Cyber Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

January - February 2026

INTRODUCTION

For the period 1st January-28th February

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 email us at cyber@gov.im.

CONTENTS

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 28,730 suspicious emails. In January and February 2026, we received 632 suspicious emails.

SUSPICIOUS EMAILS

632 REPORTED

in January and February

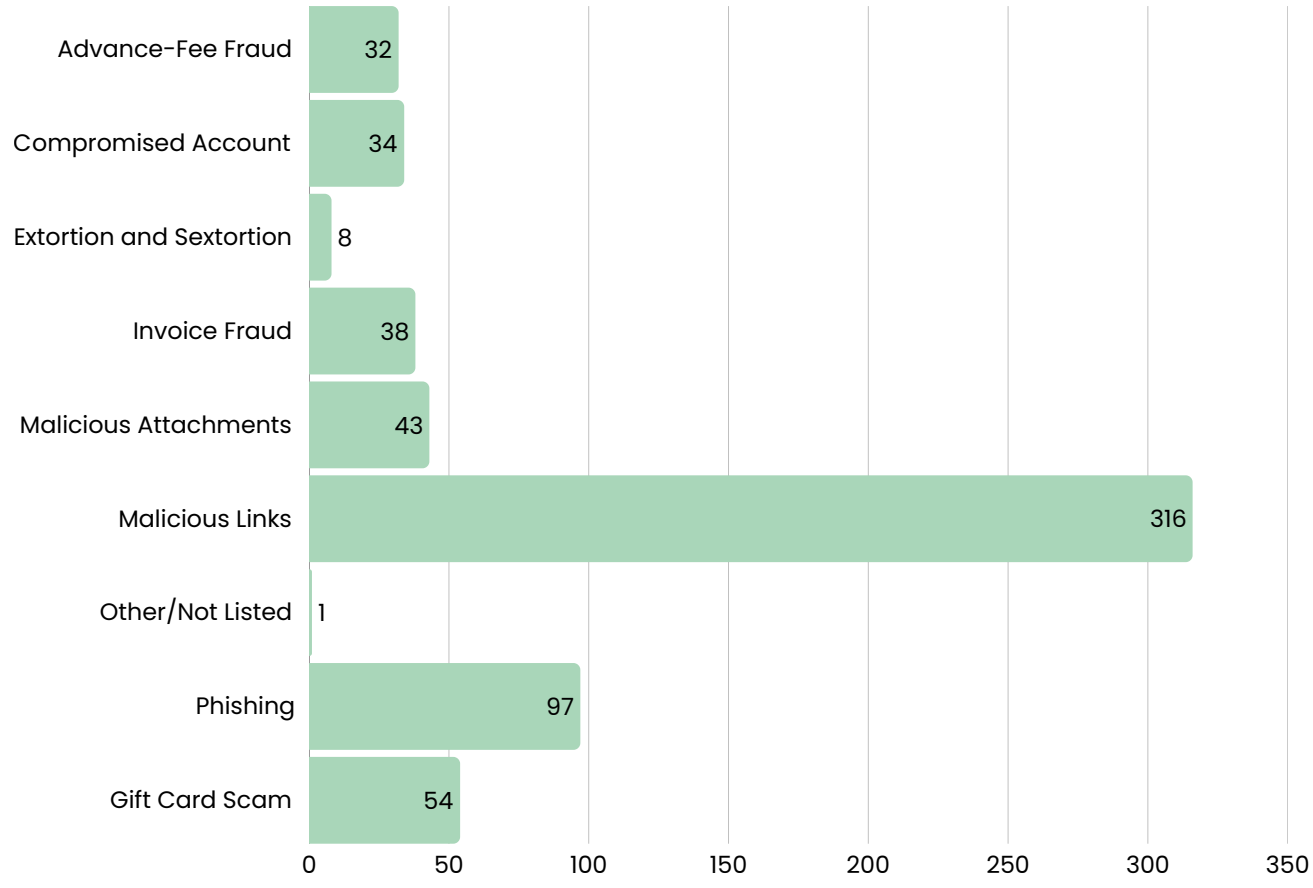
Detail

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 invoice fraud and gift card scams.

Top 5 Phishing Scams Imitating Popular Services:

1. Anti-malware Software
2. Manx.net
3. Business Proposals
4. Geek Squad
5. PayPal



CONCERNS

102 REPORTED

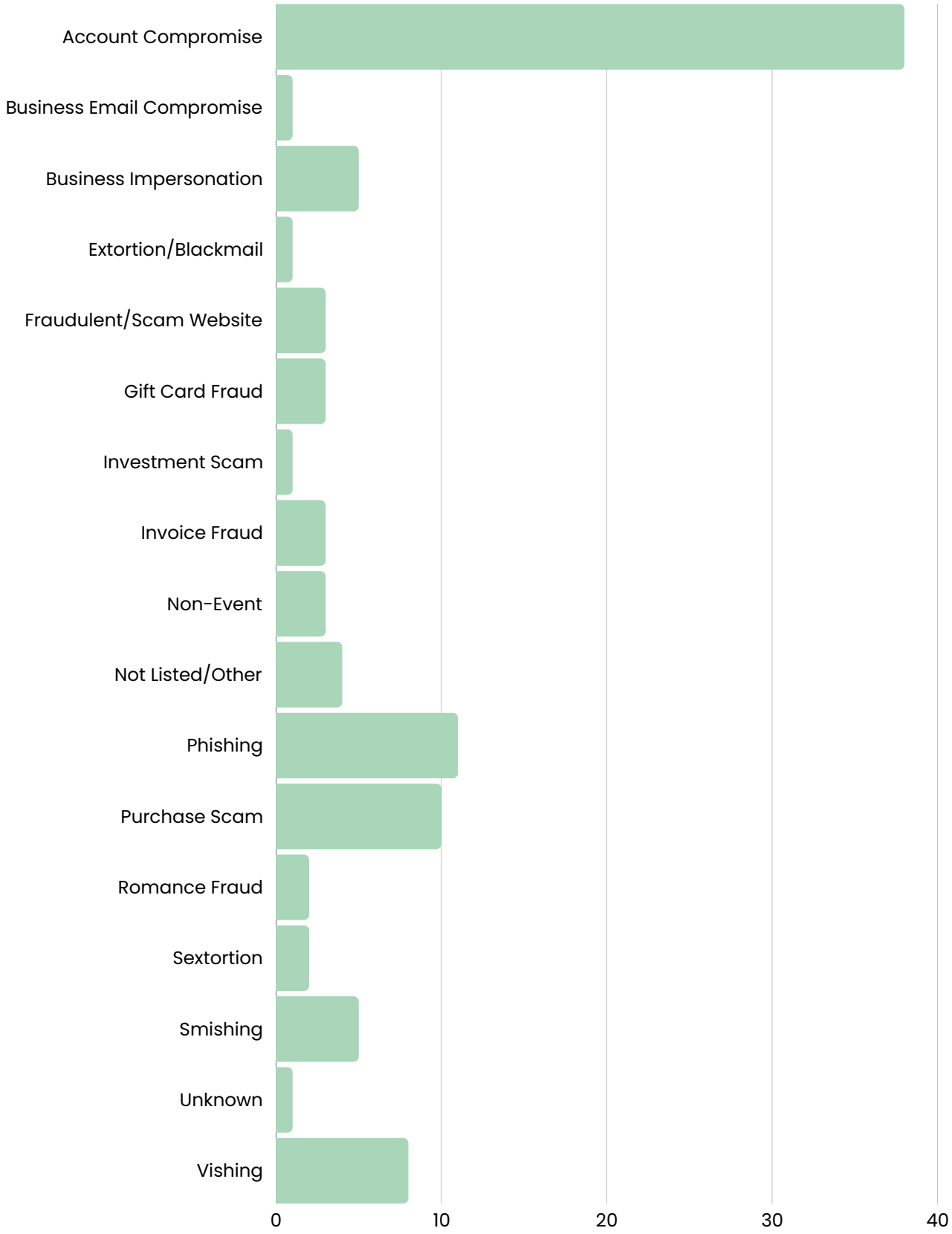
in January and February

Detail

The chart (on page 4) shows a breakdown of cyber-concerns reported to us over January and February.

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: January and February



ISLE OF MAN THREAT COMMENTARY

BUSINESS AND ORGANISATIONS

SECURE ACCOUNT RECOVERY, CONTAINMENT AND TRAINING: UNDERSTANDING WHAT COMPROMISE REALLY MEANS

Many organisations rely on managed service providers (MSPs), cloud platforms, and outsourced IT support to administer critical systems and recover from incidents. While these services can provide valuable expertise, outsourcing technology does not remove your own responsibility for security, and it should never be assumed that an account or service is fully secure simply because a password has been changed or a provider says the issue has been resolved. In cloud and outsourced environments, security remains a shared responsibility, and businesses must understand what actions have actually been taken, what risks remain, and whether the root cause has truly been addressed.

Recent Local Incidents

Throughout January and February, the CSC continued to receive reports of compromised business email accounts being used to target other local businesses and members of the public. The reports affected a wide range of sectors showing that this activity was not limited to one industry and that trusted local relationships continued to be exploited by attackers.

The chain effect seen in previous reporting also continued with several incidents showing how one compromised business could be used to target another. Further compromises were identified through SERS submissions, reports from local businesses, and alerts from customers and contacts. This demonstrates how quickly a single compromise can spread across existing business relationships on the Island.

These incidents also highlight the importance of understanding that regaining access to an account and simply resetting passwords doesn't always mean the threat has been removed. Attackers typically maintain a foothold inside the business in various ways. Malicious activity will likely continue if further containment steps are not taken, such as revoking active sessions, removing unfamiliar mail rules, and setting up Multi-Factor Authentication (MFA).

Businesses need to understand how the compromise occurred, what access may still remain, and whether recovery actions have genuinely removed the attacker’s foothold. Without this, businesses risk being led to believe their systems and data are secure while leaving the underlying compromise unresolved.

Why These Incidents Matter

Cyber-incidents can and do happen to organisations of all sizes, and good preparation is one of the most important factors in limiting damage. Effective recovery is not just about restoring access; it is about making sure an attacker no longer has any route back into the environment, understanding the extent of the incident, and ensuring that business operations can continue safely. A poorly handled recovery can allow compromise to persist, increase downtime, and create additional financial, operational, and reputational harm.

This risk becomes even more significant where third parties administer systems on behalf of the organisation. MSPs and other suppliers often require privileged access to customer environments, which can bring security benefits through specialist expertise, but it also increases the attack surface. If a third party owns systems, administrator accounts, or recovery processes are weak, attackers may be able to exploit that trust to gain access to the environment. Organisations should therefore understand not only what their providers do, but how they do it and how compromise would be detected, contained, and recovered from in practice.

What Compromise Can Really Mean

A common mistake during incident response is to treat compromise as a single event that is resolved once a password is reset. In reality, compromise can be broader and more persistent. Signs of account compromise can include changes to security settings, unexpected password reset messages, logins from unusual locations or times, suspicious messages sent from accounts, or unauthorised activity taking place elsewhere using the same credentials. Attackers may also use persistence mechanisms, such as malicious email forwarding rules, altered recovery details, or existing logged-in sessions, to maintain access even after the victim believes the issue has been fixed.

This is particularly important when working with external IT support or service providers. If an organisation receives reassurance that an account is secured without confirmation of what was investigated, what was removed, and whether all sessions and access paths were revoked, then the business may be relying on assumptions rather than evidence. Effective containment requires more than regaining access to an account; it requires checking for signs of persistence, understanding the impact of the incident, and ensuring the attacker’s access has genuinely been removed.

Key Protections and Why They Are Necessary

- **Understand shared responsibility:** Using a cloud platform or external provider does not transfer all security responsibility. Organisations must still ensure services are configured securely, used appropriately, and aligned to security needs.
- **Have an account recovery and containment process before you need it:** Organisations should know in advance how to respond to suspected compromise, including how to reset access safely, revoke sessions, review recovery settings, and check for persistence such as forwarding rules or other unauthorised changes.
- **Don't rely solely on reassurance, verify the recovery:** If a provider says an issue is resolved, ask what was investigated, what was found, and what was done to remove access. Restored access does not always mean the compromise has been fully contained.
- **Control privileged access tightly:** Administrative accounts are highly valuable to attackers. Limit their use, separate them from normal user accounts, and apply strong controls such as MFA and privileged access management where possible.
- **Build supplier security into procurement and contracts:** Security expectations should be agreed before an incident occurs. Organisations should understand how providers handle incidents, what they will report, and what standards they are expected to meet.
- **Train staff to recognise signs of compromise:** Training should go beyond phishing awareness. Staff should know how to spot unusual account behaviour, unexpected MFA prompts, suspicious admin changes, or other signs that an account may have been compromised.

The CSC website has advice and guidance on a wide range of cyber-security topics, including what to consider when a compromise occurs. Visit our advice and guidance page here: https://csc.gov.im/advice-guidance/

PERSONAL

BANK IMPERSONATION VISHING SCAMS

Vishing, or 'voice phishing', is a scam in which criminals use phone calls to impersonate trusted organisation such as banks. These calls are designed to create urgency and alarm, often by claiming there has been suspicious activity on an account, so that victims act quickly before verifying whether the contact is genuine. In many cases, scammer can also spoof telephone numbers so the call appears to come from a legitimate source.

How These Scams Work

Fraudsters pose as trusted organisations or individuals, such as IT support teams, government bodies, delivery services, or charities. These approaches can vary widely, ranging from requests for remote access to devices, to demands for urgent payments via bank transfers, gift cards, or donation platforms. Regardless of the scenario, the aim is to create pressure and extract money or sensitive information before the victim has time to think.

Typically, fraudsters claiming to be from a bank's fraud team will say that a payment has been attempted, the account has been compromised, or the victim's money needs to be protected. They may then ask the victim to share a one-time passcode, approve or reject an in-app prompt, confirm security details, or transfer money to a safe account. Similar scams begin with a text message and are the followed by a phone call to make the approach seem more convincing.

Common Dangers

- **Financial loss:** If a victim shares a verification code, approves a fraudulent payment or access prompt, or transfers money themselves, criminals may be able to authorise payments or gain access to banking services. In cases where the victim is persuaded to move their own money, recovery can be much more difficult.

- **Account compromise:** Personal or banking information disclosed during the call can be used to access accounts, register cards to criminal-controlled devices, or carry out further fraudulent activity.

- **Identity exposure:** Information gathered during the scam may also be reused in future phishing, impersonation, or identity fraud attempts.

Recent example

A recent local report involved a victim receiving a 'No Caller ID' phone call from someone claiming to be from their bank. The caller stated that a fraudulent payment had been made and instructed the victim to provide a 6-digit code and press 'Reject' in the banking app to stop it, these are security steps that the scammer exploited to access the account. Shortly afterwards, the victim was unable to access the mobile banking app and contacted their bank directly, where they were informed that £5,000 had already been taken from the account. A further £7,959 had also been moved from a joint account in an apparent attempt to extract more funds, although this was unsuccessful.

How to protect yourself

- **Hang up and call back using a trusted number:** If someone claims to be from your bank, end the call and contact the bank using the number on the back of your card, on a statement, or from the banks official website.

- **Never share one-time passcodes or security credentials:** Genuine banks will not ask you to reveal one-time passcodes, full PINs, passwords, or other login credentials over then phone.

- **Do not move money to a 'safe' account:** Criminals frequently use this tactic to pressure victims into authorising their own loss. If anyone tells you to transfer funds to protect them, it's a scam.

- **Slow the situation down:** It is okay to reject, refuse, or ignore requests that create panic or demand immediate action. Criminals rely of victims feeling rushed.

- **If you think you have been caught out:** Contact your bank immediately, secure the account, and report the incident to the Police. Local incidents can also be reported to the Cyber Security Centre so that further advice and warnings can be issued where appropriate.

THREAT REPORT: SPOTLIGHT

EXPOSED CREDENTIALS: UNDERSTANDING THE RISKS IN DATABASES, DATA STORES, AND REPOSITORIES

The security of an organisation no longer hinges solely on firewalls, anti-virus tools or perimeter defences. Instead, one of the most significant and fast-growing threats comes from something far more basic. Exposed credentials, passwords, API keys, cloud access tokens, and other secrets are now among the most sought-after commodities in cyber-crime, routinely traded on underground forums and exploited in large-scale attacks.

The volume, sophistication, and business impact of credential-related breaches has escalated dramatically in recent years. These exposures frequently originate from insecure administrative or development practices, misconfigured cloud environments, and infostealer malware which have led to massive data leaks and criminal markets being flooded with billions of valid logins. Attackers no longer need to 'break in'. With exposed credentials, they can simply log in, bypassing traditional security controls altogether. The consequences can include operational outages, financial fraud, reputational damage, regulatory penalties, and long-term supply-chain compromise.

In this edition's Spotlight, we'll take a look into what exposed credentials really means for an organisation, what you can do to actively reduce credential and secret leakage, and things to consider during and after a compromise.

Understanding the Problem: What Are Exposed Credentials?

Exposed credentials refer to any authentication secrets (e.g. usernames, passwords, API keys, database connection strings, SSH keys, access tokens, session cookies, etc.) that become accessible to unauthorised individuals. These exposures commonly occur through:

- Misconfigured cloud storage (e.g. S3 buckets)
- Leaked secrets in data repositories (e.g. GitHub)
- Infostealer malware exfiltrating saved browser login information
- Poor logging or debugging practices during or after development
- Improper credential-sharing habits between team members

When these secrets are compromised, attackers can directly authenticate into services without needing to exploit vulnerabilities. This bypasses traditional perimeter security entirely, making exposed credentials highly valuable to attackers.

Recent Examples Highlighting the Scale of the Problem

- **Mass Credential Leak (June 2025)**

Over 16 billion usernames and passwords, many freshly stolen, were found circulating online. Investigators confirmed the data was not recycled meaning most accounts remained valid and exploitable at the time of discovery. The dataset spanned Apple, Google, GitHub, workplace tools, banking logins, Virtual Private Networks (VPNs), and more.

- **AWS Cloud Credential Exposure Incident (2024–2026)**

Misconfigured AWS cloud instances allowed attackers to obtain sensitive credentials including AWS customer keys, database credentials, Git credentials, API keys, SSH keys, and more. These were later found stored openly in an unprotected S3 bucket and sold through a well-known communication app.

Potential Business Impact

Direct Unauthorised Access

With valid credentials, attackers can access:

- Databases containing sensitive customer or business information
- Cloud consoles enabling resource modification or deletion
- Source code repositories enabling supply-chain attacks
- Internal business tools, privileged systems and intellectual property

Regulatory and Legal Exposure

Businesses face fines, lawsuits, and mandatory disclosure requirements when credentials grant access to:

- Personal data (GDPR)
- Healthcare data (HIPAA)
- Financial records

Reputational Damage

Leaks involving source code or intellectual property, such as Git credentials stolen in the AWS attack, or inappropriately stored sensitive client/customer information can damage long-term market trust.

How to Protect the Business

Enforce Strong Secret Management Practices

- Use secret managers
- Rotate secrets automatically and frequently
- Never store secrets in plaintext, logs, code, or config files
- Never run text or documents holding secrets through AI or unauthorised tools

Use Multi-Factor Authentication and Passkeys

Modern attacks can sometimes bypass MFA using session cookies, but MFA still dramatically increases resilience. Passkeys and hardware keys provide stronger resistance to phishing and token theft.

Implement Least-Privilege Access Controls

Restrict all credentials to the minimum scope necessary. Limit wildcard or admin rights and enforce role-based access.

Adopt Zero-Trust Principles

Assume every request is untrusted until validated. Monitor and continuously verify identities, devices, and sessions.

Protect Developer Environments

- Scan code repositories for hard-coded secrets
- Use Git hooks and automated scanners
- Segregate development, staging, and production

Harden Cloud Resources

- Disable public bucket access by default
- Use resource policies with IP allow-lists
- Enforce encryption and automatic logging

Ask Questions

The third parties and service providers you work with may have access to sensitive data. It is essential to ask the right questions about how they handle and protect this information, understand their incident response plan in the event of a breach, and ensure you are satisfied with their overall security posture.

What to Do If Credentials or Data Have Been Exposed

- **Immediately rotate all exposed credentials:** This includes passwords, API keys, session tokens, SSH keys, and cloud access keys.
- **Invalidate active sessions:** Attackers often leverage stolen session cookies to bypass MFA. Ending active sessions is essential.
- **Assess your environments:** Audit your cloud and database logs, repository access history, and administrative activity.
- **Investigate for lateral movement:** Attackers often pivot into internal systems after initial entry, especially from exposed Git or database credentials.
- **Notify relevant stakeholders:** Internal leadership, impacted customers, regulators. (if required by law)
- **Strengthen controls to prevent recurrence:** Use lessons from the compromise to improve:
  - rotation policies
  - adoption of security controls
  - logging and monitoring
- **Company-wide Security guidance:** Your organisation's staff are both the first and last line of defence when it comes to cyber and information security. Technology can only do so much, so it is critical that all users of your business systems and networks are appropriately trained.

Conclusion

Exposed credentials are one of the fastest and most damaging cyber-risks businesses face today. Recent leaks involving credentials, misconfigured cloud assets, and supply-chain level access demonstrate that attackers now operate with unprecedented access to authentication data and, in many cases, these leaks were avoidable by not exposing data over the public Internet.

Are you confident in where and how your credentials are being stored? Can you be sure that your suppliers and service providers are safeguarding your private keys and access points? If the answer is no, your organisation may already be exposed, and attackers don't wait for you to discover the problem. Acting now is essential.

INTERNATIONAL THREATS

CYBER-ATTACKS DISRUPT EDUCATION IN THE UK AND ITALY

Two separate cyber-incidents in early 2026 highlighted the continued vulnerability of educational institutions to disruptive attacks. In the UK, Higham Lane School in Nuneaton was forced to remain closed after the Christmas holidays when a cyber-attack severely affected core IT services, leaving staff without access to essential systems including telephone, email, servers, and the school management platform. In Italy, Rome's Sapienza University suffered a major cyber-incident that led to the precautionary shutdown of institutional network systems and caused widespread disruption to digital services across the university.

In both cases, the organisations moved quickly to contain the threat and begin recovery. Higham Lane School's parent trust confirmed that incident response procedures had been initiated and that independent cyber-specialists had been engaged, while relevant authorities, including the Information Commissioner's Office (ICO), were notified. Sapienza likewise established a technical task force, notified the appropriate authorities, and worked with national-level support to contain and remediate the incident. With key online system unavailable, the university was forced to communicate updates through social media and establish temporary in-person information points for students.

Although the full technical details were not publicly confirmed in either case, the operational impact was significant. The UK incident demonstrated how even a single school can be forced to suspend normal teaching activity when digital systems become unavailable, while the Sapienza case showed how a university-wide outage can affect access to public websites, internal systems, and student-facing services. External reporting suggested that Italian incident may have involved ransomware and possible data encryption, though this had not been formally confirmed by the institution at the time of reporting.

These incidents serve as a reminder that the education sector remains an attractive target for cyber-criminals and disruptive threat actors. Schools, colleges, and universities often rely on digital systems to support teaching, communications, administration, and student services, meaning that outages can quickly escalate into major operational disruption. The cases also reinforce the important of having well-rehearsed incident response plans, access to specialist support, resilient backups, and alternative communication arrangements in place to maintain essential services during recovery.

PRO-RUSSIAN HACKTIVISTS TARGET ITALIAN OLYMPIC SITES AND DIPLOMATIC DIGITAL SERVICES

Italian officials reported that they had prevented a series of cyber-attacks targeting Foreign Ministry offices, including diplomatic infrastructure linked to Washington, as well as Winter Olympics-related digital assets associated with Milan and Cortina. The activity was described publicly by Italy's foreign minister as being of Russian origin and took place in the run-up to the opening stages of the Milan–Cortina Winter Olympics.

A pro-Russian hacktivist group known as NoName057 claimed responsibility for the activity via Telegram, presenting the attacks as retaliation for Italy's continued support for Ukraine. Public reporting indicated that the campaign was primarily disruptive in nature and involved distributed denial-of-service (DDoS) activity against a range of public-facing targets, including websites and hospitality-related digital services in Cortina d'Ampezzo.

Although Italian authorities stated that the attacks had been blocked, the incident highlights the cyber-risks that accompany high-profile international events, particularly where geopolitical tensions are involved. Public-facing systems such as event websites, hospitality platforms, ticketing services, and associated communications infrastructure are attractive targets for hacktivist groups seeking to create visibility, cause disruption, or send a political message.

This case serves as a reminder that organisations supporting major events should treat cyber-resilience as a core part of operational planning. Even when attacks are limited to short-term disruption rather than destructive compromise, the impact on public confidence, communications, and service availability can still be significant. Preparedness measures such as DDoS protection, incident response planning, and close coordination between event organisers, suppliers, and national authorities are essential to reduce the impact of such campaigns.

CYBER-GLOSSARY

2-factor authentication (2FA): A security process that requires two different forms of verification to confirm your identity, and is closely related to 2-step verification (2SV), which works in a similar way by adding an additional check to help protect your accounts.

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 cyber-attack 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 cyber-security 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

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