Cyber Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

July - August 2025

INTRODUCTION

For the period 1st July-31st August

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**
International Threats	**12**
Cyber Glossary	**18**
About Us	**20**

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 28,100 suspicious emails. In July and August 2025, we received 1,506 suspicious emails.

SUSPICIOUS EMAILS

1,506 REPORTED

in July and August

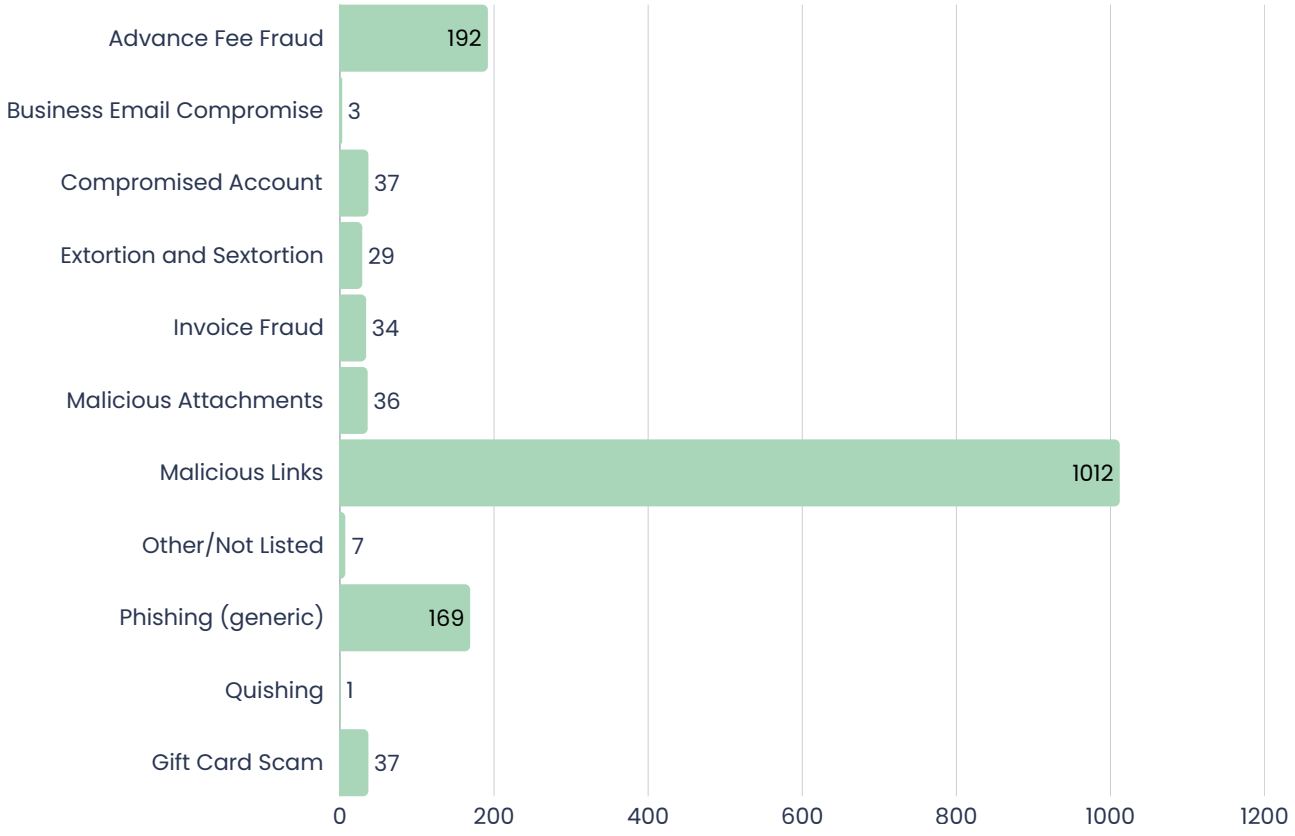
Detail

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. Anti-malware software
3. Investment Platforms
4. Competition and Rewards
5. Cloud Storage Warnings



CYBER CONCERNS

69 REPORTED

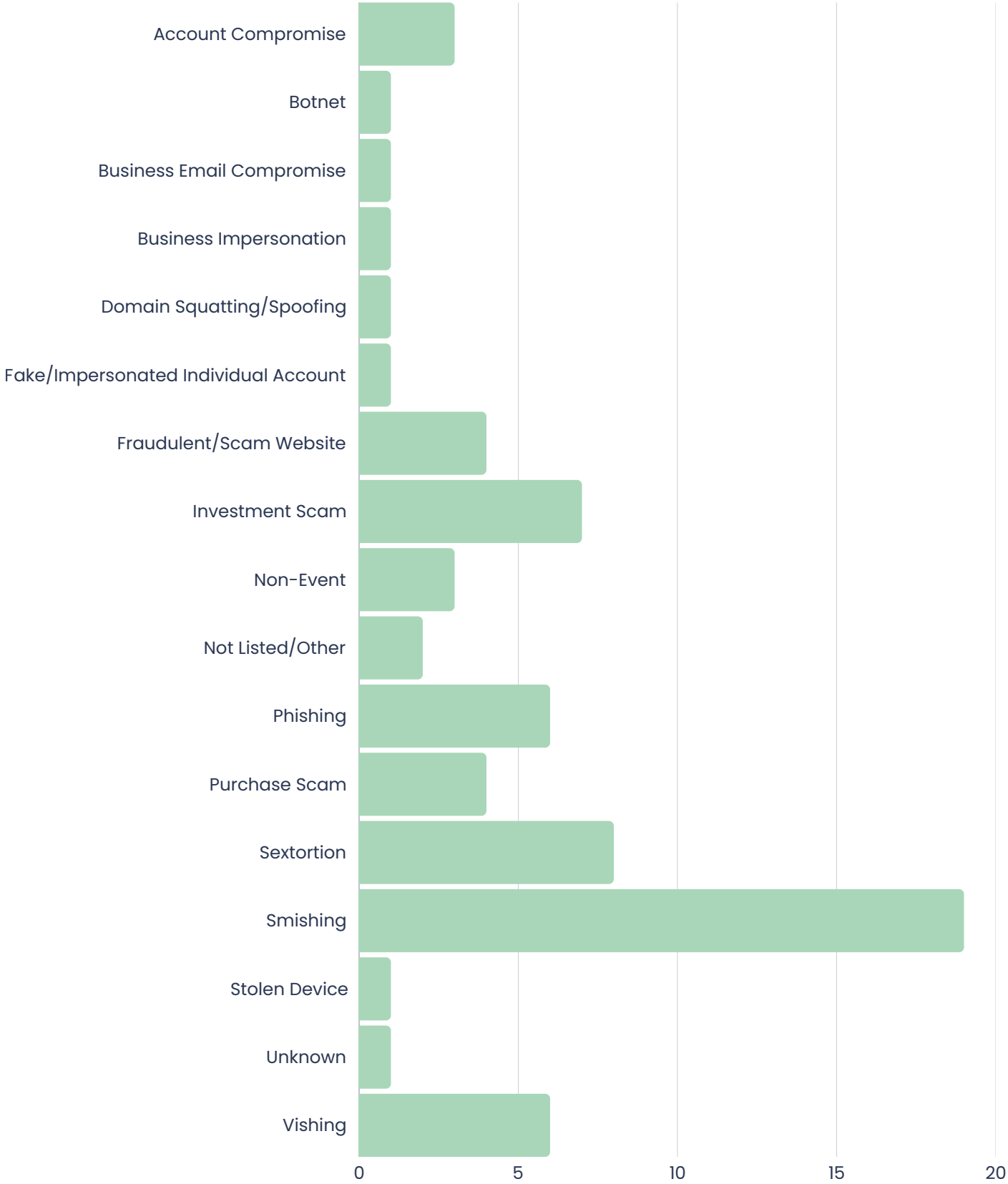
in July and August

Detail

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

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 local 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: July and August



ISLE OF MAN THREAT COMMENTARY

PERSONAL

MULTI-FACTOR AUTHENTICATION (MFA)

MFA (multi-factor authentication) is a security method that adds an extra layer of protection beyond your password. Even if your password is stolen, attackers would still need your phone, fingerprint, or security key, making break-ins much harder. Since passwords are often reused and exposed in data breaches, MFA adds a crucial extra layer of protection to keep accounts and data safe. Some platforms call it 2FA or 2SV; all are simply variations of the same idea: extra security beyond your password.

Key Benefits of enabling MFA include:

- Keeping your accounts safer – It's much harder for hackers to break in.
- Protecting you if your password leaks – A stolen password isn't enough.
- Adding peace of mind – Extra protection for your personal and financial info.
- Shielding you from common scams – Like phishing or password-guessing attacks.

If MFA is not enabled, an account is at higher risk of being hijacked by attackers. The Cyber Security Centre regularly receives reports of residents having had their email account taken over by online scammers, which might have been prevented by protecting their account with MFA. And in one case, a victim's X (formerly Twitter) account was hijacked after the attacker successfully logged in and changed the account's contact details. The compromised account was then used to impersonate a family member and post fraudulent ticket sale adverts, potentially exposing others to financial harm. We also received a report of a local business that had been affected by the compromise of an email account where MFA had not been enabled. These reports highlight the importance of enabling Multi-Factor Authentication (MFA) on all online accounts as MFA would have acted like a second wall, blocking the attacker.

We strongly recommend that all residents and organisations review their account security settings and enable MFA wherever possible. This is essential not only for protecting personal accounts but also for safeguarding business email accounts, which are often targeted by scammers to send fraudulent messages or access sensitive data.

JUNK MAIL

When scam and phishing emails show up, many people instinctively block the sender, thinking it's the proper thing to do and hoping it'll stop more emails coming through. Using the 'Block' option will block that specific email address, but scammers tend to only use their email addresses for a very short time, meaning there is little or no benefit to blocking their email addresses.

If the emails are appearing in your main inbox, a much better approach is to mark suspicious messages as junk or spam. By doing this, you train your email system to recognise similar messages in the future. Spam filters are designed to learn from your feedback, so each time you recategorise a message, it helps the system automatically divert comparable scams away from your inbox. This not only keeps your inbox cleaner but also improves your overall protection against fraud.

During July and August, Manx.net was the most impersonated service in reported scam attempts. One resident told us they felt frustrated after receiving disturbing or recurrent bogus emails and found that blocking the sender made no difference. This reflects a common misconception: many people believe blocking will stop scammers, but, in reality, it rarely has any effect. Instead, using the 'Report Spam' option is far more effective, as it helps your email provider's filters learn and adapt to block similar malicious messages in the future.

BUSINESS & ORGANISATIONS

FINANCIAL FIRM BREACHED THROUGH REMOTE ACCESS

Recently, a cybersecurity alert was raised when unauthorised access to a financial company was advertised on a dark web hacker forum. The listing described access via Remote Desktop Web, with control over command-line tools and system-level functions, suggesting a serious compromise of the company's internal infrastructure. The environment was identified as a Microsoft Windows Server 2016 domain supporting a small team and a high revenue.

Initial findings pointed to the possible re-use of an outdated multi-factor authentication (MFA) token, which may have been exploited to gain unauthorised access. The case underscores the importance of monitoring for dark web threats, maintaining strong authentication practices, and ensuring the quick removal of unused credentials.

DOMAIN IMPERSONATION

Domain impersonation is a cyber threat where malicious actors register domain names that closely resemble legitimate businesses, with the intent to mislead users, steal credentials, spread malware, or damage reputations.

A common tactic involves creating look-alike websites that mimic official pages, often using subtle misspellings or alternate domain extensions. For instance, 'iom-secure.com' instead of the legitimate 'iombank.com'. These deceptive sites are typically used for phishing, malware distribution, or brand abuse.

If you suspect domain impersonation targeting your organisation, please contact the CSC. Our team can help assess the situation, guide you through the appropriate response, and coordinate takedown efforts with hosting providers. We're here to support your organisation.

To reduce the risk of domain impersonation and protect your organisation's online presence:

- **Register common variants** of your domain name, including misspellings and alternative top-level domains (TLDs).
- **Monitor domain registrations** regularly for suspicious or similar names.

THREAT REPORT: SPOTLIGHT

NETWORK ATTACHED STORAGE (NAS): ARE YOU SERVING YOUR ORGANISATION ON A PLATE TO CYBER CRIMINALS?

Network Attached Storage (NAS) devices offer small and medium-sized businesses a cost-effective way to store, share, and manage data. While cloud adoption is growing, many organisations still rely on NAS and will continue to do so during their transition to online platforms.

From transferring large files and archiving documents to streaming media and reducing local storage demands, NAS provides versatile functionality. However, this convenience can come at a steep cost if security is neglected.

The Hidden Risk
Although NAS servers can be isolated from the Internet or restricted to internal IP ranges, they are all too often left exposed making them prime targets for cybercriminals. Attackers don't need social engineering or complex hacks, a vulnerable server is enough to infiltrate a network and cause serious damage.

Many businesses assume they are too small to be targeted, but cybercriminals often seek out low-profile, easy targets. It's quick, easy, and attracts little attention.

Real-World Vulnerabilities
Even reputable brands can present risks if not properly managed:

- Synology – CVE-2024-10441 (CVSS 9.8): Critical remote code execution via improper output encoding in DSM.
- QNAP – CVE-2024-48859 (CVSS 5.3): Authentication flaw allowing remote compromise of QTS and QuTS hero OS.
- Western Digital – CVE-2023-22815 (CVSS 8.8): Post-authentication command injection affecting multiple My Cloud models.

These vulnerabilities are easily discoverable and exploitable with public tools, leaving networks and data wide open.

What You Can Do

For Business Leaders:

- Treat your digital environment like your physical one. Secure it, maintain it, and restrict access.
- Work with IT to maintain asset registers for visibility and threat reduction.
- Follow 'secure-by-design' principles from design to operation.
- Regularly review and test policies, procedures, and processes.

For IT Administrators & Individuals:

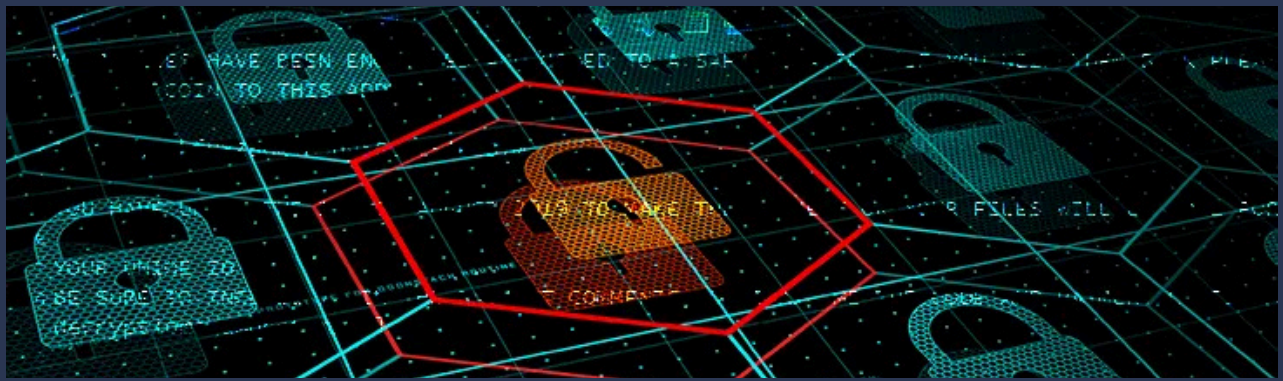
- Update regularly—monitor and install patches and firmware updates.
- Restrict Internet exposure—avoid exposing web interfaces unless necessary.
- Use strong authentication—enable 2FA and complex passwords.
- Monitor logs and traffic for unusual activity.
- Backup frequently—keep offline backups for ransomware or data loss recovery.

Notable Mentions

- Plex Media Server: Popular for organising and streaming media.
  - CVE-2025-34158: Remote Code Execution vulnerability (CVSS 10.0).
- File Transfer Protocol (FTP): Widely used but inherently insecure. Use secure and encrypted protocols (e.g. sFTP, FTPS) in well-configured environments.

For both Plex and FTP:

- Regularly monitor for updates (enable auto-update if possible).
- Use strong passwords.
- Restrict Internet access where possible; if required, ensure:
  - Firewalls are configured and maintained.
  - Principle of least privilege is applied (no remote admin access).



INTERNATIONAL THREATS

UK RISES TO THIRD PLACE AMONGST MOST TARGETED COUNTRY FOR CYBERATTACKS

The United Kingdom has been identified as the third most targeted nation in the world for cyberattacks, following the United States and Canada, according to a recent cybersecurity report. Between April and June 2025, UK organisations faced more than 100 million malicious attempts, signalling a sharp increase in cybercriminal activity.

Experts attribute the surge to the UK's highly digital economy, which presents multiple avenues for cyber exploitation. Common attack methods include phishing emails, fake text messages, malicious websites, and malware-laden attachments. Cybercriminals frequently impersonate well-known entities such as Amazon, Google, and HM Revenue and Customs to trick individuals into divulging sensitive financial or personal information.

The report also noted a seven per cent increase in malware threats compared with the previous quarter, reflecting a broader global trend. Cybersecurity analysts warn that without appropriate and strong protection measures, both businesses and individuals are increasingly vulnerable to data breaches, ransomware attacks, and financial fraud.

Authorities and industry specialists are urging companies to adopt stronger cybersecurity protocols, including staff training on recognising suspicious communications, regular system updates, and comprehensive monitoring of digital networks. Consumers are similarly advised to remain vigilant, carefully verify messages from unfamiliar sources, and maintain up-to-date antivirus protection. The findings underline the growing sophistication of cybercriminals and the critical importance of proactive security measures. With attacks rising in frequency and complexity, the report highlights that both the public and private sectors must invest in resilience and awareness to protect sensitive information and maintain confidence in the nation's digital infrastructure.

SALESFORCE & SALESLOFT

During the past two months, a wave of cyberattacks has shown how vulnerable modern organisations are, especially when third-party tools, supply-chain connections, or misconfigured cloud systems are involved. Over 700 organisations have been affected through breaches tied to Salesloft and Salesforce, underscoring the scale of the threat. From finance and healthcare to telecoms, education, and government, July and August 2025 confirmed that no sector is safe.

Late August revealed a breach involving Salesforce and the AI chatbot Salesloft Drift. Threat actors exploited compromised OAuth tokens, which grant applications limited access to user accounts without requiring passwords, to steal data from hundreds of organisations. Exposed data included access keys (AWS), passwords, Snowflake tokens, names, phone numbers, metadata, and business contact details. Firms confirming compromise include SpyCloud, Tanium, Proofpoint, and Tenable.

Two high-profile organisations suffered cyberattacks involving Salesforce integration:

Louis Vuitton – Global customer data compromised
In early July, Louis Vuitton confirmed a cyber-attack spanning the UK, Italy, and South Korea. Data stolen included names, contact details, purchase histories, and passport numbers. Linked to ShinyHunters, the breach likely stemmed from a third-party vendor, highlighting supply-chain risks. Around 419,000 Hong Kong customers were affected, prompting regulatory investigations.

Allianz Life – Over 1.1 million records exposed
Mid-July saw Allianz Life disclose a breach involving a third-party cloud CRM system. Attackers used social engineering to access names, Social Security numbers, and dates of birth. Attributed to ShinyHunters, the incident underscores vendor vulnerabilities. Allianz has offered identity protection services and pledged stronger security measures as experts warn of potential fraud and phishing.

Implications and what organisations should do:

- **Secure Vendor Integrations:** Audit third-party tools (CRM, chatbots, OAuth). Enforce least privilege and strong authentication.
- **Patch Fast:** Zero-days spread quickly – maintain a vulnerability management process and isolate unpatched systems.
- **Watch for Credential Abuse:** Monitor logs for unusual data flows or token misuse, as seen in the Salesforce-Drift breach.
- **Limit Data Exposure:** Apply data minimisation and segment systems to reduce the blast radius of a breach.
- **Be Incident-Ready:** Prepare clear response and communication plans – speed matters when breaches occur.

Overall, July and August 2025 have shown attackers increasingly exploit weak links in supply chains and software services, not just classic perimeter defences. Many organisations are being brought down not by what they host themselves but by what they connect to.

UK TELECOMS HIT BY CYBER INCIDENT AS GLOBAL ALERT WARNS OF CHINESE HACKING CAMPAIGN

In recent weeks the UK has witnessed a sharp escalation in cyber-incidents that underscore growing concern about threats appearing to originate from China, particularly in light of new intelligence released by CISA, the FBI, the UK's NCSC and other agencies. Among these, two developments stand out: the telecoms provider Colt was struck by a cyberattack in mid-August that disrupted its support services, and global advisories have exposed the vast scale and persistence of the foreign state actors espionage campaign, which is now clearly understood to be targeting infrastructure in the UK among many other countries.

Colt Technology Services confirmed that an internal system, separate from customer infrastructure, was compromised on 12 August; services including its Customer Portal and Voice API platform were taken offline as a precaution. Internally held data including employee salary records, contracts and network design details are reported to have been stolen. Meanwhile, joint advisories from CISA, the FBI, NSA, and international partners have made public the tactics used by Chinese state-sponsored threat actors . These bodies have detailed how unpatched network-edge devices (edge routers, backbone routers, firewalls) are being exploited to gain stealthy access to telecommunications, government, transport, lodging and military networks. The reports emphasise years-long campaigns, command-and-control domains hidden in historical DNS logs, persistent access via compromised router firmware, and the exploitation of publicly known vulnerabilities rather than zero-days.

This changing posture of awareness marks a turning point: state-linked cyber threats are now routinely named, attributed, and tied directly to risks facing UK critical infrastructure. The UK government and its allies have issued successive advisories urging critical infrastructure operators to hunt for indicators of compromise, patch known vulnerabilities swiftly, lock down access controls, monitor network-edge equipment intensively, and ensure resilience in telecoms and supply-chain systems. As the scale and duration of foreign state actors and related operations become more visible, the imperative for strong cyber-hygiene and state-private cooperation has never been clearer.

CYBERATTACKS SURGE ACROSS DUTCH CARIBBEAN GOVERNMENTS AND INSTITUTIONS

The Dutch Caribbean, comprising Curaçao, Aruba and Sint Maarten, is facing a clear reminder of how disruptive cyberattacks can be for smaller jurisdictions with limited resources. A series of incidents this summer disrupted essential government services, highlighting the region's vulnerability and the urgent need for stronger cyber resilience.

The crisis began on 24 July, when Curaçao's Tax and Customs Administration was crippled by a ransomware attack. Services such as the Motor Vehicle Tax Department were shut down, phone lines went silent, and recovery took weeks, even with cybersecurity experts flown in from the Netherlands. Officials confirmed that full restoration of customer support and internal systems required extensive effort.

Just days earlier, the Joint Court of Justice, which serves multiple islands including Bonaire, Saba and Sint Eustatius, suffered a major outage between 23 and 28 July, delaying legal proceedings and forcing the public to resend emails. In Aruba, a compromised parliamentary email account sparked a phishing campaign, prompting urgent warnings to citizens.

Experts warn these attacks exploit systemic weaknesses, such as outdated infrastructure and reliance on third-party tools like Citrix NetScaler, and mirror a growing ransomware trend across the Caribbean. Similar incidents have hit the Bahamas, Turks and Caicos, and Costa Rica.

The situation echoes Bermuda's 2023 cyber crisis, which paralysed government IT systems for months and disrupted courts, customs and payments. That event pushed Bermuda to create a Cybersecurity Incident Response Team (CSIRT) and tighten legislation, measures now seen as essential for other island nations.

For smaller jurisdictions, the message is clear: a single cyberattack can cripple critical services for weeks, making strong defences and rapid response capabilities essential.

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 is on 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 Isle of Man's cybersecurity conference is to take place at the Comis Hotel in Santon next month. CYBERISLE 2025 will give people the chance to hear industry experts from across the British Isles talk about critical cyber threats.

Key speakers from global leaders such as Microsoft, Arctic Wolf and Sophos will share their insights about ever-evolving threats.

Attendees will learn more about topical issues, such as the recent attacks on the retail sector. They will also be given some practical advice about the role every individual plays in keeping the Island safe.

Minister for Justice and Home Affairs, Jane Poole-Wilson MHK, said:
'CYBERISLE is designed to give people and organisations the practical knowledge and tools they need to stay secure in today's digital landscape.

'I strongly recommend registering for a free ticket and taking full advantage of the opportunity to hear from leading experts visiting from across the British Isles. Their insights will be key in helping us to build a safer, more resilient island in the face of rising cyber threats.'

Key sessions include:

- *Emerging Cyber Threats:* Highlighting the latest trends in cybercrime.
- *Recent Attacks on the Retail Sector*: Review of the 2025 cyberattacks on UK retailers.
- *Understanding AI as a Cyber Threat*: Insights into how AI is reshaping the threat landscape.
- *Building resilience*: How to prepare and respond in the event of an incident

CYBERISLE will take place on **Wednesday, 15 October** and free tickets are available here.

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