Cyber Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

# ISLE OF MAN CYBER THREAT UPDATE

September - October 2026

# INTRODUCTION

For the period 1st September 2026 - 30th October 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** |
| **Business Article: Who's Guarding the Gateway?** | **5** |
| **Personal Advice: The Job That Costs You** | **11** |
| **Spotlight Article: Botnets** | **16** |
| **Cyber-Glossary** | **24** |
| **About Us** | **28** |

# 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 30,000 suspicious emails. In **September** and **October 2026**, we received **331 suspicious emails**.

# SUSPICIOUS EMAILS

## 331 REPORTED

in September and October

## Detail

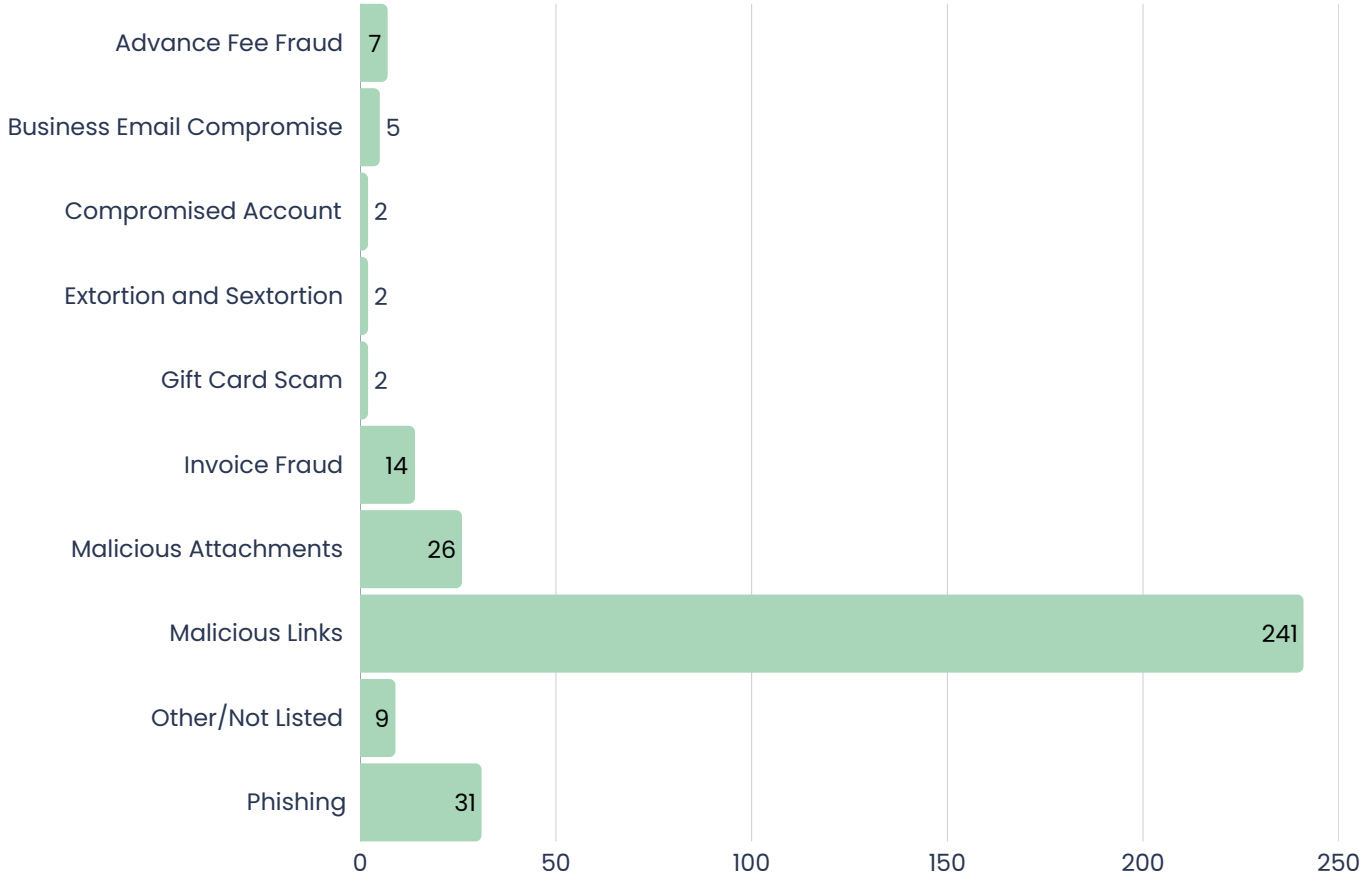
The graph below shows the frequency of specific characteristics identified in submitted SERS emails. Please note that some emails have more than one recorded characteristic.

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. TV Licensing
2. Manx.net
3. Anti-malware Software
4. Apple
5. Retail Stores (CO-OP, Walmart)



# CYBER CONCERNS

## 415 REPORTED

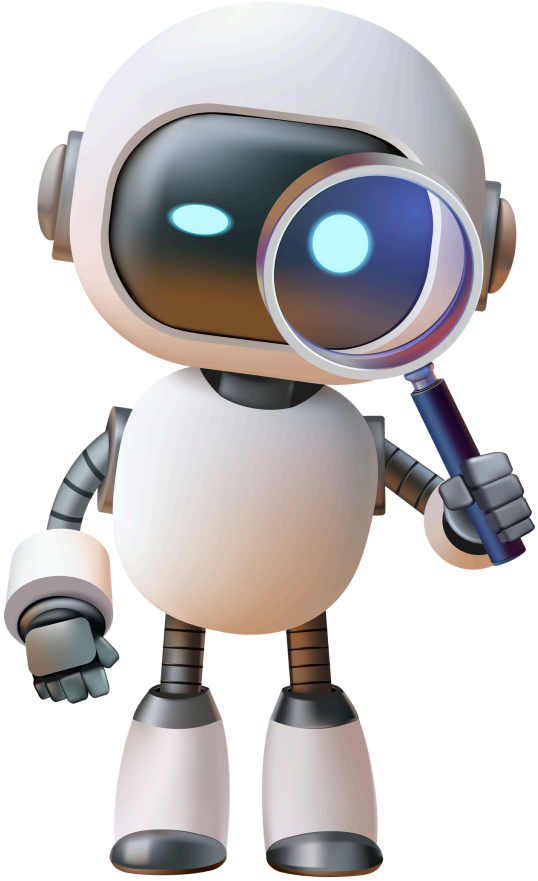
in September and October

# Detail

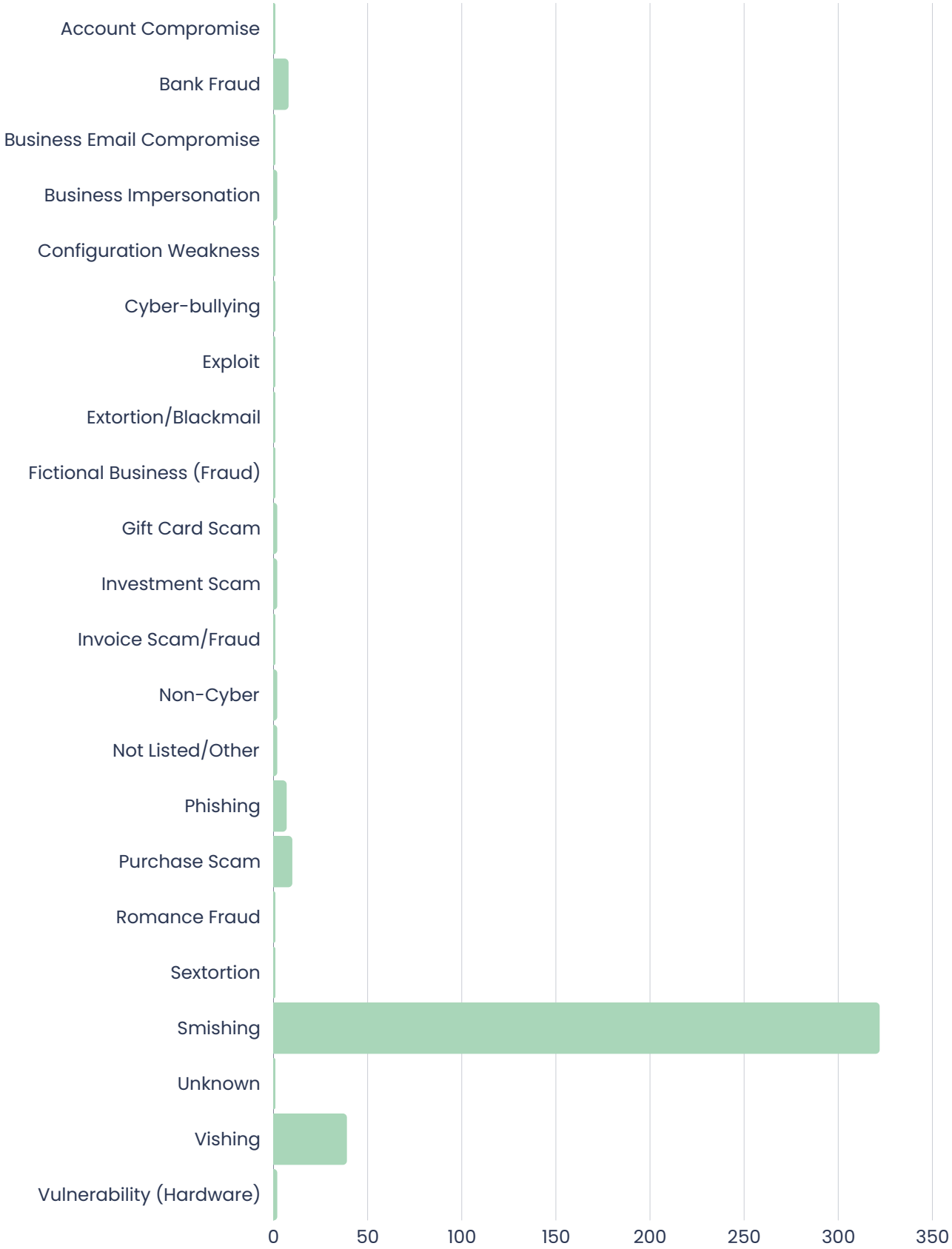
The chart (on page 4) shows a breakdown of cyber concerns reported to us over **September** and **October 2026**.

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 September and October 2026



# BUSINESS ARTICLE

## WHO'S GUARDING THE GATEWAY? WHEN YOUR CYBER DEFENCES BECOME THE THREATS

For years, organisations have been told to protect their computers. Keep software updated. Install security tools. Use strong passwords and multi-factor authentication. Replace unsupported systems. Train staff to recognise phishing emails.

Today, a business laptop is likely to be significantly better protected than its equivalent from a decade ago. It may receive automatic operating system and application updates, use encryption, and be centrally managed and protected by endpoint detection and response software. Its security status may also be continually monitored.

But what about the equipment sitting between that laptop and the outside world?

The firewall protecting the office. The virtual private network (VPN) gateway providing remote access. The router connecting the organisation to the internet. The security appliance inspecting traffic. Or perhaps the forgotten internet-facing device installed years ago for a project that nobody quite remembers.

These devices are supposed to protect the network. Increasingly, however, they are also exactly where attackers are looking.

Edge devices are prime targets because they sit at the boundary between an organisation and potentially hostile external networks. Attackers exploit vulnerabilities, weak default settings and configuration errors in these devices to obtain an initial foothold, move further into networks and maintain access.

## The devices we rely on, but rarely think about

Edge devices are systems positioned at the boundary of your organisation's technology environment. They often control or enable connections between your internal systems and the wider internet.

They can include:

- firewalls
- routers
- VPN and remote-access gateways
- secure web gateways
- email security appliances
- load balancers
- internet-facing management systems
- network-attached storage
- internet-connected operational technology
- other security and networking appliances



Many organisations depend on these devices every minute of every working day. Yet there is an important difference between an employee's laptop and a firewall. If a laptop stops working, somebody complains. If it runs slowly, the IT helpdesk gets a ticket. If it needs replacing, the employee knows it exists and where it is.

A firewall can be different. It might have been purchased several years ago, installed and largely forgotten because it has continued doing its job. Ironically, that reliability can become part of the problem. When technology quietly works for years, it becomes surprisingly easy to stop asking whether it is still safe.



## Attackers have noticed the imbalance

Why wrestle with the security protecting an employee's laptop if there is an outdated VPN appliance directly accessible from the internet?

An attacker does not care whether something was purchased as a security product. To them, it is simply another device running software that may contain vulnerabilities. Edge devices can be particularly attractive because of where they sit and what they are trusted to do.

A compromised laptop might provide access to one user's account or device. A compromised gateway could put an attacker at the entrance to the wider network. It is the cyber equivalent of compromising the security desk controlling access to an entire building, rather than breaking into individual offices.

## When the guard becomes the intruder

Imagine a business with excellent endpoint security. Every laptop is automatically patched. Multi-factor authentication is enabled. Staff receive cyber awareness training. Endpoint monitoring can identify unusual behaviour. The organisation feels reasonably well protected. But its VPN appliance was installed several years ago, and responsibility for maintaining it is unclear. The employee who configured it has left. It isn't included in the normal laptop or server patching process. Nobody has recorded the manufacturer's end-of-support date for it. Then a serious vulnerability is discovered.

The manufacturer releases an update. Security organisations publish warnings. Attackers begin scanning the internet for vulnerable devices. But nobody in the business realises its appliance needs attention. From the organisation's perspective, nothing appears wrong.

The firewall is running and the VPN still connects. The lights are still blinking. From an attacker's perspective, however, a new door may have opened.

## Why do edge devices get forgotten?

Organisations cannot protect assets they do not know about.

Businesses grow, offices move, suppliers change, companies merge and temporary projects become permanent. Over time, the original reason for installing a device can disappear while the device itself remains. A reliable inventory is therefore far more important than it sounds.

For any business, the underlying principle is simple: know what is connected to your organisation and who is responsible for it.

## "We can't update it because it might break something"

Edge infrastructure is often essential infrastructure. Taking a laptop offline for twenty minutes is usually manageable. Taking the organisation's firewall or remote-access service offline, however, can affect everyone.

Before long, a temporary postponement can become a permanent risk. This is particularly dangerous because criminals do not wait patiently while organisations arrange maintenance windows.



## The end-of-support trap

Eventually, every technology product reaches the point where its manufacturer stops supporting it. That can mean losing access to new features, but for an internet-facing security device, the consequences can be far more serious. Once support ends, newly discovered security vulnerabilities may no longer receive fixes. Attackers are all too aware of this.

Visibility matters as much as prevention
What happens if an attacker does compromise one of these devices? With laptops and servers, organisations increasingly collect detailed security information that can help identify suspicious activity. Some network appliances, particularly older products, provide much less visibility. This matters because, after an incident, investigators need to establish what happened, when it happened and what the attacker did next.

Without suitable logs, an organisation may know an incident has occurred but be unable to establish exactly what the attacker accessed. That can make an already difficult incident much harder to contain and investigate.



## Questions to ask

**1) What do we have?** — Maintain an inventory of all internet-facing devices and security appliances, including each device's manufacturer, model, software or firmware version, location and purpose. Unknown infrastructure is unmanaged infrastructure.

**2) Who owns it?** — Every device should have a named internal owner and, where relevant, a named supplier responsible for maintaining it. Avoid leaving responsibility vaguely with "IT".

**3) Is it still supported?** — Record end-of-support dates. Plan and budget for replacement before support expires, rather than waiting until afterwards.

**4) Is it up to date?** — Establish how vulnerability alerts and manufacturer security notices are monitored. Treat critical vulnerabilities affecting internet-facing devices with urgency, rather than simply placing them in the next routine maintenance cycle.

**5) Is it configured securely?** — Remove unnecessary services and management interfaces. Restrict administrative access. Change default credentials and configurations. Use strong authentication, including multi-factor authentication where supported. Expose only what genuinely needs to be exposed.

**6) Would we notice if somebody compromised it?** — Ensure important security events are logged and, wherever possible, send those logs somewhere separate from the appliance itself. Otherwise, an attacker controlling the device may also control the evidence needed to detect their activity.

**7) When did we last check?** — Include edge equipment in vulnerability management, asset reviews, penetration testing arrangements, supplier assurance, business continuity and disaster recovery planning.

# PERSONAL ADVICE

## THE JOB THAT COSTS YOU: SPOTTING FAKE JOB OPPORTUNITIES

Searching for a new job can be exciting but stressful. Whether you are looking for your first role, changing careers or returning to work after a break, almost all job searches now begin online. Scammers exploit this by creating convincing fake job advertisements, posing as genuine employers and targeting people looking for work.

These scams often target people under pressure to find work, who may act quickly without fully considering the risks or checking that an opportunity is genuine. A fraudulent recruiter may offer an attractive salary, promise flexible remote working or rush the hiring process to discourage applicants from carrying out the usual checks. Some ask applicants to pay for training, equipment or administrative fees; others seek sensitive information such as passport details, banking information or copies of identification documents.

Victims may suffer financial loss, identity theft or malware infections after opening malicious files sent by a fraudulent employer. These incidents can also add anxiety and stress to an already challenging time.

Staying alert to scams, recognising warning signs in job postings and verifying potential employers can help reduce your risk and protect you during your job search.



## What are fake job scams?

Fake job advertisements can appear in emails, text messages, social media and online job boards. Cybercriminals pose as legitimate employers, recruiters or agencies to steal money or personal information, or gain access to your device. Even large, trusted job-search platforms such as LinkedIn, Indeed and Glassdoor can carry fraudulent listings.

## How do fake job scams work?

A typical scam might begin when someone applies for a role and receives an unusually quick response offering them the job without an interview. The only condition is that they must pay the company for training or administrative fees. Once the money is sent, the recruiter disappears.

Other scams involve requests for copies of identification documents. Applicants may be asked to upload a passport, proof of address or driving licence, which the cybercriminal then uses to commit fraud.

Applicants may also receive a file that appears to be a legitimate training document, application form or interview preparation guide. Instead, it could contain malicious software designed to infect and compromise their device.



## Recent Local Incidents

A fake employment opportunity claiming an association with the social media platform TikTok has recently been reported on the Island. The scammers claim to work for TikTok's Business Partnership department and promise £180 to £200 a day, along with sign-up bonuses, referral incentives, trips abroad and other prizes to entice people to take part.

People are initially contacted through WhatsApp and asked to complete simple tasks in return for small payments. These payments build trust and make the opportunity appear legitimate.

Once trust has been established, victims are offered further tasks with promises of larger payments and the prospect of permanent employment.

To complete these tasks, victims are encouraged to pay significant sums of their own money, with the promise that the funds will be returned in full, together with a commission, once all tasks are complete. In reality, these promised earnings never arrive, and the scammers keep the victims' money.

This case highlights a common tactic in fake job scams: using small initial payments to create a false sense of legitimacy before persuading victims to commit increasingly large sums of their own money.



## What are the signs to look out for?

Whether you are a recent graduate or a seasoned professional, recognising the warning signs of fake job postings is essential to protecting your time, money and personal information. Key signs that an online job listing may be fraudulent include:

- **Vague descriptions of the role:** No company name, unclear responsibilities or expectations, or no way to find out more about the role.
- **Roles offering an unusually high salary:** Pay significantly above typical rates for very little experience or effort.
- **Unprofessional communication:** Poorly written messages, spelling or grammar mistakes, or communication limited to messaging apps.
- **Hiring on the spot:** A job offer with little or no interview process.
- **Requests for sensitive information early on:** Requests for passport scans, identification documents, banking details or National Insurance numbers before a formal hiring or contract-signing process.
- **Requests for payment:** Legitimate employers do not usually ask applicants to pay for training, equipment or administrative fees.

**If it sounds too good to be true, it probably is.**



## How can you verify a potential opportunity?

Before proceeding with a job opportunity, take time to independently verify that both the role and the organisation are genuine.

First, visit the company's official website and check whether the vacancy is listed. Compare the publicly available contact details with those in the job advertisement. If you are unsure, contact the organisation directly using the details on its official website.

Search for the recruiter or agency online. Look for an official website, company information and independent reviews.

Check email addresses in the listing carefully. Scammers often use addresses that resemble those of a genuine company but contain spelling mistakes or extra characters.

Try a quick online search using terms such as:

"[Company] recruitment scam"
"[Company] job scam"
"[Recruiter Name] scam"
Other victims may already have reported similar experiences or shared them online.

## Keep in mind

Genuine employers look for talented people who are the right fit for their organisation. They should not pressure you into making payments, sharing sensitive information or downloading unfamiliar software. If an opportunity feels pressured, secretive or too good to be true, pause and verify it independently before continuing with your application.

# SPOTLIGHT ARTICLE

## BOTNETS: THE INVISIBLE THREAT HIDING IN YOUR HOME OR BUSINESS NETWORK

When people think of a cyberattack, they often think of desktops, laptops or smartphones. However, cybercriminals also target a much wider range of internet-connected devices, including home routers, security cameras, smart speakers, smart TVs, printers and other Internet of Things (IoT) technology.

As homes and businesses become more reliant on technology, the number of potential targets continues to grow. A single vulnerable device can give attackers a foothold in the wider network, putting personal information, business operations and other devices at risk.

What makes this threat particularly concerning is that compromised devices often continue working normally, giving little indication that anything is wrong.

Cybercriminals can link compromised devices into a network known as a botnet. This allows an attacker to coordinate and control large numbers of devices simultaneously, using them to carry out attacks.



## What is a botnet?

A botnet is a network of devices infected with malware and remotely controlled by cybercriminals.

Each compromised device, or bot, follows commands from a malicious operator known as a botmaster. These commands are typically relayed through a command-and-control (C2) server or a peer-to-peer (P2P) network of bots.

## What are botnets used for?

- Spam Email Campaigns
- Distributed Denial of Service (DDoS) Attacks
- Fake Traffic Generation
- Spyware and Information Theft
- Remote Desktop Protocol (RDP) Attacks
- Cryptocurrency Mining



## How devices become involved in a botnet

Before a device can become part of a botnet, it must first be compromised by an attacker. This process can occur without the owner's knowledge and may take only a few seconds once a vulnerable device is found online.

Many IoT devices are designed with affordability, convenience and ease of use in mind, while security features may be limited or overlooked. Inadequate security controls, insecure configuration or poor maintenance can leave devices vulnerable in several ways.

**Weak or Default Credentials:** Devices with default credentials are vulnerable if users leave those credentials unchanged. Changing them during initial setup helps address this risk. Weak or easily guessed passwords also make devices easier to compromise.

**Unpatched Vulnerabilities:** Infrequent, unavailable or unapplied firmware updates can leave devices exposed to attacks that exploit known vulnerabilities.

**Exposed Interfaces:** Some devices have web-based administration portals or remote management services accessible over the internet. If these services are poorly secured or exposed unnecessarily, attackers may attempt to gain control remotely.

**Malware Infections:** Devices can also become compromised through malicious software. This may occur when malware is installed directly onto the device, delivered through another compromised system on the network, or downloaded through a malicious application.

**Pre-Installed Backdoor:** In some cases, low-cost or poorly regulated IoT devices may leave the factory with botnet malware already installed, allowing attackers to control them once they connect to the internet.

Once compromised, a device typically connects to attacker-controlled infrastructure to receive commands alongside other infected devices in the botnet.

## Common devices targeted

**At Home:**

- Routers
- Smart speakers
- Smart TVs
- Security cameras (including smart doorbells)
- Network Attached Storage (NAS) devices

**In a Business:**

- Servers
- Workstations
- Laptops
- Network appliances
- Security camera systems
- Point-of-sale devices and payment terminals

Any internet-connected device can potentially become part of a botnet if it is compromised



## Signs of exposure

**Unexplained activity:** Unusually high processor, memory or storage activity, or fans running excessively without an obvious cause, may indicate a problem. Other signs include unexpected flashing lights or unscheduled device restarts.

**Slow internet:** Your connection is slower than usual and your router is under heavy load, even when you are not downloading, uploading or installing updates.

**Unknown network connections:** A device is attempting to connect to unfamiliar destinations or transmitting network traffic that does not match expected behaviour.

**Slow reboots and shutdowns:** Malware may cause a device to take longer than usual to restart or shut down.

**Applications crashing:** Software that previously ran smoothly becomes unreliable or starts crashing.

**Alerts or complaints:** Antivirus software may flag suspicious activity, or you may receive alerts about attempted logins. People you know may also report receiving spam or malicious emails from you.

## Risks to businesses

A botnet infection can cause significant financial losses. Businesses may need to invest time and resources in investigating the incident, removing malicious software, restoring affected systems and strengthening security. If left unresolved, the infection may continue to cause service outages and disruption, reducing revenue and productivity.

Customers, business partners and other stakeholders expect organisations to maintain secure, reliable services. If a business device is used to facilitate cybercrime or attack other organisations, trust in the business can quickly suffer.

A compromised device can give an attacker a foothold in the network. From there, they may attempt to move laterally to other systems, steal sensitive information, deploy additional malware or maintain ongoing access. This increases the risk of further incidents, including ransomware attacks and personal data breaches.

## How to stay protected

### Public & businesses

**Avoid buying devices with weak security:** Choose devices with robust security features and enable multi-factor authentication (MFA) where available.

**Use strong, unique passwords:** Change default credentials during initial setup and use a strong, unique password for each device.

**Keep software and firmware updated:** Applying updates promptly helps protect devices against known exploits commonly used by cybercriminals.

**Be cautious of emails and hyperlinks:** Treat unexpected links and attachments with suspicion. Avoid opening suspicious attachments, following untrusted links or installing files from unknown sources to reduce the risk of infection.

**Use reputable security software:** Keep antivirus software up to date and run regular scans on supported devices to identify and remove potential threats.

**Review connected devices:** Regularly check the devices connected to your network. Unknown or unexpected devices may indicate unauthorised access.



## Business-specific guidance

**Maintain a comprehensive asset inventory:** Keep an accurate inventory of all internet-connected devices to ensure they are monitored, managed, and updated correctly.

**Implement strong access controls:** Use strong passwords and MFA for administrative accounts and remote access services. In additional, apply the principle of least privilege so that users are limited to only the permissions required for their role.

**Patch systems properly:** Establish a process for regularly updating operating systems, applications, network appliances, and IoT devices to address newly discovered vulnerabilities.

**Segment networks:** Separate critical business systems from IoT devices, guest networks, and other less trusted environments. This limits the spread of malware through the network if a device becomes compromised.

**Monitor network activity:** Regularly review network traffic for unusual patterns, unexpected outbound connections or other suspicious activity that may indicate a device is participating in a botnet.



## Summary

Botnets are networks of compromised devices controlled by cybercriminals. They can include computers and mobile phones, as well as routers, smart speakers, camera systems, printers and many other connected devices. Because infected devices often continue operating normally, owners may not realise they are being exploited.

Compromised devices can be used to distribute spam, carry out DDoS attacks, steal information and support other forms of cybercrime.

Weak or default passwords, unpatched vulnerabilities and malware infections can all lead to devices becoming part of a botnet. Strong, unique passwords, MFA where available and regular firmware updates help reduce this risk.

Proactive device management and good cyber hygiene are essential for both individuals and organisations to reduce the risk of devices becoming part of a botnet.



# CYBER-GLOSSARY

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

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

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

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

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

**Common Vulnerabilities and Exposures (CVE):** The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures.

**Common Vulnerability Scoring System (CVSS):** The CVSS is an industry standard that provides a numerical score from 0.0 to 10.0 to rate the severity of software vulnerabilities.

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

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

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

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

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

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

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

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

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

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

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

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

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

**Multi-Factor Authentication (MFA):** A method of verifying a person's identity using two or more authentication factors, such as a password and a one-time code. 2-Factor Authentication (2FA) is the most common form of MFA.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# ABOUT US

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

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

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



**Disclaimer**

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

**Open Government Licence**

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