Cyber Security Centre for the Isle of Man

ANNUAL CYBER THREAT UPDATE

1st April 2025 - 31st March 2026

CONTENTS

INTRODUCTION

As Director of the Cyber Security Centre for the Isle of Man, I am pleased to publish the Annual Cyber Threat Update.

Over the last year high profile cyber incidents at Marks & Spencer, the Co-Op and Jaguar Land Rover have shown the impact cyber incidents can have.

Island residents are often insulated from these events but empty shelves in our local supermarkets highlighted we are not immune.

These incidents, and the statistics contained in this report, show that cyber criminals will target individuals and organisations of all sizes, operating in any sector.

In this year's report we also consider the threat landscape globally and the key themes that have emerged over the last twelve months.

The reports that we receive from local residents and businesses, together with the volatile geopolitical situation, show that the challenge continues to grow. Given these challenges, we would encourage businesses to develop plans for continuity and recovery so that they would be better prepared to respond well to any disruptive cyber-attacks. This reflects that no matter how large or small, almost every business depends on technology to function.

Mike Haywood, Director, Cyber Security Centre for the Isle of Man

THREAT LANDSCAPE

The cyber security threat landscape is increasingly being shaped less by pure technology and more by the convergence of geopolitics, emerging technology and societal behaviour. Although these have always had a place in the cyber threat landscape, some of the most disruptive and high-impact attacks throughout 2025 and into 2026 have been less “hack” and more abuse of legitimate systems and processes.

For the Isle of Man, these global dynamics present manageable risks, provided they are recognised early and addressed proportionately.

GEOPOLITICAL INFLUENCE

Geopolitical tensions continue to act as a force multiplier for cyber risk. State and state-aligned actors are increasingly using cyber operations to influence political campaigns and disrupt business operations leading to considerable reputational and economic impacts. Critical infrastructure, financial services and supply chains are persistent targets.

While the Isle of Man is unlikely to be a direct target, its close integration with the UK, EU and global systems mean it remains exposed to secondary impacts, including supply-chain compromise, opportunistic ransomware, or regulatory changes driven by international pressure. Cyber resilience must therefore be considered in a broader economic and political context, and not simply as an IT concern.

RANSOMWARE REMAINS THE DOMINANT THREAT

Ransomware continues to pose the most immediate and disruptive cyber risk to organisations. Attackers remain focused on data theft, extortion and business disruption, particularly within regulated industries and smaller enterprises.

For Isle of Man organisations, the decisive factor is not threat level but preparedness. Proven hygiene measures such as offline backups, patching, access control and rehearsed incident response remain the most effective means of reducing both impact and recovery time. It is also essential that the right people and skills are utilised for incidents as an overreliance on the in-house or managed IT provider may not be suitable for eradication and recovery in the event of an incident like account compromise or ransomware.

AI EXPOSURE AND OPPORTUNITY

Artificial Intelligence (AI) is now a defining feature of the threat landscape, and this will only continue through 2026 and beyond. On the offensive side, AI enables more convincing phishing, automated reconnaissance and adaptive malware, increasing the effectiveness of criminal and influence operations while lowering entry barriers considerably. On the defensive side, AI is rapidly improving detection, response and fraud prevention, offering smaller organisations the chance to compensate for limited resources and skills shortages.
AI presents organisations with many opportunities but only if implemented with appropriate governance. Uncontrolled adoption introduces risks around data exposure and regulatory compliance so focus must be placed in robust implementation planning and the ability to respond to incidents.

SOCIAL MEDIA AND THE HUMAN FACTOR

Social media platforms remain key vectors for fraud and social engineering. Impersonation scams continue to evolve in sophistication, which, in a close-knit community such as the Isle of Man, means the impact of these activities can be amplified, but equally so can mitigation. Public awareness and trusted messaging remain as highly effective defensive tools.

DIGITAL SOVEREIGNTY

Perhaps the most notable shift is the rise of digital sovereignty as a strategic priority. Driven by geopolitical fragmentation, this includes increased focus on data residency, cloud assurance and dependency on foreign-owned platforms.
For the Isle of Man, sovereignty does not imply self-containment. Rather, it requires informed choices, transparency over dependencies, and credible contingency planning balancing global connectivity with local resilience and regulatory confidence.

QUANTUM AND LONG-TERM RISK

Large-scale quantum decryption is not expected in the near term, but concerns around long-term confidentiality persist. International trends already show early adoption of post-quantum cryptography for sensitive data. Quantum readiness is a future-proofing exercise, ensuring systems, policies and suppliers do not create avoidable long-term exposure.

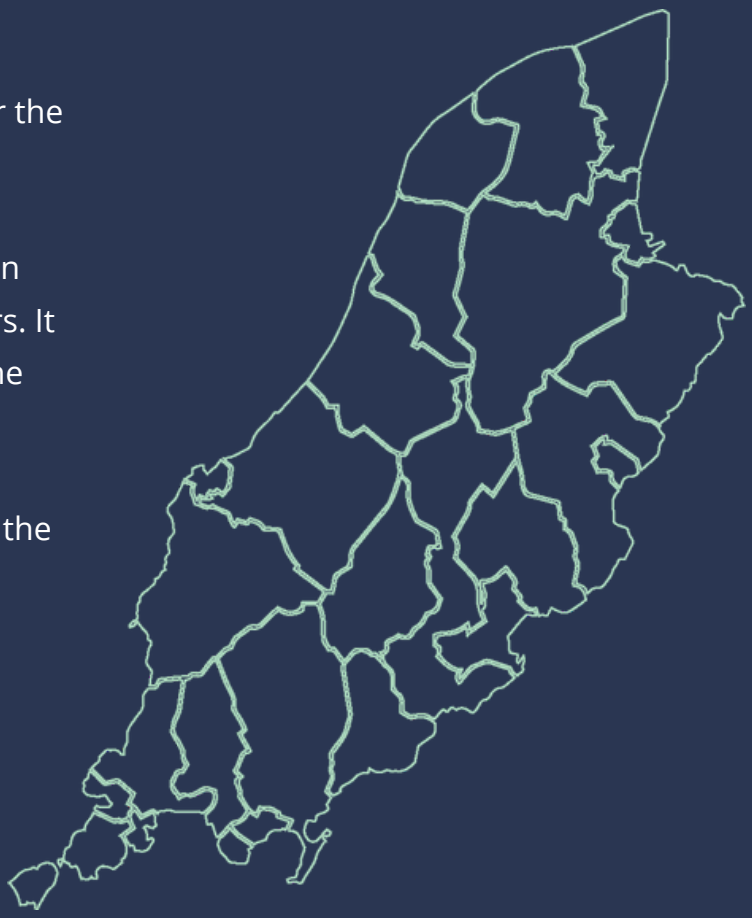
As a result of the fast-paced nature of quantum-based technologies, the Island's businesses will likely experience changes in the way data and business operations function in the not-too-distant future even though the threat is not immediate. Business leaders should consider how their data is being stored and transmitted, not just for the present, but for the future.

ISLAND THREAT SUMMARY

This report summarises the cyber threat environment impacting the Isle of Man over the past year. Drawing on data from the Cyber Security Centre's reporting mechanisms, including Cyber Concerns and the Suspicious Email Reporting Service (SERS), alongside intelligence from partner organisations and open-source reporting, it outlines the most prevalent threats, emerging trends, and key risks observed across the Island.

The report provides an overview of headline reporting figures and examines the primary scam and fraud types affecting individuals and organisations. It highlights trends in malicious and suspicious email activity, including impersonation attempts, and illustrates how cyber threats are adapting to exploit local contexts and behaviours.

In addition, the report outlines the Cyber Security Centre's activity over the reporting period, including public engagement, preventative advice, incident response, and collaboration with local and international partners. It concludes with an assessment of the wider cyber threat landscape and identifies the factors most likely to influence cyber risk to the Island in the period ahead.



OVERVIEW

6,423

Total emails reported to SERS

390

Reported Cyber Concerns

£1,048,492

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.

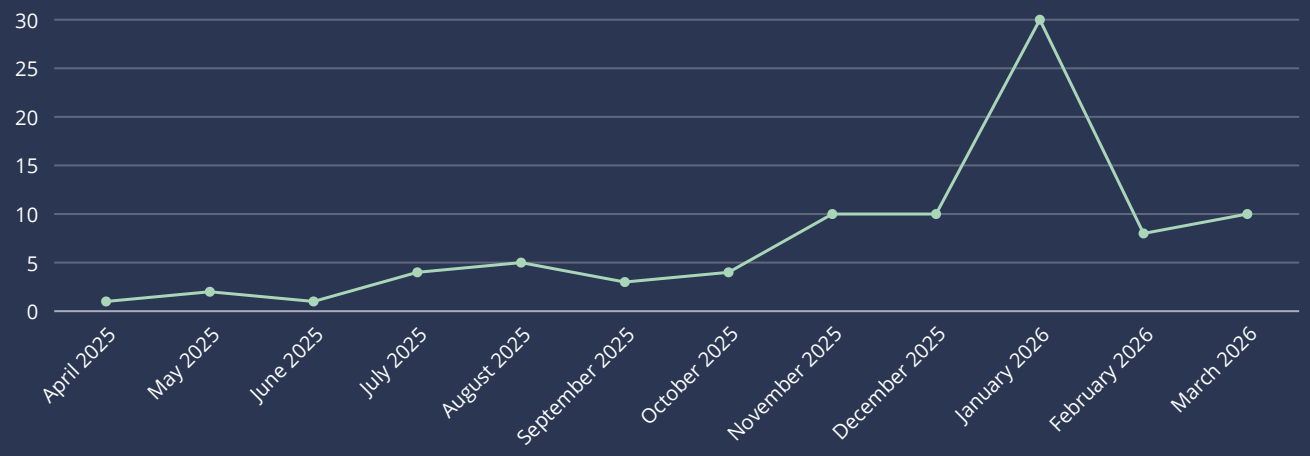
Despite the striking financial figures presented above, it is anticipated that the actual values will prove to be notably higher as cyber crime is vastly unreported.

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

Account compromise remained a high-impact incident type this year, with 88 confirmed cases and nearly 300 suspected compromises reported through SERS. Most stemmed from social engineering where emails mimicked routine security or service notifications. Attackers were especially successful during periods of organisational or platform change, using verification, migration, or update themes to exploit uncertainty.

Once access was gained, threat actors maintained control by adding mailbox rules, changing recovery details, or abusing tokens and malicious apps. Compromised accounts were then used for fraud and further phishing, including gift card scams, invoice fraud, and purchase scams. Most incidents were detected proactively via SERS, so many did not appear in cyber concern reports.

REFLECTION

The CSC continued to provide targeted advice and awareness on account compromise, particularly during periods of change when phishing activity was more likely to succeed. We also reinforced practical guidance on recognising suspicious verification requests and securing accounts before compromise could be exploited further.

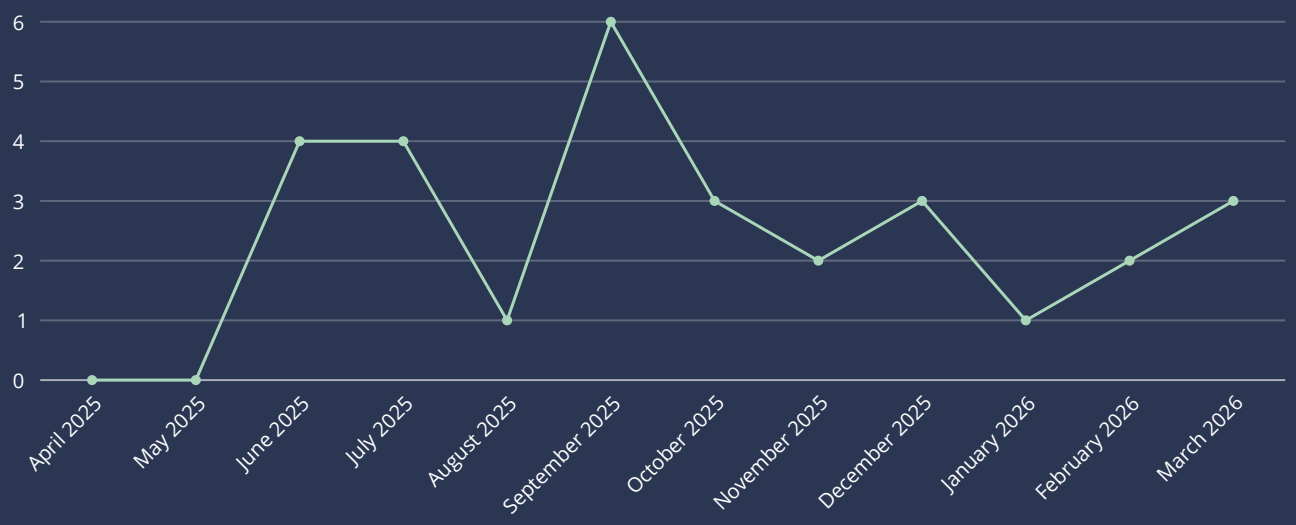
88
Reported Cyber Concerns

£115,271
Reported financial losses

£1,310
Average financial loss per report*

FRAUDULENT/SCAM WEBSITE

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



CASE STUDY

In the past year, fraudulent Facebook adverts and lookalike websites continued to target Isle of Man residents, imitating familiar brands and local services to appear credible. Scams ranged from £2 Smeg kettles and Currys-style laptop offers to fake Go Easy transport discounts and lost parcel pages using postal branding.

These adverts used official logos, stock images, and island-specific language to lure victims to external sites with convincing checkout pages. After a small initial payment, victims often saw further unauthorised charges and spam.

Losses were relatively high compared to previous years, around £15,000 across the year. Residents can reduce risk by treating social media ads offering significant discounts with caution, navigating directly to official websites, checking URLs and contact details, and being wary of foreign pricing, inactive support emails, or pushes to move to messaging apps. Genuine local offers are typically announced through official channels and covered by trusted news sources.

REFLECTION

The CSC increased monitoring of fraudulent websites and supported disruption activity where malicious sites were identified. Public warnings and practical advice helped residents recognise localised scams, misleading adverts and suspicious website features before engaging.

29
Reported Cyber Concerns

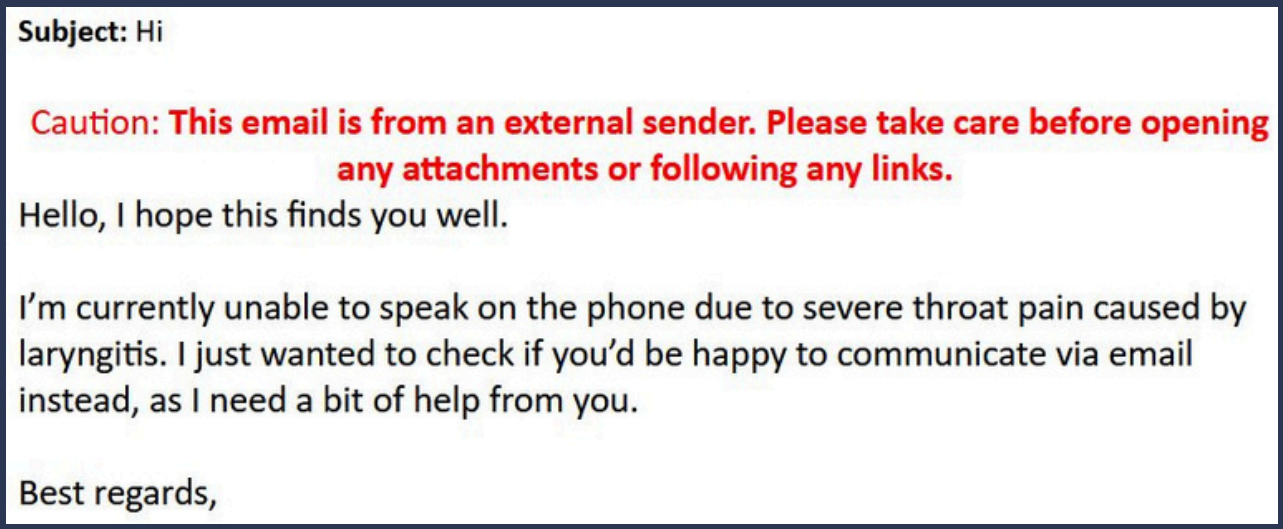
£15,260
Reported financial losses

£526.20
Average financial loss per report*

GIFT CARD FRAUD

Cyber criminals 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 cyber criminal and it is incredibly difficult to retrieve funds.

During this period, we only received 22 external cyber concern reports, with the majority of scams being reported through SERS. This underscores how underreported cyber crime is, and with the significant funds involved and the difficulty in rectification, this is an important area to highlight.



Subject: Hi

Caution: **This email is from an external sender. Please take care before opening any attachments or following any links.**

Hello, I hope this finds you well.

I'm currently unable to speak on the phone due to severe throat pain caused by laryngitis. I just wanted to check if you'd be happy to communicate via email instead, as I need a bit of help from you.

Best regards,

CASE STUDY

Gift card fraud has remained extremely prevalent in the past year, most reports made have identified the main cause still being the high compromise rates of Manx.net email accounts. Once a victim's account is taken over, scammers impersonate the account holder and send urgent gift card requests to anyone in the address book; family, friends, and local businesses alike.

While many organisations now recognise these messages as suspicious, a number of individuals still believe the request is genuine because it appears to come from a trusted contact, leading to financial loss.

REFLECTION

The CSC strengthened its response to gift card fraud by improving the identification of compromised email accounts and highlighting the warning signs of impersonation. Awareness activity also helped individuals and organisations recognise common tactics earlier, reducing the likelihood of financial loss.

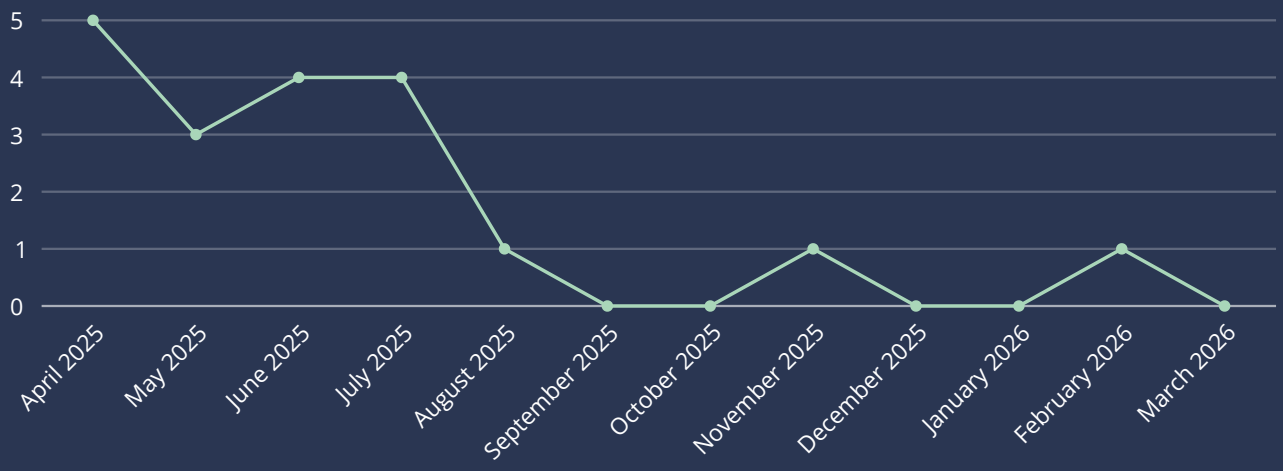
22
Reported Cyber Concerns

£3,100
Reported financial losses

£140.90
Average financial loss per report*

INVESTMENT SCAMS

Investment scams are becoming increasingly common, with fraudsters using a variety of tactics to lure victims. Criminals often use shares or cryptocurrency as bait, with promises of quick returns, to attract victims. More often than not, these shares or cryptocurrencies do not exist. In other cases, some individuals with existing shares may be targeted, whereby they are asked to move or transfer shares; these shares are not moved, and the company behind the contact has no authority to conduct any business with these shares.



CASE STUDY

Over £92,000 was lost to investment scams in the past year. In one case, a victim lost £50,000 after being approached via Facebook and with the conversation quickly moving onto WhatsApp. They were directed to a fraudulent trading site showing convincing dashboards, fake trade histories, and demonstrations of easy withdrawals. The scam was framed as gold spot trading and required the victim to create a cryptocurrency wallet and transfer funds to the sites wallet address. Criminals used professional-looking sites and social profiles to build trust before shifting victims onto encrypted messaging for pressure and persuasion.

Scammers posed as traders or coaches, maintaining regular contact and encouraging larger deposits by showcasing fabricated profits. After searching for help, the victim encountered a link to Scamhelp.net, illustrating how recovery scams target people already defrauded by offering to retrieve lost funds for a fee. Victims are advised not to engage with unsolicited recovery services and instead report incidents to the CSC, their bank, and the police, while preserving messages, wallet addresses, and transaction details to support investigations.

REFLECTION

The CSC continued to support victims of investment scams by promoting reporting routes and practical guidance on recognising high-pressure tactics, fake trading platforms and recovery scams. This work also helped reinforce the importance of early reporting to banks, law enforcement, and relevant support services.

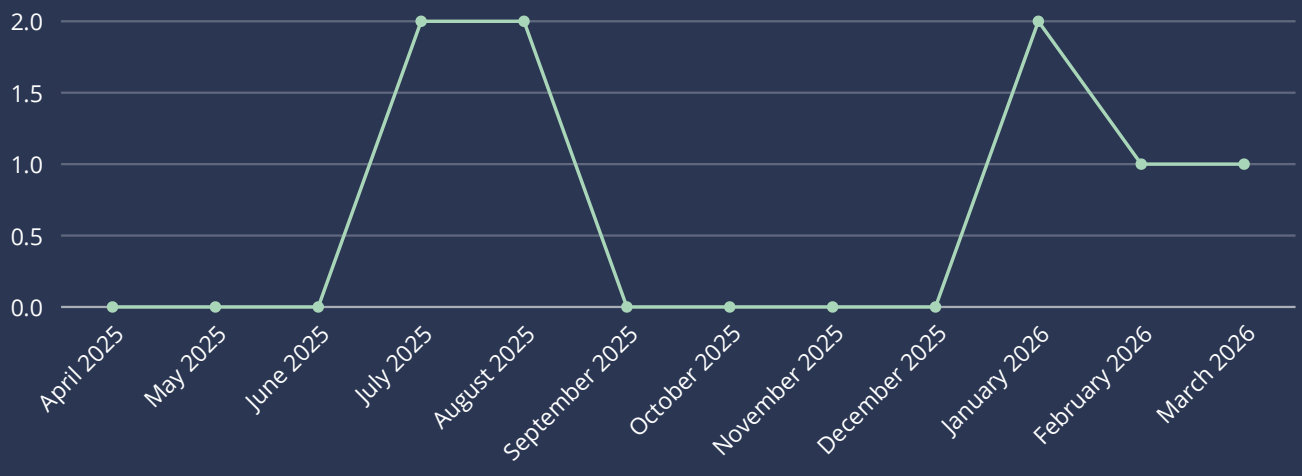
19
Reported Cyber Concerns

£92,484
Reported financial losses

£4,868
Average financial loss per report*

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 the past year, a local organisation lost roughly £142,000 in an authorised push payment (APP) invoice scam. An attacker used a lookalike email domain to impersonate the business, informed a supplier of new bank details, and intercepted a genuine invoice. The attacker then forwarded falsified payment instructions to the organisation, leading to two transfers into a fraudulent account. The issue was only discovered when the real supplier queried missing funds.

The investigation found no email compromise. The attacker relied solely on typo-squatting and impersonation to insert themselves into normal billing processes and exploit weak checks around bank detail changes. Following the incident, the organisation strengthened procedures so that any supplier bank detail update now requires additional verification.

To reduce similar risks, organisations should require multi-person approval for high-value payments, verify bank detail changes via known contact channels, and continue targeted awareness for finance teams on impersonation and invoice fraud indicators.

REFLECTION

The CSC used incidents of invoice fraud to reinforce the importance of independent verification for payment changes and supplier details. Guidance issued over the year focused on reducing the risk of impersonation, typo-squatting and weaknesses in internal payment approval processes.

8
Reported Cyber Concerns

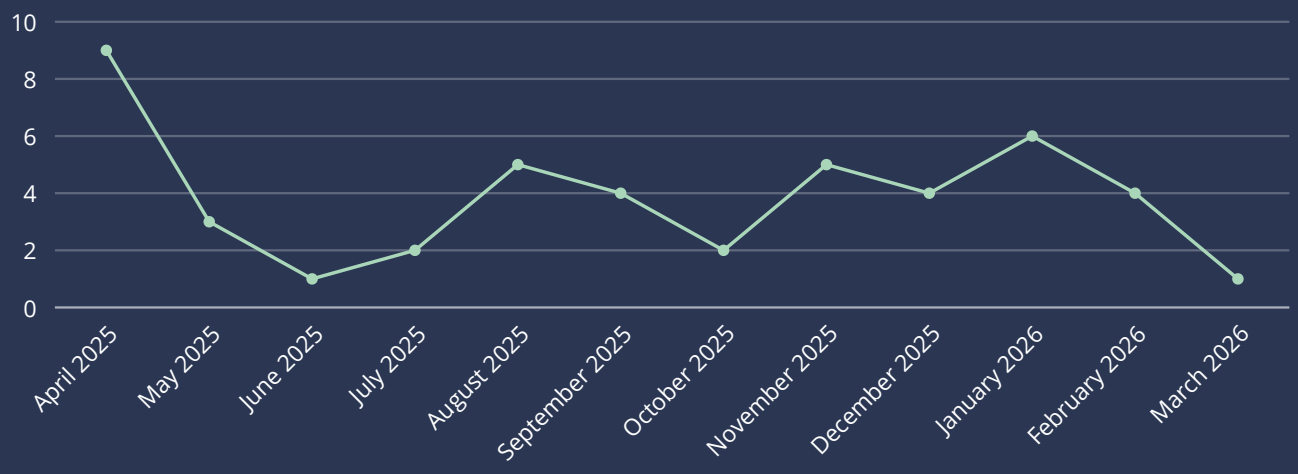
£265,875
Reported financial losses

£33,234
Average financial loss per report*

PURCHASE SCAMS

Purchase scams occur both in the real world and online. Island residents can be targeted from all over the world while online, making any recovery of funds extremely difficult. There is significant variety in purchase scams, from pets to flat deposits; the common factor is that victims often fail to take precautions on social media that they would take when buying items elsewhere. Facebook purchases make up a significant number of reports given how easy it is to create fake advertisements and profiles.

Typically, purchase scams are often of a smaller amount in comparison to other scams but are far more frequent.



CASE STUDY

In the past year, Facebook Marketplace continued to be used for advance-fee purchase scams, with the most damaging cases involving fake rental properties. Victims were drawn in by low-cost listings and quickly moved to WhatsApp by accounts using plausible local names. Landlords then demanded deposits and fees, often split across multiple bank accounts, to secure the property. In one case, a bank fraud warning blocked a transfer, but the victim was persuaded to proceed, reflecting a growing trend of scammers applying urgency and reassurance to bypass security prompts.

Common patterns included pressure to pay before viewing, requests to move platforms, changing or mismatched payee details, and repeated claims that everything was legitimate despite warning signs. The safest approach remains: never pay before viewing and verifying, avoid off-platform communication, and always treat bank fraud warnings as genuine.

REFLECTION

The CSC continued to raise awareness of purchase scams where advice focused on helping residents recognise pressure tactics, verify sellers and avoid off-platform payments or communication.

46
Reported Cyber Concerns

£69,928
Reported financial losses

£1,520
Average financial loss per report*

ROMANCE SCAMS

The bulk of the reported £213,200 in losses due to romance fraud comes from one report, however; other reports allude to other victims sending significant amounts of money to cyber criminals. The figures that we cannot confirm have not been included, and we suspect the actual figure for romance scams to be much higher.

What is particularly concerning 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 STUDY

In the past year, romance scammers continued to build long-term trust on social media and dating platforms before shifting victims to private messaging and introducing payments.

In one case, a victim spent nearly two years communicating with a profile impersonating a public figure and a fake management team, receiving itineraries and booking details to justify repeated instalment payments. They lost £7,000 before realising the identity was false.

In another case, a scammer on a niche dating site used a credible-looking profile to persuade the victim onto an encrypted app, then pressured them to pay for a venue booking and gift cards sent to an external email. A final admin fee raised suspicion, and a reverse image search revealed the photos were stolen.

Common signs included prolonged grooming, pressure to pay before meeting, shifting payee details, and requests for irreversible payments like bank transfers or gift cards. The largest loss this year was significantly higher than last year’s, demonstrating that the tactics remain convincing. Victims should verify identities, refuse gift card or off-platform payments, and stop if they feel pressured.

REFLECTION

The CSC continued to highlight the tactics used in romance scams, including long-term grooming, emotional manipulation and requests for irreversible payments. Guidance and awareness activity aimed to encourage earlier reporting and help victims, families and friends recognised the warning signs sooner.

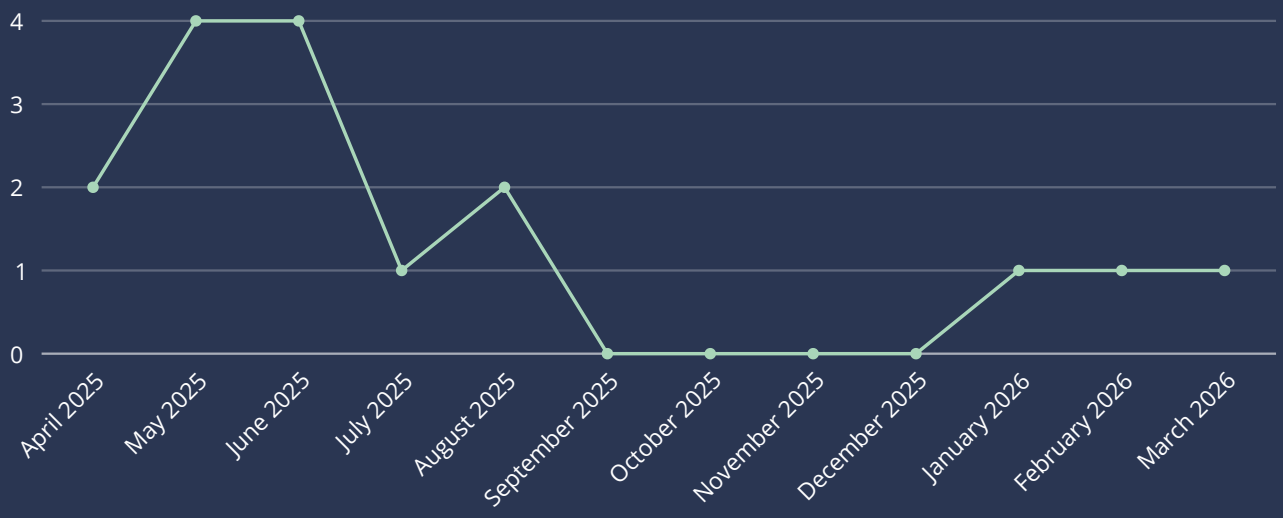
7
Reported Cyber Concerns

£213,200
Reported financial losses

£200,000
Largest report of financial loss

SEXTORTION

Sextortion is a type of scam where criminals attempt to extort money or sexual favours from someone through threats to share evidence of sexual/indecent activities. This scam is a type of online blackmail, targets victims of any age and you don't have to have shared sexual images or information to be a victim of sextortion.



CASE STUDY

In the past year, we continued to see sextortion attempts following a consistent pattern: unexpected contact from a new profile or email, a quick push to a private messaging app, and threats to share alleged intimate material unless payment is made. Scammers often claimed a device had been hacked, old passwords/public data were used to seem credible, and attached fabricated proof to create urgency. Messages typically demanded fast payment, set countdowns, and warned victims not to tell anyone, all classic coercion tactics.

The most effective defence is not giving criminals something that they can exploit: never share intimate images or videos, even with contacts who appear trustworthy. Once shared, material can be copied, edited, and reused to escalate threats, and paying rarely stops further demands. If you receive a sextortion message, do not respond, do not pay, and remember it is designed to provoke panic, pausing breaks the pressure cycle and helps you stay in control.

REFLECTION

The CSC reinforced guidance around sextortion, emphasising that these scams are designed to create panic and pressure victims into responding quickly. Awareness messaging focused on encouraging victims not to engage, not to pay, and to report incidents so that support could be provided at an earlier stage.

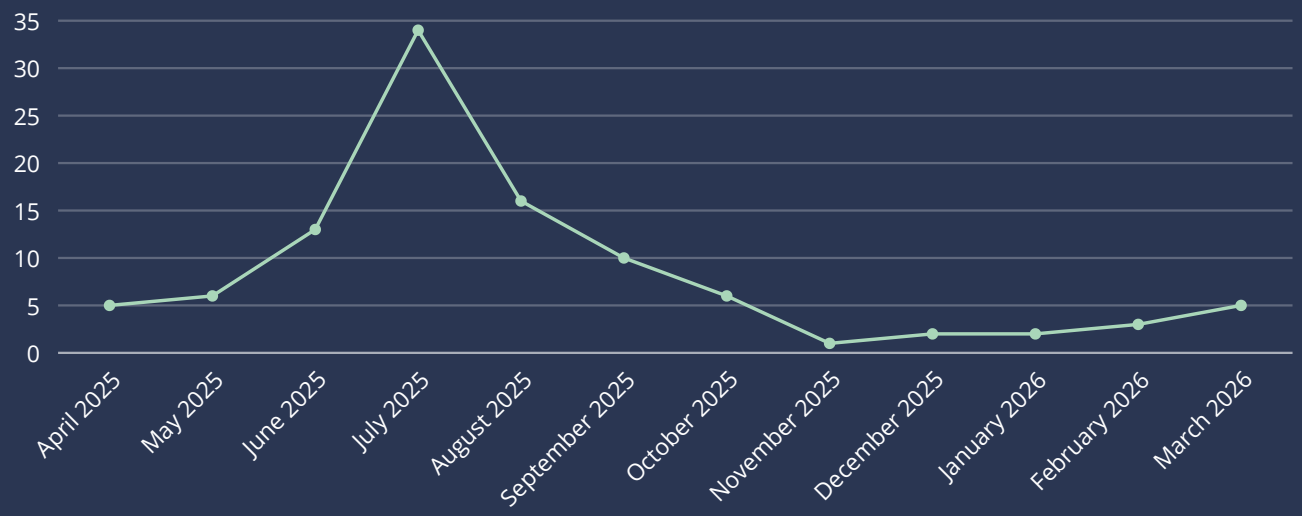
16
Reported Cyber Concerns

£9,430
Reported financial losses

£7,000
Largest report of financial loss

SMISHING

Over the year, we saw a number of SMS-based phishing scams. These scams peaked in July with the winter heating allowance/parking fine scams. As always, criminals are utilising trusted names and brands as well as using spoofed numbers to create an element of trust.



CASE STUDY

In the past year, we continued to receive reports of SMS-based phishing, with parcel delivery texts remaining the most common lure. Scammers used trusted names, spoofed caller IDs, and urgency to push recipients to lookalike payment or sign-in pages.

Alongside parcel scams, we saw increases in parking fine and winter heating allowance texts. One parking scam threatened extra charges and licence issues, linking to a fake payment page. A heating allowance scam impersonated the Department for Work and Pensions, asserting incorrect details and urging recipients to re-apply via a shortened link, even instructing them to 'reply 1', a common pressure tactic aimed at harvesting personal and card information.

Key warning signs stayed consistent: unexpected texts about deliveries, fines, or benefits, generic or shortened links, unusual web addresses, messages from unfamiliar numbers, and threats of urgent penalties or fast payments.

REFLECTION

The CSC continued to raise awareness of fraudulent messages, drawing attention to common lures. Public guidance focused on helping people identify suspicious links, fabricated branding, and urgency-based tactics used to harvest information or payments.

103
Reported Cyber Concerns

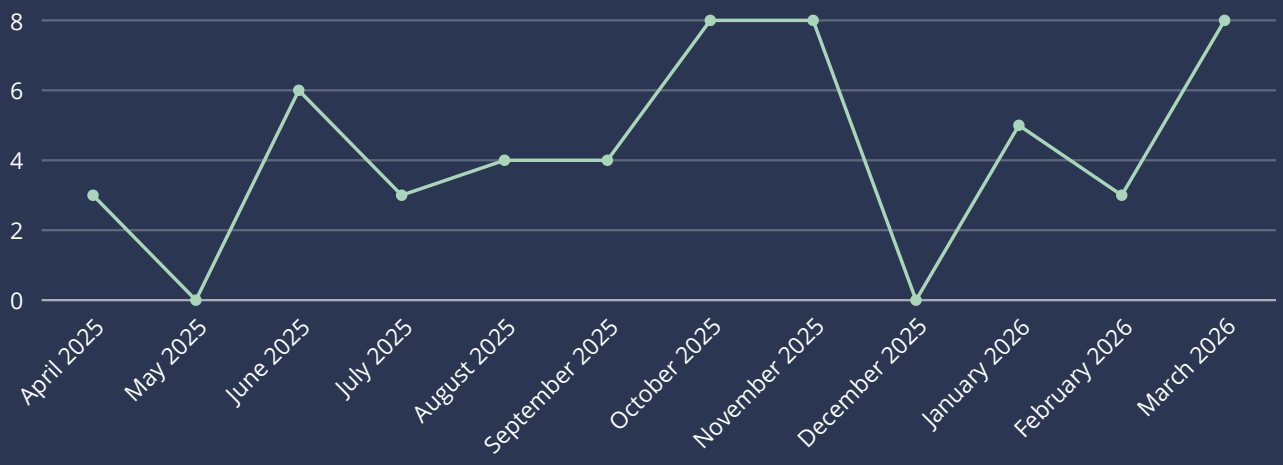
£4,340
Reported financial losses

£42.13
Average financial loss per report*

VISHING

Voice phishing, referred to as vishing, is where scammers impersonate trusted entities over the phone in order to trick victims into providing sensitive information. Just like with smishing scams, vishing scams are typically utilising public information, including names and addresses, along with trusted names and brands while using spoofed numbers to create an element of trust and legitimacy.

As seen by the figures below vishing has continued to have the second biggest financial impact on Island residents.



CASE STUDY

A victim received two calls from someone impersonating their bank's fraud team. While on the call, they opened their banking app and discovered over £50,000 in card payments had already been processed. The caller reassured them the charges could be reversed to keep them engaged. Shortly after, a WhatsApp message arrived from someone posing as a financial regulator, directing the victim to a refund link, at which point they realised it was a scam and disengaged.

A review suggested the card details were likely compromised before the call, with the vishing sequence designed to gather more information or push additional authorisations under the appearance of helping recover funds.

The case reflects familiar tactics: convincing spoofed identities, back-to-back contacts to build legitimacy, urgency, and a final push to click a link or share security details.

REFLECTION

The CSC continued to highlight the risks posed by vishing scams, particularly where criminals impersonate trusted organisations and exploit imitated caller IDs. Advice throughout the year focused on verifying unexpected calls through official channels and resisting pressure to share information or act immediately.

52
Reported Cyber Concerns

£259,604
Reported financial losses

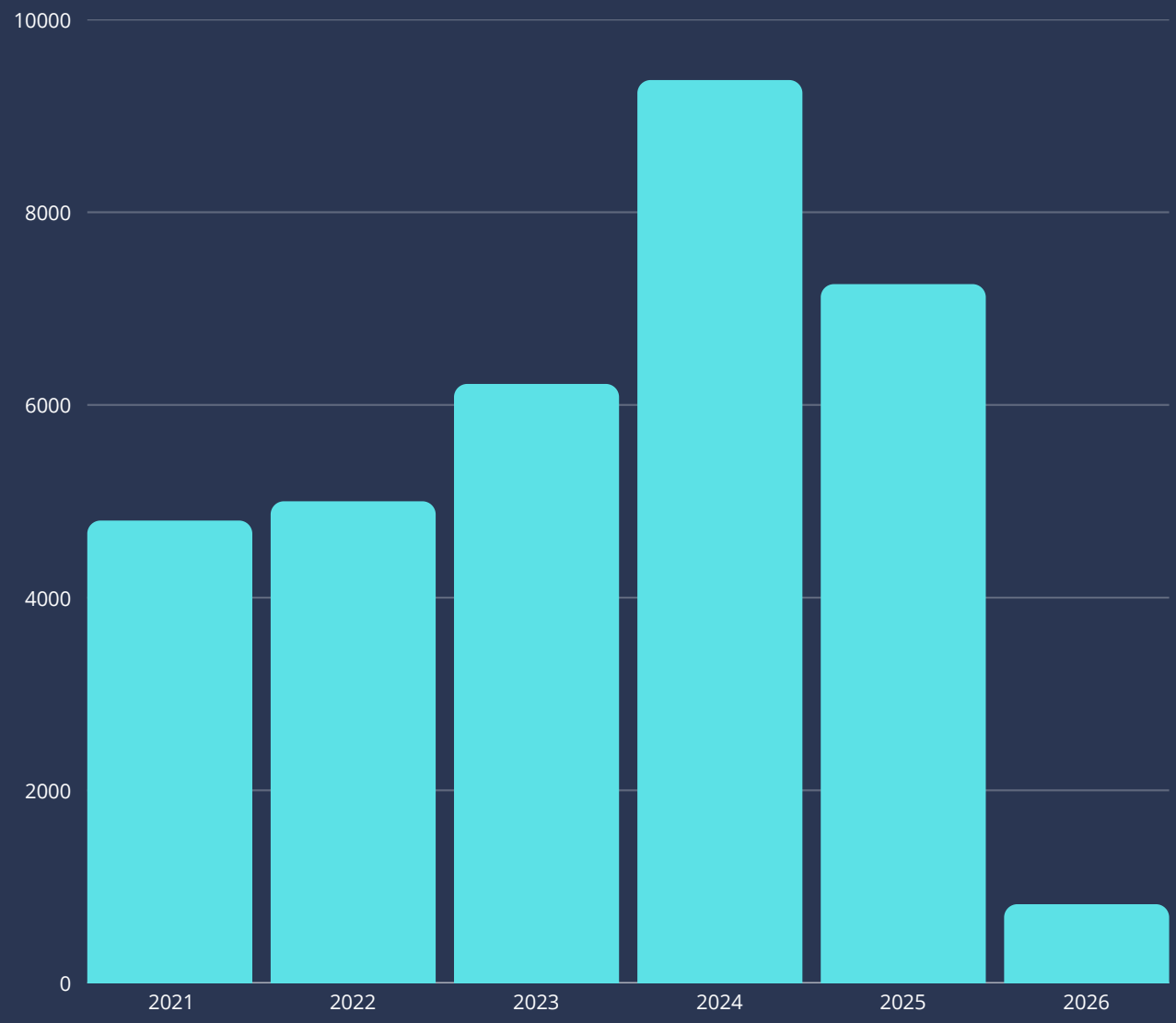
£4,992
Average financial loss per report*

SUSPICIOUS EMAIL REPORTING SERVICE (SERS)

In the past year, we received 6,423 suspicious emails forwarded to us through our SERS.

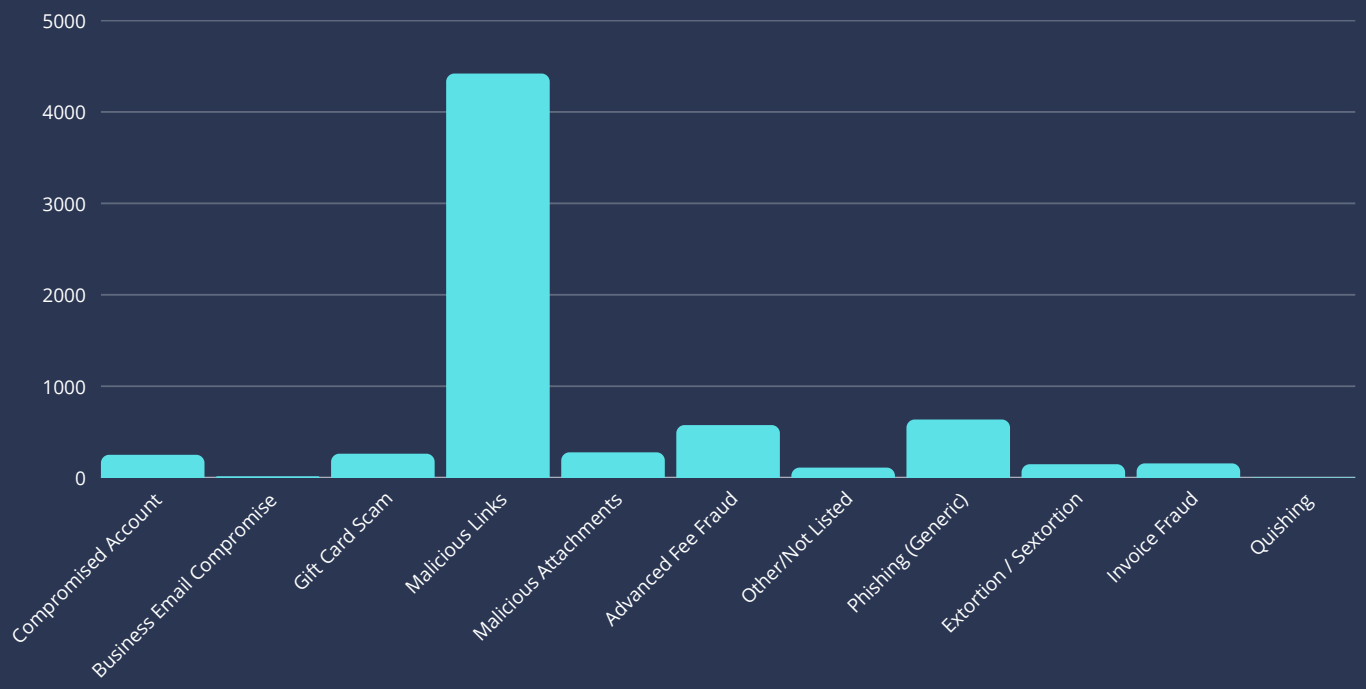
Note: The above figure represents the total reports for the period of 1st April 2025 - 31st March 2026

COMPARATIVE BAR CHARTS SHOWING THE DIFFERENCE IN REPORTS EACH YEAR



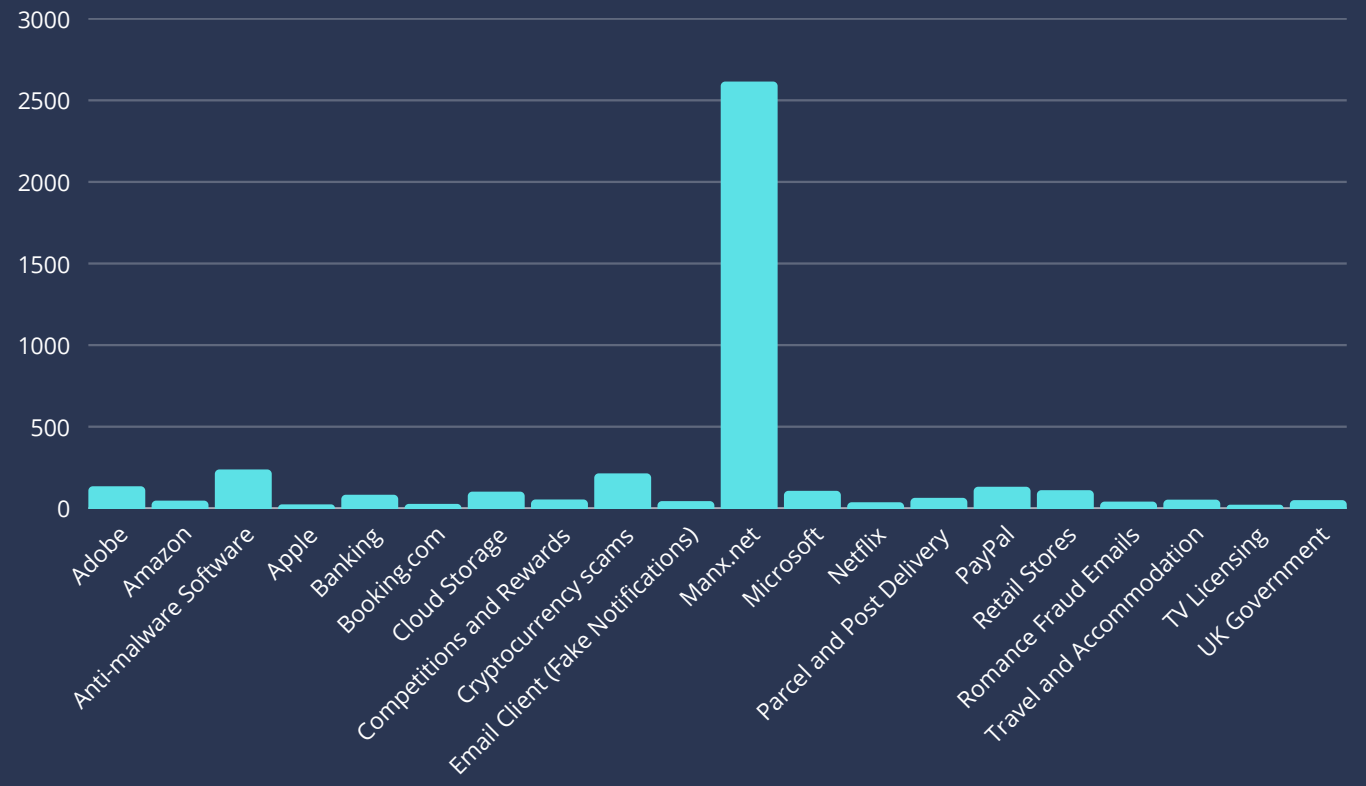
Note: As a result of the change to the reporting period for this annual threat report, the 2026 total reflects suspicious email reports received during the period 1st January to 31st March 2026 only, therefore is not directly comparable with previous full calendar year totals.

THREAT TYPES OF EMAILS



COMMONLY IMITATED BUSINESSES AND INDUSTRY SECTORS

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



SERS AND THE NCSC

When submitting to our SERS, emails are also passed onto the the UK National Cyber Security Centre (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.

436k scam URLs removed by the NCSC since launch, as of March 2026

53m reported scams

OUR ACTIVITIES

NATIONAL INFRASTRUCTURE SECURITY BILL (NISB)

OCSIA continues to advance the development of the National Infrastructure Security Bill as part of its work to strengthen the resilience of the Island's critical national infrastructure.

During the past year, a series of engagement and awareness sessions were held. In September 2025 the Department presented an overview of the proposed bill at the Chamber of Commerce Digital Forum. Attendees were updated on the policy direction and the Department's intention to continue working closely with industry and public bodies.

A public consultation on the draft bill opened on 1 December 2025 and closed on 9 January 2026. Overall, respondents agreed that dedicated legislation is needed. There was broad support for the definitions of the National Infrastructure and Critical National Infrastructure. Suggestions included refinement of some definitions within the bill and continued engagement with stakeholders during the development of regulations.

The Department published the full consultation response document in January 2026. The findings will help inform the next phase of drafting, ensuring that the bill is workable, proportionate and aligned with the expectations of those it affects.

Further information, including the latest updates and resources relating to the proposed bill, can be found at csc.gov.im/national-infrastructure-security-bill-nisb

VULNERABILITY ADVISORY SERVICE

We continue to operate a vulnerability advisory service, which proactively identifies critical cybersecurity risks by scanning publicly accessible IP address spaces for vulnerabilities and exposures 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.

ENGAGEMENT ACTIVITIES

Throughout the year we have remained committed to enhancing cyber awareness and preparedness across the Isle of Man. Working closely with communities, organisations and partner agencies, we continue to help residents protect themselves against evolving cyber threats.

As part of Cyber October awareness campaign, the Eastern Neighbourhood Policing Team, together with the Cyber Security Centre, delivered a series of talks to elderly and vulnerable members of the community. These sessions focused on raising awareness of common cyber security threats and providing practical advice on how to stay safe online.

Alongside this work, the Cyber Security Centre delivered presentations to several local clubs and community groups, supporting broader efforts to promote good cyber hygiene across the Island.

Our external engagement on email account compromises has included issuing urgent public advisories, such as the warning about an active phishing campaign that caused multiple confirmed business email breaches and highlighted the risk of silent compromise. We have also provided public guidance explaining how email compromises occur and how individuals and organisations can secure their accounts.

CYBERISLE

The Island's premier cybersecurity conference, CYBERISLE, was held on 15 October at the Comis Hotel and this year's theme, 'Building a Resilient Island', highlighted the importance of strengthening digital infrastructure and ensuring the Island has appropriate security measures in place. As global cyber threats continue to evolve, initiatives such as the forthcoming National Infrastructure Security Bill will form an essential part of the Island's approach to resilience.

The conference focused on practical strategies to support this, bringing together experts, practitioners and policymakers. Sessions explored incident response, public-private collaboration, supply chain security, and regulatory readiness.

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

www.ocsia.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