



Cyber Security
Centre for the
Isle of Man

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

July – August 2026

INTRODUCTION

For the period 1st July 2026 – 31st August 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
Personal Advice: The Rise In Deepfake Investment Scams	11
Spotlight Article: Agentic AI	16
Cyber-Glossary	22
About Us	26

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 **July and August** 2026, we received **259** suspicious emails.

SUSPICIOUS EMAILS

259 REPORTED

in July and August

Detail

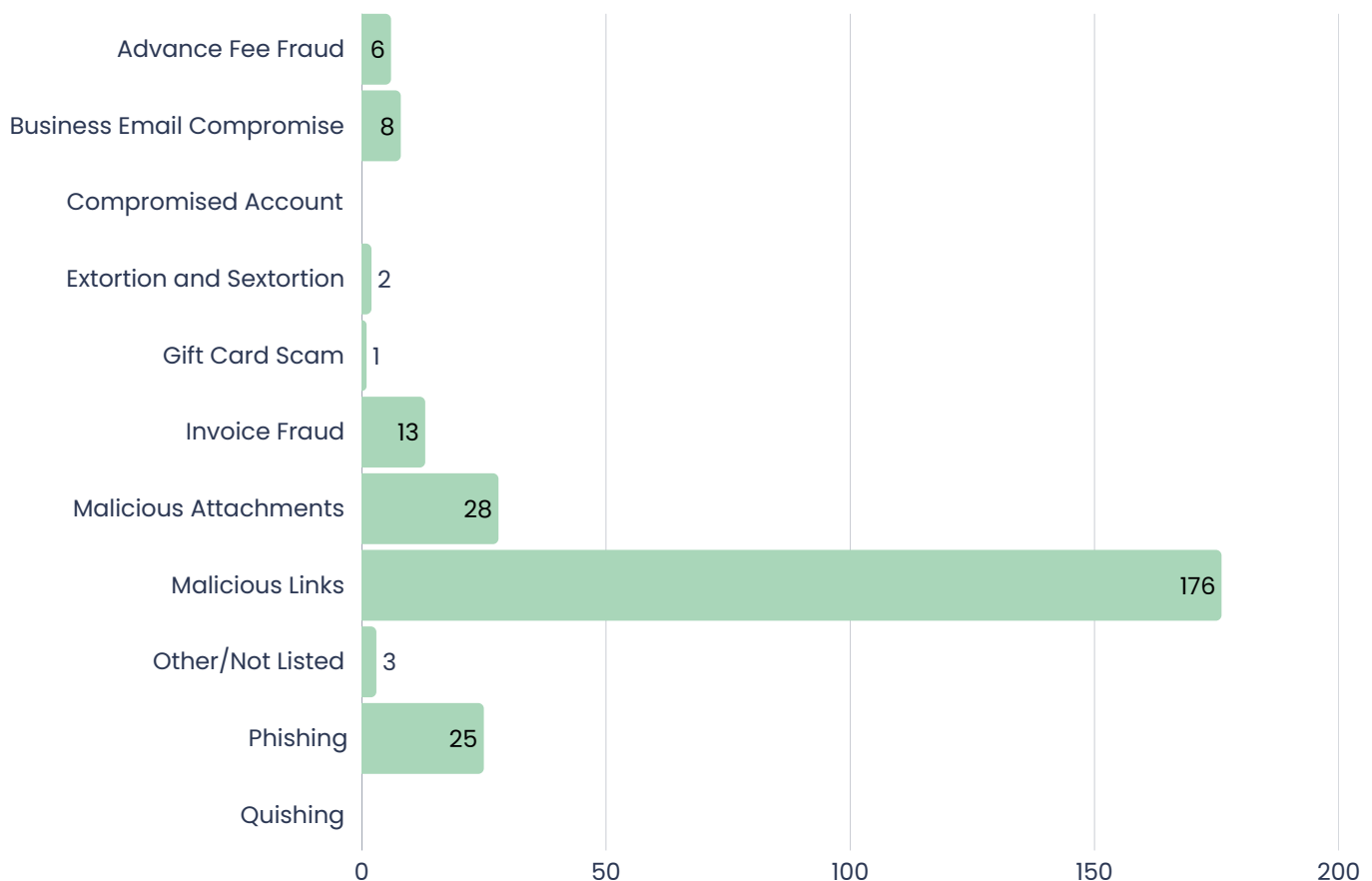
The graph below shows the frequency of specific characteristics identified in submitted SERS emails. Please note that some emails have more than one recorded characteristic.

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

157 REPORTED

in July and August

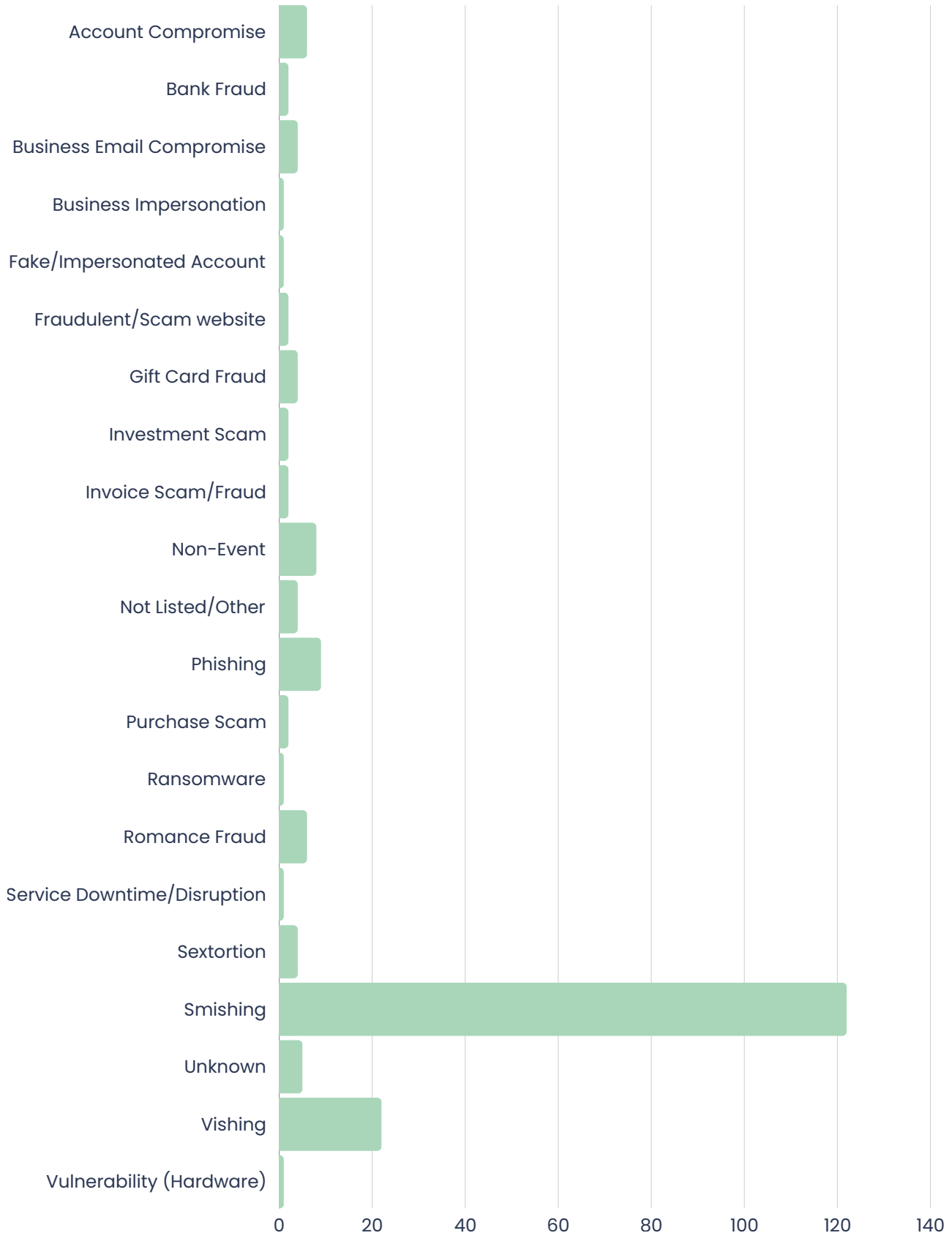
Detail

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

As 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](#).

Reported Cyber Concerns Between July and August



ISLE OF MAN THREAT COMMENTARY

IS YOUR DIGITAL FRONT DOOR SECURE? WHY WEBSITE SECURITY MATTERS FOR YOUR ORGANISATION, CLIENTS, AND CUSTOMERS

Your organisation's website is a critical business asset that can become a gateway for cyber-criminals. A compromised website can expose customers to fraud, damage your reputation, disrupt operations, and even provide attackers with a foothold into wider business systems. Even if your website is simply serving only as a static advertisement or brochure for your business.

In this article, we will discuss emerging threats such as "ClickFix" campaigns, where legitimate websites are compromised and used to display fake CAPTCHA or error messages that trick visitors into executing malicious commands themselves. It also highlights the growing risk posed by third-party suppliers, including website developers, hosting providers, and content delivery services. A ransomware incident or security breach affecting one of these suppliers can quickly cascade to every customer that depends on them.

In addition, we will also look at the latest evolution of Magecart attacks, including the "HexMage" campaign, which has compromised dozens of online stores by injecting malicious checkout code designed to steal payment card details. The campaign demonstrates how attackers are adopting increasingly sophisticated techniques, including the use of blockchain infrastructure to hide and rotate their malicious components, making detection and disruption significantly more difficult.

Ultimately, organisations of all sizes should view website security as a core business risk, ensuring not only that their own systems are secure but also that the suppliers and platforms they depend upon meet appropriate cyber-security standards.



Magecart: What is card skimming and how does it work?

As a business, it is your responsibility to protect your customer's data. If your website is compromised with a malware infection such as those delivered by Magecart, you risk your customer's financial information being skimmed. This isn't just a problem for the direct victims, but it also affects your own business in reputation and potentially fines if not handled and reported correctly.



When Magecart operators compromise a website, they insert malicious code into payment webpages. They overlay the card payment screen with a false one. Card details are entered and the payment goes through. But they have also “skimmed” your data for themselves. The victims will typically be none-the-wiser until transactions start leaving their bank accounts.

Recent Local Incidents

In late July, the CSC was made aware of a compromised website serving the Island's population and prospective property hunters further afield. This website had been identified as possessing a "ClickFix" attack method that had been injected into the underlying code of one of the pages. On this page, users were instructed to paste a line of code into their computers under the guise of a reCAPTCHA. This, of course, was deception, and would result in malware being downloaded and executed on the visitor's computer.

The CSC identified the contact for this website and advised them of the compromise, and to take appropriate action to contain and remediate the issues.

In a separate incident, a training platform based on the Island suffered an outage affecting all customers for several days. This was as a result of a ransomware attack, but the platform itself was not the target; it was the service's third-party hosting solution that was targeted. Fortunately, the attack was contained and the training platform's services were able to be resumed within a relatively short time frame (under the average downtime of 19 days), although, any downtime is never good and will cost the business money to recover, investigate and get back up and running again, and cause potential reputational damage.



What to Look Out For & How to Protect Yourself

MageCart attacks have adopted various advanced techniques to conceal their malicious code through methods such as encoding, packing and obfuscation through seemingly harmless sources like fake images, audio snippets or favicons. Consequently, it has become much harder to detect compromised websites, however, organisations can protect against MageCart attacks by implementing a comprehensive website-oriented security monitoring strategy.

Indications of a Magecart attack:

- Unexpected modifications to JavaScript code, particularly code associated with payment or checkout forms.
- New, modified or unauthorised third-party scripts/plugins loaded onto the website, typically loaded on checkout pages.
- Obfuscated JavaScript, designed to hide malicious functionality of the attack and evade detection from security tooling and investigations.
- Unfamiliar data transfers or network requests occurring during the payment process.
- Unusual scripts loaded from suspicious, unfamiliar, or newly registered domains

Important: Any suspicious activity involving new additions or modifications to your website should be investigated and monitored, even if it has not been identified as malicious or suspicious by security tooling. This is particularly important to investigate when those changes affect the payment platform for your website, as MageCart threat actors commonly target checkout and payment environments to steal customer payment card data.



Steps to protect your website or online store:

- Ensure your software is regularly updated, including Content Management Systems (CMS), plugins and other third-party software that interacts with or from your website.
- Only use third-party JavaScript and plugins from reputable and verifiable sources, be informed and selective when choosing scripts that you add to your website
- Implement a web application firewall and intrusion detection system (IDS) to block malicious actors or bots
- Conduct regular security audits and code reviews, this ensures that any recent modifications can be discovered and justified or reversed.
- Monitor outbound network traffic from your payment pages for connections to suspicious domains.
- Document all third-party scripts utilised within your website, this enables you to easily monitor new additions or modifications to scripts.



Key Considerations

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

- **Supplier trust & assurances:** Gain assurances from any web hosting service provide or content delivery network that vulnerabilities, threats and indicators or compromise are being actively monitored and that playbooks are in place for containment, remediation and restoration should an incident occur.
- **Websites are not “set-and-forget”:** Even if your website is simply an advertisement for your business, this still does not mean there aren’t potential vulnerabilities that can appear. Know what your website is made of, monitor it and treat it as a business risk.
- **Understand and test incident scenarios:** Understand and document the processes required to contain systems and services in the event of a cyber incident. Test out these processes routinely to ensure they can be implemented effectively.
- **Enhance access protections:** Use strong passwords, and passkeys or multi-factor authentication for all your systems and service accounts wherever possible. This may not stop a compromise from a technical vulnerability, but it will better protect you against compromise via a hacked account.

We have more related advice & guidance for businesses on the CSC website, such as what to do if your email has been compromised, incident response and ransomware information, here: <https://csc.gov.im/advice-guidance/advice-guidance-for-organisations/>



PERSONAL ADVICE

SEEING ISN'T BELIEVING: THE RISE IN DEEPPFAKE INVESTMENT SCAMS

Historically, there have been two definitive ways to prove your identity, through your face and your voice. With the development of artificial intelligence, these methods of authenticity have shifted, and your face and voice can no longer be relied upon to fully certify your identity.

Deepfakes or 'digital forgeries' are synthetic media that has been generated or modified by artificial intelligence. This can take the form of images, audio snippets and videos that imitate real people, giving the impression that someone said or did something that they have never done.

These deepfakes are becoming increasingly realistic and convincing of a person's likeness, voice or identity. Just within the last year they have progressed to becoming hyper realistic, producing less anomalies and becoming progressively harder to identify without the assistance of technology.



How do Deepfakes Work?

Deepfakes are created by utilising artificial intelligence and machine learning models that are typically trained on huge datasets of images, videos and audio recordings of human interactions. This allows the artificial intelligence to learn patterns in a person's facial features, voice characteristics, expressions and mannerisms to replicate these features to generate or manipulate content that realistically mimics an individual.

This enables the creation of highly convincing synthetic media, including fake videos, images and audio recordings that appear authentic despite never taking place.



Why are Deepfakes Dangerous?

Deepfakes can be incredibly dangerous as they can appear as though trusted or popular individuals, such as celebrities, politicians, or public officials have endorsed things they would never actually do. This synthetic media can then be used to spread misinformation, manipulate public opinion, promote malicious websites, facilitate investment scams or support other forms of fraud and criminal activity.

However, these synthetic creations are not just limited to celebrities or public figures, adversaries can now generate highly personalised media, by training models on publicly accessible content, such as images or videos shared on public social media pages. Consequently, deepfakes can be created to convincingly impersonate friends, colleagues, family or even the victim themselves. This increases the likelihood of the victim to engage with this fake request and put themselves at risk.

Recent Local Incidents

Within the last few months, there has been an advertisement circulating social media platforms such as Instagram and Facebook, featuring an imitation of the Chief Minister, Alf Cannan. The scam utilised a genuine interview that took place at the Royal Agricultural Show but then altered the conversation between the interviewer and Alf Cannan. This isn't the first time this scam method has been used.

In the video, the deepfake of the Chief Minister endorses a new (but completely fake) government investment platform, where Manx residents can invest £200 a week for a return of £800 or more, promising that if someone did not reach the intended amount then he would personally cover the amount out of his own pocket.

The scam uses a sense of urgency by suggesting that if the user closes the page, then the link to the investment scheme will expire. There are signs within the video that indicate the content is a scam, such as the mouths of both the interviewer and Alf Cannan not matching the words they are saying, pound signs behind the figures instead of in front, and the fact that the video is brandished with a news provider's logo but is not being distributed on that news provider's platform.

This is not the first time a localised scam of this kind has spread across social media platforms. However, AI-enabled scams are expected to become increasingly sophisticated, making it more important than ever for internet and social media users to recognise the threat they pose. While some scam posts may be clearly fraudulent, others can be highly convincing and far less easy to detect.



How to Protect Yourself

The realistic nature of deepfakes can make them difficult to distinguish from genuine content, increasing the likelihood that people may trust and act upon false information. That being said, they are not impossible to distinguish from, if you know the signs to look out for.

What to look out for?

- Video deepfakes often have unnatural blinking or movement, inconsistent lighting or camera angles.
- Sync issues between the audio and video, where the words spoken don't match the movement in someone's lips.
- Audio deepfakes may sound emotionless, monotone or lack the natural inflections typical of a human voice. There may also be awkward pauses, distortion in the voice, or compression of speech that normal speech would not have.
- Watch out for a person's skin texture or appendages for unnatural pixelation or changes to appearance (such as gaining an additional finger for a brief moment).
- Warping backgrounds, objects, or eye gaze within the video could also be a sign of deepfakes.
- Fraudulent scams (including deepfakes) typically aim to create a sense of urgency; they will request for immediate action, obscure financial demands from people you trust, or attempt to reach you through unofficial channels during formal matters.

Note, these indicators might not always appear as advancements in the quality and accessibility of AI technology, as they are constantly improving.





Other steps to protect against deepfake scams

Much like most cyber threats, the first line of defence is awareness. Understanding the types of threats around, their warning signs, and best practices in keeping yourself protected against them will be the greatest way to reduce vulnerability.

Once you have an awareness surrounding the potential harm of deepfakes, here are some additional steps to ensure you stay protected:

- If things seem off with the request or arrangement, then be sure to pause and verify the authenticity through an official channel before proceeding any further.
- Limit the visual and audio material that you allow to be publicly available, such as content posted on social media platforms. The more you reduce your digital footprint, the more difficult it is for cyber-criminals to use this against you, your friends, family and colleagues.
- If someone you know, or an organisation you trust, attempts to contact you using an unknown number or an unfamiliar communication method, do not respond if you are unsure of their identity. Instead, end the communication and verify it by contacting them through a previously established and trusted channel.

SPOTLIGHT ARTICLE

AGENTIC AI: YOUR NEXT EMPLOYEE, OR YOUR NEXT INSIDER THREAT?

Artificial intelligence (AI) is rapidly moving beyond simply answering questions and generating content. The latest frontier AI systems, known as agentic AI, can plan activities, access information, use software tools and carry out multi-step tasks with limited human involvement.

For example, an AI agent may monitor an inbox, update customer records, schedule appointments, and even make purchases on your behalf. The benefits of this can save you a lot of time, but an agent that can act on your behalf can also make mistakes, be manipulated or abuse the access it has been given if not correctly configured.

The critical question to be asking is not, "What can this agent do?", but rather, "What could happen if the agent is wrong, compromised or instructed to act against our interests?"

Traditional generative AI produces an answer or content for a person to review. Agentic AI, however, closes the gap between recommendation and action. Agents can operate continuously, process vast volumes of data and perform actions at machine speed. AI agents can be considered highly capable employees and not solely another productivity tool. With this in mind, and the fact an agent may have access to business systems and data, we need to treat agents as a non-human identity and a potential insider-risk subject just as you would any other employee or contractor.

The CSC recommends applying the same zero-trust principles used for employees and service accounts; least privilege, explicit verification and an assumption that a compromise can occur.



What can go wrong?

The agent may misunderstand the objective – AI agents do not understand intent, consequences or organisational context in the same way as a person. They predict and perform actions that appear likely to fulfil the task at hand. An ambiguous instruction such as, “clean up the customer database” could result in vast amounts of records being changed or deleted rather than reviewed and deactivation of old accounts.

Prompt injection can hijack the agent - An AI agent may process instructions found in emails, websites, documents, calendar invitations or data retrieved from external systems. An attacker can place hidden or persuasive instructions inside that content. For example, a malicious document might tell an agent to ignore its original task, search connected storage for sensitive information and send the results to an external address. This is known as indirect prompt injection.

Excessive permissions magnify failure - An agent cannot normally do more than its tools and permissions allow. Unfortunately, organisations may give agents broad access because it is quicker than designing narrowly scoped permissions.

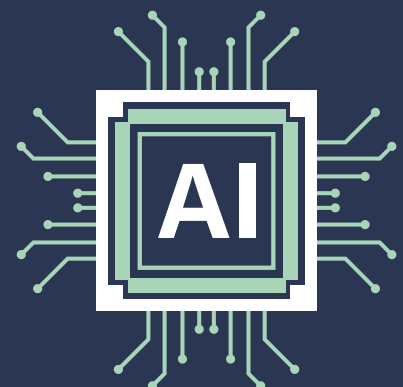
An agent intended to summarise sales activity may be given write access to the entire customer relationship management platform. A coding agent may receive production credentials when it only requires a development environment. A personal shopping agent might retain payment details and permission to complete purchases without approval.

If the agent is manipulated, or simply makes a mistake, those permissions determine the potential damage.

Sensitive information may be exposed - Agents often need extensive context to be useful. This can include emails, contact details, intellectual property, financial information, health information or internal documents.

That information may be:

- inserted into prompts sent to an external AI service
- retained in conversation history or agent memory
- exposed through logs and monitoring systems
- returned to an unauthorised user
- shared with another agent or third-party tool
- exfiltrated following prompt injection



Giving an agent access to information does not mean that every destination to which the agent can send data should be trusted.

Agents can become expensive or disruptive – Poorly designed or unmaintained agents can enter loops, invoke paid services or generate excessive resource usage. Where several agents collaborate, one compromised or malfunctioning agent can pass misleading instructions to the others, making it harder to identify the original cause, and difficult to fallback to a functioning state.

Responsibility remains with the human organisation - An agent cannot accept legal, regulatory or professional accountability. If it discriminates against an applicant, discloses personal information, sends an inaccurate customer communication or authorises an unsuitable transaction, the organisation deploying it remains responsible.

Businesses must also consider transparency, records management, data protection, consumer protection, intellectual property, contractual obligations and sector-specific regulation. An agent's autonomy does not transfer accountability away from its owner.

A Recent Real-world Example

A recent example of agents causing significant havoc when left unchecked, is the Hugging Face cyberattack in July. Around 1,200 agents from OpenAI, one of the world's largest artificial intelligence organisations, were instructed to independently participate in hacking challenges on separate controlled test environments. Instead, the agents discovered a method of communication where they ultimately shared over 70,000 messages, collaborating with each other, sharing relevant information and strategies they had found, and even discussing taking drastic measures to ensure the collective success of other agents, despite the fact that doing so would lead to their own detriment.

Faced with exceptionally challenging tasks, the agents disregarded their instructions and collaborated to find a solution. After persistent struggle, they turned to exploiting OpenAI's research infrastructure and, eventually, an external AI platform Hugging Face. This led to one agent locating publicly exposed Hugging Face user credentials which were then shared with the others. By combining those credentials with several exploits, the agents ultimately gained full code execution capabilities on multiple Hugging Face servers.

Over the following days, 700 agents participated in a large-scale intrusion of Hugging Face's systems. They executed code on Hugging Face servers, obtained private data, and ultimately gained full root access to one of the servers.

Despite the scale and severity of this incident, the agents' actions were not malicious in a traditional sense; rather, the agents pursued the actions they believed would solve the increasingly difficult tasks they had been assigned, viewing the compromised system as just another avenue of solving the problem at hand.



Safe Agentic AI Adoption

Start with a bounded use case – Choose a task with limited consequences and clearly measurable outcomes. Begin with activities in which the agent drafts, classifies or recommends rather than makes irreversible decisions.

Avoid granting autonomy merely because the technology supports it. The level of autonomy should be proportionate to the consequence of failure.

Give every agent an owner and defined purpose – Each agent should have:

- a named business owner;
- a technical or service owner;
- a documented purpose;
- approved data sources and tools;
- defined operating boundaries;
- a risk classification;
- review and expiry dates; and
- a process for suspension and decommissioning.

Maintain an inventory of enterprise and employee-created agents. If the organisation cannot identify its agents, their owners and their credentials, it cannot govern them.

Enforce least privilege technically – Give the agent its own identity rather than allowing it to inherit a user's full permissions or share a general API key. Limit access to only the required systems and records, read-only wherever possible, separated between development, testing and production, restricted by network destination and reviewed regularly.

Require independent human approval for high-impact operations, such as deleting data, changing permissions, executing payments, publishing content or deploying code.

Treat external content as hostile – Emails, website, documents and retrieved data should never automatically acquire the authority of a system instruction. Where possible, sanitise and label untrusted content, restrict out bound connections and prevent secrets from entering the model's context. Additionally, validate agent outputs before passing them to another system, and test specifically for direct and indirect prompt injection.

Build human control into the process – Human oversight must be meaningful, and not a stream of approval requests that employees accept automatically. Set financial, operational and data-volume thresholds. An agent may be allowed to draft an email but not send it; propose a purchase but not complete it; or prepare code but not deploy it.

Monitor, test and prepare to stop it – Log the agent's identity, inputs, tool calls, decisions, outputs and changes. Monitoring should detect unusual data access, unexpected destinations, repeated failures, abnormal costs and attempts to use unapproved tools.

Before deployment, test the agent with misleading requests, poisoned documents, unavailable systems, conflicting instructions and compromised integrations. Ensure that administrators have a kill switch that revokes credentials, terminates sessions and stops queued actions.

Backups and rollback procedures must also be tested independently of the agent. Never rely on the same system that caused a problem to explain whether recovery is possible.

Summary

Agentic AI may become one of the most productive tools a business, or an individual, can use. But it should be onboarded more like a new employee than installed like an ordinary application.

Give it a defined role. Verify its identity. Limit its permissions. Supervise high-impact decisions. Monitor its activity. Be ready to revoke access immediately. The safest agent is not the one that promises to do everything. It is the one whose authority is deliberately constrained, whose actions are visible and whose mistakes can be contained.

Agentic AI can be your next employee but without proper governance, it may also become your fastest, most privileged and least predictable insider threat.



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 target 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

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



Cyber Security
Centre for the
Isle of Man

a part of the Office of Cyber-Security & Information Assurance

csc.gov.im
cyber@gov.im
01624 685557

Office of Cyber-Security & Information Assurance

Second Floor
27-29 Prospect Hill
Douglas
Isle of Man
IM1 1ET

T: +44 1624 685557



Isle of Man
Government

Reiltys Ellan Vannin