Cyber Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

May - June 2025

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)	**1**
Reported Cyber Concerns	**3**
Isle of Man Threat Commentary	**5**
External Threat Commentary	**11**
Cyber Glossary	**15**
About Us	**17**

SUSPICIOUS EMAIL REPORTING SERVICE (SERS)

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

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

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

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

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

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

Since the launch of SERS, we have received over 28,900 suspicious emails. In May and June 2025, we received 787 suspicious emails.

SUSPICIOUS EMAILS

787 REPORTED

in May and June

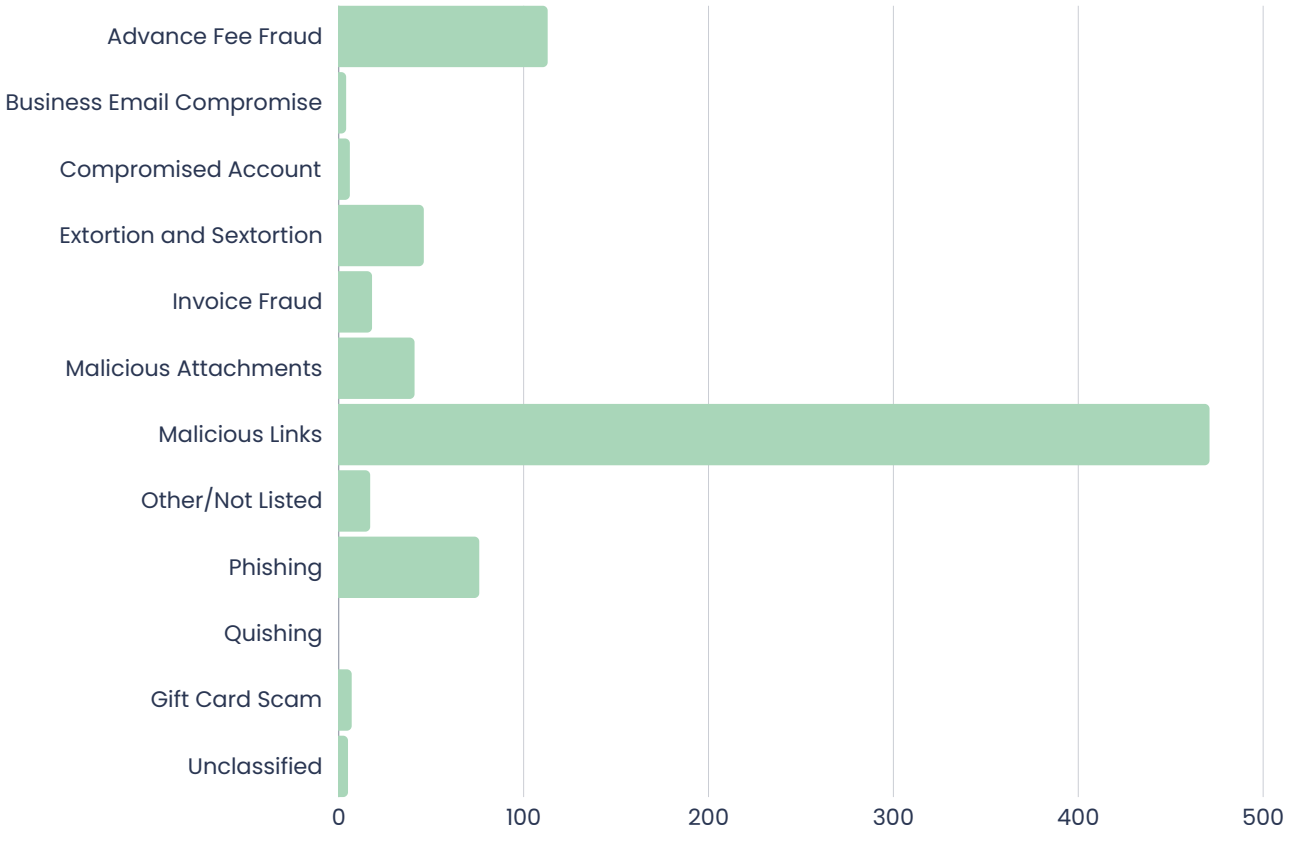
Detail

The graph below shows the frequency of specific characteristics identified in submitted SERS emails. Please note that some emails have more than one recorded characteristic.

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

Top 5 Phishing Scams Imitating Popular Services:

1. Manx.net
2. Cryptocurrency
3. PayPal
4. UK Government
5. Travel Booking Websites



CYBER CONCERNS

69 REPORTED

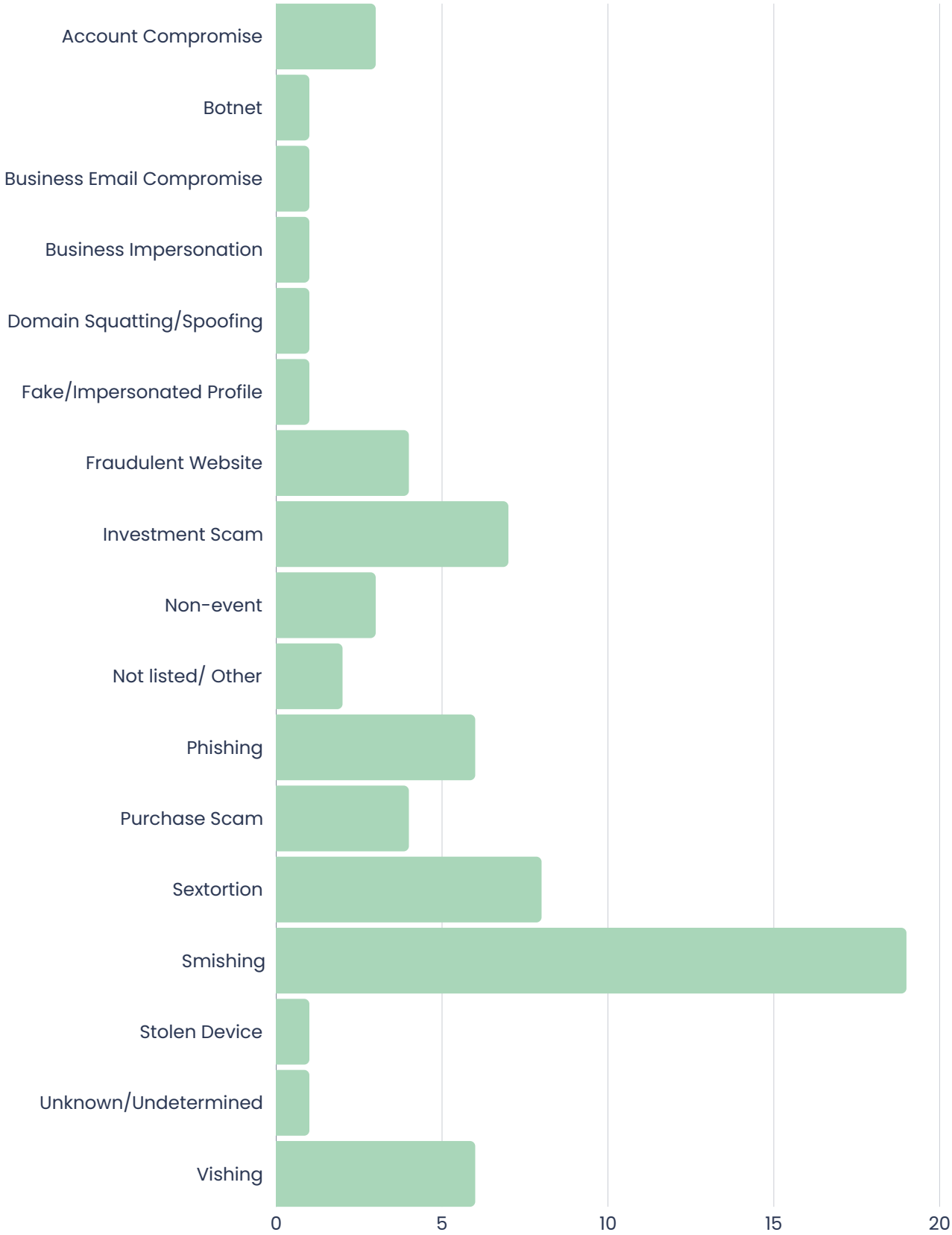
in May and June

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

VISHING, LEGITIMATE PROCESSES FOR ILLEGIMATE GAINS

A report was received whereby a member of the public fell victim to a sophisticated account takeover scam involving impersonation, social engineering, and the misuse of legitimate security processes. The scam began with two phone calls from individuals claiming to represent Revolut. The callers informed the victim of alleged fraudulent activity on her account and the need to issue a replacement debit card, an approach designed to create urgency and establish credibility.

To reinforce the illusion of legitimacy, the scammers triggered a One-Time Passcode (OTP), a genuine security feature used by banks to verify identity. The victim received the OTP on her phone, believing it was part of a secure process initiated by Revolut. However, this code was likely used by the criminals to gain access to her account in real time. This is a classic example of social engineering, where a legitimate security mechanism is manipulated to serve malicious purposes.

Following the OTP, the victim received an SMS containing a link, presumably to a fraudulent website designed to mimic Revolut's interface. She was instructed to upload sensitive documents, including her passport and ID, which she did. The scammers later claimed the documents were not received and insisted on a minimum payment of £60 to proceed. This payment was made, but it became clear that the funds went directly to the criminals. Subsequently, a total of £3,209 was withdrawn from the victim's account.

We have seen many cases in which scammers exploit trust in familiar processes—like OTPs and identity verification to manipulate victims into handing over control. The use of real-time communication, urgency, and impersonation of trusted institutions makes these scams particularly convincing. It also highlights the need for public awareness: receiving an OTP does not always mean you are in control of the process, especially if it was initiated by someone else.

BUSINESS EMAIL COMPROMISE: COULD YOUR ORGANISATION BE SPOOFED?

In 2025, the Isle of Man Treasury received a series of suspicious emails that appeared to originate from a local wholesaler. These emails were crafted to resemble legitimate financial correspondence and bore the hallmarks of a Business Email Compromise (BEC) attack and was designed to manipulate financial transactions. However, one detail made the deception easier to detect: the emails were sent from *thewholesaler*@manx.net, a free email address hosted on Manx.net, rather than from *the wholesaler's* official domain.

This discrepancy raised immediate red flags. The use of a public email provider instead of a corporate domain made it easier for recipients to question the legitimacy of the message. Upon investigation, the Office of Cyber-Security and Information Assurance (OCSIA) confirmed with *the wholesaler's* Finance Department that the account was not genuine and likely created to impersonate the company.

While this particular attack was relatively easy to spot, more sophisticated attackers often attempt full domain spoofing, making fraudulent emails appear as though they come directly from a trusted business address. In such cases, email authentication protocols become essential.

To defend against domain spoofing and impersonation, organisations should implement three key email security protocols:

- SPF verifies that emails are sent from authorised servers.
- DKIM ensures messages haven't been tampered with and confirms sender authenticity.
- DMARC builds on both, allowing domain owners to instruct mail servers to reject or quarantine unauthenticated messages and provides visibility through reporting.

These tools work together to protect your domain, but they don't stop attackers from using unrelated or lookalike domains, like in this case. That's why technical controls must be paired with user awareness and proactive communication.

FROM LINKEDIN TO LIES: HOW SCAMMERS CONSTRUCT CONVINCING COVERS

Concerns were raised about a company operating under a certain name, initially associated with a specific domain. By April, that website had disappeared, only to be seemingly replaced by a new domain with a slightly altered name. The legitimacy of this new site was unclear, particularly in relation to the officially registered company bearing a similar name. This shift in online presence triggered further scrutiny, especially as the digital trail left behind began to raise red flags.

A LinkedIn page linked to the company featured a post introducing the company's CEO. However, it was noted that the image of the CEO appeared to be AI-generated, a synthetic face created using generative technology, likely to obscure the identity of the real operator or to fabricate a professional persona entirely. This tactic is increasingly common in online scams, where AI-generated images are used to create convincing but entirely fictitious individuals.

The situation became more concerning when it was discovered that the registered office address for the company and its CEO was listed at a residential address. The actual homeowner confirmed that he had leased the property to someone with the same name as the CEO two years prior, but the person shown on LinkedIn was not the same individual he had met. Moreover, the homeowner expressed distress that his address was now publicly associated with the company and appeared in Google search results alongside negative reviews, potentially damaging his personal reputation and privacy.

This case illustrates how digital footprints, whether accurate, outdated, or fabricated, can be exploited by scammers. Publicly available information such as company registrations, LinkedIn profiles, and residential addresses can be stitched together to create a façade of legitimacy. When combined with AI-generated content, such as fake profile photos or even AI-written bios and testimonials, these scams become increasingly difficult to detect at a glance.

To address such threats, we work to take down fraudulent websites by contacting the domain registrars, hosting providers, and associated service platforms. These entities are informed of the criminal activity being conducted through their infrastructure and are asked to suspend or remove the offending content.

SCAMMED TWICE: THE CRUEL CYCLE OF RECOVERY FRAUD

In a troubling example of how scammers exploit victims not once, but twice, an individual who had previously lost funds in a cryptocurrency investment scam was targeted again, this time through a recovery scam. The victim was contacted by someone claiming to represent Anivestix[.]net, and using a UK mobile number. They stated that the victim was entitled to compensation for losses incurred through dealings with a company called EllandRoad Capital (all of these supposed 'companies' are simply fronts for criminal investment scams) .

To receive the supposed compensation amounting to 0.26 BTC the victim was told to set up a new cryptocurrency wallet and contribute 5–10% of the compensation value as a deposit. This tactic is common in recovery scams, where fraudsters demand upfront payments under the guise of processing fees, legal costs, or security deposits. After transferring the required amount to their crypto wallet, the victim was instructed to send it to an account on exchangetitan.com, allegedly to "create a bridge in blockchain".

Once the funds were sent, communication ceased. No compensation was received, and the deposit was never returned. Attempts to contact the scammer were unsuccessful, leaving the victim not only without their original funds but now also out of pocket from the second scam.

This case highlights the emotional and financial vulnerability that scammers prey upon. After an initial loss, victims are often desperate for resolution, making them more susceptible to promises of recovery. Scammers exploit this by using official-sounding language, fake company names, and increasingly, AI-generated content, such as emails, documents, or even fake representatives, to appear legitimate.

This case serves as a reminder that scammers often return to the same victims, using new tactics and technologies to exploit their hope for justice. Awareness, caution, and scepticism are essential tools in protecting yourself from further harm.

IS THIS REAL OR A SCAM? THE NEW CHALLENGE OF DIGITAL TRUST

In a recent incident reported to the SERS, a member of the public expressed concern about an email that appeared to be from a local bank. The message looked highly official, with genuine-looking email addresses, branding, and links. It asked the recipient to update their tax status by clicking a link or scanning a QR code to access an online form. Despite its professional appearance, the recipient was unsure of its legitimacy, noting that the request felt unexpected and the language used seemed slightly off for a bank. The individual, a long-term Manx resident with straightforward tax affairs, questioned why such information would be needed and whether the email was safe to engage with.

The email was ultimately confirmed to be legitimate. However, the fact that it raised suspicion even among cautious and digitally literate individuals, highlights a growing challenge for legitimate businesses: ensuring their communications are clearly distinguishable from scams. In an era where phishing emails and impersonation attempts are increasingly sophisticated, even genuine messages can trigger doubt, especially when they arrive unexpectedly or request personal information.

The individual was advised that SERS could not verify the content of the message and ,as a precaution, it was recommended that they contact the bank directly using a trusted phone number.

This case shows how important it is for businesses to design communications that are not only secure but also easily trusted by recipients. In a time saturated with fraud attempts, trust is built not just through security, but through clarity, consistency, and transparency. Even legitimate emails can be disregarded if they resemble scams making thoughtful communication design a critical part of customer engagement and protection.

THEY HAVE YOUR NUMBER—NOW WHAT? A LOOK INTO SCAM MESSAGES

During the period we received a report from a concerned member of the public about a suspicious group text message. The message, titled “Group Chat,” was sent to a list of 10 to 11 recipients and claimed to be a notification of a Penalty Charge Notice (PCN) for a parking violation. It warned of an outstanding fine due on 1 July 2025 and threatened serious consequences such as damage to credit history and licence suspension. The message included a link to a non-governmental website and urged recipients to act immediately.

This incident highlights the importance of critical thinking and digital awareness when receiving unexpected messages. Anyone receiving such a message should immediately ask themselves two essential questions:

How do they have my phone number or personal details?”

If you receive a message out of the blue, especially one that includes personal threats or demands, pause and consider how the sender might have obtained your contact information. Was your number part of a data breach? Did you share it on a public platform or with an untrusted app? Scammers often collect phone numbers through leaked databases, online forms, or social engineering tactics. If the message is part of a group chat with other unknown numbers, it’s a strong sign that your data may have been harvested in bulk.

“Who is contacting me, and why?”

Always question the legitimacy of the sender. Does the message come from an official source? Is the web link trustworthy and clearly associated with a government domain? In this case, the domain used is not a legitimate government website, despite its official-sounding name. Scammers often impersonate authorities to create a sense of urgency and fear, pressuring recipients into clicking malicious links or providing sensitive information.

This case serves as a reminder that cybercriminals rely on panic and haste to exploit individuals. By taking a moment to ask these two questions, recipients can protect themselves from falling victim to phishing scams.

EXTERNAL THREAT COMMENTARY

THIRD-PARTY RISK: THE HIDDEN WEAKNESS IN CYBERSECURITY DEFENCES

As organisations grow more interconnected, their exposure to cyber threats increases—not just through their own systems, but through the partners and providers they rely on. Recent cyber incidents from May and June 2025 show how third-party risk is becoming one of the most dangerous and underestimated vulnerabilities in cybersecurity.

In healthcare, the ransomware attack on Synnovis, a pathology provider for major NHS hospitals, caused widespread disruption. Blood testing and diagnostics were halted, and sensitive patient data was leaked. The hospitals themselves weren't breached, but their reliance on Synnovis left them exposed. This incident showed how a single supplier can become a critical point of failure.

A similar situation unfolded at Glasgow City Council, where a cyberattack disrupted public services. The breach originated from a third-party IT provider, not the council's own systems. Although no data theft was confirmed, the attack forced systems offline and created uncertainty for residents.

Even in the fintech sector, where cybersecurity is often a top priority, third-party risk played a role. At Coinbase, attackers exploited weaknesses in access controls and system segmentation, likely worsened by external integrations. Once inside, they were able to move laterally and access sensitive user data.

These examples highlight a growing trend. Cybercriminals are increasingly targeting supply chains and service providers to bypass direct defences. Organisations must now assess not only their own security posture but also that of every vendor and platform they depend on.

Managing third-party risk means more than signing contracts. It requires regular audits, strict access controls, and clear expectations for cybersecurity standards. It also demands preparation for the possibility of failure, with response plans that account for supplier breaches and communication strategies that maintain public trust.

The lesson is clear: your cybersecurity is only as strong as the weakest link in your digital ecosystem. And that link might not be under your control—but the consequences will be.

CYBER RESILIENCE IN ACTION: WHAT THE M&S ATTACK TEACHES US ABOUT RECOVERY AND BUSINESS CONTINUITY

The recent cyber attack on Marks & Spencer (M&S) has once again highlighted the evolving sophistication of cyber threats and the critical importance of resilience and business continuity in the face of disruption. According to M&S Chairman Archie Norman, the breach began with a "sophisticated impersonation" of a third party, which allowed attackers to infiltrate the company's systems undetected for days.

The attack, which took place in April 2025, caused widespread operational disruption. Shelves were left empty, online services were limited, and the company was forced into what Norman described as "rebuild mode", a process that will continue for "some time to come".

While the full extent of the damage is still being assessed, the incident shows: cybersecurity is not just about prevention, it's about preparation for recovery.

Why Resilience Matters

No organisation is immune to cyber threats. Even with robust defences, attackers are finding new ways to exploit human error, third-party vulnerabilities, and social engineering tactics. What sets resilient organisations apart is not the absence of attacks, but their ability to respond, recover, and continue operating.

M&S's experience illustrates this well. Despite the severity of the breach, the company acted quickly to notify authorities, including the National Crime Agency and, and made a strategic decision not to engage directly with the attackers . This approach reflects a growing recognition that post-attack decisions are as critical as pre-attack defences.

"Make sure you can run your business on pen and paper."

This isn't just a throwaway line, it's a reminder that business continuity planning (BCP) must account for total system failure. Whether it's maintaining manual processes, having offline backups, or training staff for emergency scenarios, continuity planning ensures that essential operations can continue even when digital systems are compromised.

The M&S attack is a wake-up call for businesses of all sizes. It shows that:

- Cyber resilience must be embedded across the organisation, not just in IT
- Communication is key, both internally and with customers, who need timely, transparent updates.
- Recovery is not just technical, it's operational, reputational, and strategic.

As cyber threats grow more complex, so too must our responses. Resilience and business continuity are no longer optional and are essential pillars of modern risk management.

NO ONE IS UNTOUCHABLE: HOW CYBER THREATS ARE HUMBLING THE WORLD'S BIGGEST ORGANISATIONS

In an era where digital infrastructure underpins nearly every aspect of modern life, the belief that size, reputation, or investment in technology can shield an organisation from cyber threats is being shattered. The months of May and June 2025 offered a sobering reminder that no entity, whether a multinational corporation, a public institution, or a critical service provider, is immune to the growing sophistication of cyberattacks.

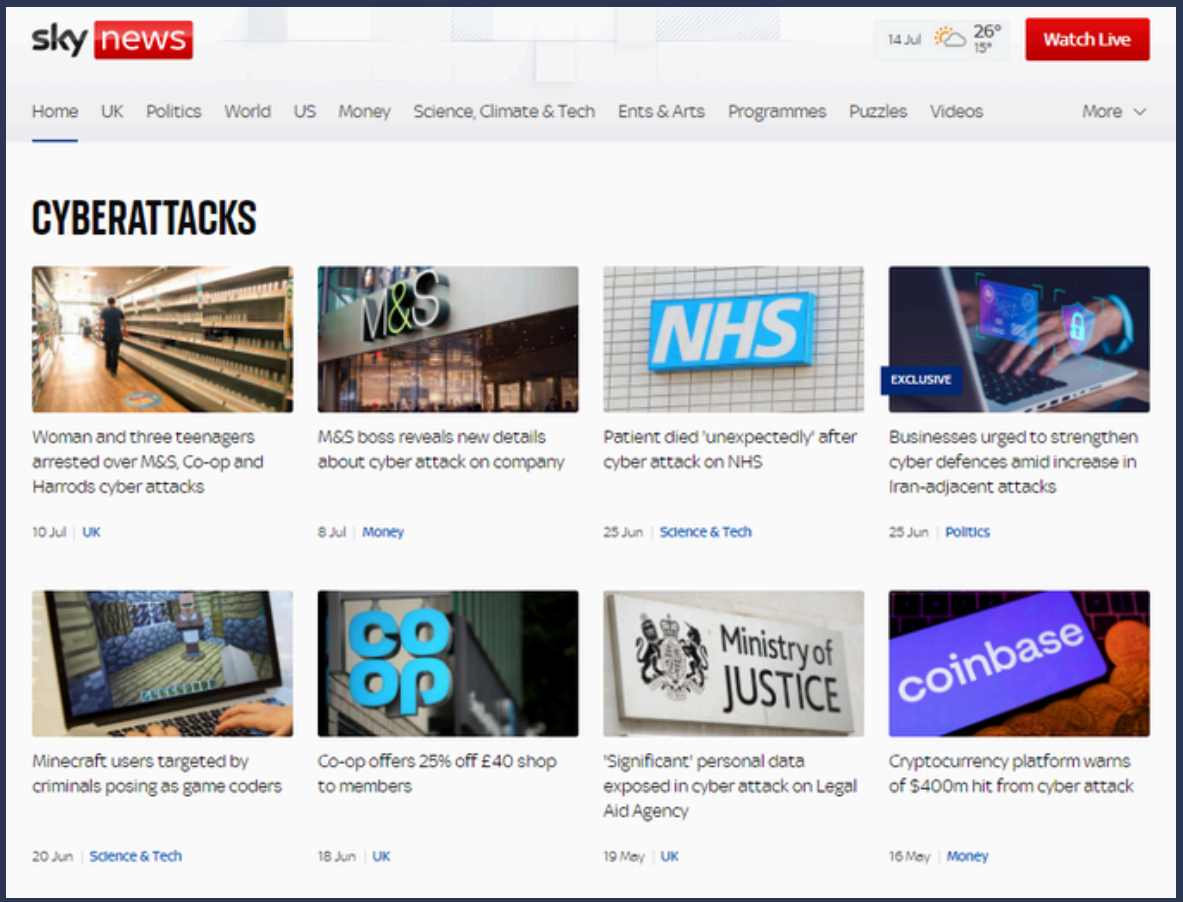
Take Coca-Cola, a global brand with vast resources and a long-standing presence in international markets. Despite its scale and likely investment in cybersecurity, the company fell victim to the Everest ransomware group. After refusing to pay a ransom, Coca-Cola saw over 1,000 internal files leaked online, including sensitive employee data such as passport scans, visa documents, and salary records. The breach not only exposed individuals to identity fraud and phishing but also highlighted how even the most fortified companies can be brought to their knees when attackers are determined and data is poorly segmented.

Meanwhile, the aviation industry, known for its reliance on cutting-edge technology and stringent operational protocols, faced its own reckoning. In just one week, Qantas, WestJet, and Hawaiian Airlines all reported cyber incidents that disrupted bookings and check-ins. These attacks, attributed to the hacker group Scattered Spider, exploited customer-facing systems using advanced social engineering. Despite the high-tech nature of the industry, legacy systems and the pressure of real-time service delivery created vulnerabilities that attackers were quick to exploit.

These incidents are not isolated. They reflect a broader trend: the increasing boldness and capability of cybercriminals, and the widening attack surface created by digital transformation. Whether it's a city council like Oxford or Glasgow, a retail giant like The North Face, or a fintech leader like Coinbase, the message is clear, no one is too big, too advanced, or too prepared to be targeted.

What unites these cases is not just the scale of the organisations involved, but the common thread of underestimating the evolving nature of cyber threats. From credential stuffing and ransomware to zero-day exploits and social engineering, attackers are constantly adapting. And while technology can help detect and respond to threats, it cannot replace the need for proactive security culture, robust incident response plans, and continuous vigilance.

In the end, the lesson is stark: cybersecurity is not a one-time investment or a box to be ticked. It is an ongoing battle, and complacency no matter how well-funded can be catastrophic.



Cyberattacks are now a frequent feature in the news

CYBER GLOSSARY

2-step verification (2SV): Sometimes called 2FA or MFA is a second way to confirm your identity to help keep your personal and financial information from being compromised or stolen.

Anti-virus software: Designed to identify and remove computer viruses, other malware and spyware on a device or IT system. To be effective, it should be kept up-to-date with the latest anti-virus signatures and definitions.

Backdoor: A backdoor is a method of avoiding normal authentication on a device. They are often used for securing remote access to a computer, or obtaining access to plaintext in cryptographic systems

Common Vulnerabilities and Exposures (CVE): The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures.

Cryptocurrency: A cryptocurrency is a digital asset that is designed to act as an exchange medium. They use cryptography to verify and secure transactions, control the creation of new assets and protect the identity of asset holders.

Dark web: A collection of thousands of websites which are not indexed by conventional search engines. They often use anonymity tools, like the Tor network, to hide their IP address and preserve the anonymity of the creators and visitors.

Encryption: A method to scramble a message, file or other data and turn it into a secret code using an algorithm (complex mathematical formula). The code can only be read using a key or other piece of information (such as a password) which can decrypt the code.

Firewall: A security system that monitors and controls traffic between an internal network (trusted to be secure) and an external network (not trusted). It is generally considered insufficient against modern cyber threats.

General Data Protection Regulation - GDPR: The General Data Protection Regulation (GDPR) 2016/679 is a European Union regulation covering data protection and individual privacy rights. It was introduced in April 2018 and enforced on May 25 2018.

Hacker: A hacker is a computer and networking attacker who systematically attempts to penetrate a computer system or network using tools and attack methods to find and exploit security vulnerabilities.

IP address: An IP address (Internet Protocol Address) is a label assigned to computer devices. An IP address is essential for Internet Protocol communication.

Keylogging: Keylogging, also known as keystroke logging or keyboard capture, is the action of recording, often secretly, the keys struck on a keyboard.

Malware: Malware is malicious or hostile software used to disrupt, damage or compromise a computer system or network

Patch management: Patch management covers acquiring, testing and installing multiple patches (manufacturer released code changes) to a computer system or application. Firmware and software vendors release patches to fix defects, change functionality and to address known security vulnerabilities.

Phishing: Phishing is a type of fraud in which the attacker attempts to steal sensitive data such as passwords or credit card numbers, via social engineering.

Ransomware: A type of malware that prevents access to the target's computer system or data until a ransom is paid to the attacker.

Smishing: A type of phishing attack that uses text messages (or other types instead of mobile messaging such as MMS or IM services) instead of email messages.

Social engineering: An attack method that tricks people into breaking normal security procedures by masquerading as a reputable entity or person in email, IM or other communication channels.

Vulnerability: A vulnerability is a weakness that allows an attacker to compromise security (integrity, confidentiality or availability).

ABOUT US

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.

CYBERISLE 2025

The Islands premier cyber-security conference returns to the Comis Hotel and Golf Resort on the October 15, in what will be its seventh year.

Previous CYBERISLEs have featured speakers including representatives from the National Cyber Security Centres, Microsoft, NCC Group, and a other key-speakers from the industry.

This year's theme, "**Building a Resilient Island**", focuses on the importance of fortifying digital infrastructure and developing the appropriate security measures to safeguard the island's critical systems. As the island addresses evolving global cyber challenges, efforts such as the forthcoming National Infrastructure Security Bill will play a key role in setting the legal and regulatory foundation for greater resilience.

The conference will focus on practical strategies for resilience, bringing together experts, practitioners, and policymakers. Keynotes and panel discussions will cover incident response, public-private collaboration, supply chain security, and regulatory readiness to strengthen the island's cyber resilience.

The event is organised by the Cyber Security Centre for the Isle of Man, a part of OCSIA, and run on a cost-neutral principle. The event is supported through sponsorship.

Disclaimer

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

Open Government Licence

Cyber Security Centre for the Isle of Man

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

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

Office of Cyber-Security & Information Assurance
Second Floor
27-29 Prospect Hill
Douglas
Isle of Man
IM1 1ET

T: +44 1624 685557

Isle of Man Government
Reiltys Ellan Vannin