report incidents immediately through our cyber concerns reporting form.

PURCHASE SCAMS

ILLEGITIMATE BUSINESS WEBSITES

We have received multiple reports over the period of victims buying goods from websites and not receiving them. Often these websites offer goods well below the typical market rate, therefore inviting potential victims to make a purchase.

To avoid such instances, we recommend any customers only use vendors they trust and to check that there is an HTTPS connection as well as reviewing company information on databases such as Companies House.

Any victim of a purchase scam with undelivered goods should be cautious that their payment details could be in the hands of scammers who could charge them at any point. Contacting your bank immediately after you have realised that you have been scammed is highly-recommended, whilst using payment gateways such as PayPal will offer you more protection.

SMISHING (MESSAGING SCAMS)

BOOKING.COM-ISLE OF MAN BANK

This month saw a unique, targeted scam were victims where targeted by both Vishing and Smishing by scammers claiming to be from either booking.com or Isle of Man Bank advising them there had been a charge to their account of over £2,000.

Due to the quick influx of reports we quickly disseminated a warning message to Island residents.

What makes this scam unique was the combined nature of both smishing and vishing. This added a sense of legitimacy to the communication, as it provided two forms of 'evidence' for potential victims to receive. In addition, reference to the Isle of Man Bank indicates that this scam was targeted specifically at Island residents rather than some of the more generic smishing attempts that we see.

PARCEL DELIVERY TEXTS

Text messages claiming to be from a parcel delivery service have been reported over the period.

The scam involves a text being received requesting payment to release a parcel for delivery, or asking the message recipients to update contact details.

Card details are then entered by the victim to either pay the 'small charge' or to verify contact details.

An amount much higher than the stated cost is then taken from victim and their card details kept; with the victims only option to cancel the card.

CLICK HERE OR SCAN TO SEE OUR ADVICE ON SMISHING.

INVESTMENT SCAMS

CELEBRITY ENDORSEMENT

There were numerous reports of victims seeing adverts on Facebook and other websites for an investment scheme endorsed by celebrity Holly Willoughby as well as a 'local Manx resident' with the promise of making a potential-victim rich.

The scammers then took the conversation to WhatsApp where details and photographic ID were requested. It seems that the victims of the scam were then asked to enter their financial information into an online form on the scammer's website, with money being taken from the victims account upon sending this information.

OTHER

UNKNOWN USB

A local financial services company was sent a USB stick direct to their address without any contextual information or prior communication. This USB was then sent to us for investigation.

Untrusted USB sticks present a significant threat to any organisation as plugging one into a computer connected to your network allows direct access to any criminal, from this they can install various forms of malware, steal data, and even deploy ransomware. One of the most prominent examples of the dangers was Stuxnet which managed to infect the closed network of Iranian uranium enrichment plants through USB drives.

The business is to be commended for its vigilance in not connecting the device without checking. We recommend you seek skilled advice or support in such circumstances.

EXTERNAL THREAT COMMENTARY

Whilst geographically separate, the Isle of Man still belongs to an interconnected digital world, therefore, understanding external cybersecurity threats is crucial for protecting digital systems and personal information. These threats can originate from various sources and cause significant damage.

ROYAL MAIL CYBER ATTACK – LOCKBIT – RANSOMWARE

On Wednesday, 11 January, Royal Mail was hit by a devastating ransomware attack that halted international deliveries for six weeks. The financial effects of the attack for Royal Mail and businesses are significant and come at a time when the beleaguered postal service faces restructuring and renewed strike action.

Only hours after the attack, the LockBit group claimed responsibility and presented their ransom demands. Negotiations were carried out over three weeks with the deadline for payment being the 9 February; Royal Mail did not pay the ransom.

Conversations between Royal Mail and the LockBit group were later leaked to the public, possibly as a deterrent for other organisations who refused to pay and likely also as punitive action. Whilst such disclosure of negotiations by a ransomware group is not something commonly-seen, it is becoming more prevalent and potentially marks a new attack vector pressure tactic. Such disclosure provides a fascinating insight into the techniques employed by threat-actors. These included a demonstration of the decryptor and a reduction in the ransom amount from £65.7 million down to £57.4 million.

The negotiations also demonstrate the sophistication of these groups with the adoption of business models such as marketing and customer service departments.

COINBASE SMISHING

A cyber-attack on the cryptocurrency trading platform, Coinbase, demonstrates the care that needs to be taken when dealing with texts or messages from unknown senders and the additional security provided by multi-factor authentication.
In early February, Coinbase employees received text messages telling them to log into the company's systems urgently. A link was provided in these messages that led to a phishing page.

One Coinbase employee provided the requested data to the attackers, however, these attackers did not have the second authentication-factor needed to access the company's systems. The attackers then switched tactics by telephoning Coinbase employees whilst pretending to be colleagues from I.T. An attacker asked a staff member to log into their computer systems and install remote-desktop software that would allow them remote-access to the employee's computer. Fortunately, the company's response team was alert to the unusual activity on an employee's computer and quickly intervened before access was gained.

GO DADDY REDIRECTS

The hosting and domain name company, Go Daddy, has recently reported that it has been the target of persistent attacks over the last few years with the most recent attack being in December 2022. Owing to past customer complaints, GoDaddy believes previous breaches in 2021 and 2020 were all part of the same attack-campaign.

It appears that a 'sophisticated threat actor group' has targeted the company by redirecting customer websites to malicious websites. It is unknown how the threat-actors gained access to deploy malware on GoDaddy's cPanel shared hosting servers. It appears that attacker's used known-compromised credentials to log in and leave vectors for re-entry. The company has now remediated the situation to prevent future attacks and has also provided recommendations for customers to secure their accounts and review their credentials.

JD SPORTS DATA BREACH

On 30 January, the Sportswear-chain JD Sports was the victim of a cyber attack that claimed to have put the data of 10 million customers at risk. JD has stated that information that 'may have been accessed' by hackers included names, addresses, email accounts, phone numbers, order details and the final four digits of bank cards. The data related to online orders placed with JD brands, size?, Millets, Blacks, Scotts and Millet Sport between November 2018 and October 2020.

Although passwords and full payment data has not been access, JD Sports are advising customers to be to be vigilant about potential scam e-mails, calls and texts from fraudsters who could use the hacked data.

JD Sports has said it would be taking measures to strengthen its security to prevent a future attack and that it is working with 'leading cyber-security experts' and with the UK's Information Commissioner's Officer (ICO).

LASTPASS ATTACK DEVELOPMENTS

LastPass have recently disclosed more details of second attack that targeted its infrastructure. An explanation has been long-awaited given the questions many have had about how the vault could have been compromised despite having certain security safeguards.

This second attack, which was made from 12 August 2022 until 26 October 2022, was made possible by exploiting a vulnerability in a third-party Plex-based media package and by installing a keylogger on a LastPass DevOps engineer's personal computer. The hacked DevOps engineer was one of only four employees who had access to the company's personal vault. The keystrokes on the engineer's computer were recorded and enabled the hacker to acquire the password for LastPass's vault. The hacker then exported the information from the vault, which include 'including the decryption keys needed to access the AWS S3 LastPass production backups, other cloud-based storage resources, and some related critical database backups.'

THREAT FOCUS: PHISHING

Phishing is when criminals masquerade as a legitimate person or organisation in an attempt to trick people into following out instructions that can lead to personal or sensitive information being stolen or to the installation of malicious software (malware). Phishing can be conducted over email, social media and other messaging platforms. Phishers also use voice calls (vishing) and SMS text messages (smishing). They will typically request the user to click a link or open an attachment. Doing so can result in malware being downloaded and installed or lead to malicious websites that aim to steal your data.

Many phishing emails will have poor grammar, punctuation and spelling but that isn't always an indicator. Criminals are improving their techniques and some can be difficult to identify. However below lists some the consideration you should make.

- Is the design and overall quality what you would expect from the organisation the email is supposed to come from?
- Is it addressed to you by name, or does it refer to 'valued customer', 'friend', or 'colleague'? This can be a sign that the sender does not actually know you.
- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'click here immediately'.
- Look at the sender's name and email address. Does it sound and look legitimate, or is it trying to mimic someone you know?
- If it sounds too good to be true, it probably is.
- Your bank, or any other official source, should never ask you to supply personal information from an email.
- Sometimes they are actually original emails coming from a compromised account. so if its not expected it is worth investigating. No matter who it comes from.

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 25th May 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 Office of Cyber-Security & Information Assurance (OCSIA) was established by a Council of Ministers Directive in October 2017. In March 2023 we established the Cyber Security Centre for the Isle of Man (CSC) which is our public facing body providing advice, guidance and practical support to Island residents and businesses.

The CSC acts as the focal point in developing the Island's cyber resilience, working in partnership with private and third sector organisations across the Island alongside the wider population. As a part of OCSIA the CSC works in the public sphere whilst OCSIA focuses on Information assurance within Government.

We are committed to supporting Island-residents and businesses by providing practical and targeted advice and guidance. This includes working in partnership with the private sector to improve their cyber resilience and raise awareness about the latest cyber threats affecting our Island.

OCSIA also hosts an annual conference 'CYBERISLE' which is held over the course of one day, and helps business leaders, individuals, community and charitable organisations understand the rapidly changing cyber-security threat landscape.

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

CSC Cyber Security Centre for the Isle of Man

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

www.ocsia.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