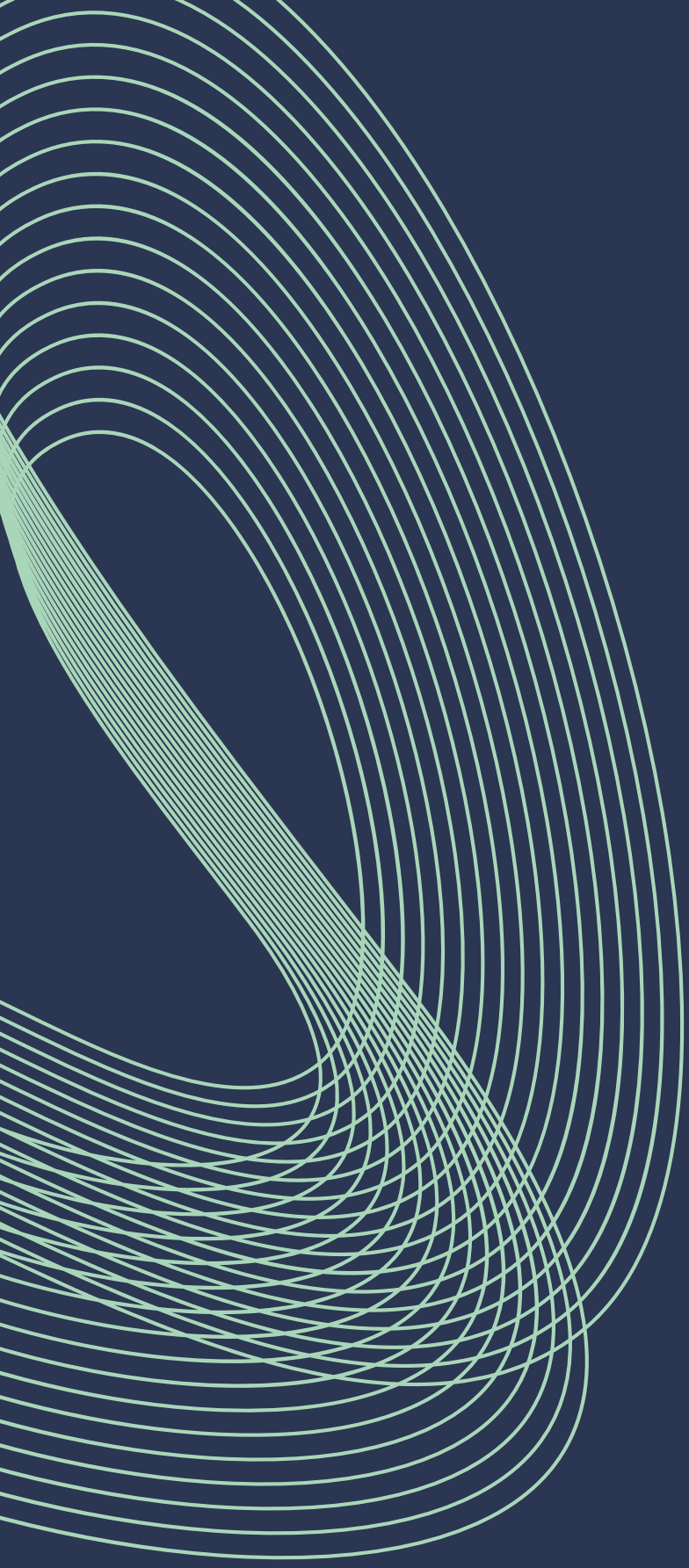
Office of Cyber-Security
& Information Assurance
Cyber-Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

November - December 2022



INTRODUCTION

For period 1st November - 31st December

Welcome to the new Cyber Monthly Threat Update brought to you by the Office of Cyber-Security & Information Assurance (OCSIA). This document provides an overview of cyber threats using our own data collected from our reporting points as well as our own intelligence sharing with private and public sector bodies.

If anyone has any information they wish to put forward to be considered for this document, please contact OCSIA on: cyber@gov.im or report it using our online cyber concerns form.

CONTENTS

SUSPICIOUS EMAIL REPORTING SERVICE (SERS)

As part of the Isle of Man Government's Cyber Security Strategy, the Office of Cyber-Security & Information Assurance (OCSIA) introduced the Suspicious Email Reporting Service (SERS) an automated system used to gather intelligence and take down malicious URLS on 23 October 2020.

If you have received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS) 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 phishing 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 10,700 suspicious emails. In November and December 2022, we received 1,163 suspicious emails.

SUSPICIOUS EMAILS

1,163 REPORTED

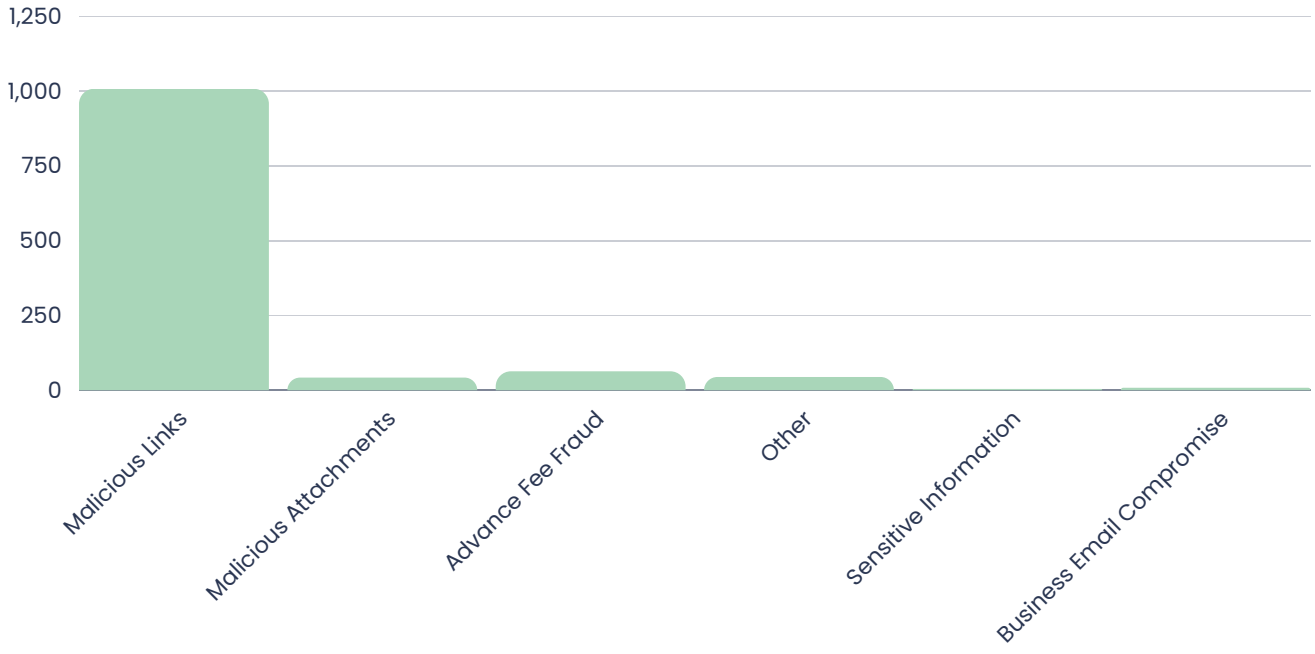
in November & December

Detail

The chart (below) details the type of emails sent by cybercriminals that have been reported to our SERS for the months of November and December. Whilst the infographic (right) showcases the top 5 most impersonated companies and services.

Top 5 Phishing Scams Imitating Popular Services:

1. Manx.net
2. Parcel Delivery
3. Romance/dating, etc.
4. Antimalware Software
5. Retail & Online Stores



CYBER CONCERNS

84 REPORTED

in November & December

Detail

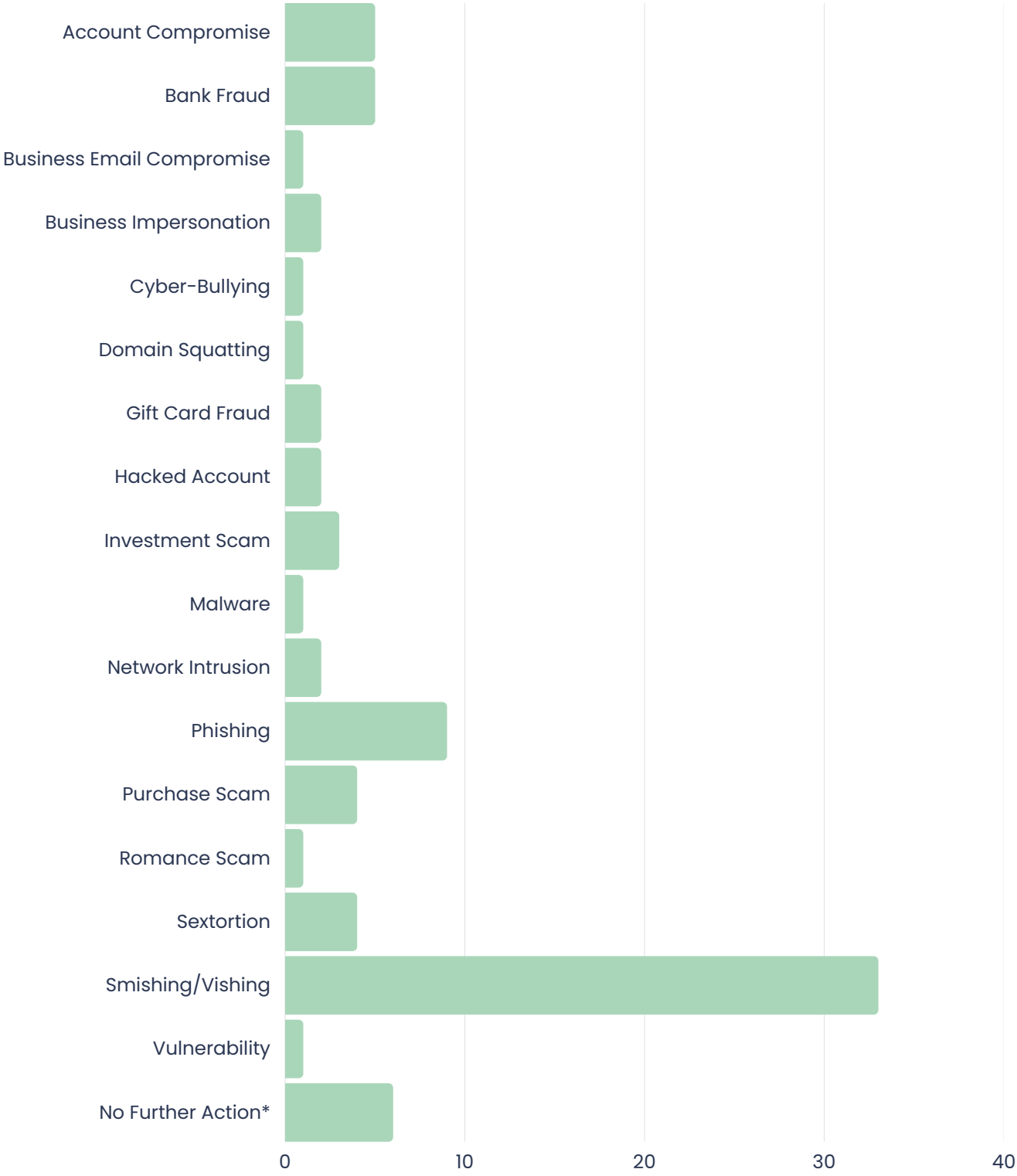
The chart (on page 4) shows a breakdown of cyber concerns reported to us over November and December.

OCSIA defines a Cyber Concern as a cyber-related issue involving the Internet, email, telephone communications or any other matter involving electronic communications that may or may not have already caused a negative impact.

OCSIA uses this data from both the public and private sector to build into our threat intelligence and external communications. Where requested, we work with the Constabulary to investigate and provide advice to victims.

Cyber Concerns differ from our suspicious email reporting service as the primary reporting point for any cyber concern that is not a phishing email. Often cyber concerns involve an already affected victim or those seeking advice.

Cyber Concerns November & December



***No Further Action:** submitted with good intentions but after further investigation was found to be a non-cyber concern or communication was found to be legitimate.

ISLE OF MAN THREAT COMMENTARY

In order to gain a more detailed understanding of the types of incidents that are contributing to trends, this section presents case studies of specific threats outlined on pages 3 and 4. These case studies, all taken from our cyber concerns reporting tool provides insight into the methods and motivations of attackers, as well as the impact that these attacks have had on the affected parties.

ACCOUNT COMPROMISE AND UNAUTHORISED ACCESS

DRIVING INSTRUCTOR HACK

There were 7 reports in the period relating to accounts being compromised. In one such instance, OCSIA received several reports about a local driving instructor whose account had been compromised and this account was used to scam funds out of potential customers.

In the reported cases, the malicious actor requested funds as an advance-payment for driving lessons, subsequently funds were transferred to a Revolut account and some reporters were only made aware of the scam when the impersonated business did not attend the booking.

From the reports we received, it's apparent that both businesses and those engaging with businesses need to establish set procedures to protect one another.

In the cases that we have seen, some victims were only made aware of the scam when they contacted the instructor through details listed on gov.im. This shows the importance of verifying a message using trusted and reliable contact details. This might be by using a telephone number or an email address originally provided but not by using social media platforms (e.g. Facebook, Instagram) to send messages.

BUSINESS EMAIL COMPROMISE

OCSIA received 2 reports of business email compromise of Island-based businesses.

In both instances, cyber-criminals gained access to business email accounts and used this access to send requests for money to existing clients or customers. One instance involved editing invoices to divert funds to the criminals bank accounts, whilst the other simply used existing business relationships to request money be paid into a criminal account.

Partner agencies were informed and criminal bank accounts were shut down.

Whilst similar to the driving instructor hack, these criminal acts were conducted through email and exploit existing relationships to extract money from victims.

SEXTORTION

We have received reports of 'sextortion' where explicit images have unknowingly been shared with cyber-criminals. Sextortion is a form of blackmail in which sexual information or images are used by a cyber-criminal to blackmail a victim.

Communication begins with a victim using an impersonated or fake social media account or WhatsApp and where a relationship develops over a period of days, weeks or months. Some tips to reduce the possibility of sextortion includes checking privacy settings, using nicknames on chat platforms, and not accepting unknown friends.

Through SERS we also see 'fake' sextortion scams where sensitive information has been gained through a data breach and has been used to add legitimacy to claims that the malicious actor has compromising images of potential victims.

We encourage members of the public who are worried to forward the email to SERS@OCSIA.IM asking for clarification.

All reports made to the platform are strictly confidential, meaning that they will are not shared with any third parties without the explicit consent of the reporter.

VISHING (TELEPHONE SCAMS)

BT OPENREACH

Vishing is consistently one of the most reported cyber concerns that we receive.

One of the prevalent scams within the period involves potential victims receiving repeated phone calls from 'x of BT OpenReach' saying that the intended victim's IP address had been compromised and was now public and needed to go to a non-BT OpenReach website to enter their IP address and other details.

The malicious actor uses standard social engineering tricks of creating urgency, establishing fear, 'trying to keep us safe', etc.

It can be easier for residents to identify scam calls, due to common knowledge about what services are or are not available on the Island.

BANKING IMPERSONATION

This month has seen a number of calls claiming to be from a banking fraud department, scaring potential victims into thinking that unapproved transactions have been made on their bank card.

Other calls involve a caller claiming to be an insider of the bank or a member of the police force, and that they need the potential victims help in catching a criminal at their bank.

The next step of the scam is where the victim moves money to an account controlled by the criminals and the victim then loses access to their funds.

CLICK HERE OR SCAN TO SEE OUR ADVICE ON VISHING.

SMISHING (MESSAGING SCAMS)

WHATSAPP FAMILY MEMBER

One of our most commonly reported concerns is the WhatsApp scam in which an unknown-number contacts the victim pretending to be a son or daughter.

The scammer creates a story by pretending to be a son or daughter and asking a mother to transfer money as soon as possible to replace the phone, and sometimes to pay a debt to a friend. If the mother replies to the message the scammer provides a friend's bank account details .

Highly successful, this scam relies on creating a sense of panic and urgency whilst playing on an existing connection between the 'relative' and victim.

OCSIA and the Constabulary publishes warning notices about these scams. The safest approach when dealing with unknown-number messages is to first assume that the message could be from a scammer. If you receive a message from a supposed family member, contact them on a known number/channel.

PARCEL DELIVERY TEXTS

Texts messages claiming to be from a parcel delivery service have been reported over the period.

The scam involves a text being received requesting payment to release a parcel for delivery, or asking the message recipients to update contact details.

Card details are then entered by the victim to either pay the 'small charge' or to verify contact details.

An amount much higher than the stated cost is then taken from victim and their card details kept; with the victims only option to cancel the card.

CLICK HERE OR SCAN TO SEE OUR ADVICE ON SMISHING.

VULNERABILITIES

DRAYTEK ROUTERS

Information reported to OCSIA identified that 363 Draytek routers used by Isle of Man businesses and residents had not yet been updated to address a critical flaw.

The flaw, if not addressed, exposes local residents to the possibility of a far-reaching compromise of computer systems that is not difficult for hackers to achieve. The consequences of a successful exploit would include sensitive-data extraction, access to devices on the network, spying on network traffic, collection of passwords and keys, and man-in-the-middle attacks.

As a result of the discovery, OCSIA published a website article and press release which received significant coverage in the local press. Subsequently, we received a number of calls from concerned businesses and residents, and offered technical support to those wishing to patch their routers.

We are aware that there are still a number of affected devices on the Island and advise that residents and businesses check the make and model of their routers.

Whilst specifically referring to Draytek OCSIA always recommends routers are kept up to date with the latest firmware which can be found through your manufacturers website.

CLICK HERE OR SCAN TO SEE OUR DRAYTEK ADVISORY

EXTERNAL THREAT COMMENTARY

Whilst geographically separate, the Isle of Man still belongs to an interconnected digital world, therefore, understanding external cyber security threats is crucial for protecting digital systems and personal information. These threats can originate from various sources and cause significant damage.

CRITICAL HIKVISION BUG ALLOWS REMOTE CCTV HACKING

The critical vulnerability in Hikvision wireless bridge products could lead to threat actors taking full admin control of an affected device.

The bug, tracked as CVE-2022-28173, affected the Chinese video surveillance giant's devices designed for surveillance systems. An advisory Hikvision published to address the flaw describes it as an access-control vulnerability.

In August, the flaw was uncovered by the cybersecurity company Redinent Innovations. Hikvision released patches to mitigate the problem on December 16. Researchers claim that the vulnerability existed due to improper parameter handling by the bridge's web management interface.

Hikvision has already had a tough time of late, with the Chinese manufacturer being banned from sensitive UK government sites due to national security fears.

Hikvision is partly-owned by the Chinese government and is the largest CCTV provider in the world, serving schools and public institutions in the UK. It supplies up to 60% of UK public bodies with CCTV cameras. Cameras from Chinese government-owned manufacturers, were used by 73% of local authorities, 35% of police forces and 63% of schools in the UK.

Hikvision users should install the patches found here as a matter of urgency.

LAST PASS SHARES INFORMATION ABOUT A RECENT SECURITY BREACH

The company Last Pass, which offers a password manager service to 33 million users, has shared details about a recent security breach with a third-party cloud-storage company that has allowed hackers to access customer information. It appears that hackers have taken a copy of every user's password vaults.

This serious breach follows a security incident that Last Pass disclosed August when it was reported that proprietary technical information and source had been stolen.

This security incident serves as a clear reminder that organisations must think about their supply-chain security and managed service provision, particularly if personal data is held and if networks of significance could be at risk.

GUARDIAN NEWSPAPER HIT BY SUSPECTED RANSOMWARE ATTACK

The Guardian has said that the attack hit on Tuesday, 20th December and had affected the company's technology infrastructure. Staff were told to work from home, yet despite the disruption to behind-the-scenes services, the company said it was confident that there would be no problems with publishing.

In a statement, the Guardian said, 'Our technology teams have been working to deal with all aspects of this incident, with the vast majority of our staff able to work from home as we did during the pandemic. We believe this to be a ransomware attack, but are continuing to consider all possibilities'.

Ransomware is malicious software used by hackers and often sent using attachments or links in emails to gain access to computer systems. The criminals then find and encrypt important or sensitive files, and demand a ransom for them to be unlocked.

TWITTER DATA LEAK – 400 MILLION USER DETAILS UP FOR SALE

Threat actors are reportedly selling data of 400 million Twitter users, including personal information such as Twitter handles, usernames, email addresses, and phone numbers for $50,000. The data is claimed to have been obtained through an unnamed 'vulnerability' using a technique called 'scraping'.

Personal details of notable politicians, athletes, international organisations, and government institutions were included in the sample shared by the author of the post. The seller of the data specifically addressed Twitter CEO Elon Musk, mentioning the ongoing investigation into Twitter's data leak of 5.4 million users in July.

On December 23, Ireland’s Data Protection Commission launched a probe into Twitter over July’s data breach.

SOCIAL MEDIA SECURITY FLAWS

Social media users looking for an alternative to Elon Musk's Twitter should be cautious when looking at Hive Social and Mastodon. With German researchers, Zerforschung, publishing an all-out warning to avoid Hive Social.

'The issues we reported allow any attacker to access all data, including private posts, private messages, shared media and even deleted direct messages,' the team wrote in its report. 'This also includes private email addresses and phone numbers entered during login.'

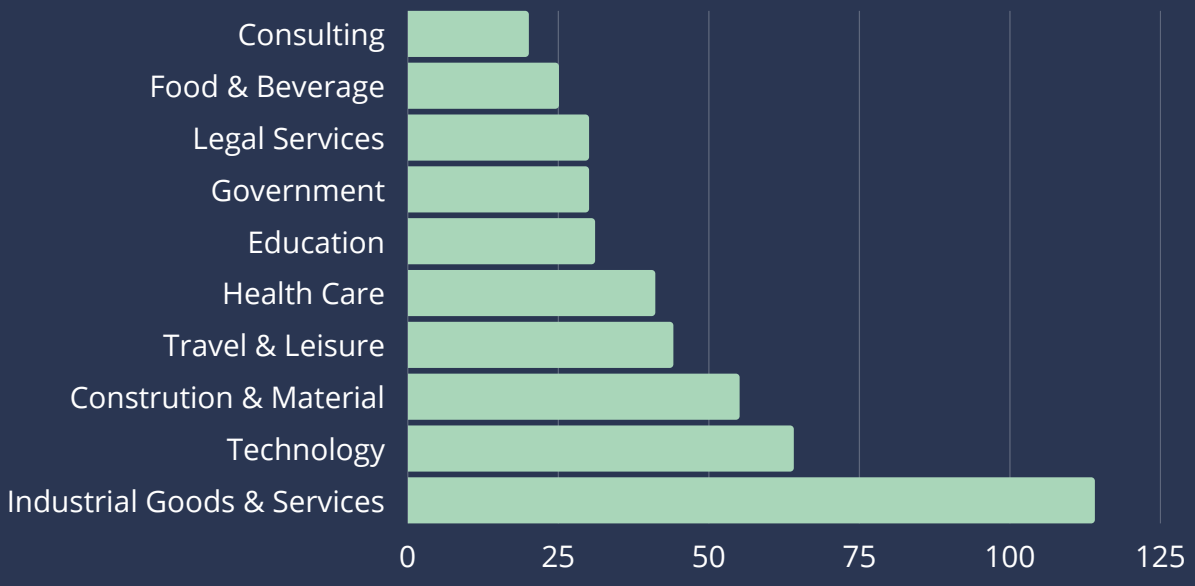
Mastodon has not escaped scrutiny with the decentralised social media platform having numerous vulnerabilities and other security issues.

THREAT FOCUS: RANSOMWARE

> **"Even with a war raging in Ukraine - the biggest global cyber threat we still face is ransomware"**
>
> Lindy Cameron - CEO, National Cyber Security Centre UK

Ransomware is a type of malware (malicious software) that locks access to, or encrypts the data on a computer system or network of systems. Victims are requested to pay a ransom in return for regaining access to the data and systems.

New strains of ransomware are being released frequently and are constantly updated. The effects of a ransomware attack can be far-reaching and are felt long after the ransomware has been cleared. There is often an attitude that certain sectors will not be hit, but the graph below illustrates the variety of businesses targeted by ransomware such as Lockbit.



Ransomware victims by sector Q3 2022 according to Digital Shadows: https://www.digitalshadows.com/blog-and-research/ransomware-in-q3-2022

CYBER GLOSSARY

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

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

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.

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 25th May 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.

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

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.

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.

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

CLICK HERE OR SCAN TO VIEW OUR FULL CYBER GLOSSARY

ABOUT US

The Office of Cyber-Security & Information Assurance (OCSIA) was established by a Council of Ministers Directive in October 2017.

It acts as the focal point in developing the Island's cyber resilience, working in partnership with private and third sector organisations across the Island alongside the wider population.

The office is committed to supporting Island-residents and businesses by providing practical and targeted advice and guidance. This includes working in partnership with the private sector to improve their cyber resilience and raise awareness about the latest cyber threats affecting our Island.

OCSIA also hosts an annual conference 'CYBERISLE' which is held over the course of one day, and helps business leaders, individuals, community and charitable organisations understand the rapidly changing cyber-security threat landscape.

In February OCSIA will be launching our cyber security awareness survey. The results of these surveys assist OCSIA in establishing the level of the Island’s cyber security awareness and better understand areas where we can support our residents and businesses in future.

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

Office of Cyber-Security
& Information Assurance
Cyber-Security Centre for the Isle of Man

www.ocsia.im
cyber@gov.im
01624 685557

Office of Cyber-Security & Information Assurance
2nd Floor
Former Lower Douglas Police Station
Fort Street
Douglas
Isle of Man
IM1 2SR

T: +44 1624 685557

Isle of Man Government
Reiltys Ellan Vannin