Cyber Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

September - October 2025

INTRODUCTION

For the period 1st September-31st October

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

CYBERISLE 2025 RECAP

On the 15th of October, the Isle of Man's premier cybersecurity conference took place at the Comis Hotel, bringing together industry experts from across the British Isles to discuss today's most critical cyber threats.

A big thank you to the 300+ attendees who helped make this year's event such a success! From thought-provoking panels to hands-on breakout sessions, the day was packed with valuable insights.

We were proud to welcome key speakers from global leaders including Microsoft, Arctic Wolf, and Sophos, who shared their expertise on the ever-evolving threat landscape. Attendees explored topical issues such as the recent attacks on the retail sector and learned how every individual plays a vital role in keeping the Island secure.

Highlights included:

- Emerging Cyber Threats – The latest trends in cybercrime.
- Recent Attacks on the Retail Sector – A review of the 2025 incidents affecting UK retailers.
- Understanding AI as a Cyber Threat – How AI is reshaping the threat landscape.
- Building Resilience – Preparing for and responding to cyber incidents.

Missed a session or want to revisit the highlights? Access presentation slides and key resources here: CYBERISLE Highlights.

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 September and October 2025, we received 1,158 suspicious emails.

SUSPICIOUS EMAILS

1,158 REPORTED

in September and October

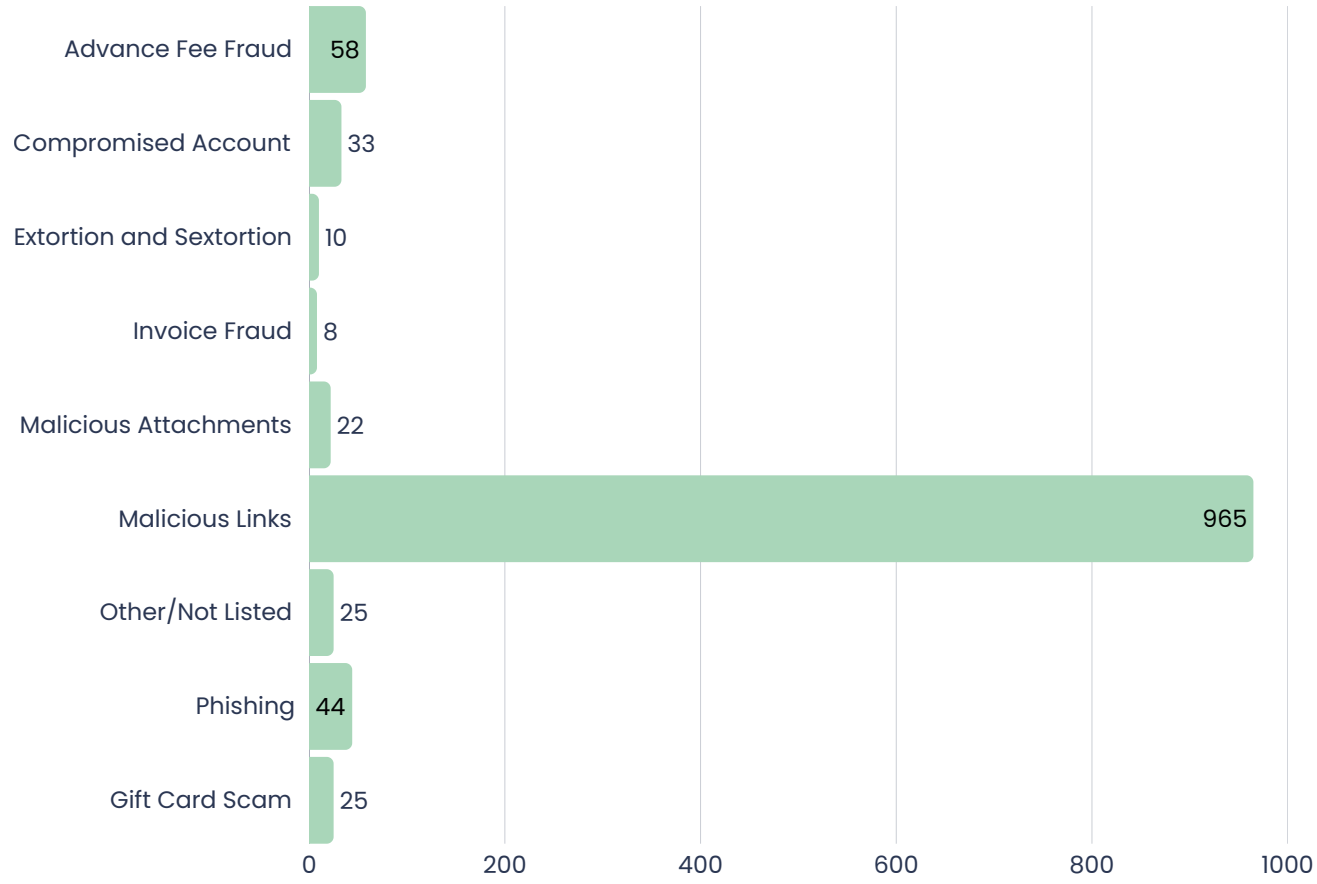
Detail

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. Banking
3. Competitions and Rewards
4. Anti-malware Software
5. PayPal



CYBER CONCERNS

79 REPORTED

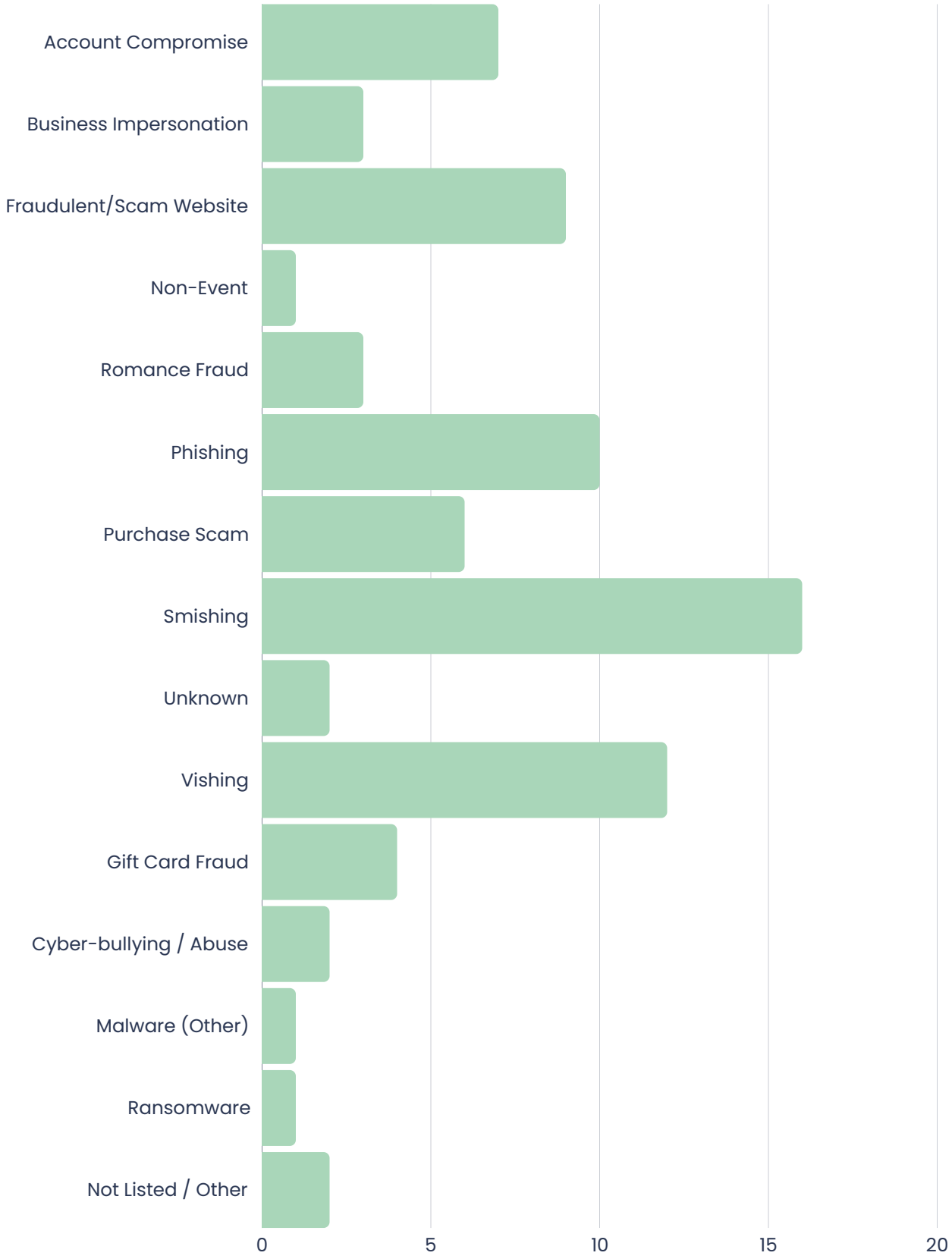
in September and October

Detail

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

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: September and October



ISLE OF MAN THREAT COMMENTARY

BUSINESS AND ORGANISATIONS

SECURITY RISKS IN SUPPLIER AND THIRD-PARTY COMMUNICATIONS: LESSONS FROM RECENT EMAIL COMPROMISES

Many businesses rely heavily on suppliers, contractors, and other third parties to deliver essential services. However, this interconnectedness also creates shared risk. When a supplier's email account is compromised, attackers can exploit the trust between companies and clients to send highly convincing phishing emails, request payments, or attempt to access internal systems. This makes supplier and third-party communication a major aspect of business risk that cannot be overlooked.

Recent Local Incidents

Several Isle of Man companies in the construction sector. These incidents appear to have begun when staff at one company received phishing emails sent from a contractor whose account had already been breached.

Because the emails came from a familiar local business, staff were more likely to trust the message, making it easier for attackers to trick recipients into clicking links or entering login details. In several cases, compromised accounts then sent further phishing emails to additional companies, allowing the issue to spread across the Island.

This demonstrates how difficult these compromises can be to detect internally without thorough investigation.

Some companies reported the incident to the Cyber Security Centre, while others were contacted proactively after their emails appeared in the Suspicious Email Reporting Service (SERS).

Why These Incidents Matter

These cases demonstrate how a single weak link in the supply chain can quickly create problems for multiple businesses. Without clear processes for investigating incidents, updating security controls, and notifying affected partners, organisations risk:

- Reputational harm, especially if customers or contractors are targeted using their compromised account
- Financial loss, including invoice fraud or unauthorised access to sensitive systems
- Disruption, while accounts are disabled and restored
- Sector-wide impact, as malware or phishing attempts are forwarded onto other local companies

Key Protections and Why They Are Necessary

To strengthen security around supplier and third-party relationships, businesses should put the following measures in place:

- Vet vendors for basic security practices before onboarding

Understanding how your suppliers protect their own accounts helps prevent your business from inheriting their risks. Poor password hygiene or lack of security awareness can directly expose your business.

- Require MFA and strong password policies

Multi-factor authentication makes it significantly harder for attackers to use stolen credentials obtained through phishing. Without MFA, a single successful phish can lead to immediate account compromise.

- Monitor access and remove it when no longer needed

Old or unused accounts are easy targets for attackers. Ensuring permissions are current reduces exposure and limits damage if a vendor or your business is breached.

- Include cybersecurity clauses in contracts

Contracts should clearly state expectations regarding incident reporting, password controls, data handling, and required investigations. This ensures everyone understands their responsibilities before something goes wrong.

- Train staff to recognise phishing, especially from familiar contacts

Staff should understand that attackers often use compromised local accounts to send convincing emails. Any unexpected message containing links or attachments should be treated with caution and staff should feel comfortable disregarding anything that is even slightly suspicious or they must verify by phoning the other company before interacting with it.

Investigate Causes and Report Early

When a compromise occurs, it is vital that the root cause is fully investigated. Businesses must understand how the breach occurred to prevent it happening again.

Prompt reporting is critical to reducing risk. Staff should alert their IT team or provider immediately when a link was clicked or a file was opened. In such cases, it is highly recommended to engage a specialist cyber-security company to conduct a full investigation. This enables accurate assessment of the incident, complete remediation of any compromise, and identification of underlying vulnerabilities to prevent future attacks.

If a compromise of business accounts has occurred, we strongly encourage local businesses to report incidents to the Cyber Security Centre as early as possible. We can offer guidance, help assess the scale of the issue and, where appropriate, warn other organisations who would likely be at risk.

Please ensure staff report suspicious emails internally and to forward them to the Suspicious Emai Reporting Service (SERS) at SERS@ocsia.im. Forwarding the email to the SERS supports wider detection and protects other local businesses.

PERSONAL

AVOID FAKE TICKET SALES ON SOCIAL MEDIA

Buying tickets online can seem convenient, but scammers are increasingly exploiting social platforms and messaging apps to sell fake tickets for concerts, sports events, and festivals. These scams often target popular events where demand is high and tickets are scarce.

How These Scams Work:

Fraudsters create convincing posts or profiles claiming to have tickets for sale. They often use urgency ('limited tickets left') and sometimes even personal stories to build trust. Victims are asked to pay upfront by bank transfer or by using digital wallets. Once payment is made, the scammer disappears; no tickets, no refund.

Common Dangers:

- Financial loss: victims often lose the full amount paid for the tickets, as scammers usually request payment through irreversible methods such as bank transfers or instant payment apps. Payments are rarely recoverable.

- Identity exposure: sharing personal details can lead to further fraud. This information might later be used for account takeover attempts or targeted phishing

- Social engineering: scammers may impersonate friends or use 'hacked' (i.e. compromised) accounts to appear credible.

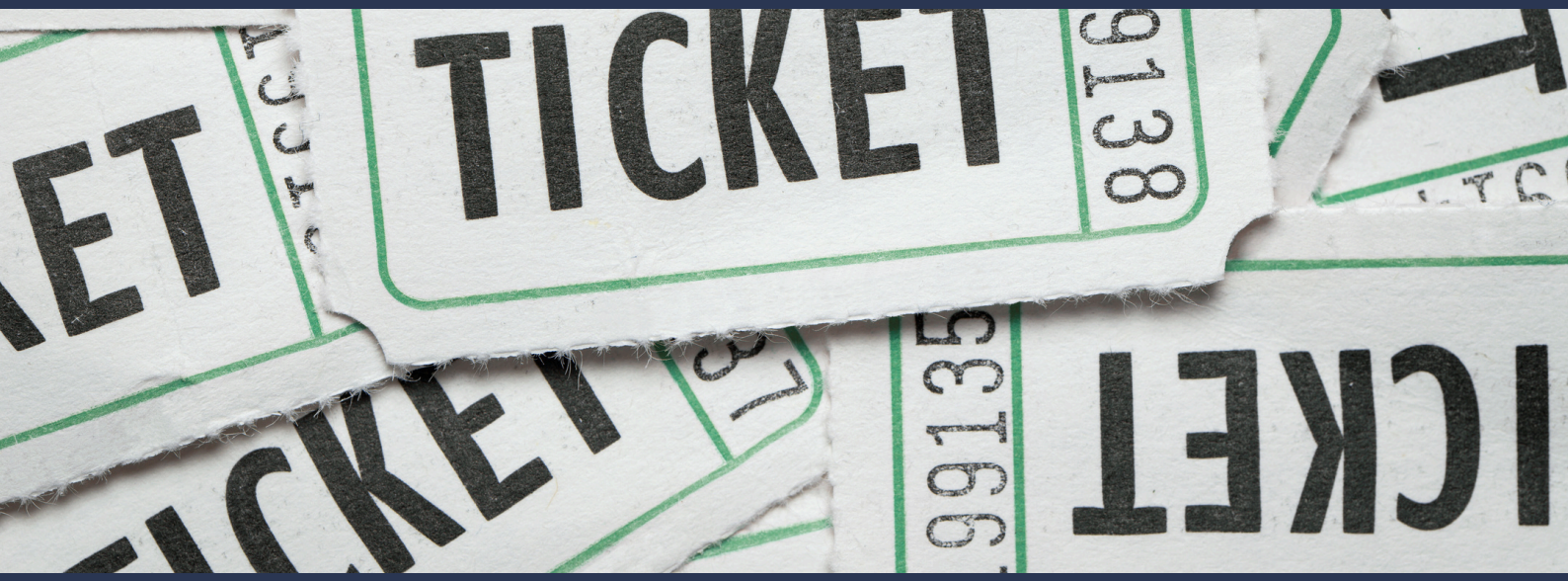
- Secondary fraud: Once a victim has been scammed, the same scammers might attempt a recovery scam, such as pretending to offer refunds or 'replacement tickets' in exchange for more money.

Recent example:

A local report involved a fake sale of Oasis tickets on Facebook. The victim paid £600 to a Monzo business account after being persuaded by a seller posing as a genuine contact. The tickets never arrived, and the seller's account was later confirmed as having been compromised, meaning that the scammer had access to it.

How to protect yourself:

- Buy only from official sources: Use verified ticketing platforms or authorised resellers.
- Avoid upfront payments to individuals: Scammers often insist on bank transfers.
- Check profiles carefully: New accounts or those with few friends are red flags.
- Verify before paying: Speak to the seller by contacting them directly or by video call.
- Report suspicious activity: Notify the platform and the Cyber Security Centre if you encounter a scam.



THREAT REPORT: SPOTLIGHT

CLICK, SCAM, REPEAT: NAVIGATING THE DIGITAL MINEFIELD OF ECOMMERCE FRAUD

Behind the sleek storefronts and seamless checkout experiences of eCommerce solutions lies a fragile ecosystem vulnerable to exploitation. Cybercriminals are no longer targeting only the giants of industry; small and mid-sized businesses, often operating with limited cyber security resources, have become prime targets. A single overlooked update or a cleverly disguised impersonation scam can unravel years of hard work, exposing sensitive customer data, draining finances, and eroding hard-earned reputations.

eCommerce platforms like WordPress, Shopify and Magento have revolutionised how businesses reach customers, but their convenience comes at a cost and shouldn't be ignored when considering your organisation's cyber security. Unpatched plugins, flawed dependencies, and sophisticated social engineering tactics are the weak links attackers exploit. Both technical and human attack vectors are at play. From large-scale breaches to AI-powered impersonation scams, the threats are evolving faster than many organisations can respond.

This edition's spotlight explores some of the vulnerabilities that make eCommerce security a weak link, highlights real-world cases where businesses paid the price, and provides practical steps to fortify defences.

eCommerce Security: The Weakest Link

Security vulnerabilities in eCommerce platforms can expose customer data, enable account takeovers, or facilitate payment fraud. Small businesses are especially at risk due to limited cybersecurity resources.

eCommerce and web hosting platforms, such as WordPress, make design and implementation easier, however, they open up business to many cyber risks due to unmaintained and flawed third party plugins and dependencies. If left unchecked, organisations can suffer from downtime, insecure data, fraudulent transactions and damage to reputation.

Magento Shoplift: A Store Without Surveillance

In late 2025 a critical remote code execution vulnerability known as SessionReaper was discovered affecting both Magento Open Source and Adobe Commerce. Attackers were able to exploit the flaw to gain full control of online stores, inject backdoors, install payment skimmers and access sensitive customer data. Hundreds of attacks were recorded within a single day and a significant proportion of Magento stores remained unpatched, which allowed the exploitation to spread quickly across small and mid-sized retailers.

The incident shows how dependent eCommerce platforms are on timely patching and the maintenance of complex third-party components. It demonstrates that attackers are actively scanning for unpatched systems and that even widely used and well-established platforms can expose businesses to major operational and financial risk if updates are missed. It serves as a reminder that software convenience must be matched with disciplined cyber hygiene.

What You Can Do

- Keep platforms, plugins and servers updated as soon as security patches are released
- Use multi-factor authentication on all administrative accounts
- Regularly scan for vulnerabilities and unexpected file changes
- Employ web application firewalls to block known exploit attempts
- Monitor transactions and server behaviour for suspicious activity

Impersonation: The Art of Deception

Attackers posing as trusted entities (e.g. banks, CEOs and suppliers) to trick victims into transferring money or revealing sensitive data is not a new concept, however, the bar to entry for impersonation scams has been significantly lowered, enabling even the lowliest of criminals to use readily available tools to commit high impact crimes. These scams are increasingly sophisticated, using AI-generated voices, deepfake videos and credible-looking clones of legitimate platforms, services and tools.

It isn’t just large organisations that are subject to impersonation. In 2024, the CSC received over 40 reports of impersonation websites and social media accounts affecting local businesses and targeting victims both in the Island and around the world.

AI Mimicry: When machine meets reality

In 2024 UK organisations were warned by Starling Bank about a surge in AI-enabled voice-cloning scams that targeted both individuals and businesses. Criminals were able to create convincing audio copies of senior staff or trusted contacts using only a few seconds of publicly available audio and then used these for fraudulent instructions and payment requests. These incidents demonstrated how easily familiar voices could be replicated and used to manipulate employees into urgent or high-risk actions.

This rise in synthetic impersonation shows how social engineering and technical capability are merging, making traditional trust cues unreliable. It illustrates the growing need for organisations to strengthen verification processes and reduce the amount of recorded audio and executive information available online. Voice alone can no longer be considered proof of identity and staff must be prepared to question requests that appear genuine.

What You Can Do

- Always confirm financial or sensitive requests using a separate communication channel
- Train employees to recognise signs of impersonation and follow strict approval procedures
- Implement email authentication controls such as SPF, DKIM and DMARC
- Establish internal ‘safe phrases’ or agreed verification steps for high-value transactions
- Limit the amount of publicly accessible audio and information relating to senior staff
- For further reading on this topic, please visit our website's Advice and Guide section, https://csc.gov.im/advice-guidance/online-business-e-commerce-security/

Notable Mentions

- CE Phoenix: Open Source eCommerce Solution.

o CVE-2025-47289: Cross-Site Scripting (XSS) (CVSS 9.0 NIST)

- W3 Total Cache WordPress Plugin: SEO and User Experience Enhancement.

o CVE-2025-9501: Command Injection (CVSS 9.0 CISA)

INTERNATIONAL THREATS

EUROPEAN AIRPORT RANSOMWARE ATTACK DISRUPTS OPERATIONS AND SPARKS GLOBAL INVESTIGATION

A ransomware attack on 19 September 2025 severely disrupted operations at major European airports after Collins Aerospace's MUSE check-in and boarding system was compromised. The outage affected airports including Heathrow, Brussels, Berlin, Dublin and Cork, forcing airlines to revert to manual processes such as paper boarding passes and mobile check-ins. Brussels Airport alone reported around 60 flight cancellations on 22 September, and queues stretched for hours at several hubs.

Investigators believe the attackers exploited a zero-day vulnerability in Citrix ADC combined with stolen credentials obtained through social engineering. Once inside, they deployed ransomware using techniques such as malicious macros, PowerShell scripts and lateral movement via SMB and RDP. Early reports linked the attack to REvil/Sodinokibi, but by late October the Everest ransomware group claimed responsibility, although attribution remains under review. Analysts note that this attack fits a growing trend of supply-chain compromises and so-called 'big-game hunting' tactics targeting critical infrastructure.

Collins Aerospace shut down affected systems and began rebuilding them from scratch, deploying patched versions of MUSE and implementing hotfixes by the 29th of September. Airports continued manual operations into early October while restoration progressed. Regulatory bodies including ENISA and national CERTs coordinated with Collins and RTX to contain the threat and strengthen resilience measures. Authorities have urged aviation operators to adopt zero-trust architectures and comply with NIS2 and EASA cybersecurity frameworks.

The UK's National Crime Agency arrested one suspect in West Sussex on the 24th of September under the Computer Misuse Act, though investigations remain ongoing. No ransom payment has been confirmed, and forensic teams are still analysing the breach. Experts warn that the incident underscores systemic risks in aviation's reliance on centralised vendor systems and demonstrates a need for appropriate fallback protocols, vendor risk assessments and inter-agency collaboration to mitigate future attacks.

ASAHI CONFIRMS RANSOMWARE ATTACK DISRUPTING GLOBAL OPERATIONS

Japanese brewing giant Asahi Group Holdings confirmed it was hit by a ransomware attack in early October 2025, causing disruption to global operations. The company, which owns brands such as Asahi Super Dry, Peroni and Grolsch, reported the attack targeted its European and Australian subsidiaries, forcing some production and distribution systems offline. While beer production continued at most facilities, certain IT systems were shut down as a precaution, leading to delays in order processing and logistics.

Asahi stated the attack did not compromise payment card data or core brewing processes, but some employee and business partner information may have been exposed. The company has not disclosed the ransomware strain, though analysts suspect a link to the BlackCat/ALPHV group based on similar tactics. Attackers reportedly encrypted critical servers and demanded a ransom, but Asahi has not confirmed whether negotiations occurred or any ransom was paid.

In response, Asahi engaged external cybersecurity experts and law enforcement agencies including Japan's National Police Agency to investigate and restore systems. The company implemented containment measures, isolated impacted networks and began rebuilding IT infrastructure. Customers were assured product safety and quality were not affected, though supply-chain delays may persist.

This attack highlights the growing ransomware threat against manufacturing and food and beverage sectors, which rely heavily on integrated IT and operational technology systems. Experts recommend strengthening network segmentation, maintaining offline backups and implementing zero-trust security models to reduce exposure. Regulatory bodies in Japan and the EU are expected to review incident reports as part of broader efforts to enforce cybersecurity resilience across critical supply chains.

Asahi confirmed the ransomware attack disclosed in October resulted in a significant data breach affecting approximately 1.5 million customers. Compromised information includes names, addresses, phone numbers, and email details, though payment card data remains unaffected. The company has begun notifying impacted individuals and is working with cybersecurity experts and law enforcement to mitigate risks. Asahi reiterated its core brewing operations were not disrupted, but the incident underscores the growing threat to global supply chains and the importance of robust data protection measures.

HARRODS CONFIRMS THIRD-PARTY BREACH EXPOSING DATA OF 430,000 CUSTOMERS

Luxury retailer Harrods has confirmed that a cyberattack on a third-party service provider led to the exposure of personal data belonging to approximately 430,000 customers. The breach, which occurred earlier this year, compromised names, email addresses, phone numbers and physical addresses. No payment card details or passwords were affected, according to Harrods' official statement.

The incident has been linked to the same threat actors behind a recent attack on Marks & Spencer, suggesting a coordinated campaign targeting retail supply chains. Investigators believe the attackers exploited vulnerabilities in a third-party marketing and customer engagement platform, enabling unauthorised access to sensitive customer records. Harrods immediately suspended its connection to the affected vendor and launched an internal investigation alongside external cybersecurity specialists.

The company has notified the UK's Information Commissioner's Office and is contacting impacted customers directly, advising them to remain vigilant against phishing attempts and identity fraud. Security experts warn that exposed contact details could be used for targeted scams, credential harvesting and social engineering attacks. Harrods has since implemented additional security measures, including enhanced vendor risk assessments and stricter data-sharing protocols.

This breach shows the growing risks associated with third-party integrations in retail environments, where attackers increasingly exploit supply-chain weaknesses to access large volumes of customer data. Industry analysts note that such incidents are driving regulatory scrutiny under frameworks such as GDPR and NIS2, with potential mandates for stronger vendor security audits and contractual compliance requirements.

Harrods has apologised for the incident and assured customers that steps are being taken to prevent a recurrence.

DISCORD VENDOR BREACH EXPOSES 70,000 USERS

In a supply-chain attack that was recently discovered, Discord revealed that one of its third-party customer support vendors, identified as 5CA, had been compromised by unauthorised actors. This breach, disclosed publicly on 3 October, affected around 70,000 users who had interacted with Discord Support or Trust & Safety. Attackers accessed names, usernames, email addresses, IP addresses, limited billing information such as card type and the last four digits, support ticket messages and, critically, submitted government ID images used for age verification.

Although Discord's core platform, credentials, full payment data and user messages were not affected, the attackers sought ransom, allegedly demanding 5 million dollars, later reduced to 3.5 million dollars. They claimed to hold 1.5 terabytes of stolen data, including more than 2 million ID photos, far beyond what Discord has confirmed. Threat intelligence sources, including Vx-Underground and media outlets such as CyberGuy, attribute the attack to a group self-identifying as 'Scattered Lapsus$ Hunters'.

Discord responded immediately by revoking the vendor's access, cutting off the ticketing system, engaging digital forensics investigators and notifying law enforcement and data protection regulators. Affected users have been contacted via official noreply@discord.com emails. Discord has also reviewed all third-party integrations and strengthened its detection controls.

Security analysts warn that this breach highlights systemic risks associated with outsourced support workflows, where privileged vendor access grants broad reach over user data. Jake Moore of ESET noted that vendor platforms often hold sensitive PII that remains 'hidden' outside primary security measures. Similar incidents this year, including those involving Salesforce-Drift, QuickBooks and Marks & Spencer, underscore the proliferation of vulnerabilities in OAuth and agency-based systems.

Recent remediation guidance emphasises immediate token revocation, multi-factor authentication, network monitoring and zero-trust policies for third-party access. Discord now requires forensically validated vendor security reviews and behavioural detection systems. This case reinforces critical lessons about supply-chain attacks: monitor and constrain third-party integrations, implement rapid incident response in edge-case scenarios and prepare contingency plans for compromises affecting OAuth and support platforms.

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.

Advance Fee Fraud: A type of scam where a fraudster convinces a victim to pay a fee in exchange for a promised future benefit (for example winning the lottery, inheritance, loan, etc).

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

Computer Emergency Response Team (CERT): A CERT is an incident response team that handles cyber incidents, for example, malware attacks or data breaches.

The Cybersecurity and Infrastructure Security Agency (CISA): CISA works to protect critical national infrastructure and government systems from cyber and physical threats.

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

Credential Harvesting: A form of cyberattack where cybercriminals steal personal or financial details such as usernames and passwords.

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.

Common Vulnerability Scoring System (CVSS): The CVSS is an industry standard that provides a numerical score from 0.0 to 10.0 to rate the severity of software vulnerabilities.

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.

Deep Fake: A digitally altered video or image of a person so that they appear to be someone else. This is typically used maliciously or to spread false information.

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.

Hotfix: A small piece of code developed to correct a major software bug or fault and released as quickly as possible.

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.

Multi-Factor Authentication (MFA): A method of verifying a person's identity in order to allow access to a digital service or system, requiring one or more proofs of identity in addition to a password or PIN (e.g. a code texted to a phone).

OAuth: An open-standard protocol that allows a user to grant a third-party application limited access to their resources on another service without sharing their login credentials.

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.

Recovery scams: A type of advance-fee fraud where criminals contact victims who have already lost money to a previous scam and pretend to be able to recover their funds for an upfront fee.

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.

SPF, DKIM, DMARC: Email authentication protocols that work together to prevent spoofing and phishing by verifying the sender's identity and email integrity.

Supply-Chain Attack: A cyberattack that compromises a third-party vendor, software, or hardware to gain access to a target organisations systems or data.

Vishing: A type of phishing attack that uses phone calls or voice messages purporting to be from reputable companies.

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

Zero-Trust Architecture: A modern cybersecurity framework built on the foundational principle: 'never trust, always verify'. It assumes no user or device should be trusted by default.

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.

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

With the exception of the Coat of Arms, CSC, Department of Home Affairs logos, and where otherwise stated, all material presented in this publication is provided under the Open Government License https://csc.gov.im/other-pages/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