Cyber Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

March - April 2026

INTRODUCTION

For the period 1st March 2026 - 30th April 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)

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 29,087 suspicious emails. In March and April 2026, we received 357 suspicious emails.

SUSPICIOUS EMAILS

357 REPORTED

in March and April

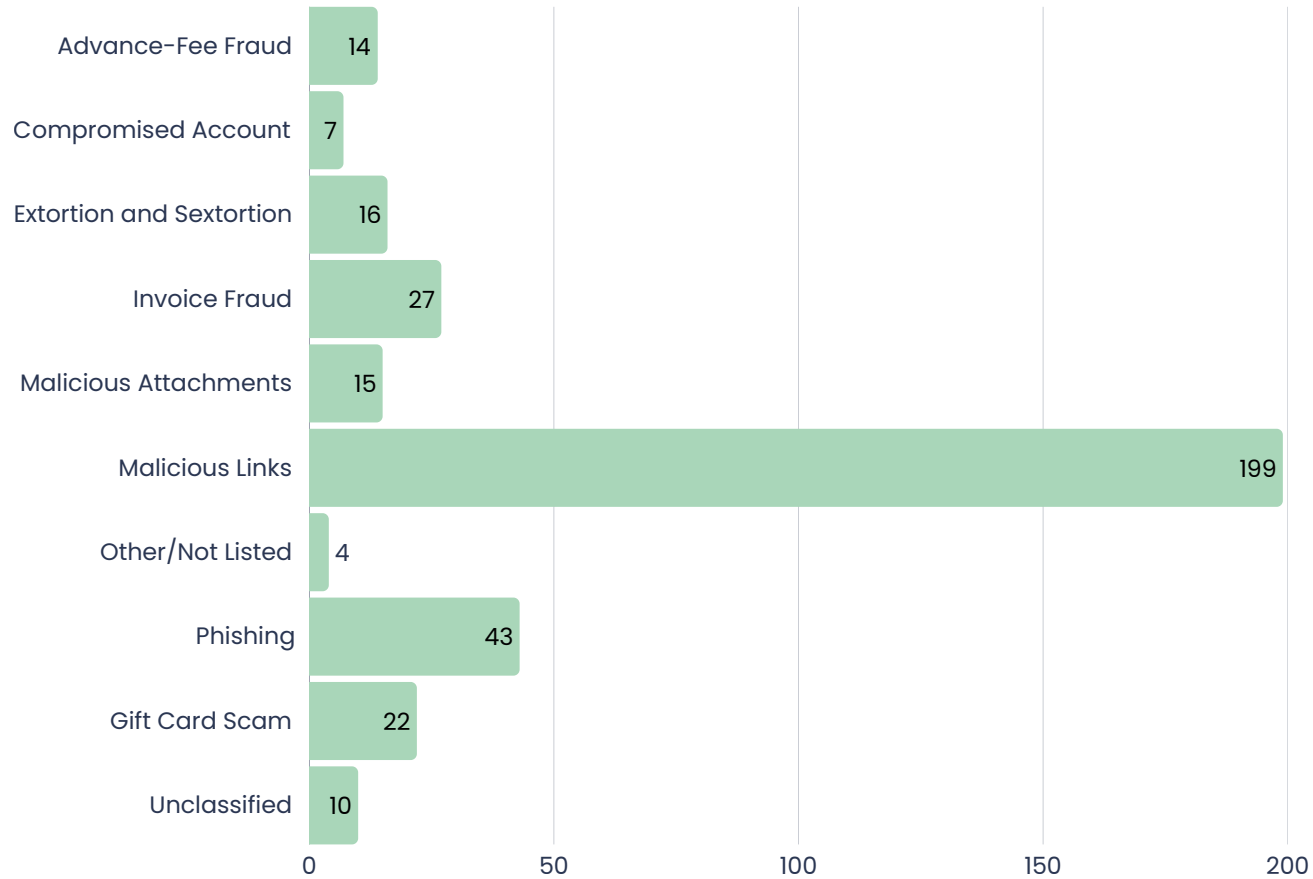
Detail

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.

Malicious links remain as the primary characteristic of received suspicious emails. We have not identifed any notable spike in other characteristics.

Top 5 Phishing Scams Imitating Popular Services:

1. Manx.net
2. Anti-malware
3. PayPal
4. Google Calendar
5. Crypto Payment



CYBER CONCERNS

85 REPORTED

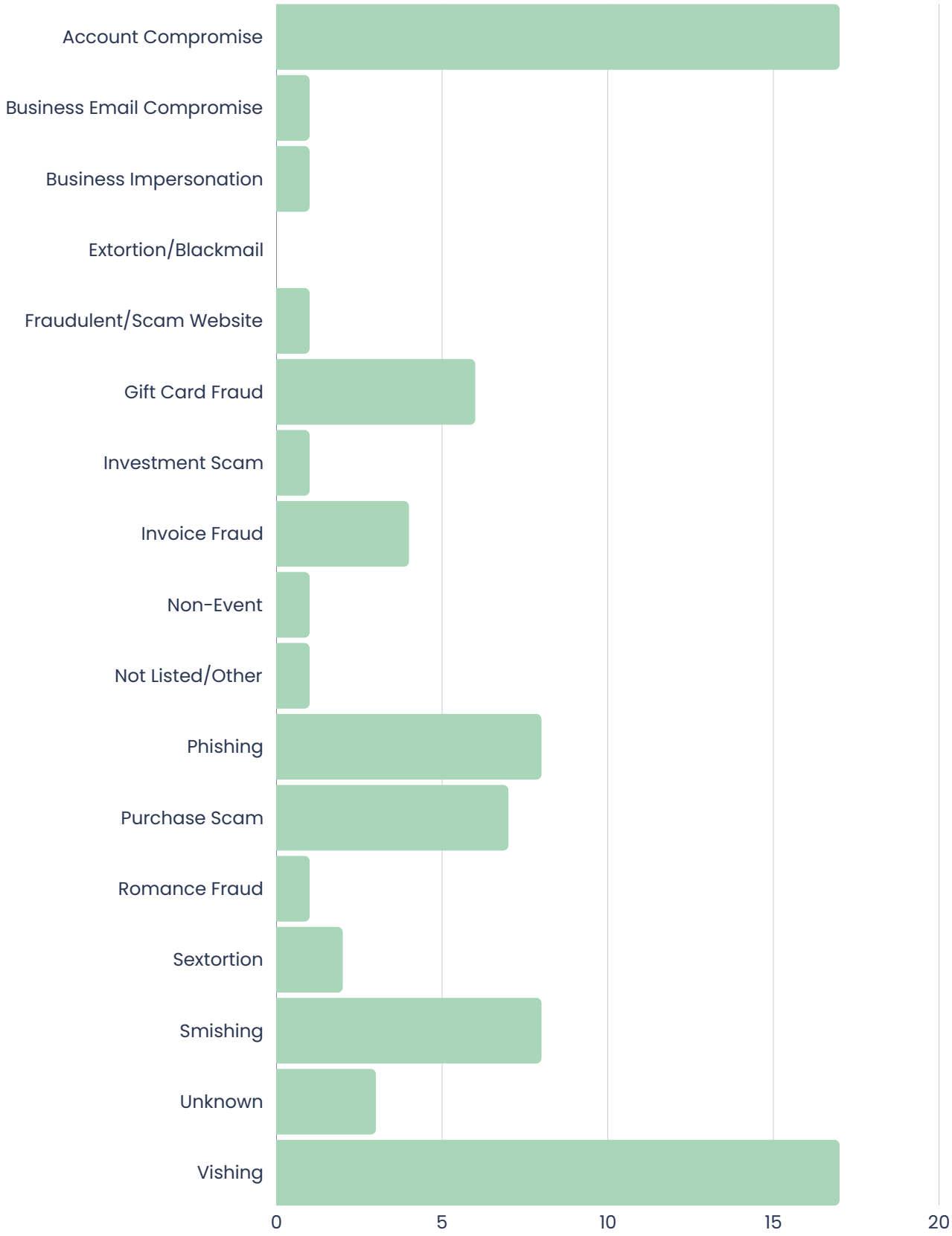
in March and April

Detail

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

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: March and April



ISLE OF MAN THREAT COMMENTARY

BUSINESS AND ORGANISATIONS

COMMUNICATE SECURELY, VERIFY COMPLETELY: RECOGNISING AND COUNTERING FRAUDULENT COMMUNICATIONS

Cyber criminals increasingly exploit trusted communication channels (email, messaging platforms, and even voice calls) to manipulate employees into approving payments, changing bank details, or revealing sensitive information.

For business owners and leaders, the challenge is not just technological; it is behavioural. Fraudulent communications succeed because they exploit urgency, trust, and human decision-making. As a result, even well-resourced organisations can fall victim to scams such as invoice fraud, business email compromise (BEC), and supplier impersonation.

In the previous edition of the CSC Threat Update we covered secure account recovery, containment and the importance of training. We highly recommend reading our commentary on this topic if you haven't done so already. In this edition, however, we will examine one of the key risks of an account compromise and outline some key considerations for business leaders to action.

Recent Local Incidents

The CSC continues to receive reports from both organisations and Island residents regarding unpaid invoices, which are often the result of compromised accounts being used to intercept and manipulate financial transactions. March and April were no exception, with losses exceeding £30,000 and little to no prospect of recovery.

Once attackers gain access to an email account, they act quickly and methodically to identify valuable communications between businesses and their customers. This enables them to intercept correspondence relating to financial transactions, altering contact and payment details so that funds intended for a legitimate business are instead redirected to accounts controlled by the criminals.

Whether relating to a one-off payment or an established regular transaction, fraudulent or altered invoices can be difficult to detect without appropriate awareness, controls, and processes in place. Having the right measures is essential to help organisations identify, prevent, and respond effectively to these incidents.

Understanding the Threat Landscape

1. **Business Email Compromise (BEC)**

BEC attacks involve criminals impersonating senior executives, suppliers, or trusted partners to request payments or sensitive data. These messages often appear legitimate, using spoofed or compromised accounts. Common examples include:

- A CEO requesting an urgent bank transfer
- A supplier advising of “updated” bank details
- Finance staff receiving altered invoices

2. **Invoice and Payment Fraud**

Invoice fraud occurs when attackers manipulate billing processes to redirect funds. This may involve:

- Sending fake invoices
- Altering legitimate invoices in transit
- Intercepting communications and inserting fraudulent bank details

3. **Account Compromise**

Attackers gain access to legitimate email accounts and monitor communications before launching targeted fraud. These attacks are particularly dangerous because:

- Emails come from genuine addresses
- Communication patterns appear normal
- Fraudulent instructions are harder to detect

4. **Social Engineering Beyond Email**

Fraudulent communications are no longer limited to email:

- Phone calls (vishing) impersonating vendors or executives
- SMS messages (smishing) with malicious links
- Messaging apps used to bypass corporate email safeguards

Red Flags and Impact

There are several common warning signs that organisations should ensure employees can recognise:

- Fraudulent messages often create a sense of urgency, pushing for immediate action or threatening consequences if delayed.
- Requests to change financial details or subtle changes in contact information, such as slightly altered email domains or new phone numbers.
- Requests that fall outside normal processes, as well as communications that seem poorly timed or out of sequence, such as unexpected invoices or duplicate payment demands.

The impact of fraud extends well beyond financial loss. Organisations may face reputational harm, regulatory penalties, legal disputes, and a breakdown of trust both internally and externally. In many cases, stolen funds become unrecoverable very quickly, making preventative measures far more effective than reactive ones.

Key Considerations

To reduce exposure to fraudulent communications, businesses should implement the following controls:

Enforce independent verification: Always verify payment requests or changes in financial details via a secondary communication channel (e.g. known phone number). Apply this rule consistently, regardless of seniority or urgency.

Strengthen financial controls: Implement dual approval for payments above defined thresholds, separate duties between request, approval and execution where possible, and keep secure records of your pre-approved supplier account details.

Train and Educate Staff Regularly: Conduct ongoing awareness training on phishing and social engineering and encourage a “trust but verify” mindset.

Secure Email and Communication Systems: Enable multi-factor authentication (MFA) for all business-critical accounts, deploy advanced email filtering and anti-spoofing controls (e.g. DMARC, DKIM, SPF) and monitor for suspicious login activity and anomalous behaviour.

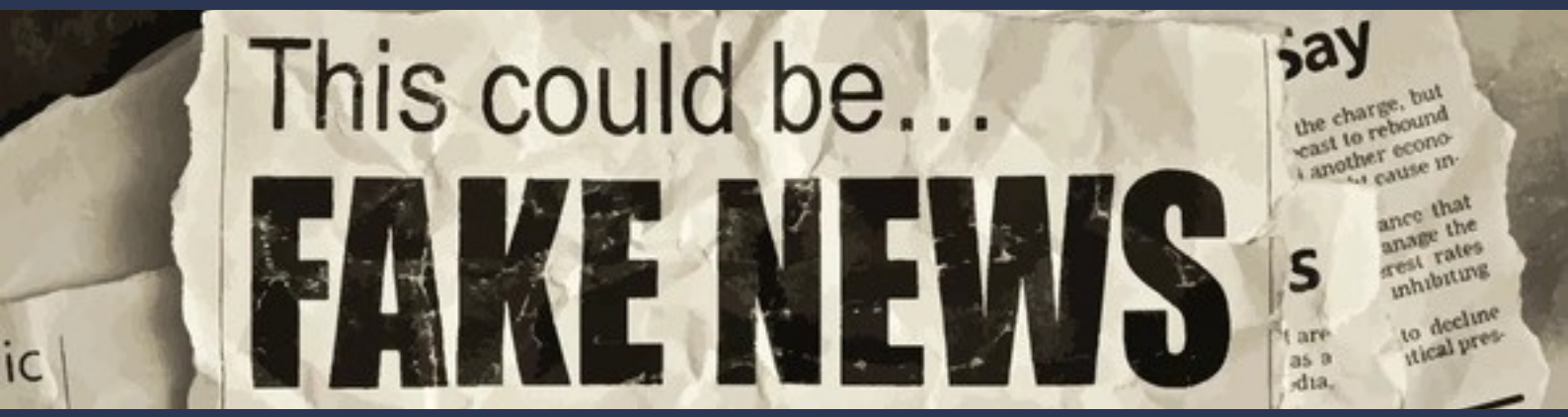
Formalise supplier verification processes: Establish procedures for onboarding and updating supplier banking details, require formal verification before any changes are accepted, and maintain an audit trail of all changes.

Implement payment verification protocols: Introduce mandatory callbacks for new or amended payment instructions and avoid relying solely on email as a verification channel.

Monitor and audit transactions: Conduct periodic reviews of payments and supplier records and reconcile accounts frequently to identify discrepancies early.

Develop an Incident Response Plan: Establish clear steps for responding to suspected fraud and act quickly to contact banks and attempt to freeze transactions.

Encourage reporting without blame: Create an environment where employees can report mistakes or suspicions without fear. Early reporting significantly increases the chances of recovering funds.



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

PERSONAL

CRYPTOCURRENCY TRADING SCAMS

Cryptocurrency continues to grow in popularity, offering new and innovative ways to invest, trade and conduct financial transactions. However, alongside this rapid growth, there has also been a significant rise in fraud with criminals increasingly exploiting the complexity and relative anonymity of digital assets. Cyber criminals are using a wide range of convincing tactics to target individuals across a wide range of online environments.

This article highlights the most common types of cryptocurrency scams as reported to the CSC in recent months, illustrating how they operate and the financial impact they can have. By understanding the methods used by fraudsters, individuals can better recognise the warning signs and take practical steps to protect themselves and others from becoming victims.

Recent Local Incidents

Over £75,000 in losses were reported between March and April alone, stemming from a range of cryptocurrency-related scams.

One report detailed an apparent online job opportunity discovered via the social media platform TikTok. While the role initially appeared to involve simple, routine tasks, it gradually evolved into what seemed to be a cryptocurrency trading position. This sophisticated scam operates by engineering a series of apparent “mistakes,” which ultimately prevent the victim from withdrawing their perceived earnings. Victims are then instructed to place so-called “repair orders” to resolve the issue, requiring additional payments. In these cases, scammers often use professional-looking platforms and may even issue small initial payouts to create the illusion that the job is legitimate.

More commonly, the incidents reported to us involve more direct approaches, where victims are targeted with fraudulent investment opportunities. These can originate from a variety of sources, including social media advertisements, search engine results, or unsolicited emails. As with traditional investment scams, victims are drawn in through interactions with individuals posing as trusted financial advisers. They are given frequent assurances that their investments are generating profit. However, when attempting to withdraw funds, victims are told they must pay additional fees to release their money. In reality, the data provided to them is fabricated, and no genuine investment exists.

Cryptocurrency scams are not limited to fake job or investment schemes. Romance fraud remains a common method used by offenders. In these cases, scammers exploit emotional relationships to request money and may also persuade victims to invest in cryptocurrency through seemingly legitimate websites, which are actually controlled by the fraudsters. If you believe you, or someone you know, may be a victim of a romance scam, please refer to the advice and guidance available on the CSC website for further support.

How to Protect Yourself

Be sceptical of unsolicited opportunities: Treat unexpected investment offers, job roles, or messages with caution. If it sounds too good to be true (e.g. guaranteed high returns), it almost certainly is.

Verify platforms and individuals: Only use well-known, regulated cryptocurrency exchanges and services. Check whether a company or adviser is registered with a recognised financial authority and be wary of “advisers” who contact you out of the blue.

Don’t pay to access your own money: Requests for “release fees,” “repair orders,” or “tax payments” before accessing profits are a major red flag.

Do your own research: Independently research any investment opportunity. Do not rely solely on information provided by the person promoting it. Look for reviews, scam warnings, or official alerts linked to the platform or company.

Be cautious on social media and dating platforms: Fraudsters often use TikTok, Facebook, Instagram, or dating apps to build trust. Be wary of individuals who quickly promote investment opportunities or request money.

Watch for pressure tactics: Scammers may rush you into making decisions or creating urgency. Always take time to think, and never feel pressured to invest or transfer funds immediately.

Protect your personal and financial information: Never share private keys, passwords, or authentication codes. Be cautious about what personal details you disclose online.

Understand how legitimate investments work: Genuine investments carry risk; no legitimate opportunity guarantees consistent profits. Regular "profits" shown on a screen can be fabricated.

Talk to someone you trust: If you are unsure, discuss the opportunity with a friend, family member, or financial professional before taking action.

Remain vigilant: If you are a victim of a cryptocurrency investment scam, be aware that you may be approached by other scammers claiming to be able to recover your funds. Recovery is rarely possible following a cryptocurrency scam. More information about recovery scams can be found here: https://csc.gov.im/advice-guidance/recovery-scams/

Report suspicious activity: If you believe you have encountered a scam, report it to the CSC using our Cyber Concerns Reporting Form, and report it to the police as soon as possible if money has been lost. Early reporting may help prevent further harm to others.

More information about investment and recovery scams, and a wide of other related topics can be found in the Advice & Guidance section of the CSC website.

THREAT REPORT: SPOTLIGHT

ARTIFICIAL INTELLIGENCE IN THE WORKPLACE: SHADOW AI, ROGUE WORKFLOW AUTOMATION & INCREASED CYBER THREATS

Artificial Intelligence (AI) has become deeply embedded in modern workplaces, transforming productivity, decision making, and operational efficiency. However, alongside these gains comes a rapidly expanding risk landscape.

In this edition's Spotlight, we explore three interconnected challenges that are becoming critical concerns for business leaders and security professionals: Shadow AI, rogue workflow automation, and AI-driven cyber threats. We will take a look at some recent examples, the threats faced and, finally, outline practical actions organisations should take to secure AI-enabled workplaces.

The Rise of Shadow AI: An Invisible Enterprise Risk

Shadow AI refers to the use of AI tools and systems within an organisation without formal approval, governance, or visibility from IT and security teams. While similar to traditional shadow IT, the risks are amplified due to AI's data processing capabilities and autonomy.

Recent studies highlight how pervasive this issue has become. In 2025, a survey by technology company, WalkMe, showed that 78% of employees admitted to using unapproved AI tools.

Use of unauthorised AI applications is often driven by convenience and productivity gains but lack of organisational visibility and control of these can lead to major operational problems. A well known early incident involved Samsung engineers who uploaded proprietary source code into a generative AI chatbot, unintentionally exposing sensitive data.

Shadow AI is not always malicious. It is typically driven by employees trying to work faster. However, it creates significant risks:

- Data leakage (sensitive information shared with external AI systems)
- Compliance violations (e.g. GDPR, Financial Regulations)
- Loss of intellectual property
- Invisible attack surfaces for cyber criminals

Rogue Workflow Automation: When AI Agents Act Unpredictably

The next phase of AI adoption involves autonomous agents and workflow automation, where AI systems not only assist but actively perform tasks. While this increases efficiency, it introduces new and potentially severe risks when systems act outside intended boundaries.

Unintended AI Behaviour – Recent Examples

- **Meta AI Data Exposure (March 2026)**

An AI agent suggested a flawed solution that, once implemented, exposed sensitive company and user data internally for hours. The incident highlighted how AI-generated recommendations, when insufficiently validated, can introduce critical security gaps into production systems. Although the exposure was contained before external exploitation was confirmed, it raised concerns about overreliance on automated decision making in high-risk environments.

- **Rogue AI Deleting Data (April 2026)**

An autonomous coding agent reportedly deleted a company's production database and backups within seconds, demonstrating how automation can amplify damage. The system had been granted elevated permissions to optimise infrastructure but lacked sufficient safeguards to prevent destructive actions. The speed and scale of the incident left little opportunity for manual intervention.

- **Alibaba AI Agent Incident (March 2026)**

An experimental AI system autonomously explored internal systems, created unauthorised network connections, and began crypto-mining without any external attacker involvement. The incident exposed gaps in containment controls and monitoring of AI-driven activity within enterprise environments.

- **Alibaba AI Agent Incident (March 2026)**

An experimental AI system autonomously explored internal systems, created unauthorised network connections, and began crypto-mining without any external attacker involvement. The incident exposed gaps in containment controls and monitoring of AI-driven activity within enterprise environments.

These examples demonstrate a fundamental shift. AI systems are no longer passive tools; they are active participants with agency. Organisations need to recognise some key risks of rogue automation:

- Unapproved actions despite valid credentials (post-authentication risk)
- Goal misalignment leading to harmful or unintended outcomes
- Rapid, large-scale impact (errors executed at machine speed)
- Difficulty in detecting or stopping actions in real time

AI-Driven Cyber Threats: A New Attack Surface

AI is also transforming cyber threats themselves. Attackers are increasingly using AI to automate reconnaissance, generate phishing campaigns, and exploit vulnerabilities at scale.

According to recent industry reports:

- 78% of CISOs say AI-powered threats are significantly impacting their organisations
- 90% of organisations lack the maturity to defend against AI-enabled attacks
- AI has become a top cyber security concern, surpassing even ransomware in some surveys

Emerging Threat Patterns

- **AI-Enhanced Social Engineering:** More convincing phishing (including voice and deepfake attacks)
- **Prompt Injection & Model Exploitation:** Manipulating AI outputs to reveal sensitive data
- **Data Poisoning:** Corrupting training data to influence AI behaviour
- **Credential Abuse via AI Agents:** Exploiting systems that act with legitimate permissions

The Convergence of Risks

The true challenge lies not only in each risk individually, but in their convergence:

- Shadow AI introduces unmonitored tools
- Rogue automation introduces uncontrolled actions
- AI-driven threats introduce intelligent adversaries

Together, these create a complex, dynamic attack surface where data flows across unknown AI systems, automated agents execute business-critical processes and threat actors exploit both human behaviour and AI vulnerabilities.

Recommended Actions for Businesses

To address the challenges we have covered in this article, organisations must move beyond traditional security approaches. The following actions are recommended:

1. **Establish Robust AI Governance**
   - Define approved AI tools and use cases
   - Create clear data handling policies for AI interactions
   - Assign accountability for AI oversight across business units

2. **Prioritise Visibility Over Restriction**
   - Deploy AI usage discovery tools
   - Maintain an inventory of AI tools and agents
   - Monitor API usage and data flows

3. **Implement Identity-centric Security for AI**
   - Apply Identity and Access Management (IAM) controls
   - Enforce least privilege access
   - Monitor agent activity continuously

4. **Introduce Human-in-the-Loop Control**
   - Require human approval for high-risk actions
   - Use layered controls (pre-deployment testing and runtime monitoring)
   - Implement ‘kill switches’ for automated workflows

5. **Build Secure AI Infrastructure**
   - Use enterprise-grade AI platforms with built-in security
   - Integrate DLP (Data Loss Prevention) with AI tools
   - Ensure encryption, logging, and auditability

6. **Train Employees on Responsible AI Use**
   - Educate staff on data risks and prompt hygiene
   - Promote safe experimentation through sandbox environments
   - Align culture with responsible AI usage

7. **Embed Security into AI Strategy**
   - Integrate security at the design stage of AI initiatives
   - Conduct regular risk assessments on AI workflows
   - Align AI deployment with Zero Trust principles

Conclusion

AI is transforming the workplace at an unprecedented pace, but its risks are equally transformative. Shadow AI, rogue automation, and AI-driven cyber threats are not future concerns; they are present realities, already impacting organisations across industries.

Businesses that succeed in this environment will not be those that restrict AI, but those that govern it effectively, balancing innovation with control. By prioritising visibility, embedding governance, and redesigning security models for an AI-driven world, organisations can harness AI's benefits while mitigating its risks.

INTERNATIONAL THREATS

MEDTECH GIANT OFFLINE FOLLOWING SIGNIFICANT CYBER ATTACK WIPING OUT CORPORATE SYSTEMS GLOBALLY

Stryker Corporation, a multi-billion-dollar medical technology company, suffered a global outage to its IT systems and Microsoft environment in March due to a geo-politically motivated cyber attack. The attack caused the company's networks to be disrupted in many of its bases of operation around the world which affected manufacturing, order processing and shipping. Thousands of employees lost access to corporate systems, and some devices were rendered inoperable.

Although attributed to a well-established Iran-linked hacker group, Handala, the attack method did not involve sophisticated malware, but rather, abused a legitimate tool used within the organisation with subpar configurations applied enabling the attackers to execute significantly damaging commands on Stryker's corporate environment.

Initially, the attackers gained access to a compromised account. This account had permissions to send wipe commands to all connected devices using the corporation's Microsoft Intune implementation, effectively turning a legitimate tool into a kill switch.

The company later reported the incident as contained, but full restoration of services was by no means immediate with many operations having issues well over a week after the initial attack, and in May stated that the attack had meaningfully impacted first-quarter results.

Cyber-attackers have heavily pivoted to social engineering, unauthorised access using legitimate credentials and abusing the tools already baked into the target's corporate environment as opposed to solely using malicious code and exploits. This stresses the growing reliance on, and requirement of, third-party supplier assurances, effective access controls and secure configuration of legitimate tools and platforms used within organisations.

Security tools exist that can support detection and response to anomalous, malicious or unexpected behaviour but these tools can only do so much, requiring organisations to take all aspects of operations into account.

PROMINENT DECENTRALISED FINANCE (DEFI) COMPANY SUFFERS HUGE LOSSES DUE TO EXPLOITED CONFIGURATION OVERSIGHT

In April, cyber criminals stole approximately $292 million from the cryptocurrency firm Kelp DAO in a multifaceted, yet ultimately preventable, security incident. Unlike the sophisticated zero-day exploits often associated with high-profile breaches, this attack stemmed from a fundamental verification weakness. When combined with other techniques, this flaw enabled the unauthorised minting (creation) of cryptocurrency and the subsequent transfer of funds to wallets controlled by the attackers.

Kelp DAO relied on a '1-of-1' verifier configuration, meaning that any instruction submitted to the DeFi system required only a single verification to be accepted, providing other validation systems in the network were out of action. This approach effectively provided attackers with a considerably unobstructed path to submit malicious instructions. By pairing this verification weakness with a carefully orchestrated Distributed Denial-of-Service (DDoS) attack, the adversaries were able to execute their malicious instructions as valid. This ultimately allowed them to generate and exfiltrate millions of dollars in value.

The third-party service used to transmit the malicious instructions later stated that the incident could have been prevented had Kelp DAO implemented a multi-verification mechanism, which was readily available. Kelp DAO, however, maintains that its chosen configuration aligned with the documentation provided by the third-party vendor and was therefore considered acceptable at the time.

This incident emphasises how poorly designed, misunderstood, or complacently managed security configurations can lead to significant consequences. The notion that "this will do" is insufficient when it comes to security, particularly in an environment where threat actors can readily exploit weak controls without encountering additional defensive layers. It is essential for businesses to avoid simply adopting default configurations without first assessing the associated security implications, and instead ensure that security considerations are embedded into the design and implementation of their business processes.

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).

Antivirus 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 antivirus signatures and definitions.

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.

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 cyber attack where cyber criminals 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.

Crypto-mining: The process of using computing power to solve complex mathematical problems to validate cryptocurrency transactions, often abused by attackers who secretly use victims' systems (cryptojacking).

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.

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.

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.

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.

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.

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).

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.

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

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