CYBER THREAT UPDATE

Annual Report 2023

With a year of Threat Updates, we take a look a some of the most notable cases and trends in 2023.

INTRODUCTION

Welcome to this special 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 reported to us 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 reach out to us at cyber@gov.im or submit it via our online cyber concerns form.

We have published advice and guidance for the contents covered in this report, which can be found on our website here.

CONTENTS

OVERVIEW

6,220

Total emails reported to SERS

701

Reported Cyber Concerns

£862,334

Reported financial loses, from our cyber concerns reporting point

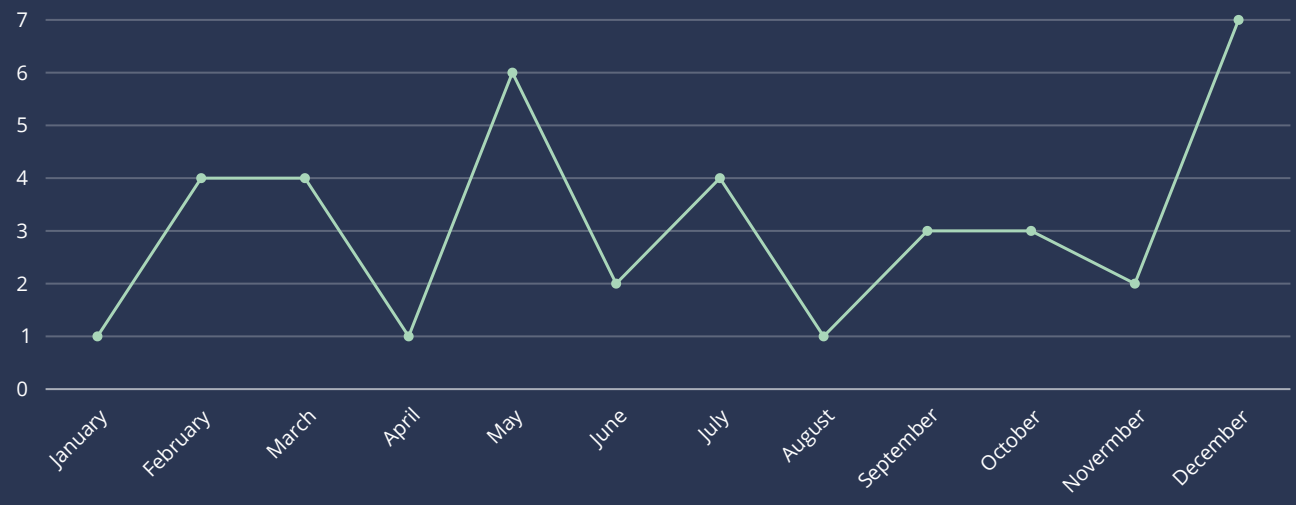
All reports pose a challenge in categorisation, as some may align with multiple categories. Accordingly, we have assigned the category that aligns most closely with the available information.

Despite the striking figures presented above, it is anticipated that the actual values will prove to be notably higher. This is due to the relatively low report numbers in comparison to incidents we're made aware of through social media and other forms.

THREATS

ACCOUNT COMPROMISE

Account compromise refers to the unauthorised access or takeover of an individual's or organisation's online account by a third-party, often with malicious intent. Account compromise poses a significant security risk and can lead to various consequences, including data breaches, financial losses, and damage to an individual's or organisation's reputation. Experiencing an account compromise is often emotionally stressful for victims, due to concerns about personal and financial security. The invasion of privacy also has the potential for identity theft and victims are often left to angry and frustrated, particularly when experiencing difficulties when trying to recover an account.



CASE STUDY

An anonymous reporter informed us that criminals had gained access to their eBay account and had used this access to purchase goods worth £8,000 over a 20-minute period. We have no further details about how access was granted. In this case, banking app approval for each purchase was not needed, possibly due to the card being attached to an account that had used the cards previously. Our recommendation would be to always enable Multi-factor Authentication (MFA) where possible, particularly if the account contains sensitive information.

38

Reported Cyber Concerns

£20,635

Reported financial loses

£543

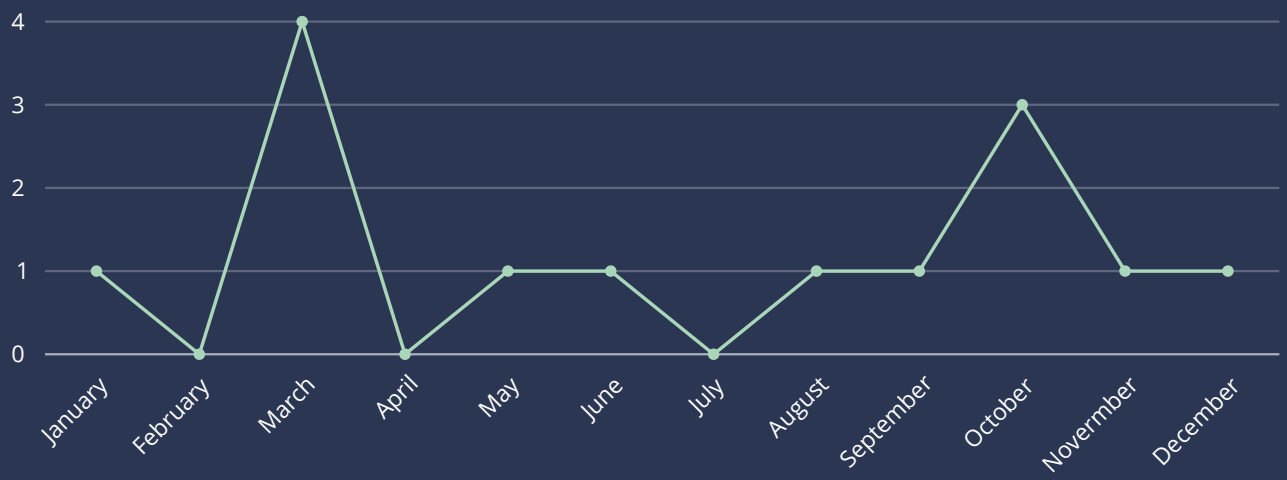
Average financial loss per report*

**Some reports had no financial loss attributed and this is purely an average figure*

BANK FRAUD

Bank fraud refers to the deliberate and illegal act of using deceit, trickery, or false means to obtain money, assets, or other property owned or held by a financial institution. These include corporate service providers, a significant sector in the island's economy.

As with all categories, if we can positively identify another method by which a criminal activity was conducted, such as business email compromise, the report will go into the most appropriate category. Therefore, not every cyber incident conducted against a financial institution appeared here.



CASE STUDY

A fraudulent bank account received a payment of $26,000 from a local CSP. The payment was made as a donation to a school (outside the IOM). The bank details were received from a trusted source, who in turn received the bank details from what is believed to be a hacked email account. The company re-confirmed the bank details with the trusted source since it was a change from the prior year. A signed receipt of the funds from the school was also received, making it difficult for the company to have noted that there was something wrong with the payment. The school then contacted us saying that they have never received the payment and that they have a live investigation to determine who is involved in this event.

14
Reported Cyber Concerns

£46,186
Reported financial loses

£26,000
Largest report of financial loss

GIFT CARD FRAUD

Cybercriminals will use a range of techniques, including impersonating a work colleague, friend or family member, in order to get you to purchase gift cards. The cards are then redeemed by the cybercriminal and it is incredibly difficult to retrieve funds.

In the period, we only received seven external cyber concerns reports, but the significant funds involved and the difficulty in rectification make this an important area to highlight.

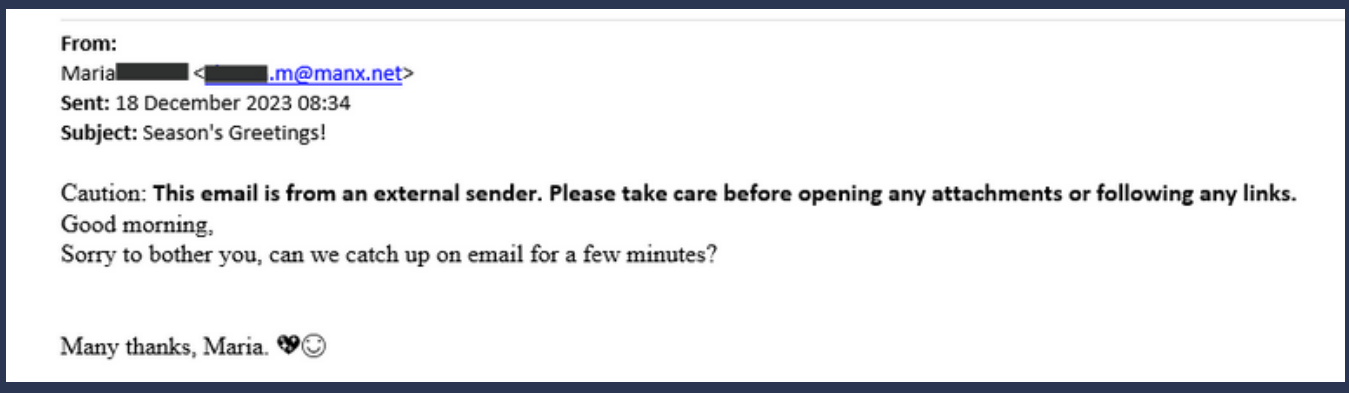
Typically, gift card fraud is commonly associated with business emails. An example of this (below) is an attempted gift card fraud on an employee at Manx Care. However, we are noticing a trend of scammers diversifying their targeting methods.

CASE STUDY

In May 2023, an individual (person X) narrowly avoided becoming the victim of a gift card fraud that led them to attempt to buy £200 worth of Apple Vouchers and transmit the codes through Messenger. Initial contact was made through Facebook through a friends legitimate profile, who requested X to purchase gift cards.

During their attempt to acquire the Apple Vouchers, X visited WH Smiths (Sea Terminal), where an astute sales assistant/shop worker recognised that this could be a scam and cautioned X regarding the nature of the request. This timely intervention heightened awareness and prompted X to reassess the situation.

X decided to validate the authenticity of the messages with their friend. To their surprise, the friend clarified that no such messages had been sent and disclosed that their Facebook account had been compromised.



From:
Maria[redacted] <[redacted].m@manx.net>
Sent: 18 December 2023 08:34
Subject: Season's Greetings!

Caution: **This email is from an external sender. Please take care before opening any attachments or following any links.**
Good morning,
Sorry to bother you, can we catch up on email for a few minutes?

Many thanks, Maria. 💔☺

7
Reported Cyber Concerns

£12,975
Reported financial loses

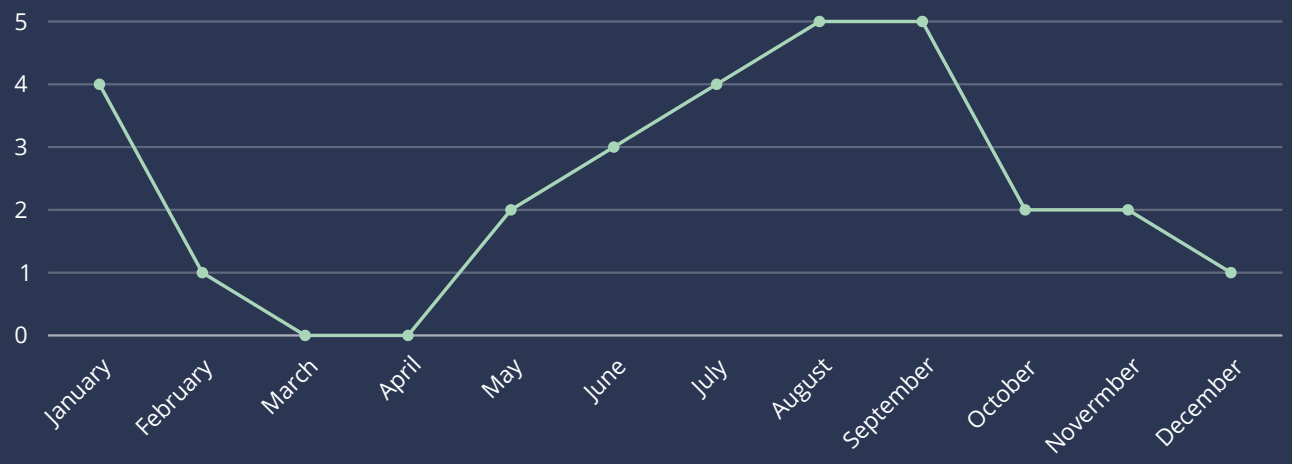
£1,853
Average financial loss per report*

**Some reports had no financial loss attributed and this is purely an average figure*

INVESTMENT SCAMS

Investment scams are on the rise and criminals employ diverse tactics to deceive unsuspecting individuals. They frequently exploit shares or cryptocurrency; enticing victims with promises of rapid returns. However, in many instances, these supposed shares or cryptocurrencies are non-existent.

Alternatively, individuals who already possess shares may be targeted and they are urged to transfer or move their shares. Unfortunately, these transfers often do not occur, and the company initiating the contact lacks any legitimate authority to engage in business involving these shares.



CASE STUDY

A scam began when a friend of the victim, whose Instagram profile displayed posts demonstrating significant earnings from cryptocurrency trading, got involved. The victim decided to invest £500 in the scheme through bitcoin guided by an alleged investment coach. After transferring the money to her Bitcoin wallet, she was instructed to send it to another account outside of her control, so the 'investment coach' could manage the investment. Within a few hours, the website falsely indicated a profit of £12,300 for the victim. However, to claim the profit, she was told to upgrade her account by depositing an additional £2,500.

The victim grew suspicious and reached out to her friend directly, outside of Instagram, only to discover that their Instagram account had been hacked, and they had no control over it. Faced with this revelation, the victim is sharing her story to caution the public and prevent others from falling victim to similar scams.

28
Reported Cyber Concerns

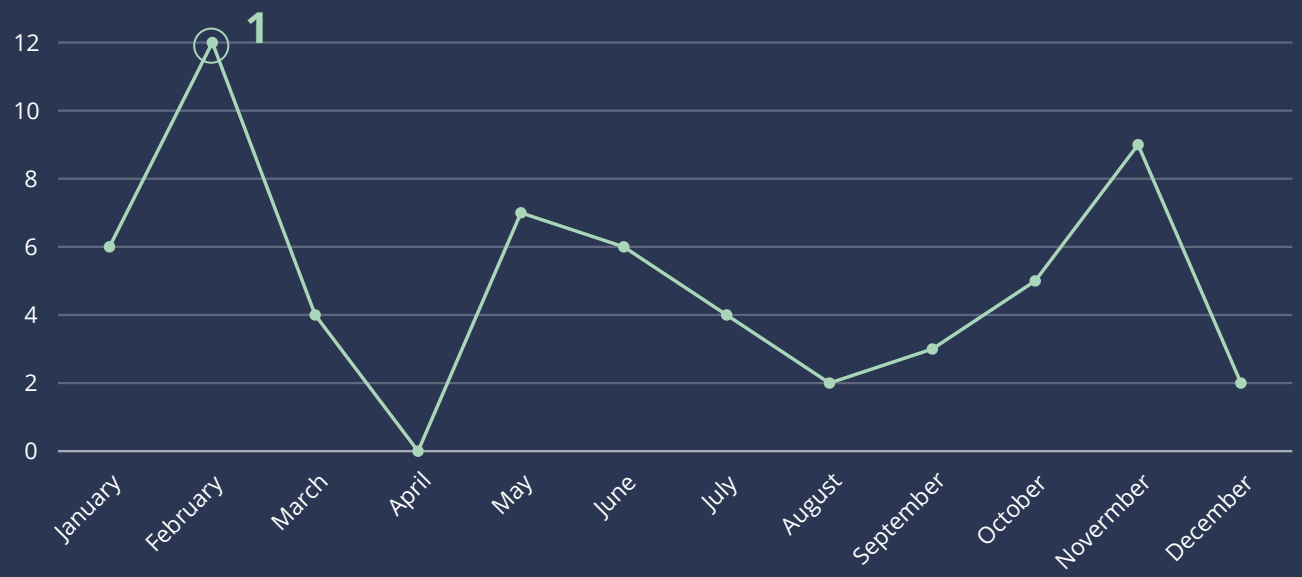
£139,970
Reported financial loses

£30,000
Largest report of financial loss

PHISHING

The majority of our phishing reports come through SERS, however, where public reports are received through our online reporting form and where advice and guidance is beneficial we record them here.

It's important to note that financial losses were low in comparison to the number of reports. Phishing often leads to account loss, which can often have a significant emotional impact.



CASE STUDY[1]

An email was sent to dozens of residents, appearing to be from the police and Interpol, with the subject line 'Request for Explanation No. 735BP'. The email contained a PDF attachment that was a forged letter showing the IOM Police and Interpol and signed by Danny Rotchell, the new Chief Inspector. This information was taken from publicly available information online. The letter accused the recipient of four offences and instructed them to see the court summons and respond as soon as possible to avoid arrest. Over 70 emails were received through SERS, and two reports were received through the WARP. A phone call was also received from Ramsey Police Station referring to two elderly email-recipients who were concerned about the content.

60
Reported Cyber Concerns

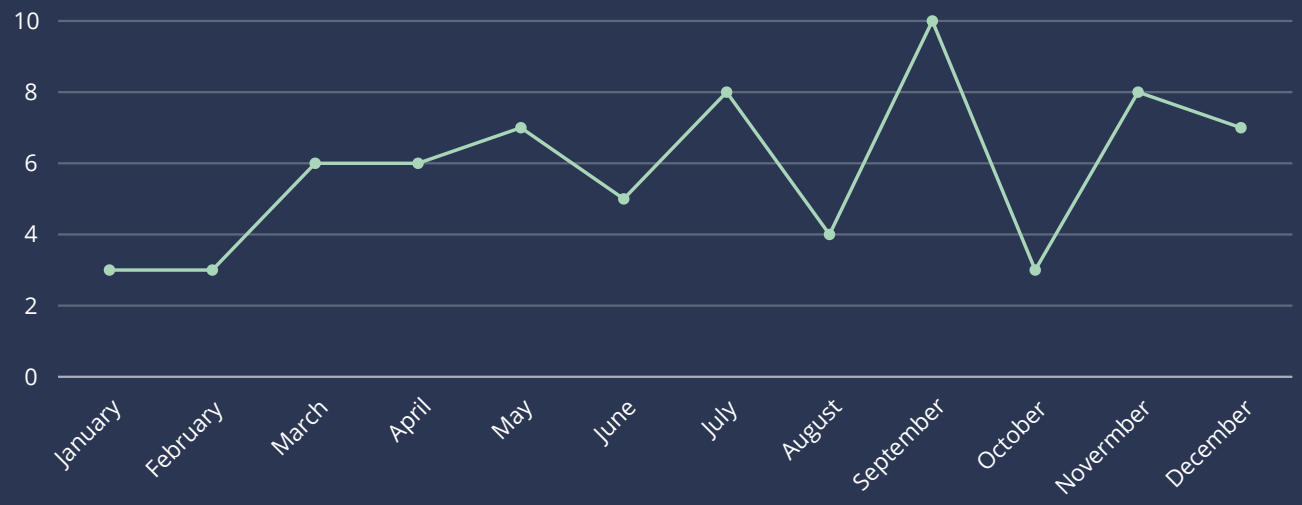
£49,037
Reported financial loses

4801
Malicious link SERS submissions

PURCHASE SCAMS

Purchase scams occur both in the real world and online. However, Island residents can be targeted from all over the world online, making any recovery of funds extremely difficult. There is significant variety in purchase scams, from pets to flat deposits; however, the common trend is a lack of precaution that would occur in real life.

Scams involving Facebook make up a significant number of reports. However, Facebook is simply the vehicle used to facilitate criminal activities.



CASE STUDY

A victim engaged with a seller on Facebook Marketplace selling tools. After the payment was sent the seller changed the terms insisting on buying additional items at an increased cost. The victim proceeded, assuming potential recourse through the police due to the seller's use of a UK bank account and seemingly authentic Facebook profile.

However, the situation escalated as the seller continuously delayed providing accurate tracking information and failed to dispatch the parcel. The victim was then blocked by the seller. We ask all residents not to assume that you can get money back on any scam. While criminals may have UK bank accounts, there are no guarantees that these have not been created for deceptive purposes. Furthermore, the money is likely to have left that account almost immediately after the completion of a scam.

70

Reported Cyber Concerns

£36,160

Reported financial loses

£516

Average financial loss per report*

**Some reports had no financial loss attributed and this is purely an average figure*

ROMANCE SCAMS

The bulk of the £12,000 below comes from one report; however, other reports allude to other victims sending significant amounts of money to cyber criminals. Those figures we cannot confirm have not been included, and we suspect the actual figure for romance scams to be much higher.

What is particularly worrying about romance scams is the emotional impact they have on the victim and their close friends and family. Often, it takes a significant period of time (and financial loss) for a victim to finally recognise that their online partner doesn't exist. We sometimes receive reports from concerned family or friends who are struggling to get their loved one to accept that they're a victim.

Romance scams are reported regularly throughout the year and can have both a serious emotional and financial impact on victims. We are aware of instances where victims have sent over £10,000 in the hope of their online partner visiting the island.

In one example, a person was scammed on Tinder by someone posing as military personnel who claimed to need money to get out of Syria. The scammer sent a copy of a person's passport, bank information, and USA Military ID. The scammer then gave the victim a small amount of money to build trust, with the money being transferred back to the scammer to 'pay their loan'.

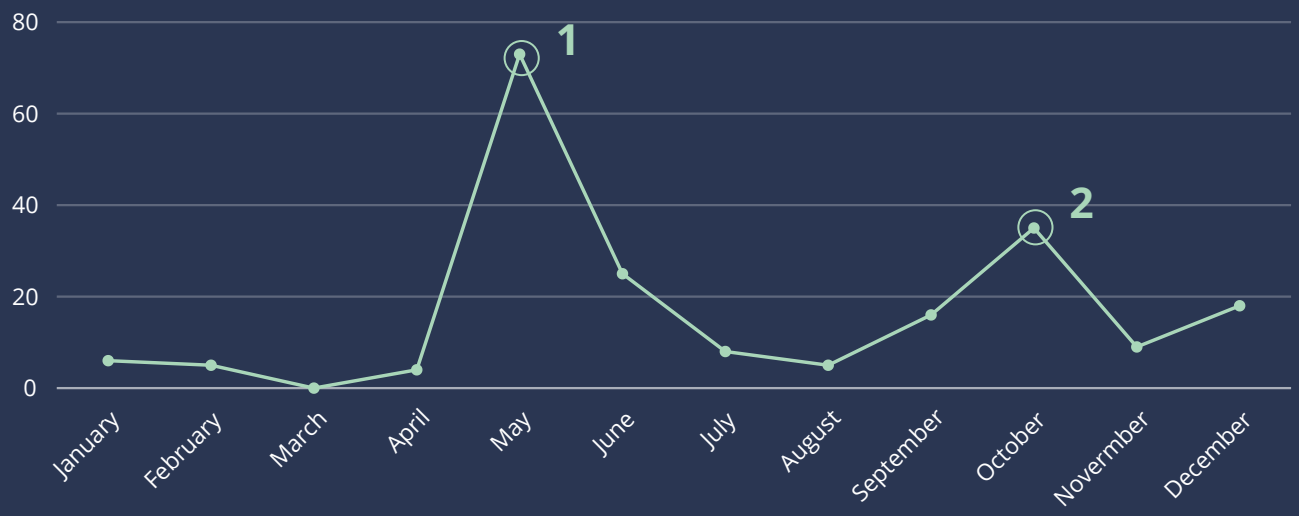
All romance scams involve manipulating the victim and preying on any potential vulnerabilities they may have. Social engineering is used to gain the victim's trust and to make them less aware of the reality that they're being scammed.

While we are aware of more romance scams than the figure suggests, we understand how emotionally traumatic romance scams can be.

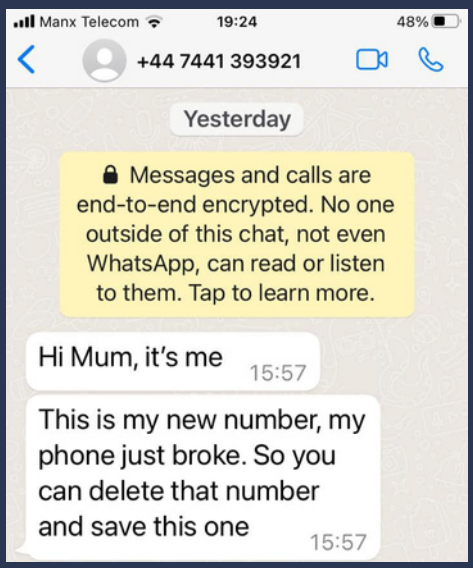
7	£12,000	£11,000
Reported Cyber Concerns	Reported financial loses	Largest report of financial loss

SMISHING

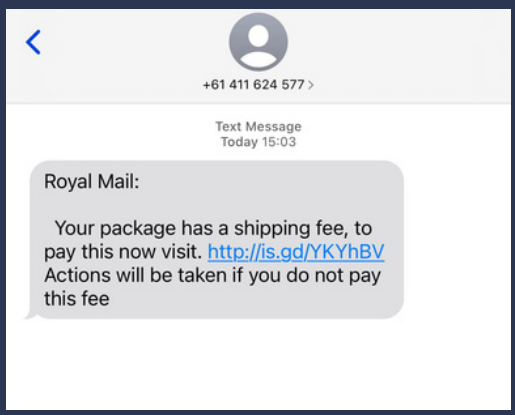
Over the year, we saw a number of SMS-based phishing scams. These scams peaked in May with the WhatsApp 'Hello Mum', which saw a significant number of victims lose money. While in October and towards the end of the year, we saw the Royal Mail/Courier delivery scams spike as residents were targeted in the run-up to Christmas.



1



2



204
Reported Cyber Concerns

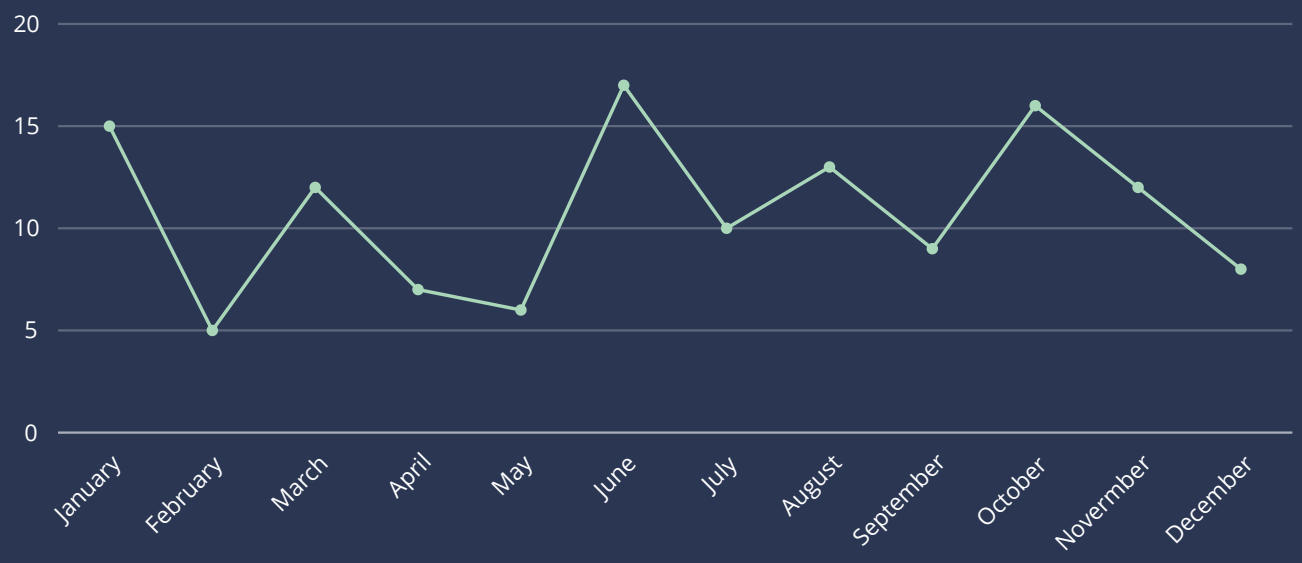
£19,209
Reported financial loses

£4,350
Largest report of financial loss

VISHING

Telephonic phishing, referred to as vishing, remained at relatively consistent levels across the year. The variety of vishing scams we received this year is a worrying indicator of the success of vishing calls with the classic 'Microsoft support' scams barely factoring into the reports.

As seen by the figures below vishing has had by far the most financial impact on Island residents. Typically, we are finding that the criminals are using publicly available information to add legitimacy to their calls.



CASE STUDY

In October, Manx residents were the target of a telephone scam campaign where the criminals pretended to be from a bank's 'Isle of Man Fraud team'. In several instances these telephone calls have led to substantial financial losses.

Unlike less-convincing automated 'robo-calls' these scammers spoke to their victims directly, claiming that there were suspicious transactions on their accounts and that money needed to be moved to a safe bank account, which was the criminal's bank account. In some or all instances, scammers seemed to know the victim's name and this, no doubt, created a sense of trust and legitimacy to the calls. The scammers were so convincing that they encouraged their victims to visit their local branch to arrange the bank transfer in person.

130
Reported Cyber Concerns

£416,771
Reported financial loses

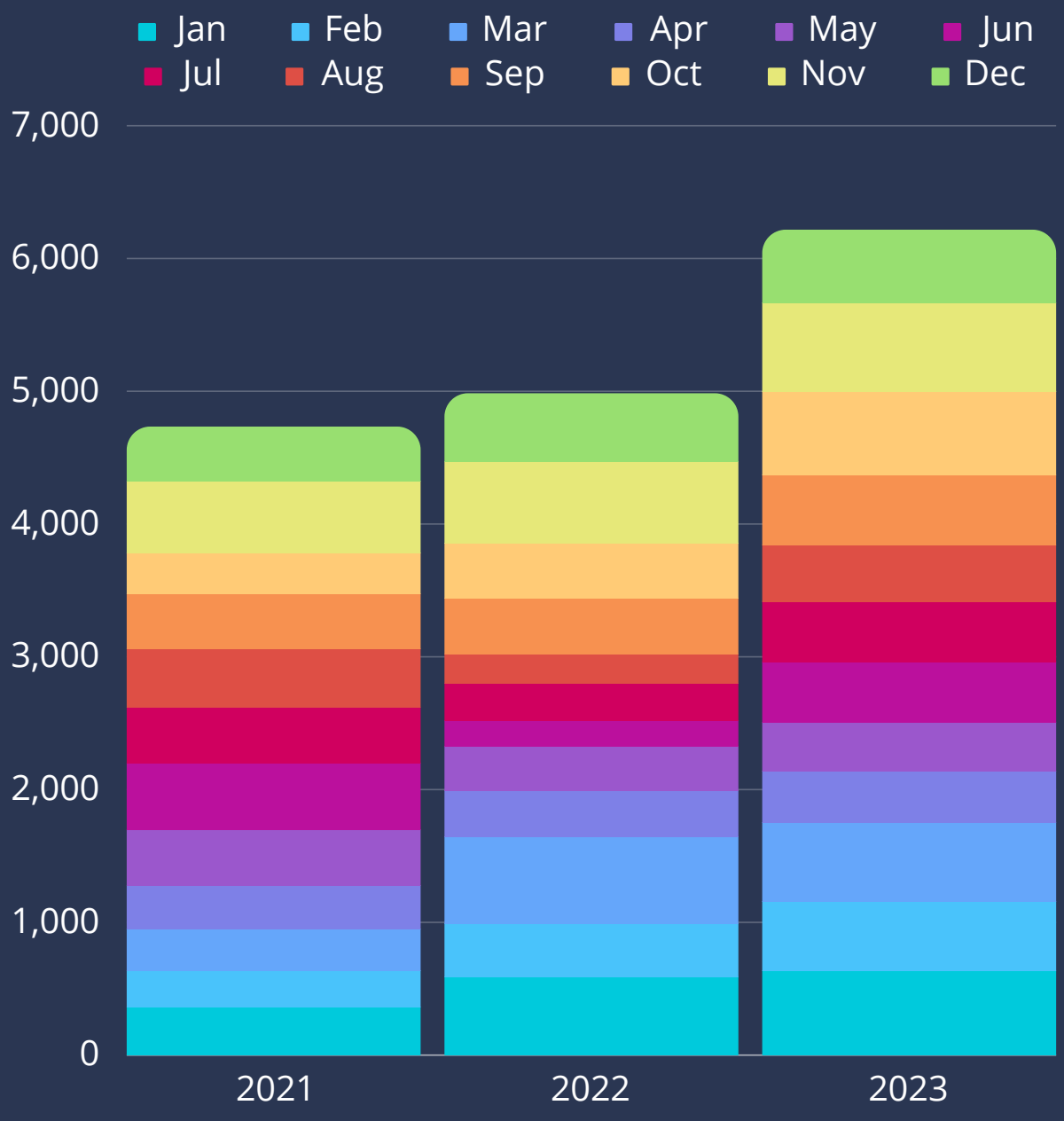
£3250
Average financial loss per report*

**Some reports had no financial loss attributed and this is purely an average figure*

SUSPICIOUS EMAIL REPORTING SERVICE (SERS)

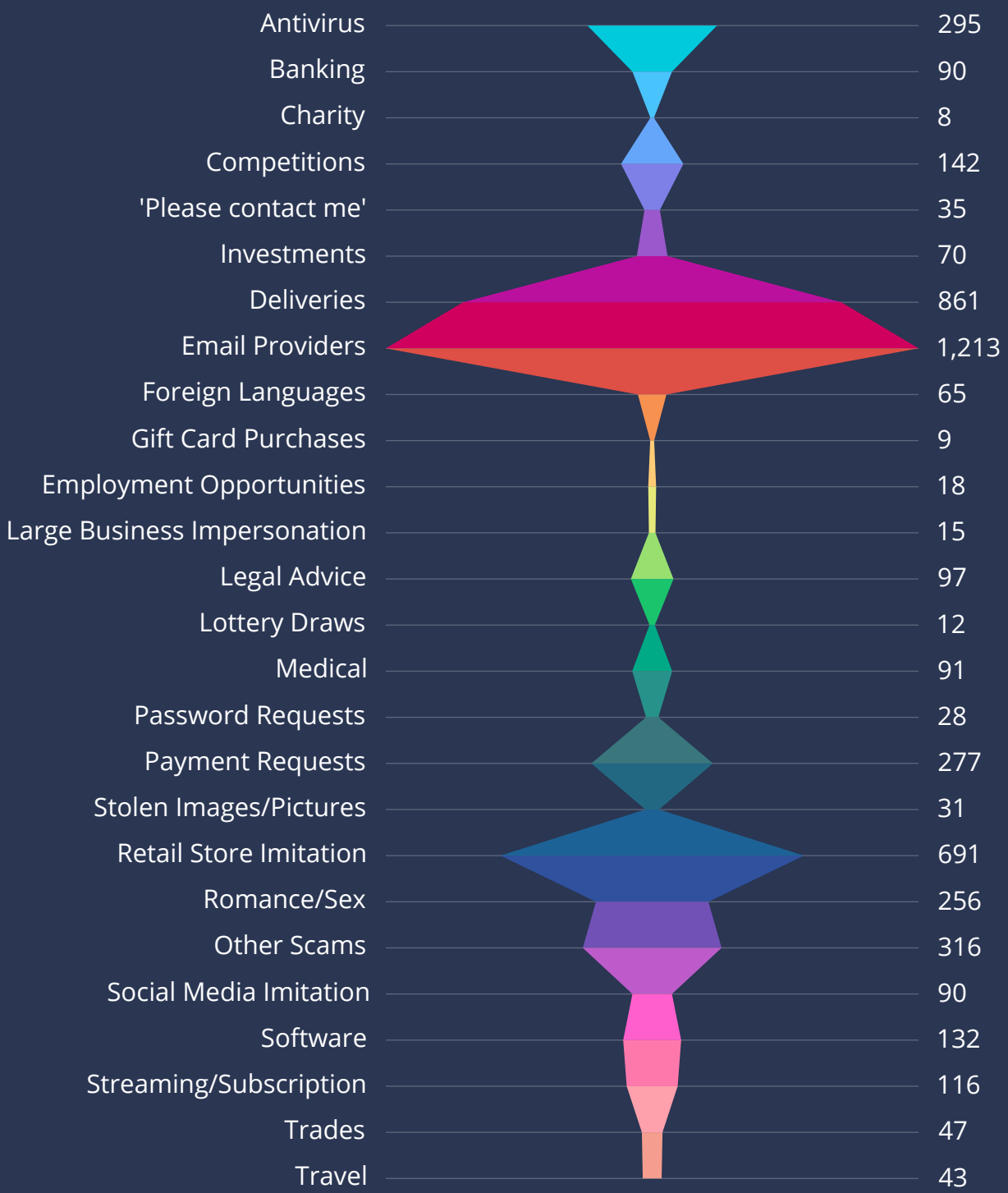
In 2023 we received 6,218 suspicious emails forwarded to us through our SERS; an increase of 25% on the 4985 reported in 2022.

COMPARATIVE STACKED BAR CHARTS SHOWING THE INCREASE IN REPORTS EACH YEAR.



Analysing the contents of the reported emails in 2023 the majority were imitating legitimate email providers with many of the reports targeting manx.net email users. The least reported email contents related to fictitious charities. An overview of the email content is shown below:

CONTENT CONTAINED WITHIN PHISHING EMAILS RECEIVED THROUGH SERS IN 2023



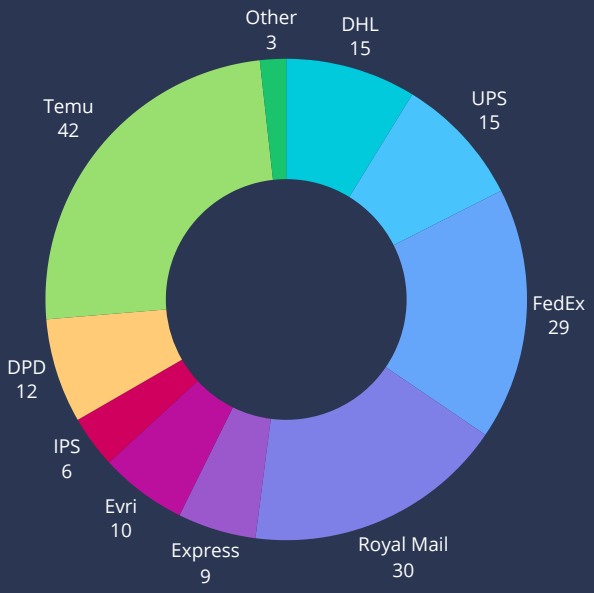
MOST POPULAR BRAND IMITATIONS IN 2023.

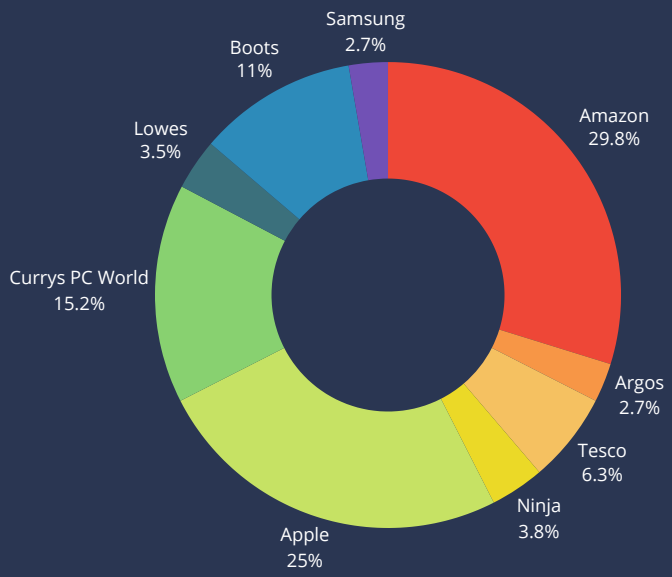
Email Providers

In 2023 the most reported phishing emails related to email providers. The most reported provider was Manx.net. Out of 6,218 total SERS we received, 1,003 were Manx.net, equalling approximately 1/6 of all submissions. Other, email providers, represented in orange, hardly featured, indicating a targeted attack on Manx.net users.

Parcel Delivery

Following email providers, delivery companies emerged as the subsequent most frequently replicated brands. Temu stood out as the most imitated, despite not being a delivery company; rather, the deceptive emails alluded to an undelivered Temu package. Royal Mail and FedEx closely trailed in terms of imitation. Smaller delivery services such as Hermes (now Evri) and Skymax were also cited in the submissions. It's worth noting that Royal Mail, having been prominently featured in smishing scams in 2023, did not feature as heavily through email.





Retail Stores

In 2023 a total of 59 distinct retail outlets were specifically mentioned. The chart on the left highlights the top 9 among them. Notably, Apple and Amazon featured prominently. Phishing emails received by the Manx public included American stores such as Walmart, Lowes, Costco, and JC Penny. This highlights that phishing campaigns typically cast a wide net, aiming to reach as many individuals as possible rather than targeting specific geographical locations.

SERS AND THE NCSC

When submitting to our SERS, emailed are also passed onto the NCSC.

The NCSC will analyse the suspect email and any websites it links to. They use any additional information you've provided to look for and monitor suspicious activity. If malicious activity is discovered the NCSC may:

- seek to block the address the email came from, so it can no longer send emails
- work with hosting companies to remove links to malicious websites
- raise awareness of commonly reported suspicious emails and methods used (via partners)

Whilst the NCSC is unable to inform you of the outcome of its review, they act upon every message received.

161k scam URLs removed by the NCSC since launch, as of December 2023

27m Reported scams

VULNERABILITY ALERTS

In 2023 we embarked on a project to deliver a vulnerability advisory service to raise awareness of critical vulnerabilities that may leave Island residents and businesses exposed to potential compromise.

THE SERVICE

Regular quarterly reviews of publicly available information on vulnerabilities identified within the Isle of Man internet address space will be undertaken and, where relevant, notifications of the vulnerability and potential impact of a compromise will be communicated to the relevant party.

Occasionally, there may be vulnerability of such concern that a public communication may be necessary. One such example of where this applied was the Draytek vulnerability announcement, which occurred in December 2022 and affected over 350 devices.

WHAT NEXT?

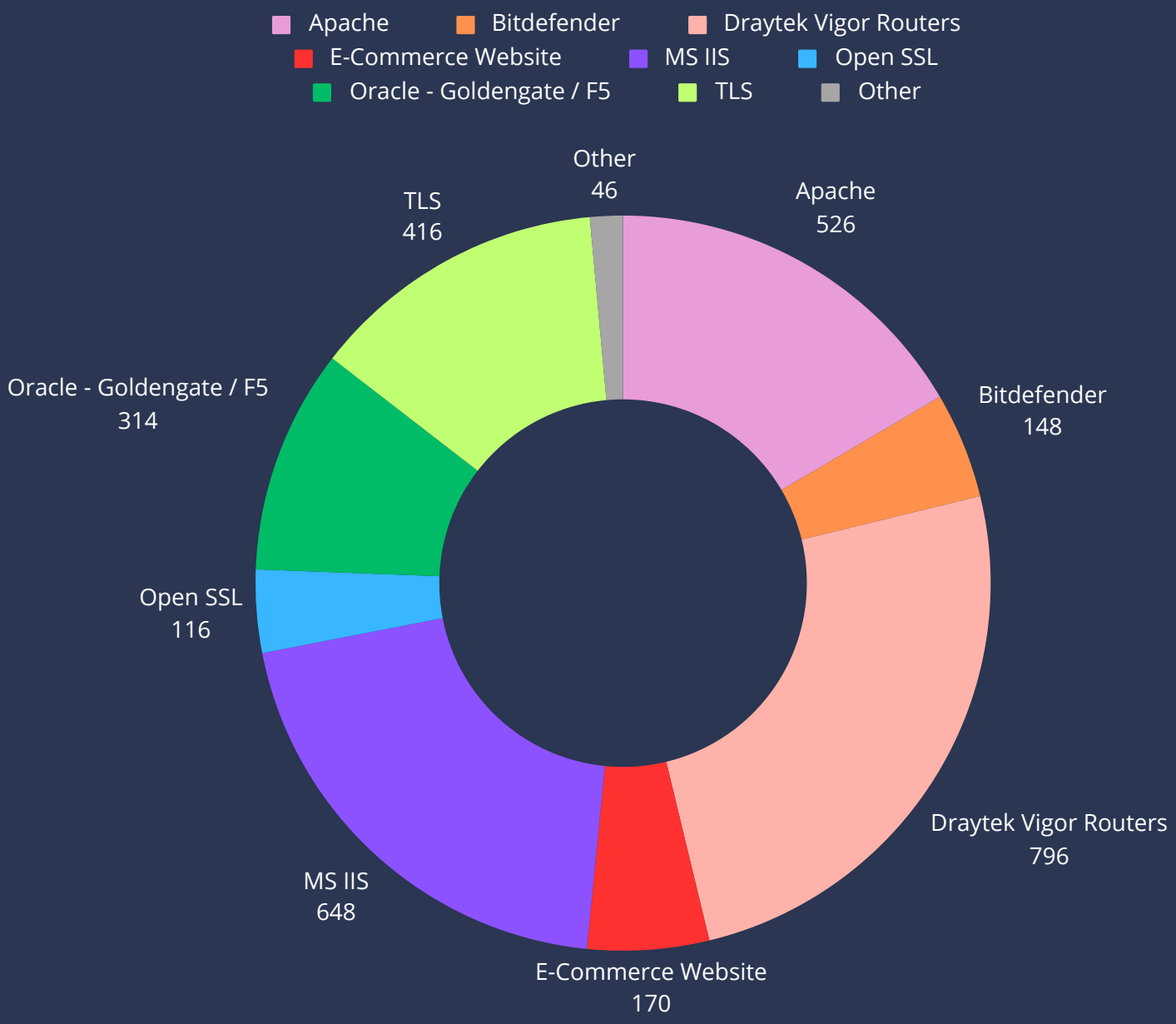
These vulnerability reports will only be sent the relevant parties and are not accessible to the general public.

However, to be informed of the latest advisories that may affect yourself or organisation follow us on social media, check our website or sign up to our mailing list to directly receive advisories.

REPORTED VULNERABILITIES FOR JANUARY - DECEMBER 2023

Vulnerabilities affecting the Isle of Man were discovered by scanning the Islands IP address space that occurred every 3 months. The graph below illustrates the number of times a vulnerability from an affected organisation/product appeared, this may mean that some vulnerabilities we're not rectified in-between quarters and appear more than once in the figures.

We've decided to purposefully emit the exact vulnerabilities discovered. If you wish to view an index of vulnerabilities click here.



ABOUT US

In October 2023 we launched the Cyber Security Centre for the Isle of Man (CSC) OCSIA's public-facing body providing advice, guidance and practical support to Island residents and businesses.

The CSC 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. As a part of OCSIA, the CSC works in the public sphere whilst OCSIA focuses on information assurance within Government.

We are committed to supporting Island-residents and businesses by providing practical and targeted advice and guidance. We will shortly be publishing a consultation on a National Infrastructure Security Bill, and are inviting anyone with an interest to express their views in this upcoming consultation. Check out the links below to be informed first when this is published.

@CyberIOM

facebook.com/OCSIAIOM

linkedin.com/company/csc-isle-of-man/

Join our mailing list

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 and where otherwise stated, all material presented in this publication is provided under the Open Government License (https://www.ocsia.im/other-pages/open-government-licence)

CSC Cyber Security Centre for the Isle of Man

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

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