ANNUAL CYBER THREAT UPDATE

2024

With a year of Threat Updates, we take a look a some of the most notable cases and trends in 2024.

INTRODUCTION

Welcome to this special 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 reported to us using data collected from our reporting points as well as intelligence obtained from partner agencies and open-source services.

We have published advice and guidance for the contents covered in this report, which can be found on our website here.

CONTENTS

OVERVIEW

+50.7%

9,372

Total emails reported to SERS

-29.1%

497

Reported Cyber Concerns

+159.8%

£2,240,478

Reported financial losses, from our cyber concerns reporting point

All reports pose a challenge in categorisation, as some may align with multiple categories. Accordingly, we have assigned the category that matches most closely with the available information.

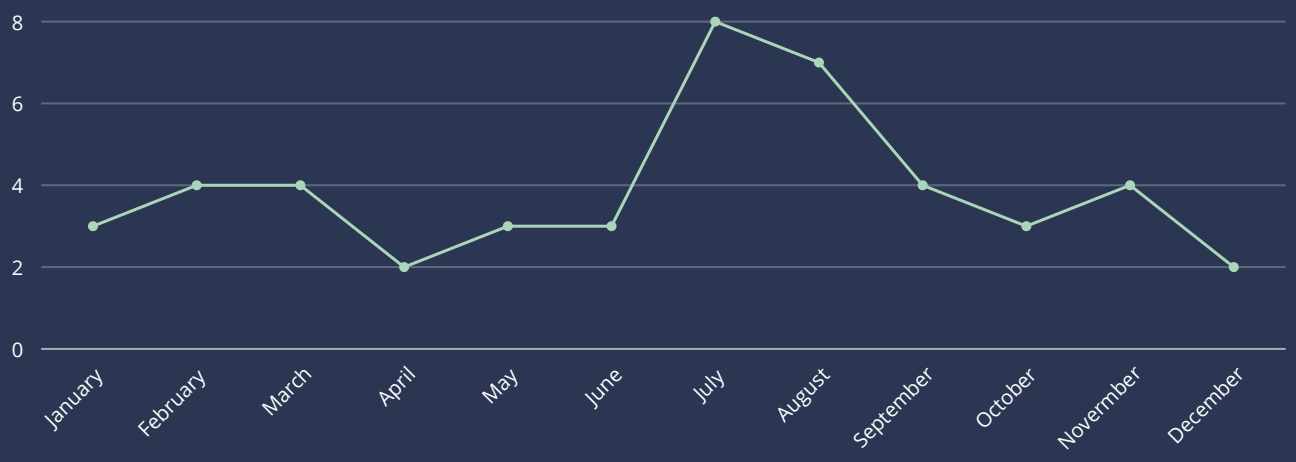
Despite the striking financial figures presented above, it is anticipated that the actual values will prove to be **notably higher** as cyber crime is vastly unreported.

THREATS

ACCOUNT COMPROMISE

Account compromise refers to the unauthorised access or takeover of an individual's or organisation's online account by a third-party, often with malicious intent. Account compromise poses a significant security risk and can lead to data breaches, financial losses, and damage to an individual's or organisation's reputation.

In the context of the Isle of Man, account compromises have typically involved the imitation of local businesses to acquire credentials.



CASE STUDY - MANX NET

Over 60 accounts were compromised in a targeted phishing attack using Manx Telecom and Manx.net branding, where victims received emails claiming their accounts would be closed unless they updated their details. These emails led to phishing pages that captured login credentials, giving attackers access to the accounts. The attackers either locked users out by changing passwords or remained undetected, using the accounts to send fraudulent emails and execute gift card scams. Victims, believing the emails were from trusted contacts, were coerced into purchasing gift cards and providing the scammer with the codes. In response, accounts were suspended, and users were advised to enable multi-factor authentication (MFA) and use stronger passwords to prevent future attacks.

Most of the account compromises were identified through SERS and are therefore not reflected in the number of cyber concerns reports.

47
Reported Cyber Concerns

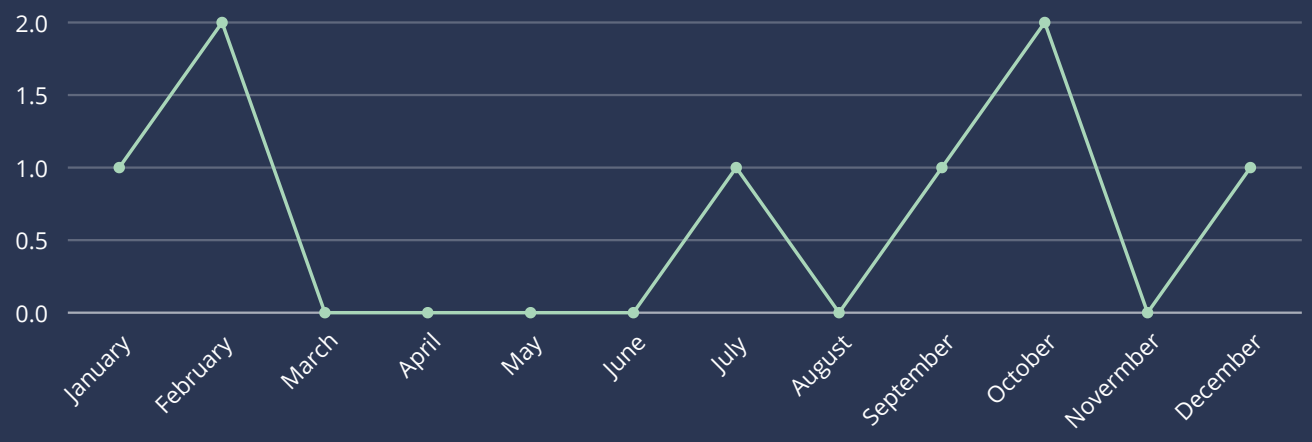
£113,472
Reported financial loses

£95,000
Largest Reported Loss

BANK FRAUD

Bank fraud refers to the deliberate and illegal act of using deceit, trickery, or false means to obtain money, assets, or other property owned or held by a financial institution. These include corporate service providers, a significant sector in the island's economy.

As with all categories, if we can positively identify another method by which a criminal activity was conducted, such as business email compromise, the report will go into the most appropriate category. Therefore, not every cyber incident conducted against a financial institution appears here.



CASE STUDY

A complainant experienced fraudulent transactions on their Wise accounts, totalling £10,501.84. The transactions affected both their corporate and personal accounts (£7,591.97 and £2,909.87, respectively), along with a Wise credit card transaction of £650, which had five prior failed attempts before being processed. The funds were transferred via a SWIFT Code and IBAN to an individual in Ukraine.

Cybercriminals can be persistent and may attempt to secure smaller payments before embarking on larger amounts

8
Reported Cyber Concerns

£11,836
Reported financial loses

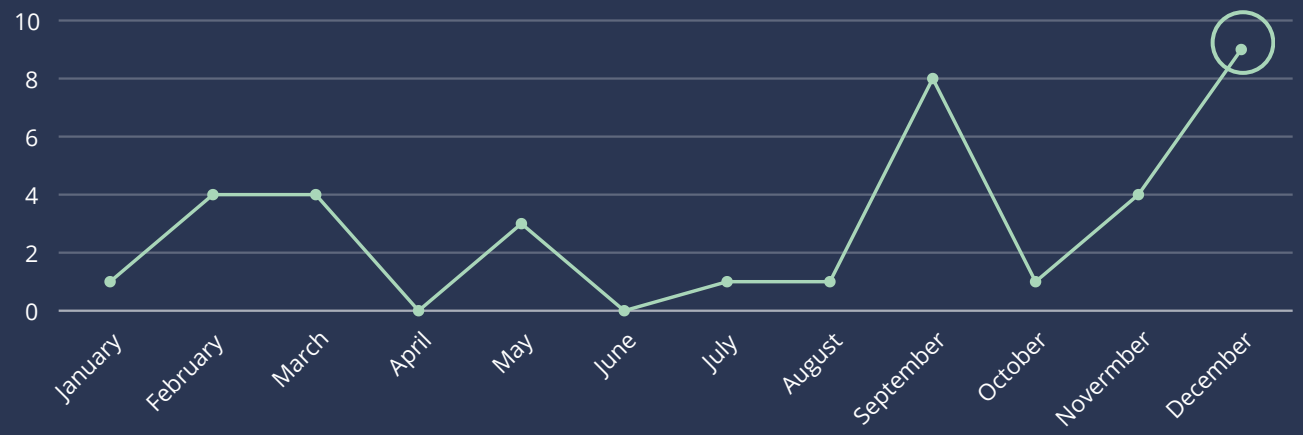
£1479
Average financial loss per report*

**Some reports had no financial loss attributed*

FRAUDULENT/SCAM WEBSITE

Fraudulent/Scam websites involves the false misrepresentation of a legitimate website or a website set-up for the sole purpose of criminal activity.

In the period, we only received thirty-six external cyber concerns reports, of which a significant number involved the impersonation of Bus Vannin/Isle of Man Transport.



CASE STUDY

In December we became aware of a Facebook page called 'Public Transport Isle of Man', along with similar variations, using stock images and official logos to advertise six months of free travel for £2. The adverts reached a significant portion of the Isle of Man population.

These ads linked to an external site that asked generic questions before directing users to click on pictures of gift boxes. The second box always revealed a 'prize' of cheap travel, leading to a page requesting personal and card details and initiating a €2 charge (foreign currency being a strong indicator this was a scam). This is seen in the relatively low financial figures shown below, comparative to the number of reports.

Victims later reported further unauthorised charges and spam emails. We advised them to contact their banks to cancel or freeze their cards.

Despite clear fraud and misuse of branding, removing these scam ads has been difficult due to Facebook's procedures and slow reporting process. Several red flags indicated a scam: the page had few followers, was newly created, and charged in euros. A genuine offer would have been covered in legitimate news outlets.

Websites are a useful tool for cyber criminals as they provide another online presence to add legitimacy to their scams.

36	£844	£23.44
Reported Cyber Concerns	Reported financial loses	Average financial loss per report*

**Some reports had no financial loss attributed*

GIFT CARD FRAUD

Cybercriminals will use a range of techniques, including impersonating a work colleague, friend or family member, in order to get you to purchase gift cards. The cards are then redeemed by the cybercriminal and it is incredibly difficult to retrieve funds.

In the period, we only received eleven external cyber concern reports, with the majority of scams being reported through SERS. This underscores how underreported cybercrime is, and with the significant funds involved and the difficulty in rectification, this is an important area to highlight.

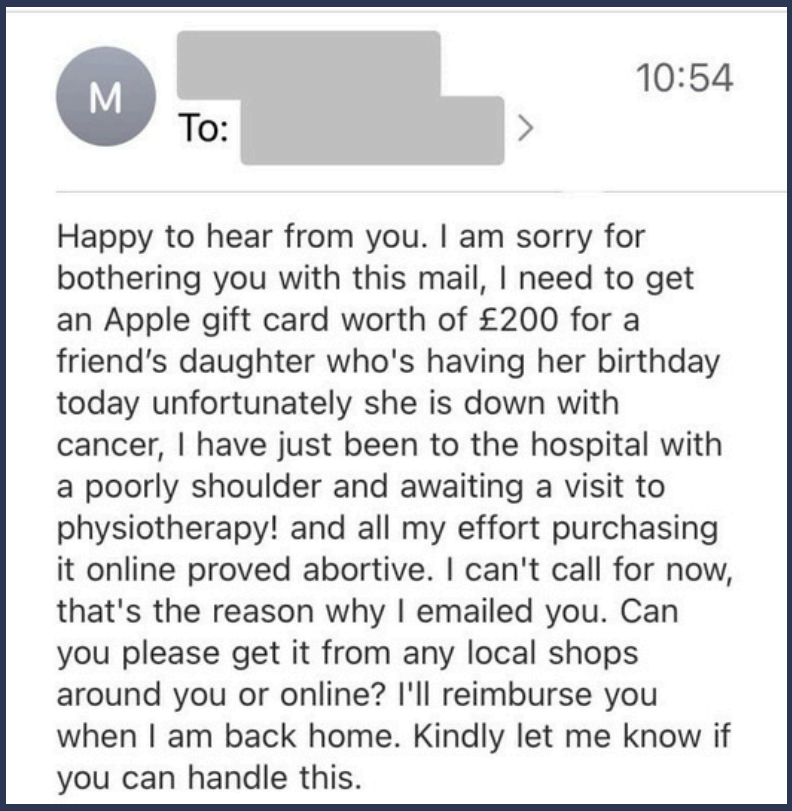
Typically, gift card fraud is commonly associated with business emails. An example of this (below) is an attempted gift card fraud. However, we are noticing a trend of scammers diversifying their targeting methods.

CASE STUDY

Gift card fraud has become prevalent in 2024, as a direct consequence of the many Manx.net email accounts that have been compromised.

Once victims had their accounts compromised, scammers would use them to send out gift card scams to anyone in the contact list. This included family, friends, and businesses.

Whilst easier to identify for organisations, there were a number of victims who believed a relative or close friend was legitimately reaching out for help.



11
Reported Cyber Concerns

£2,150
Reported financial loses

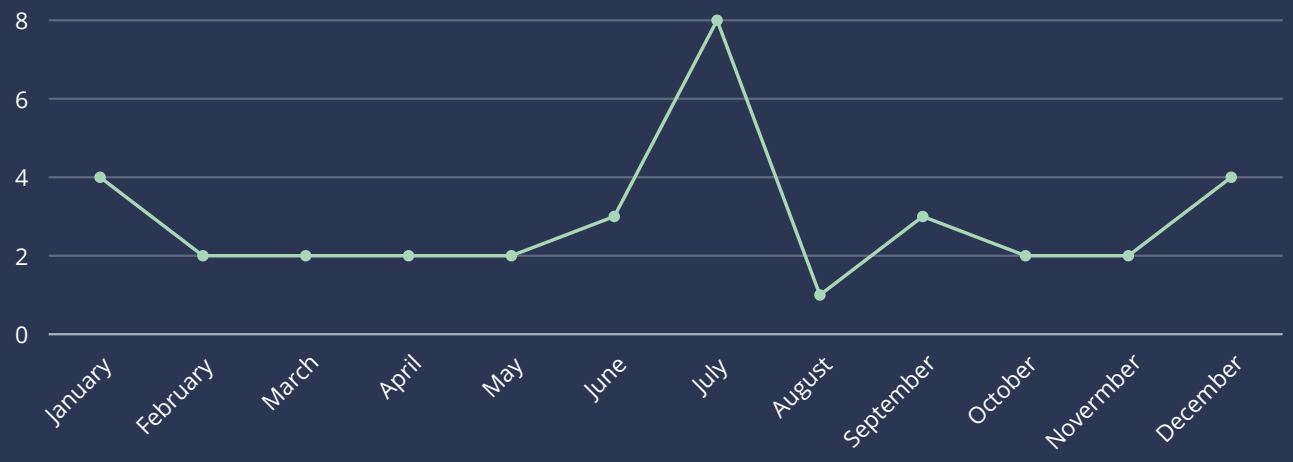
£195.45
Average financial loss per report*

**Some reports had no financial loss attributed*

INVESTMENT SCAMS

Investment scams are on the rise and criminals employ diverse tactics to deceive unsuspecting individuals. They frequently exploit a persons interest in shares or cryptocurrency: enticing victims with promises of rapid returns. However, in many instances, these supposed shares or cryptocurrencies are non-existent.

Investment scams are by far the largest contributor to the overall losses on the Isle of Man, as each victim often transfers significant amounts of money as they are shown or transferred some 'returns' on their 'investments'. In reality the money is never invested and victims are duped by flashy website graphics and as often mentioned, if it's too good to be true, it probably is.



CASE STUDY

Around £125,000 was lost in March and April. One victim lost over £85,000 after investing in cryptocurrency through a fake trading platform, while others were deceived by fraudulent schemes using false celebrity endorsements, including Jeremy Clarkson and Richard Hammond. Reported scam platforms included 'Crypto.com Trust,' 'Delta-Stock.com,' and 'OnePlusCapitalCSD' however criminals will use any website to add legitimacy to their operation.

Scammers posed as traders, making initial contact with victims online and then calling victims multiple times a day and pressuring them to deposit more money. This was incentivised by displaying supposed rapid profits encouraging victims to increase their returns. Many of these scams involved remote-access software like AnyDesk, which cybercriminals use to monitor victims' activity, steal passwords, misuse digital certificates, and launch potential supply-chain attacks.

35

Reported Cyber Concerns

£1,278,920

Reported financial loses

£36,540

Average financial loss per report*

**Some reports had no financial loss attributed*

INVOICE SCAM/FRAUD

An invoice scam is a type of fraud where criminals send fake invoices to businesses or individuals, hoping they will pay without verifying the details. Scammers may impersonate legitimate suppliers, use phishing tactics, or intercept real invoices and alter payment details to divert funds to their accounts.

CASE STUDY

In September 2024, a local organisation lost £37,640 in an authorised push payment (APP) scam after an employee's email account was compromised through phishing. The attacker, posing as a trusted entity, sent urgent emails with fake invoices, prompting multiple fraudulent payments. The scam remained undetected for weeks until a routine review identified breaches of internal payment procedures.

An investigation revealed the attacker tricked the employee into entering login credentials and a two-factor authentication (2FA) code on a malicious site, granting full access to the email account. This allowed them to manipulate communications and request payments without suspicion.

In response, the organisation secured the compromised account by resetting the password, terminating active sessions, and reviewing email rules for unauthorised changes. They also implemented enhanced email security measures, Security Awareness Training (SAT) to educate employees on recognising phishing attempts, and Managed Detection and Response (MDR) for Microsoft 365 to monitor for future threats.

To further prevent similar incidents, the organisations should include verification procedures such as the 'three-eyes check', where at least two additional employees must review and approve payments before processing. This extra layer of oversight helps detect anomalies, ensuring fraudulent transactions are identified and stopped before funds are transferred.

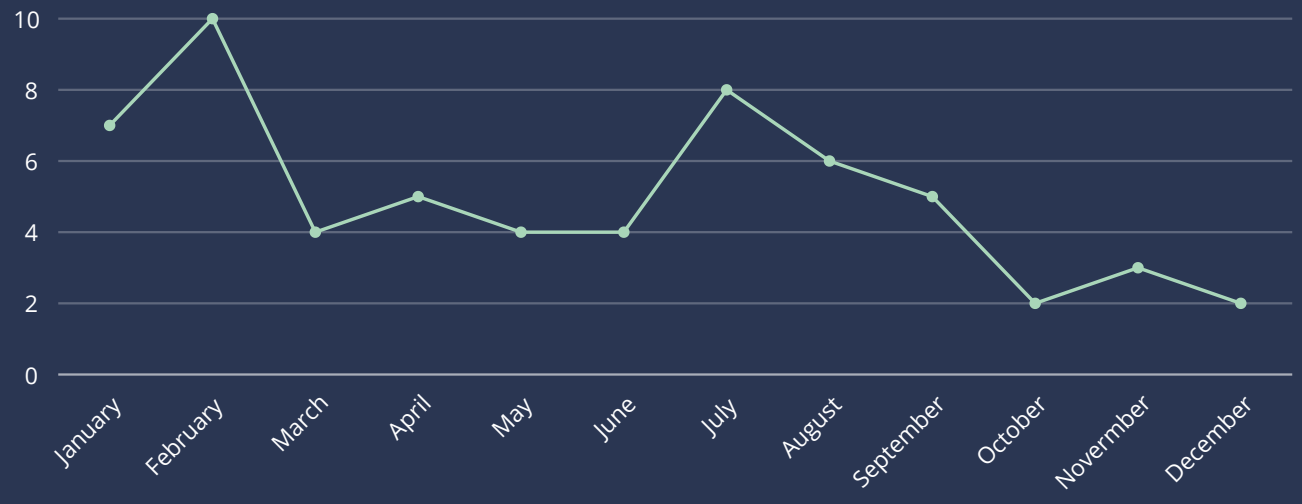
5	£44,540	£8,908
Reported Cyber Concerns	Reported financial loses	Average financial loss per report*

**Some reports had no financial loss attributed*

PURCHASE SCAMS

Purchase scams occur both in the real world and online. However, Island residents can be targeted from all over the world online, making any recovery of funds extremely difficult. There is significant variety in purchase scams, from pets to flat deposits; however, the common trend is a lack of precaution that would occur in real life. Scams involving Facebook make up a significant number of reports. However, Facebook is simply the vehicle used to facilitate criminal activities.

Typically purchase scams are often of a smaller amount (comparable to other scams) but are far more frequent.



CASE STUDY

A buyer on Facebook Marketplace attempted to purchase garden furniture for £200 and sent a £30 delivery fee via PayPal's 'goods and services' option. The seller falsely claimed they hadn't received the payment because it wasn't sent via the 'friends and family' option, which lacks buyer protection. Suspecting a scam, the buyer blocked the seller on Facebook Messenger and WhatsApp. Days later, they received an unexplained £115 deposit from a stranger. Concerned, they contacted their bank, which reversed the deposit, cancelled their card, and secured their account.

In another case, a buyer ordered a neon sign from a Facebook seller, making three payments totalling £34 via PayPal's 'friends and family' option. The seller never delivered the item, and since 'friends and family' payments lack buyer protection, the victim couldn't dispute the transactions despite having proof of chats and payments.

60
Reported Cyber Concerns

£24,204
Reported financial loses

£403.40
Average financial loss per report*

ROMANCE SCAMS

The bulk of the £40,500 below comes from just two reports; however, other reports allude to other victims sending significant amounts of money to cybercriminals. Those figures we cannot confirm have not been included, and we suspect the actual figure for romance scams to be very much higher.

What is particularly worrying about romance scams is the emotional impact they have on the victim and their close friends and family. 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.

CASE STUDIES

Two scams over the year highlight that whilst financial losses weren't incurred, scammers will invest significant amounts of time to manipulate victims in the hopes of conning them out of money.

In the first case, a scammer posing as 'Alice Wellberk' on Meetisleofmansingles.co.uk used WhatsApp (+44 7908 922293) to gain trust by sharing explicit content before attempting to obtain the victim's bank details. The individual, unaware of such scams, reported the incident to the police and blocked the scammer before any money was lost.

In the second case, another victim was targeted by someone claiming to be 'Chery Jenny Bryce' a U.S. Army soldier. Communicating via WhatsApp (+1 920 939 9442), the scammer sought personal details and pressured the victim to pay fake parcel tracking fees. This person is known to have lost £150 by paying a fake medical invoice, but it is thought over £400 was lost. This is recorded under Invoice Fraud.

Towards the end of the year we received the report of a £25,000 loss. Whilst details were limited, we know the victim believed they were sending money to a male from Nigeria. The £25,000 was sent in various payments over a longer period, with the final payment sent in the hopes of the love interest coming to the Island to marry.

7
Reported Cyber Concerns

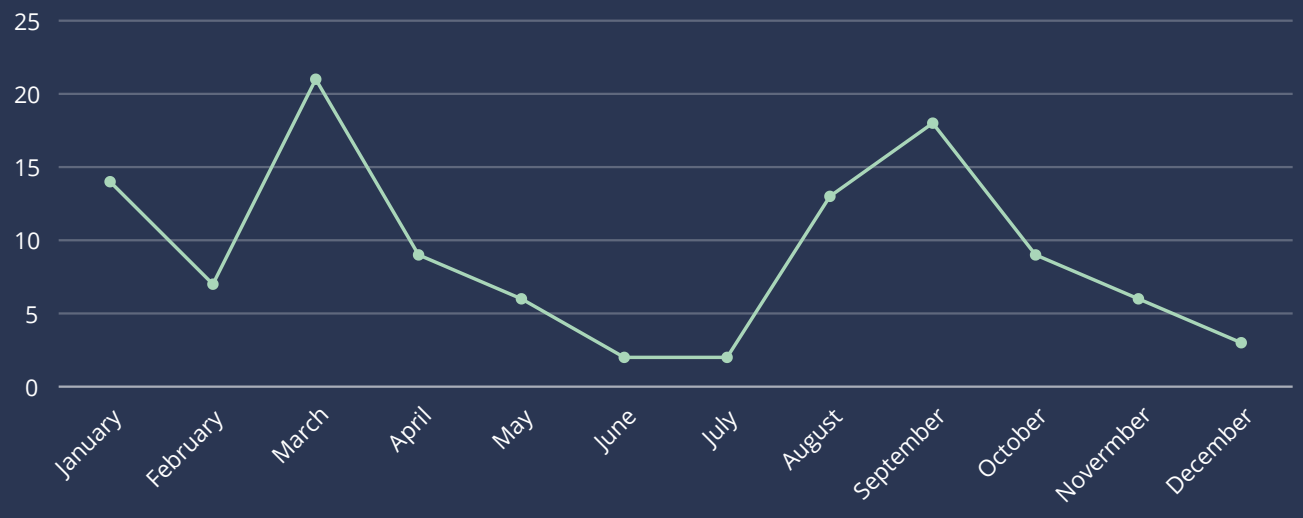
£40,500
Reported financial loses

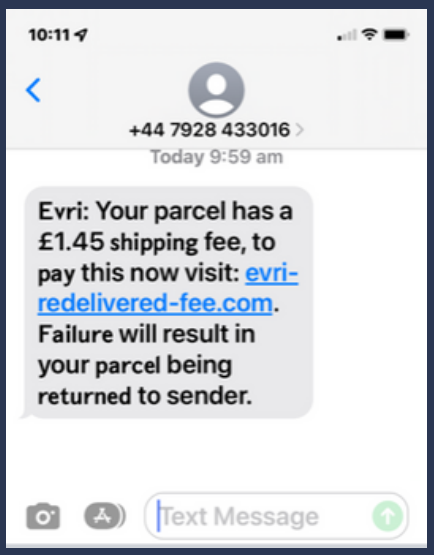
£25,000
Largest report of financial loss

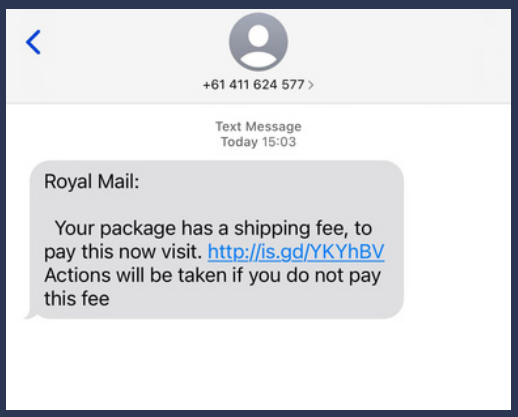
SMISHING

Over the year, we saw a number of SMS-based phishing scams. The primary text-based scam we were made aware of were the parcel delivery scams, which curiously peaked in both March and September. As always, criminals are utilising trusted names and brands as well as using spoofed numbers to create an element of trust.

Whilst we have seen a large number of reports, it's an encouraging sign than we have seen comparatively low financial losses, indicating that residents and organisations are becoming far more sceptical of these scams.







110
Reported Cyber Concerns

£2,390
Reported financial loses

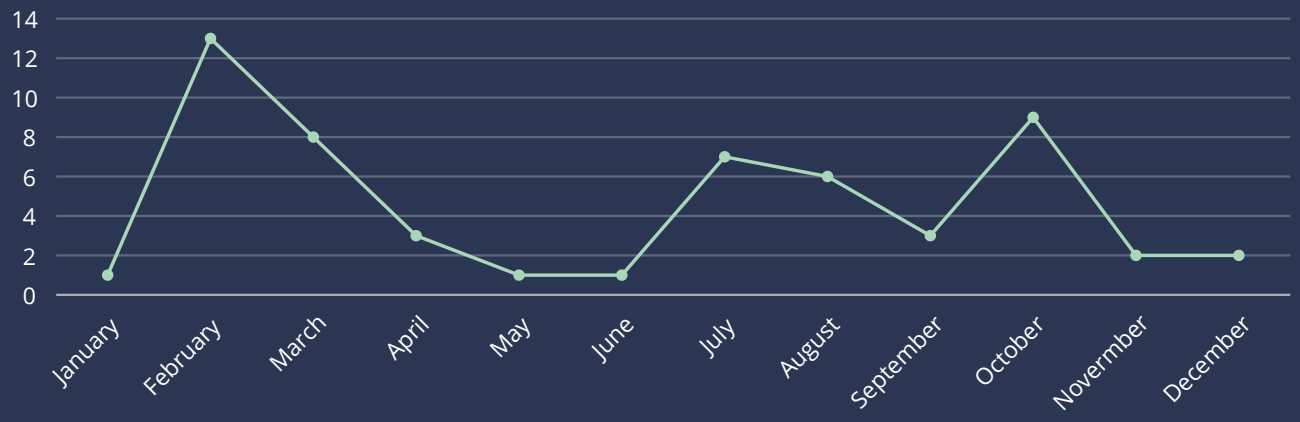
£21.72
Average financial loss per report*

**Some reports had no financial loss attributed*

VISHING

Telephonic phishing, referred to as vishing, remained at relatively consistent levels across the year. The variety of vishing scams we received this year is a worrying indicator of the success of vishing calls but as with Smishing criminals are utilising trusted names and brands as well as using spoofed numbers to create an element of trust.

As seen by the figures below vishing has had the second biggest financial impact on Island residents. Typically, we are finding that the criminals are using publicly available information, including names and addresses to add legitimacy to their calls.



CASE STUDY

£66,100 was fraudulently removed from an bank account after an attacker impersonated a bank employee. The incident began when a company employee received a call on the organisation's mobile number from what appeared to be NatWest Bank. The caller claimed fraudulent activity had been detected and asked the employee to confirm a code. No code was received, and when the employee questioned this, the caller provided a URL for the bank, instructing them to log in and check the accounts. Upon accessing the site, a code was displayed, but it is unclear whether the employee shared it.

During the interaction, the employee noticed AnyDesk, a remote access tool, displayed on the screen but does not recall downloading it. A subsequent investigation by the company's IT Provider found no evidence of malware or unauthorised software but conducted 15 hours of work to secure the systems. The fraud was immediately reported to the bank, but the stolen funds had already been withdrawn.

In 2024 we were engaged with CURA regarding Caller Line Identification, more information can be found on page 16.

56
Reported Cyber Concerns

£391,674
Reported financial loses

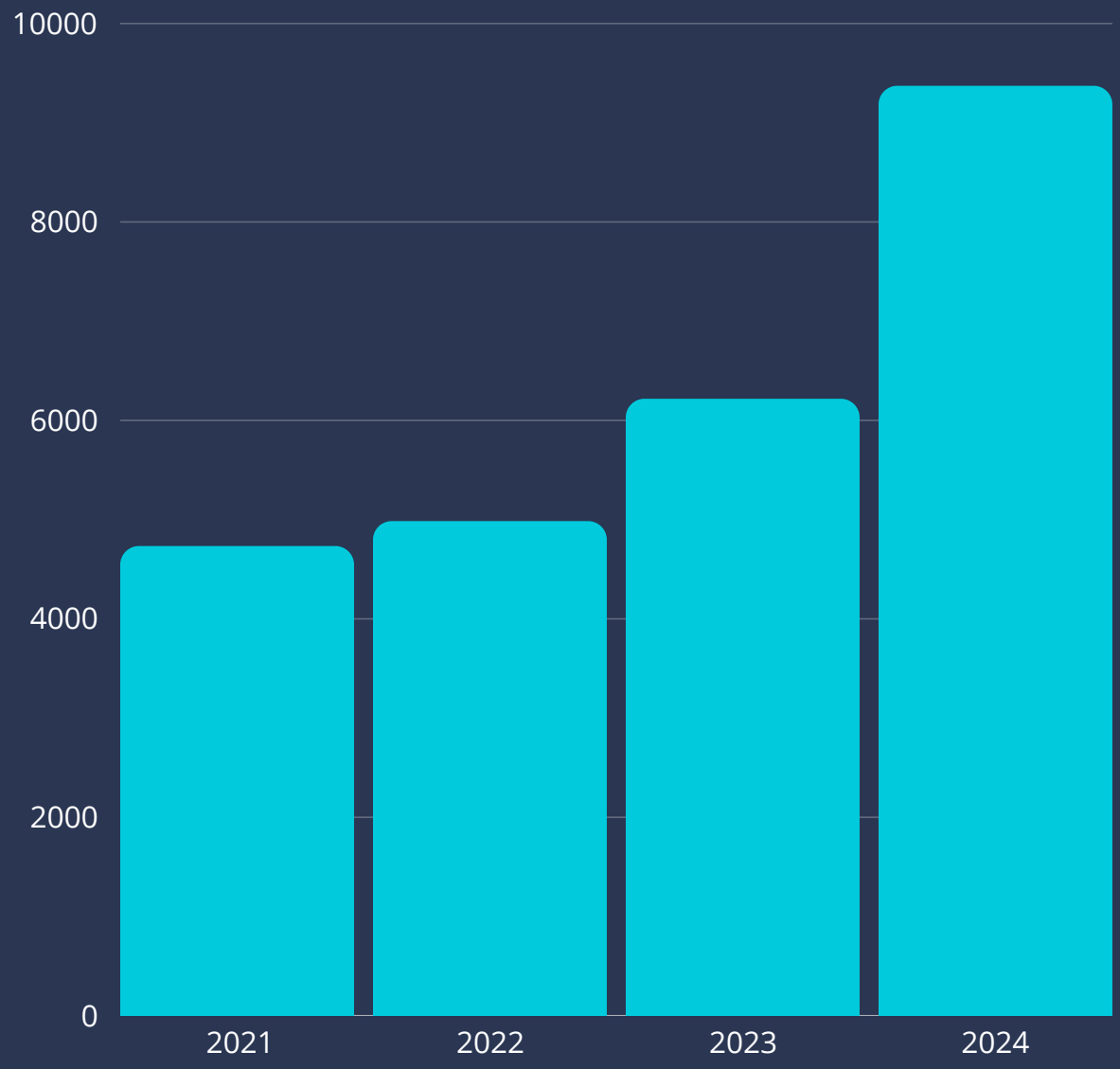
£6,994
Average financial loss per report*

**Some reports had no financial loss attributed and this is purely an average figure*

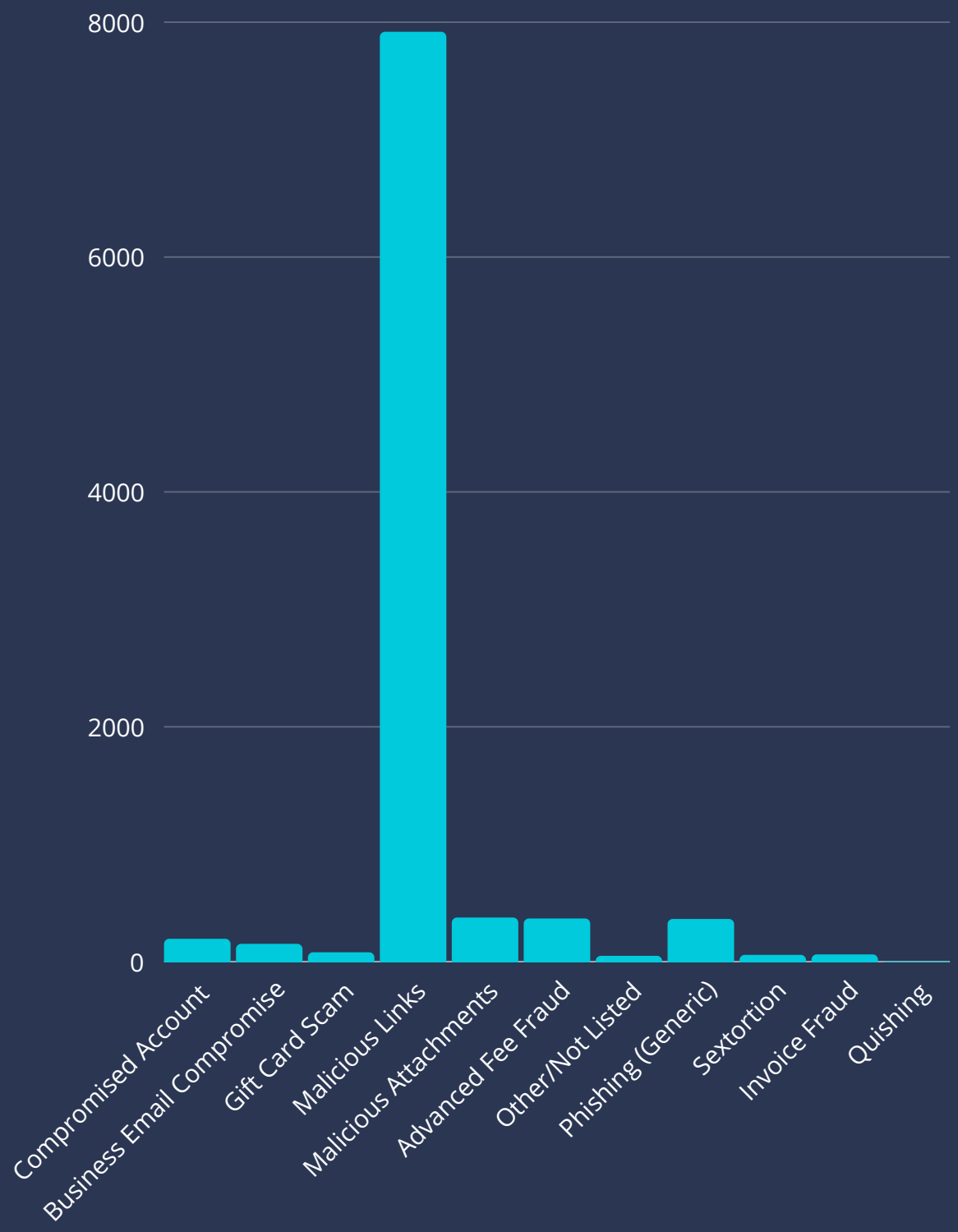
SUSPICIOUS EMAIL REPORTING SERVICE (SERS)

In 2024, we received 9,372 suspicious emails forwarded to us through our SERS; an increase of 50.72% on the 6,218 reported in 2023.

COMPARATIVE BAR CHARTS SHOWING THE INCREASE IN REPORTS EACH YEAR

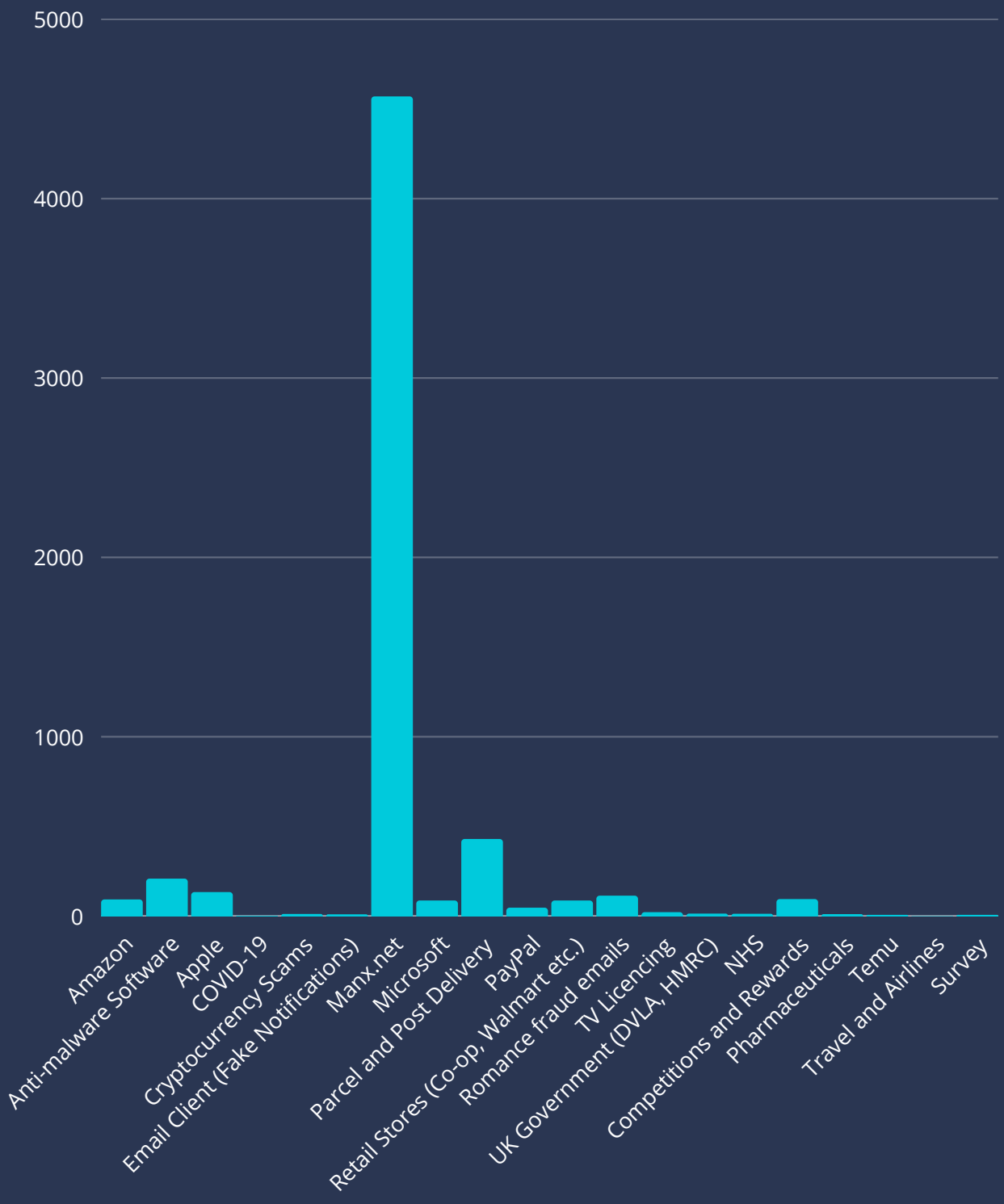


2024 SERS EMAILS: THREAT TYPES OF EMAILS



Analysing the contents of the reported emails in 2024, the majority were imitating legitimate email providers with many of the reports targeting manx.net email users.

2024 SERS EMAILS: COMMONLY IMITATED BUSINESSES AND INDUSTRY SECTORS



Note that the emails displayed above are only for those which reference a specific businesses or sector.

SERS AND THE NCSC

When submitting to our SERS, emailed are also passed onto the NCSC.

The NCSC will analyse the suspect email and any websites it links to. They use any additional information you've provided to look for and monitor suspicious activity. If malicious activity is discovered the NCSC may

- seek to block the address the email came from, so it can no longer send emails
- work with hosting companies to remove links to malicious websites
- raise awareness of commonly reported suspicious emails and methods used (via partners)

Whilst the NCSC is unable to inform us of the outcome of its review, they act upon every message received.

205k scam URLs removed by the NCSC since launch, as of December 2024

38m reported scams

OUR ACTIVITIES IN 2024

NATIONAL INFRASTRUCTURE SECURITY BILL (NISB)

As part of efforts to secure the Island's critical national infrastructure, the Department of Home Affairs is looking to introduce the National Infrastructure Security Bill. The bill will set requirements for organisations in order to ensure that they are prepared for and are resilient against a cyber attack. Information on these requirements can be found here or in our handy guide down below.

CLICK TO READ THE GUIDE

To find out more visit csc.gov.im/nisb

CALLING LINE IDENTIFICATION (CLI)

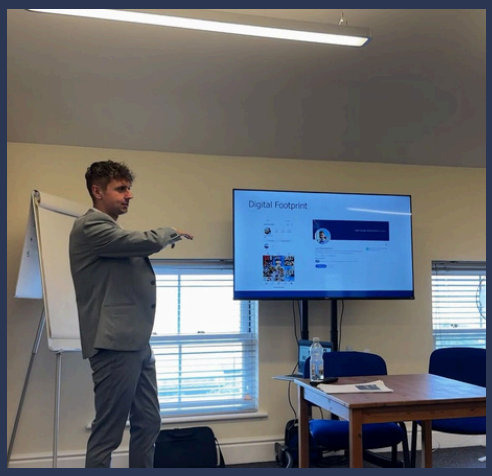
Calling Line Identification (CLI) Facilities play an important part in helping limit fraudulent activities through allowing the telephone number of a person making a call to be displayed to the person receiving the call, who can then decide whether to answer or not.

Advancing technology is making it easier for fraudsters to interfere with or change CLI information presented to people receiving calls.

With this in mind, Government, specifically the Office of Cyber Security and Information Assurance (OCSIA) and the Authority (CURA) worked collaboratively to ensure that the Island's residents and reputation have further protection from fraudulent use of CLIs using the Island's telecoms networks.

OCSIA, as part of its duties in relation to cybersecurity, is continually monitoring risks and threats that may impact the Island and the Authority supports that work, seeking to collaborate as appropriate.

ENGAGEMENT ACTIVITIES



We remain committed to enhancing cyber awareness and preparedness across the Isle of Man. Through targeted advisories, awareness campaigns, and presentations for schools, clubs, businesses, and community groups, we continue to equip residents with the information to protect themselves against the latest cyber threats.

VULNERABILITY ADVISORY SERVICE

We continue to operate a Vulnerability Advisory Service. This service proactively identifies critical cybersecurity risks by scanning publicly accessible IP address spaces for vulnerabilities that could be exploited by malicious actors. When issues are detected, we notify the relevant equipment owners or service providers, offering key details such as criticality scores and affected IP addresses to support risk assessment and mitigation.

RANSOMWARE AND SANCTIONS — ENGAGEMENT WITH AML

We have been engaged with the Cabinet Office Anti Money-Laundering Team to update guidance on payment in the event of ransomware. As part of this, we worked to produce a document outlining the considerations and requirements of organisations experiencing an attack, reaffirming our position on NOT paying a ransom. This was supplemented by a number of presentations to stakeholders including the AML forum as well as Gambling Supervision Commission licence holders.

CYBERISLE

The Island's premier cybersecurity conference, CYBERISLE, took place on October 10th, bringing together over 300 attendees, including representatives the National Cyber Security Centres of the UK, Republic of Ireland, and Northern Ireland as well as from Microsoft and the NCC Group. The event featured insightful panels, practical breakout sessions, and expert speakers who shared valuable knowledge.

As CYBERISLE goes from strength to strength each year we are looking forward to be launching CYBERISLE 2025 in the coming months.

ABOUT US

The 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.

@CyberIOM

facebook.com/OCSIAIOM

linkedin.com/company/csc-isle-of-man/

Join our mailing list

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