Cyber Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

May - June 2026

INTRODUCTION

For the period 1st May 2026 - 30th June 2026

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)	**1**
Cyber Concerns	**3**
Isle of Man Threat Commentary	**5**
The Evolution of Phishing	**9**
Spotlight: Are You Ready For The Patch Wave?	**12**
International Threats	**16**
Cyber-Glossary	**18**
About Us	**22**

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 the takedown of malicious 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 29,445 suspicious emails. In May and June 2026, we received 358 suspicious emails.

SUSPICIOUS EMAILS

358 REPORTED

in May and June

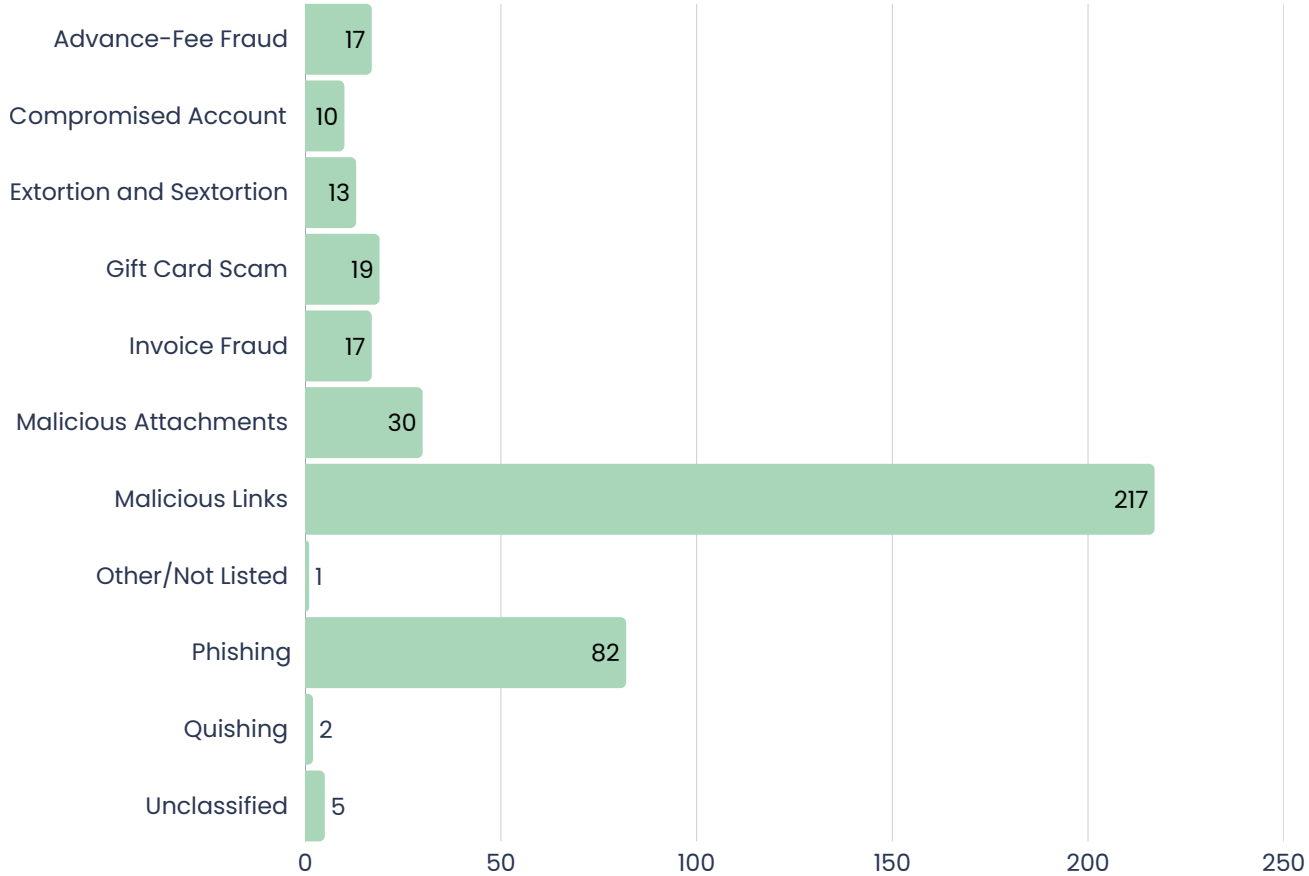
Detail

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

Whilst malicious links do make the bulk of submissions as usual, this period is notable for the increased prevalence of phishing and malicious attachments.

Top 5 Phishing Scams Imitating Popular Services:

1. Manx.net
2. Anti-malware
3. Microsoft
4. Manx Telecom
5. Geek Squad / Tech Support



CYBER CONCERNS

66 REPORTED

in May and June

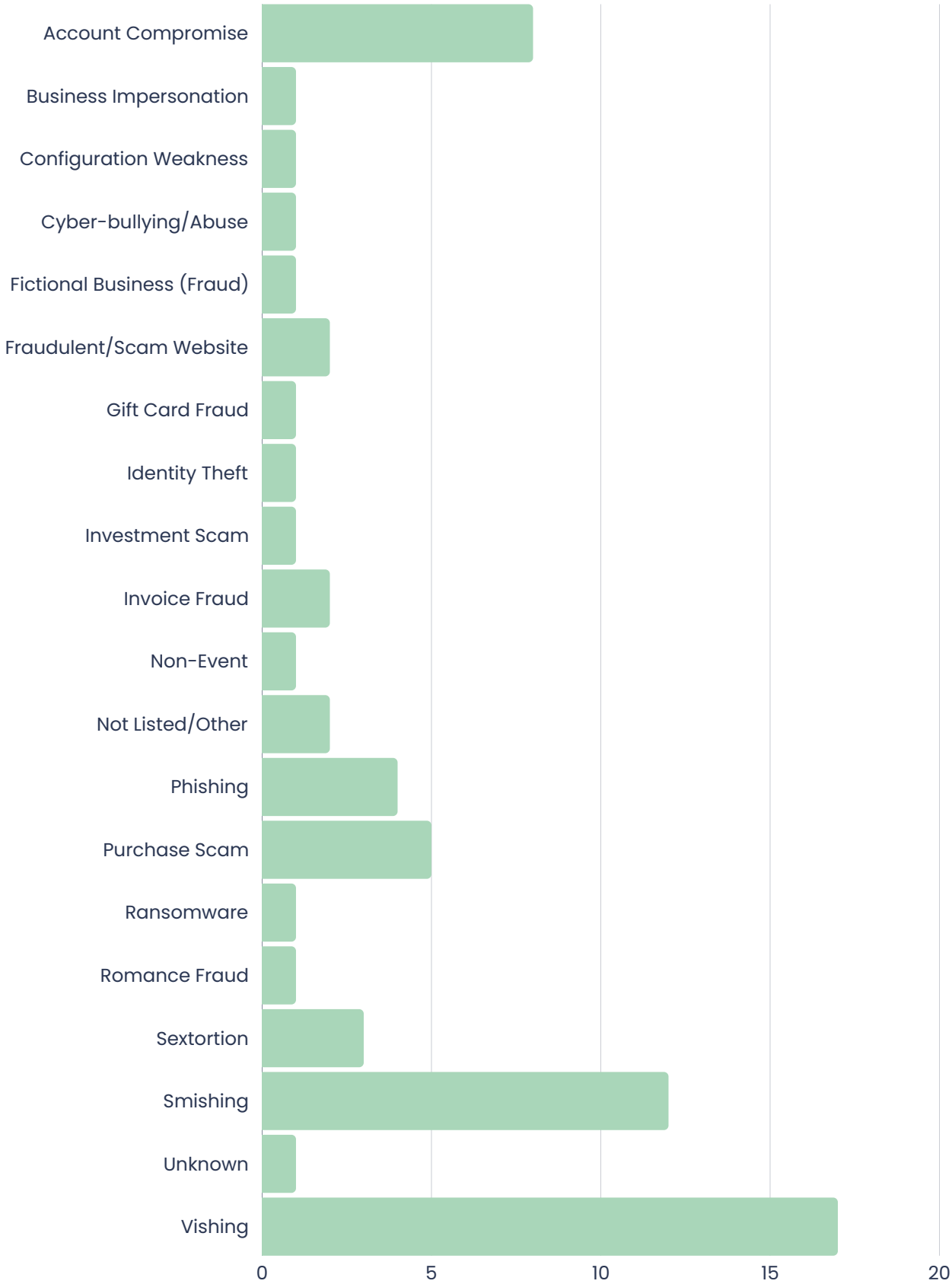
Detail

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

As highlighted throughout this report, we can only provide effective 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: May and June



ISLE OF MAN THREAT COMMENTARY

BUSINESS AND ORGANISATIONS

STAFF ARE YOUR FIRST AND LAST LINE OF DEFENCE: THE IMPORTANCE OF CYBER THREAT AWARENESS AND TRAINING

A single unexpected email, invoice, phone call, or message can be enough to put an organisation at risk. Many cyber incidents do not begin with a technical failure, but with a routine business action being manipulated by a criminal. This could be a member of staff approving a payment, responding to a supplier, clicking a link, entering login details, or assuming that a request is genuine because it appears to come from a trusted contact.

For businesses, staff awareness is therefore essential. Employees are often the first to encounter suspicious activity, but they may also be the final opportunity to stop an incident before money, data, or access is lost. This does not mean staff should be expected to identify every threat on their own. Instead, they should be supported with regular training, clear reporting routes, strong verification procedures, and a workplace culture where concerns can be raised quickly and without blame.

Cyber security awareness is most effective when it reflects how people actually work. Staff should understand the types of threats they are likely to face in their role, what warning signs to look for, and what steps to take if something doesn't feel right. When combined with appropriate technical controls and business processes, well-informed staff can play a vital role in preventing cyber incidents from escalating.

Recent Local Incidents

The CSC received several local reports between May and June that demonstrate why staff awareness, verification and escalation processes are so important.

One report involved a local organisation receiving two fraudulent supplier invoices over consecutive weeks. Internal concerns were raised at the input stage on both occasions, but key verification steps, such as callback checks and supplier validation, were not completed. One fraudulent invoice for over £10,000 was paid, while a second invoice was stopped before payment. The report highlighted failures in financial controls, verification, and escalation protocols.

Another report involved the compromise of a business email account. Attackers used the genuine account to continue an existing conversation with a client and instruct them to send payment to a different bank account. Email rules had also been created to hide the attacker's activity from the account holder. The client sent over £22,000 to the fraudulent account.

These incidents demonstrate how convincing modern scams can be and highlight the need for staff training to be supported by clear processes. If anything seems unusual, staff should know how to pause, verify, and escalate before any action is taken.

Why Staff Awareness Matters

Staff are often closest to the processes criminals want to exploit. They handle invoices, speak with customers, process payments, manage accounts, respond to emails, and use business systems every day. This makes them a frequent target, but also a critical part of an organisation's defence.

Awareness training should help staff understand:

- What common scams look like
- How criminals use urgency, pressure and trust
- Why payment changes must be verified independently
- How to recognise suspicious links, attachments and login pages
- What to do if they click something or enter details
- When and how to report concerns
- Who to escalate to if something feels unusual

Training should be practical and role-specific. For example, finance staff may need more detailed training on invoice fraud and payment verification, while front-line staff may need to focus on suspicious calls, customer impersonations, phishing emails, and data handling.

A strong reporting culture is just as important as training. Staff should be encouraged to report concerns early, even if they are unsure or think they may have made a mistake. Early reporting may allow your organisation to reset credentials, stop payments, contact banks, warn customers, or contain a compromise before further harm occurs.

Red Flags and Impact

Businesses should ensure staff can recognise common warning signs, including:

- Requests to change bank details or payment instructions
- Urgent or confidential payment requests
- Pressure to bypass normal processes
- Messages discouraging staff from checking with others
- Slight changes in email addresses, domains, or contact details
- Unexpected attachments, links, or login prompts
- Invoices that appear out of sequence or duplicate previous requests
- Messages from known contacts that seem unusual in timing, tone, or content
- Requests that rely on secrecy, authority or urgency

The impact of these incidents can extend beyond the initial financial loss. Businesses may face operational disruption, reputational harm, loss of customer confidence, strained supplier relationships, and potential legal or regulatory consequences.

In payment fraud cases, funds can be moved quickly, making recovery difficult. Preventing the incident, or escalating concerns before a payment is made, is usually far more effective than trying to recover money afterwards.

Key Considerations

To reduce the risk of staff-targeted cyber attacks, businesses should consider the following actions:

Provide regular, practical staff training: Training should be relevant to the organisation and include realistic examples, such as phishing, invoice fraud, account compromise, smishing, vishing, and supplier impersonation.

Create clear reporting routes: Staff should know exactly who to contact if they receive a suspicious message, click a link, enter credentials, or notice unusual account activity.

Verify payment changes independently: Any request to update bank details or make an urgent payment should be verified using a trusted contact method, such as a known phone number already held on file. Staff should not rely on contact details provided within the suspicious email.

Encourage a no-blame reporting culture: Employees are more likely to report concerns early if they know they will be supported.

Strengthen financial controls: Use dual approval for payments above agreed thresholds. Where possible, separate responsibilities for requesting, approving, and processing payments.

Formalise supplier processes: Maintain trusted supplier records and require formal checks before accepting new or amended bank details.

Secure business email accounts: Enable multi-factor authentication, monitor for suspicious login activity, and review mailbox forwarding or deletion rules that may indicate compromise.

Use technical controls to support staff: Email filtering, anti-spoofing controls, endpoint protection, and account monitoring can reduce the number of threats that reach staff.

Test and refresh procedures: Staff awareness should not be a one-off annual exercise. Businesses should regularly review lessons learned from incidents, update processes, and ensure staff understand current threats.

PERSONAL

THE EVOLUTION OF PHISHING: HOW SCAMS ARE REACHING PEOPLE ACROSS DIFFERENT CHANNELS

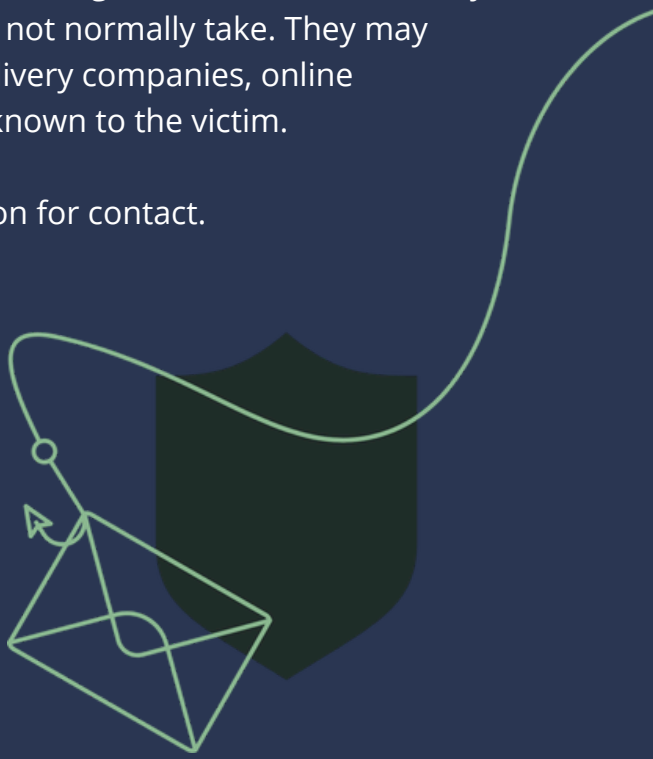
Phishing is often associated with suspicious emails, but scam attempts now reach people through many different channels. Cyber criminals may use emails, text messages, phone calls, messaging apps, social media, online adverts, QR codes, fake websites, and even video meeting invites to trick victims into sharing information, clicking links, downloading malware, or transferring money.

While the delivery method may change, the underlying tactics often remain the same. Scammers create urgency, impersonate trusted organisations or individuals, and pressure victims into acting before they have time to stop and think. This can include a fake bank warning sent by text, a phone call claiming there has been suspicious account activity, a WhatsApp message pretending to be from a family member, or a fake online meeting invite asking the user to install an “update” before joining. Recent reporting has also highlighted fake meeting invites abusing platforms such as Zoom, Microsoft Teams and Google Meet.

How These Scams Work

Phishing, vishing and smishing all rely on social engineering. This means criminals try to manipulate people into taking actions they would not normally take. They may impersonate banks, government services, police, delivery companies, online retailers, technology providers, charities, or people known to the victim.

Scammers often begin by creating a believable reason for contact. This may include an alleged suspicious payment, a blocked account, a missed delivery, a refund, an unpaid fine, a prize, or an urgent security issue. They then pressure the victim to act quickly, often by clicking a link, calling a number, entering login details, sharing a one-time code, installing software, or moving the conversation to another platform.



Some scams are relatively simple, such as a text message containing a suspicious link. Others are more involved. For example, a victim may receive a call, then be contacted again through WhatsApp, Google Meet, or another service. Criminals may also use personal information and familiar platforms to make the scam more believable.

A WhatsApp message may feel personal, a phone call may feel urgent, and a Google Meet or video call may appear more official. However, legitimate organisations will not ask for passwords, one-time codes, screen sharing access, or urgent payments through unexpected calls or messages.

Recent Local Incidents

Recent reports to the CSC show that scam attempts are increasingly being delivered through a range of communication channels, including phone calls, text messages, and video calling platforms.

One report involved a resident receiving a message on Facebook Messenger claiming they had won money. The message stated that the victim needed to transfer £500 in order to release an apparent £10,000 prize. This type of scam is designed to make the victim believe they are receiving a larger financial reward, while pressuring them to pay an upfront fee first.

Another report involved a victim receiving a call from someone claiming to be from Santander, followed by a WhatsApp call from another individual who appeared legitimate and had detailed personal information about them. During the call, the victim was instructed to enable screen sharing, log into online banking, share a one-time code and authorise a payment. This resulted in a reported loss of £4,000 with further attempted transactions stopped before completion.

These incidents highlight how phishing, vishing and smishing scams are no longer limited to suspicious emails or traditional phone calls. Criminals are adapting their methods and using familiar platforms to appear more convincing, create urgency and pressure victims into taking action. Whether contact comes through email, text, WhatsApp, Google Meet or a phone call, unexpected requests involving payments, account security, one-time codes, screen sharing or personal information should always be treated with caution and verified independently.

How to Protect Yourself

Stop and take a moment: If you receive an unexpected call, text, email, WhatsApp message, or meeting invite, do not feel pressured to respond immediately. Scammers often rely on urgency to stop you thinking clearly.

Verify the contact independently: If a message or call claims to be from your bank, a government service, police, or another organisation, contact them using a trusted method. Use the official website, a number on the back of your bank card, or contact details you already know. Do not use numbers, links, or email addresses provided in the suspicious message.

Do not share sensitive information: Never share passwords, PINs, one-time passcodes, banking details, or personal information with someone who has contacted you unexpectedly.

Be careful with links and downloads: Avoid clicking links or downloading apps from unexpected messages. If you need to access an account, go directly through the official website or app.

Check the sender carefully: Look for unusual numbers, spelling mistakes, slightly altered names, or email addresses that do not match the organisation they claim to represent.

Be cautious of video calls and meeting invites: If you receive an unexpected Google Meet, WhatsApp, Teams, or video call claiming to be from a bank or support service, treat it as suspicious. Do not join, download software, or provide personal information unless you have independently confirmed it is genuine.

Act quickly if you think you have responded to a scam: If you have shared banking details, made a payment, provided a one-time code, or allowed access to your device, contact your bank immediately. Change affected passwords and report the incident as soon as possible.

Report suspicious contact: Reporting suspicious messages, calls and scams helps build a clearer picture of the threats affecting Island residents and may help prevent others from being targeted.

More information about phishing, vishing, and smishing scams and a wide range of other related topics can be found in the advice and guidance section of the CSC website. Visit our advice and guidance page here: **https://csc.gov.im/advice-guidance/**

THREAT REPORT: SPOTLIGHT

ARE YOU PREPARED FOR THE PATCH WAVE? WHY REGULARLY PATCHING YOUR SYSTEMS AND SOFTWARE IS MORE IMPORTANT THAN EVER BEFORE

For many years, cyber security teams have followed a familiar rhythm; identify vulnerabilities, test updates, deploy patches, and move on to the next maintenance cycle. Today, that rhythm has changed dramatically.

We are entering what many cyber security professionals describe as a 'patch wave'. A period where organisations are facing an unprecedented volume of software vulnerabilities, security updates, and remediation requirements. The driving force behind this change is not simply the growing number of cyber threats. Increasingly, it is the rapid development and adoption of Artificial Intelligence (AI).

The same technology helping organisations innovate faster is also fundamentally changing how vulnerabilities are discovered, exploited, and patched. AI-assisted development tools have transformed software engineering. Developers can now generate code faster than ever before, accelerating innovation and reducing development timelines.

However, faster development means:

- More applications being created
- More code being written
- More dependencies and open-source components being used
- More opportunities for security flaws to emerge

At the same time, AI is enabling security researchers and threat actors alike to analyse code at a scale that was previously impossible. Microsoft recently warned that advanced AI models are capable of autonomously identifying weaknesses, linking vulnerabilities together, and producing proof-of-concept exploits, significantly reducing the time between vulnerability discovery and exploitation. What previously took weeks can now take minutes.

The result? Vulnerabilities are being discovered faster than organisations can traditionally patch them.

The Time Between Vulnerability Discovery to Exploitation is Decreasing

Historically, organisations often had weeks or months to respond after a vulnerability became public. That window is shrinking.

Security experts are reporting that AI-driven vulnerability analysis is finding software weaknesses "at industrial scale", accelerating both defensive research and offensive exploitation. This means that once a patch is released, attackers can quickly analyse the update, identify what was fixed, and target organisations that have not yet applied the patch. This creates significant risk for organisations with infrequent or irregular patch cycles.

Vulnerability disclosures in 2026 have already reached record levels, with AI-assisted discovery identified as a major contributor to the surge. Furthermore, a number of publicly available AI models are now capable of producing the code and processes to exploit these vulnerabilities.

Why Attackers Love Unpatched Systems

Cyber criminals rarely need sophisticated zero-day exploits when unpatched systems remain readily available.

Many ransomware groups actively scan the internet for organisations that have failed to apply publicly available updates. Once a vulnerability becomes known and a patch is released, attackers often assume that:

- Some organisations will delay patching
- Legacy systems may be too challenging to update quickly
- Operational concerns will slow remediation efforts

In effect, every unpatched system becomes a potential target. This is one reason why the United States Cybersecurity and Infrastructure Security Agency (CISA) maintains its Known Exploited Vulnerabilities (KEV) catalogue, highlighting vulnerabilities that are already being exploited in real-world attacks and should be prioritised immediately.

The New Reality: Patching Is a Business Risk Function

Patching is no longer simply an IT maintenance activity. It is now a core cyber resilience function.

Boards, executives, and risk owners should view patch management as an essential control that helps:

- Protect business operations
- Reduce ransomware exposure
- Safeguard customer and organisational data
- Maintain regulatory compliance
- Improve organisational resilience

How Organisations Can Prepare for the Patch Wave

To keep pace with the accelerating patch cycle, organisations should:

1. **Know What You Own** - Maintain a complete and accurate asset inventory. You cannot patch systems that you do not know exist.

2. **Prioritise Based on Risk** - Not every vulnerability requires immediate action.
   Focus on:
   - Internet-facing systems
   - Critical business applications
   - Vulnerabilities listed in CISA's KEV catalogue
   - High-likelihood exploitation scenarios

3. **Reduce Patch Latency** - The shorter the interval, the lower the exposure.
   Measure the time between:
   - Patch release
   - Risk assessment
   - Deployment

4. **Test and Automate** - Automated patch deployment and vulnerability management tools can significantly reduce administrative burden and improve consistency.

5. **Build Security into Procurement** - Ensure suppliers and service providers maintain robust patch management processes as part of contractual requirements.

Conclusion

Artificial intelligence is accelerating every aspect of the cyber security landscape. It is helping developers create software faster, researchers uncover vulnerabilities sooner, and defenders identify and address weaknesses more effectively. However, these advantages are not limited to the good actors. The same capabilities are enabling cyber criminals to find, exploit, and scale attacks against vulnerabilities at an unprecedented pace.

As vulnerability discovery accelerates, organisations that treat patching as a routine maintenance task will increasingly struggle to keep pace. Those that view patch management as a strategic cyber resilience capability will be far better positioned to withstand the growing volume of threats.

INTERNATIONAL THREATS

MAJOR TECH SUPPLIER TATA ELECTRONICS SUFFERS DATA BREACH EXPOSING APPLE AND TESLA DATA

Tata Electronics confirmed a cyber incident affecting some of its systems after the extortion group, 'World Leaks', claimed it had stolen and published more than 200,000 files. The alleged 630GB data set reportedly included engineering documents, manufacturing specifications, emails, system logs, and employee records. However, the company stated that response protocols were activated immediately and that business operations remained unaffected.

Researchers reviewing the leaked data identified documents appearing to contain confidential information belonging to Apple and Tesla. The Apple-related files included manufacturing and quality inspection documentation for iPhone components, while the Tesla-related material appeared to contain engineering drawings and component specifications. Employee passports and other sensitive operational information were also exposed.

Tata Electronics has not disclosed how the attackers gained access, which systems were affected, or whether the incident directly led to the alleged data exposure. World Leaks reportedly issued a ransom demand before releasing the files via its darkweb leak site. Unlike traditional ransomware attacks that encrypt systems, this incident appears to have focused primarily on data theft and extortion.

The incident serves as a reminder of the cyber security risks associated with global supply chains. As a major manufacturing partner for Apple and supplier to Tesla, a compromise of Tata Electronics could expose information belonging to multiple organisations. Even where companies maintain strong internal security controls, sensitive information may still be at risk when shared with suppliers and other trusted third parties.

Organisations should treat suppliers with access to sensitive information as an extension of their security environment. Controls should include due diligence, clearly defined security requirements, restrictions on supplier access, and regular reviews. Organisations should also understand what information is held by third parties and ensure contracts provide clear arrangements for incident notification, investigation, and recovery. While supplier incidents may not disrupt operations directly, the exposure of intellectual property, personal information, or internal documentation can still lead to fraud, impersonation, and further targeted attacks.

VISHING SCAM CAUSES AURORA TO LOSE NEARLY $1.1 MILLION FROM CITY BANK ACCOUNTS

The City of Aurora in the United States lost nearly US$1.1 million from its payroll bank accounts after an employee received a phone call from an attacker impersonating a bank representative. The caller appeared legitimate and created a false sense of urgency, persuading the employee to disclose sensitive account information that was subsequently used to make fraudulent transfers from the city's accounts.

City officials became aware of the fraudulent payments shortly after the transactions occurred and immediately began efforts to limit the impact and recover the funds. Law enforcement and the city's financial institution were notified, while external cyber security specialists were brought in to support the investigation. Authorities are working with financial institutions to identify those responsible and recover as much of the stolen money as possible. The city also maintains insurance intended to help reduce financial losses from incidents of this kind.

Officials stated that there was no evidence the city's network or data systems had been compromised. However, the financial institution was conducting a forensic audit to establish whether any employee information held on its systems had been affected. The city said employees would be notified promptly if the investigation found that their information had been exposed.

The incident demonstrates how social engineering and vishing attempts can bypass technical protections by targeting people rather than systems. Fraudsters may impersonate banks or other trusted contacts and pressure victims into sharing account details, credentials, security codes, or information needed to authorise payments. A convincing caller and an urgent request can make it difficult for employees to recognise the warning signs, particularly where the attacker already possesses information about the organisation.

Organisations should require independent verification of unexpected financial requests using trusted contact details, particularly where sensitive information or payments are involved. Strong approval processes, transaction alerts, transfer limits, and separation of financial duties can reduce the risk of a single employee authorising or enabling fraudulent activity. Staff should also receive regular training on vishing tactics and be encouraged to pause, challenge urgent requests, and report suspicious calls immediately.

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. See also: Multi-Factor Authentication (MFA).

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).

Artificial Intelligence (AI): Systems or software that can perform tasks normally requiring human intelligence, such as learning, problem-solving, pattern recognition, and decision-making.

Business Email Compromise (BEC): A fraud technique where attackers impersonate trusted individuals (e.g. executives or suppliers) via email to trick victims into transferring money or sensitive information.

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.

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.

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.

Extortion/Sextortion: A type of fraud where criminals threaten to release sensitive, private, or fabricated information unless the victim pays money or complies with their demands.

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**.**

Gift Card Fraud: A scam where criminals trick victims into purchasing and sharing gift card codes as a form of payments, allowing the funds to be redeemed anonymously.

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.

Identity and Access Management (IAM) Controls: Security measures and policies used to manage digital identities and control user access to systems and data, ensuring only authorised individuals can access specific resources.

Impersonation: A tactic where a cyber criminal pretends to be a legitimate person or organisation to deceive victims into providing information, money, or access.

Investment Fraud: A scam where criminals exploit interest in financial opportunities by promoting fake or misleading investment schemes to steal money.

Invoice Fraud: A type of scam where attackers pose as a legitimate supplier and send fake or altered invoices to redirect payments to fraudulent accounts.

Known Exploited Vulnerabilities (KEV): A list maintained by CISA that identifies vulnerabilities known to be actively exploited by threat actors, helping organisations prioritise patching and remediation efforts.

Least Privilege: A security principle where users or systems are granted only the minimum level of access necessary to perform their tasks, reducing potential damage if compromised.

Legacy System: An older computer systems, software application, or technology that is still in use despite no longer receiving security updates or patches, making it more difficult to secure or maintain.

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 using two or more authentication factors, such as a password and a one-time code. 2-Factor Authentication (2FA) is the most common form of MFA.

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

Proof-of-Concept (PoC) Exploit: Code or a demonstration created to show that a vulnerability can be successfully exploited.

Purchase Scam: A type of fraud where criminals advertise goods or services that do not exist, or never intend to deliver, in order to obtain payment from victims.

Quishing: A type of phishing attack that uses malicious QR codes to direct victims to fraudulent website or trigger other malicious activity.

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.

Romance Fraud: A scam where criminals build fake online relationships to gain trust and emotionally manipulate victims into sending money or personal information.

Security Patch: A software update released to fix security vulnerabilities and reduce the risk of a system being compromised.

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.

Spoofing: A technique used by attackers to impersonate a trusted person, organisation, device, or service in order to deceive victims and gain access to information, systems, or funds.

Supply Chain Attack: A cyber attack that compromises a third-party vendor, software, or hardware to gain access to a ttarget organisations' systems or data.

Third-Party: An external organisation, supplier, contractor, or service provider that has a business relationship with an organisation and may have access to its systems, data, or services.

Verification: The process of confirming the identity of a user, device, organisation, or piece of information before trust or access is granted.

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-day Exploit: An attack that takes advantage of a software vulnerability before a fix or security patch is available from the vendor.

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