Cyber Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

November - December 2025

INTRODUCTION

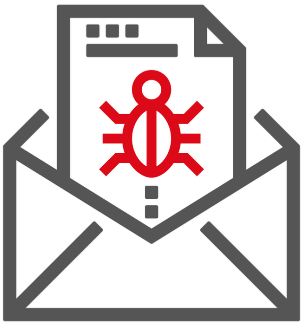
For the period 1st November-31st December

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 or submit it via our online cyber concerns form.

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 34,500 suspicious emails. In November and December 2025, we received 1,381 suspicious emails.

SUSPICIOUS EMAILS

1,381 REPORTED

in November and December

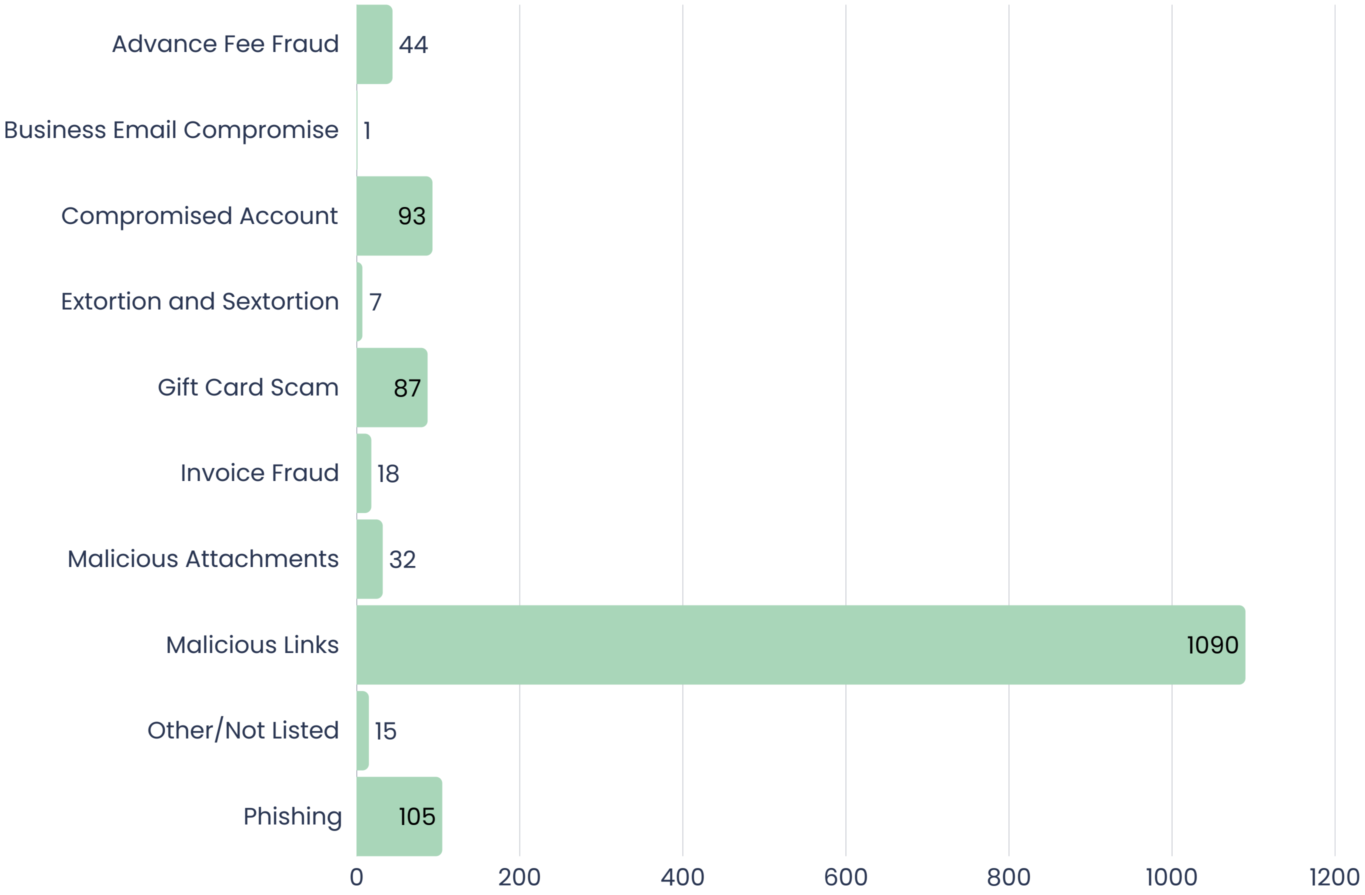
Detail

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 number of compromised email accounts.

Top 5 Phishing Scams Imitating Popular Services:

1. Manx.net
2. Romance/Adult-website adverts
3. Competitions and Rewards
4. Anti-malware Software
5. PayPal



CYBER CONCERNS

78 REPORTED

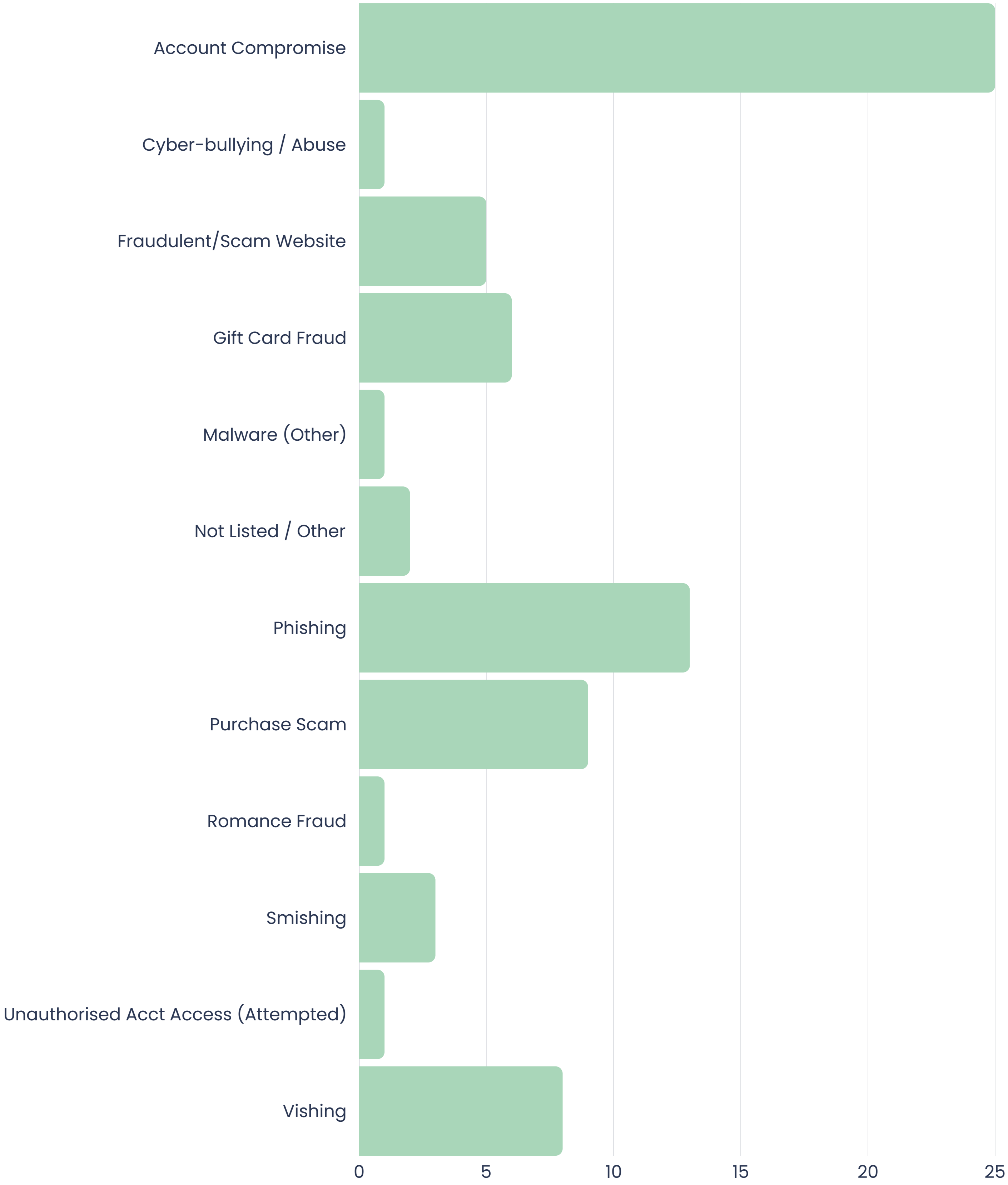
in November and December

Detail

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

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: November and December



ISLE OF MAN THREAT COMMENTARY

BUSINESS AND ORGANISATIONS

ATTACK CHAINS AND EFFECTIVE RECOVERY: WHEN CHANGING YOUR PASSWORDS DOESN'T RESOLVE THE ISSUE

As was reported in our previous threat update, a number of Isle of Man companies became the victim of email account compromise, and unfortunately, these chains of compromise continued throughout November and December. Due to the approach taken by the attackers, simply changing the password in many cases did not secure the compromised accounts.

Let's look into why locking out an attacker doesn't mean they no longer have access or control over your mailbox.

Recent Local Incidents

There was a notable theme in the types of companies being targeted in the previously reported chain of email account compromises, however, it soon became clear towards the latter part of the year, that the sprawl of compromises was not limited to certain sectors. From construction and architecture firms to healthcare and recreational venues, the relationships one organisation has can result in a multitude of other businesses being targeted, and this is exactly what we saw happening.

Following on from an account compromise, businesses took action to secure their accounts, however, it was identified that the attackers were setting auto-forwarding and delivery rules, and applying their own recovery details to maintain persistence into email systems.

These businesses had changed the locks, but failed to close the windows left open by the attackers, allowing accounts to still be abused in attacks.

How Attackers Stay In Control

When an attacker compromises an account, they are well aware that they may not have access for long, so they employ persistence mechanisms. Even if they no longer have direct access to the mailbox, this doesn't stop them from exfiltrating data and continuing to cause damage.

- **Auto-forwarding** - Setting this up means emails are automatically sent to the attacker. Who needs access to your mailbox when the mail is delivered to their mailbox instead?
- **Mailbox Rules** - Attackers can set up rules whilst they have access, this can include deleting email threads and sent emails meaning you will be none-the-wiser about any conversations being had between the attacker and their victims. It also means anybody emailing you to warn you of a compromise might be deleted before you even get a chance to see it.
- **Recovery Details** - Most email systems provide the user with the option to set up a recovery email or phone number. The intention is that if you ever get locked out (such as forgetting your password), you can regain access via this method, however, attackers can also abuse this mechanism to maintain persistence into your mailbox.

Key Considerations

Changing your password following an account compromise is only one step. Here are some key considerations to further secure your accounts, and protect stakeholders and customers:

- Check for, and remove, unfamiliar auto-forwarding and delivery rules
- Remove any unknown recovery details
- Actively monitor for unusual activity on accounts, including attempted access
- Remain aware and ensure your staff are trained to recognise and respond to cyber-related concerns
- Inform your customers and stakeholders when a compromise occurs to reduce the impact and potential of further chained compromises

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

PERSONAL

ONLINE MARKETPLACE SCAMS AND TAKING ADVANTAGE OF LOCAL EVENTS

November and December are typically times where people spend more money on gifts, and with so many places to buy online, the opportunity to be scammed drastically increases. Social media marketplaces are not as regulated as more reputable online stores and this has opened the doors for scammers to make a quick buck by taking deposits for items that don't exist or selling products that do not meet expected standards.

In response to this, the CSC published 'The 24 Days of Cyber Safety'; a collection of valuable tips to shop smart, secure your accounts and finances. But, this article isn't just for Christmas, you can find it on our website along with other useful advice and guidance on a wide range of cyber security topics.

In the last two months of 2025, we also saw localised phishing attacks increase as a result of a telecommunication service provider's plans of transitioning email services to another provider in early 2026. The cyber criminals identified this as a good time to target unsuspecting Island residents under the guise of the providers. These phishing emails prompted users to enter credentials which resulted in a number of compromises.

Once compromised, the attackers were then able to send further phishing emails to the contacts of compromised accounts. These phishing attacks usually involved gift card fraud, whereby the attacker would pose as the sender and request the recipient to purchase gift cards and provide the codes.

Why Gift Cards?

Gift cards, once redeemed, are effectively unable to be refunded and in most cases will not be voided in time before the cybercriminals are able to make use of them. Making financial transactions to fraudulent bank accounts is still common, but gift cards are difficult to trace and this kind of fraud is popular.

Cybercriminal enterprises have sophisticated infrastructure, enabling them to resell these ill-gotten gift cards with relative ease. In many cases, they sell these gift cards to unsuspecting people thinking they are getting a good deal when, in reality, they are yet another victim in the cybercriminals' scheme.

If you are ever contacted by someone asking you to make a purchase on their behalf, make sure it is a legitimate request.

Recent example:

A recent incident involved an individual who received an email that appeared to come from a trusted friend, requesting that several gift cards be purchased on their behalf because they were ill and couldn't get out of the house. Believing the request to be genuine, the person bought the cards and shared the activation codes, only to later discover that their friend's email account had been compromised by a scammer.

Unfortunately, this type of gift-card fraud continues to be reported to us frequently, and throughout the latter part of 2025 alone, several hundred pounds have been lost to these scams.

How to protect yourself:

- **Be sceptical of urgent requests** – If someone emails asking for gift cards, especially with urgency or secrecy, treat it as a red flag. Legitimate organisations and colleagues will never ask for gift cards as a form of payment.
- **Verify the sender by another method** – Always confirm unusual requests by contacting the person directly using a known phone number or messaging channel. Don't reply to the suspicious email.
- **Don't click links or follow instructions blindly** – Scammers often create a sense of pressure. Take a step back and validate the request before acting.
- **Never share gift-card numbers or codes** – As soon as a scammer has the code, the money is gone. Treat gift-card details like cash: once sent, they can't be recovered.
- **Enable multi-factor authentication (MFA)** – MFA helps protect your own accounts from being taken over and used to target others.
- **Report suspicious messages immediately** – You can report these emails to our Suspicious Email Reporting Service (SERS). Early reporting helps protect others.

THREAT REPORT: SPOTLIGHT

STOP THE SPOOF: DEFENDING YOUR ORGANISATION FROM DIGITAL COPYCATS

Business impersonation has become one of the fastest-growing cyber threats facing organisations of all sizes. Criminals now routinely clone legitimate websites, mimic branding, and create convincing domains to trick customers, partners, and employees.

These fraudulent websites often serve as vehicles for credential harvesting, malware distribution, or financial fraud, allowing attackers to undermine trust and cause significant reputational and financial damage.

How Business Impersonation Works

Attackers typically begin by registering a domain that closely resembles a legitimate business address, using common misspellings, swapped characters, or different top-level domains (e.g. '.com' to '.cm'). These 'lookalike' domains are then used to host fraudulent websites that mimic the organisation's visual identity. The sites may replicate login portals, payment pages or product offerings, appearing legitimate enough that even vigilant users can be deceived.

In many cases, spoofed websites are paired with phishing campaigns, SMS messages ('smishing'), or social media advertisements that drive unsuspecting victims to the fraudulent pages. More sophisticated campaigns may integrate certificate spoofing, malicious QR codes, or search-engine poisoning to appear in legitimate search results.

The Business Impact

Beyond direct financial fraud, impersonation attacks erode customer trust and can create long-term reputational damage. Businesses may face increased support costs, disrupted operations, and regulatory exposure if personal data is compromised. For public-facing organisations, even a single convincing spoof can undermine years of brand building and risk regulatory scrutiny around digital identity management practices.

Isle of Man businesses are just as at risk as any other organisation. The CSC has received multiple reports from targeted organisations and concerned customers throughout 2025. It is essential for local business owners to monitor and defend their brand and reputation before the damage is done. Organisations need to be prepared to respond and recover when they are targeted by impersonators.

Detecting and Monitoring Spoof Websites

Here are a few things businesses can consider to pro-actively monitor and defend against impersonation scams:

1. Domain Monitoring

- Track newly registered domains that resemble your brand, product names, or executive identities.
- Use automated domain-monitoring services or threat intelligence platforms to alert you to suspicious registrations.

2. Brand Protection and Attack Surface Management

- Consider leveraging digital risk protection (DRP) or attack surface management tools that continuously scan for cloned websites, malicious ads, social-media impersonation, and unauthorised use of logos.
- Many solutions can automatically request takedowns of fraudulent sites.

3. TLS Certificate Monitoring

- Monitor certificate transparency logs to identify when certificates are issued for lookalike domains.

4. Dark Web and Social Media Monitoring

- Identify early signs of coordinated impersonation, credential leak activity, or planned spoofing operations.

Protecting Your Organisation

Harden your digital identity

- Register common domain variants to reduce the attack surface.
- Monitor and remember to renew your legitimate domains. If your domain registration lapses, you are at risk of cybercriminals 'domain squatting' and using it for illegitimate purposes, including blackmail to give possession of the domain back .
- Maintain consistent digital branding so anomalies are more noticeable to customers.
- Use DMARC, SPF, and DKIM to authenticate outbound email and reduce opportunities for spoofing.

Empower your customers and staff

- Provide clear advice on identifying legitimate contact channels.
- Run awareness campaigns that highlight recent impersonation risks.
- Encourage reporting of suspicious activity.

Have a rapid response plan

- Establish a process for verifying and taking down spoof sites (via hosting provider, registrar abuse reporting processes).
- Prepare communications templates to inform customers and stakeholders promptly.

Business impersonation and spoof websites pose a significant cyber threat, but organisations can reduce risk greatly through proactive monitoring, strong digital identity controls, and clear communication.

With the right tools and strategy in place, businesses can protect both their brand and their customers from the growing threat of online fraud.

You can find more information on the topic of website imitation on the CSC website, here: https://csc.gov.im/advice-guidance/website-imitation-and-copycats/

More information about brand impersonation, spoofing and email security can be found on the UK NCSC website:

- **https://www.ncsc.gov.uk/section/respond-recover/ml-brand-impersonation**
- **https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing**

INTERNATIONAL THREATS

CLOP RANSOMWARE: UNIVERSITY OF PHOENIX DATA BREACH IMPACTS NEARLY 3.5 MILLION INDIVIDUALS

The University of Phoenix has disclosed a massive data breach affecting 3,489,274 individuals, after attackers linked to the Clop (Cl0p) ransomware group infiltrated its systems during the summer of 2025. The incident centres on the exploitation of a zero-day vulnerability in Oracle's E-Business Suite (EBS), a platform widely used for financial operations and sensitive enterprise data management.

Investigations revealed that attackers gained unauthorised access over the course of a few days in August 2025, leveraging a critical flaw. The compromise went undetected until November, when the University appeared on Clop's dark-web data leak site. The University publicly acknowledged the breach in early December.

The stolen dataset includes highly sensitive personal and financial information, such as full names and contact details, dates of birth, social security numbers and bank account data.

At the time of the breach, there was no patch available for the vulnerability, however, several defensive measures could have been implemented to avoid such a situation from happening, such as pro-active monitoring and well-configured intrusion prevention systems and rules.

As a result of the breach, the University is offering those affected free identity protection services, fraud reimbursement, credit monitoring, identity theft recovery and dark web monitoring.

LONDON COUNCILS REPORT DISRUPTION AMID CYBERATTACK

Several London councils have activated emergency plans following a significant cyberattack that disrupted critical public services, forced IT shutdowns, and raised concerns over potential data exposure.

The incident, confirmed in late November 2025, has impacted at least three major boroughs; the Royal Borough of Kensington and Chelsea (RBKC), Westminster City Council (WCC), and Hammersmith & Fulham Council (LBHF), all of which share IT infrastructure and services.

According to official statements, the cyberattack led to the shutdown of key systems, including phone lines, online services, and back-office systems, leaving residents unable to contact their local authorities through normal channels. Councils were forced to activate business continuity and emergency response measures to maintain essential services such as social care, emergency support, and waste collection.

Although the full scope of the incident remains under investigation, early statements from Kensington and Chelsea indicate that some data may have been accessed and copied. Initial assessments suggest this could involve historic records, but investigators have not yet ruled out risks to personal or financial information.

The disruption has affected over 360,000 residents across the impacted boroughs, limiting access to online reporting tools, payment portals, customer service channels, and key administrative functions.

The incident has renewed calls for improved investment in cyber resilience, segregation of shared services, and enhanced incident response readiness across local authorities.

UNAUTHORISED ACCESS OF SOUTH KOREAN ECOMMERCE GIANT LEADS TO 33.7 MILLION CUSTOMER DATA BREACH

South Korea's largest e-commerce platform, Coupang, has confirmed a massive data breach affecting 33.7 million customer accounts, marking one of the most significant privacy incidents in the nation's history. The breach is understood to have persisted undetected for nearly five months.

Investigations by Coupang and South Korean authorities have revealed that the intrusion originated through overseas servers and was allegedly made possible by a former Coupang employee, who retained access keys even after leaving the company. This allowed prolonged access to authentication services and customer data.

Coupang maintains that payment information, credit card numbers, and login credentials were not compromised. This is due to strict laws requiring certain sensitive data to be encrypted. However, names, email addresses, phone numbers and delivery addresses were compromised opening up the potential for customers to be targeted by other attacks in future.

Given the scale of the breach, Coupang may face large regulatory penalties under South Korean privacy laws. Regulators have also ordered the company to remove newly added terms that attempted to disclaim liability for unauthorised third-party access.

Experts emphasise that while some types of data are not legally required to be encrypted in South Korea, the aggregation of non-sensitive personal information can create powerful attack vectors for criminal exploitation.

ROMANIAN WATER AGENCY CYBER INCIDENT: RANSOMWARE COMPROMISES OVER 1,000 SYSTEMS

Romania's National Water Management Authority (ANAR) suffered a large-scale ransomware attack in Mid-December, compromising approximately 1,000 IT systems across the country. The attack hit 10 of the agency's regional water basin administrations, disrupting critical digital systems but leaving operational water infrastructure intact.

Investigators found that attackers misused Microsoft's BitLocker encryption feature (a legitimate Windows tool) to lock files on compromised systems. A ransom note left on infected machines demanded that the agency make contact within seven days, consistent with typical ransomware negotiation tactics.

Despite the extensive IT disruption, ANAR confirmed that operational technology (OT) systems responsible for controlling hydrotechnical structures remained fully functional. Staff reverted to using manual coordination using telephones and radio communications. This ensured uninterrupted oversight of water management and flood forecasting.

This separation between IT and OT prevented potential risks to public safety and maintained continuity across essential operations.

While ANAR avoided operational disruption this time, European cases, including previous destructive incidents in Denmark and Norway, demonstrate the potential physical and societal impact of cyberattacks on water systems.

CYBER GLOSSARY

2-step verification (2SV): Sometimes called 2FA or MFA is a second way to confirm your identity to help keep your personal and financial information from being compromised or stolen.

Account Compromise: A security condition in which an adversary has obtained or controls valid authentication material for an account (such as passwords, MFA methods, session tokens, or OAuth grants), giving them the ability to authenticate as the legitimate user whether or not they have attempted or succeeded in accessing the account.

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

Anti-virus software: Designed to identify and remove computer viruses, other malware and spyware on a device or IT system. To be effective, it should be kept up-to-date with the latest anti-virus signatures and definitions.

Backdoor: A backdoor is a method of avoiding normal authentication on a device. They are often used for securing remote access to a computer, or obtaining access to plaintext in cryptographic systems

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

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

Common Vulnerabilities and Exposures (CVE): the 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.

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

Cryptocurrency: A cryptocurrency is a digital asset that is designed to act as an exchange medium. They use cryptography to verify and secure transactions, control the creation of new assets and protect the identity of asset holders.

Dark web: A collection of thousands of websites which are not indexed by conventional search engines. They often use anonymity tools, like the Tor network, to hide their IP address and preserve the anonymity of the creators and visitors.

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

Encryption: A method to scramble a message, file or other data and turn it into a secret code using an algorithm (complex mathematical formula). The code can only be read using a key or other piece of information (such as a password) which can decrypt the code.

Firewall: A security system that monitors and controls traffic between an internal network (trusted to be secure) and an external network (not trusted). It is generally considered insufficient against modern cyber threats.

General Data Protection Regulation (GDPR): The General Data Protection Regulation (GDPR) 2016/679 is a European Union regulation covering data protection and individual privacy rights. It was introduced in April 2018 and enforced on May 25 2018.

Hacker: A hacker is a computer and networking attacker who systematically attempts to penetrate a computer system or network using tools and attack methods to find and exploit security vulnerabilities.

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

IP address: An IP address (Internet Protocol Address) is a label assigned to computer devices. An IP address is essential for Internet Protocol communication.

Keylogging: Keylogging, also known as keystroke logging or keyboard capture, is the action of recording, often secretly, the keys struck on a keyboard.

Malware: Malware is malicious or hostile software used to disrupt, damage or compromise a computer system or network.

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

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

Patch management: Patch management covers acquiring, testing and installing multiple patches (manufacturer released code changes) to a computer system or application. Firmware and software vendors release patches to fix defects, change functionality and to address known security vulnerabilities.

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

Ransomware: A type of malware that prevents access to the target's computer system or data until a ransom is paid to the attacker.

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

Smishing: A type of phishing attack that uses text messages (or other types instead of mobile messaging such as MMS or IM services) instead of email messages.

Social engineering: An attack method that tricks people into breaking normal security procedures by masquerading as a reputable entity or person in email, IM or other communication channels.

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

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

Unauthorised Account Access: Any access attempt or authenticated session into an account (such as email, social media, or business platforms) by an unauthorised party; categorised as Unauthorised Account Access (Attempted) when no authenticated session is established (e.g., blocked by policy or failed MFA) and Unauthorised Account Access (Successful) when an unauthorised authenticated session is established (with or without subsequent actions).

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

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

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

ABOUT US

The Cyber Security Centre for the Isle of Man (CSC) is dedicated to enhancing the cyber resilience of organisations and individuals across the island. As a public-facing entity, the CSC provides comprehensive advice, guidance, and practical support to both residents and businesses.

The CSC is committed to bolstering cyber defences by offering tailored solutions, resources, and educational programmes. Its primary focus is on empowering Island-based entities and individuals with the necessary knowledge and tools to effectively safeguard against cyber threats.

Through proactive initiatives, including targeted advisory notices, vulnerability scanning, and awareness campaigns, the CSC aims to elevate the overall cyber awareness and preparedness of the Isle of Man community. By fostering a culture of vigilance and best practices, the CSC aims to fortify the cyber resilience of organisations and individuals, ensuring a safer digital environment for all.

Disclaimer

The material in this document is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances. OCSIA accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Open Government Licence

CSC 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