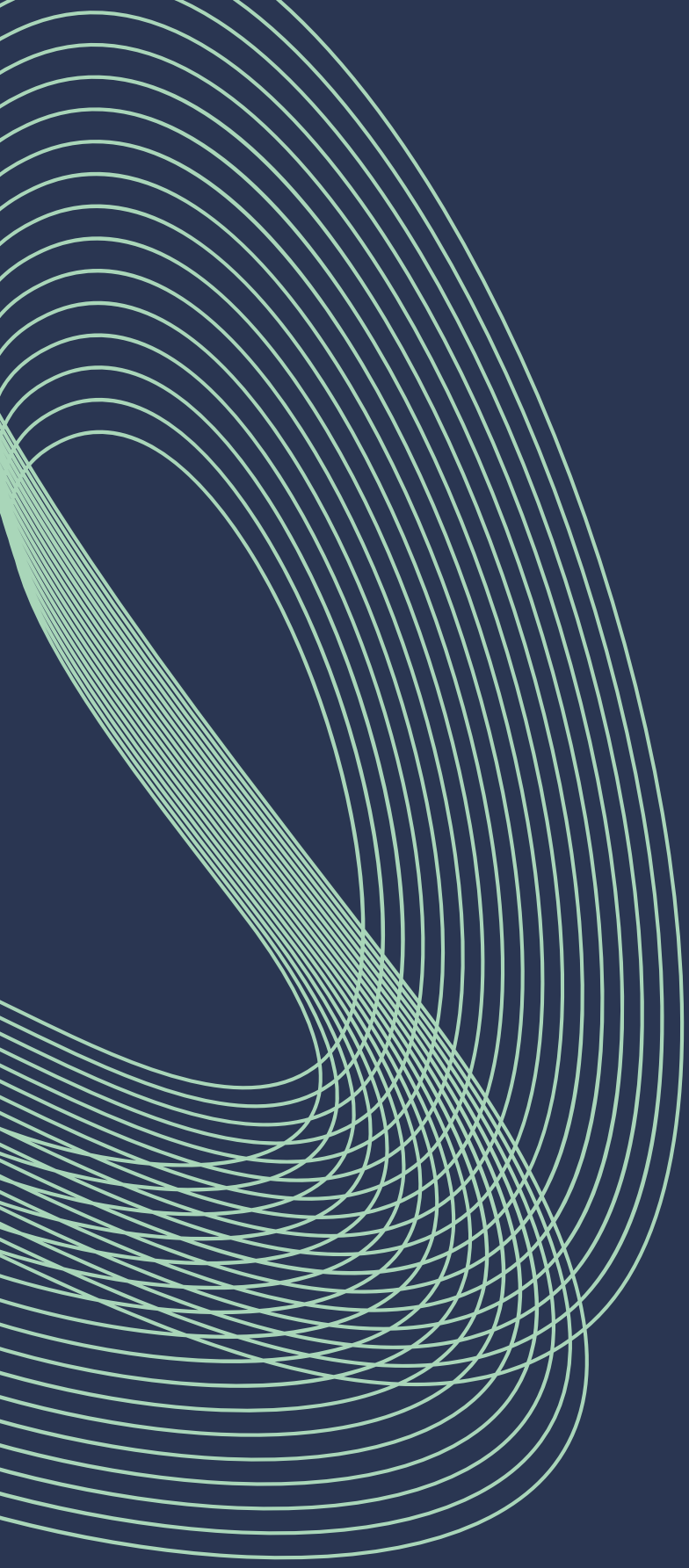
Cyber Security Centre for the Isle of Man

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

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

July - August 2023



INTRODUCTION

For period 1st July - 31st August

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-sharing with the private sector.

If anyone has any information they wish to put forward to be considered for this document, please contact the CSC 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 14,572 suspicious emails. In July and August 2023, we received 886 suspicious emails.

SUSPICIOUS EMAILS

886 REPORTED

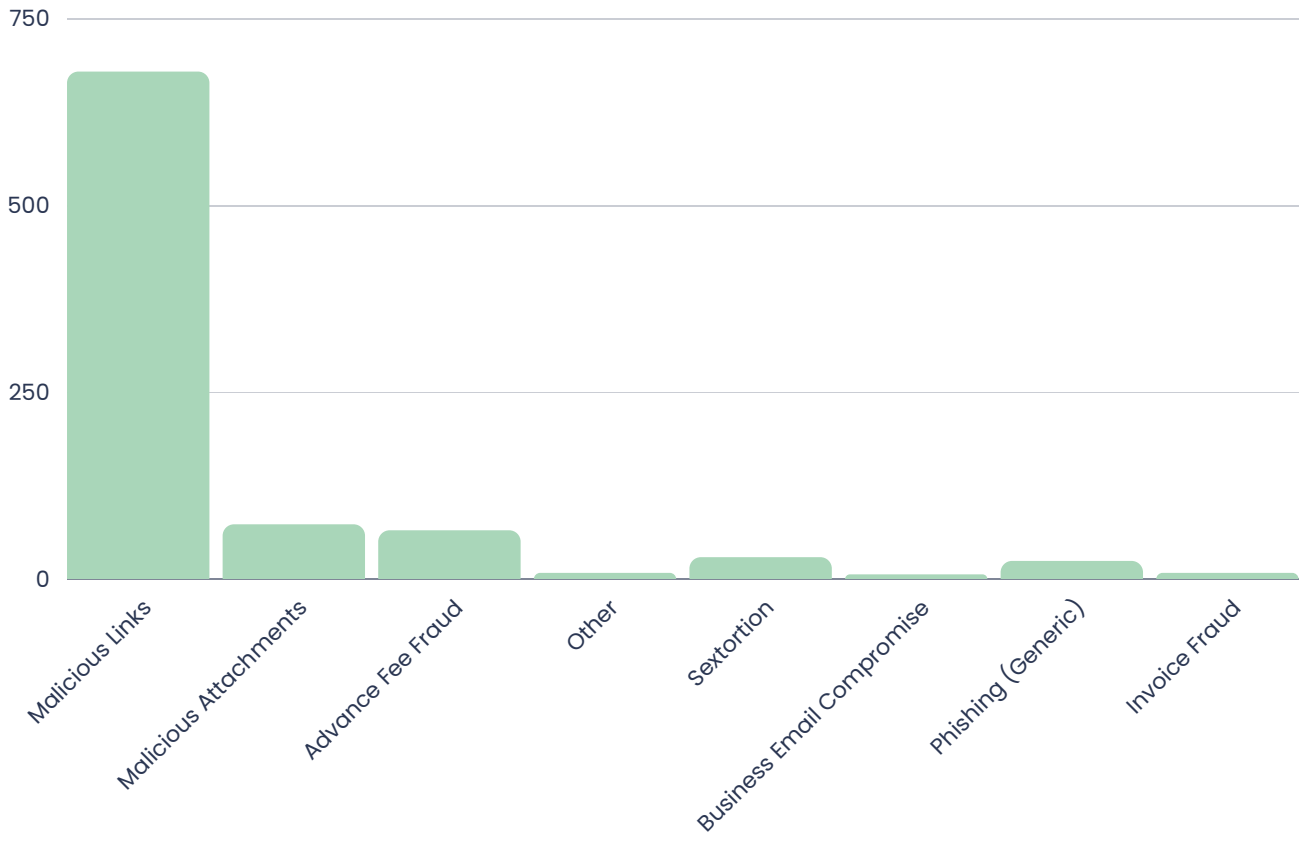
in July & August

Detail

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

Top 5 Phishing Scams Imitating Popular Services:

1. Parcel Delivery
2. Manx.net
3. Anti-virus software
4. Amazon
5. Retail Stores



CYBER CONCERNS

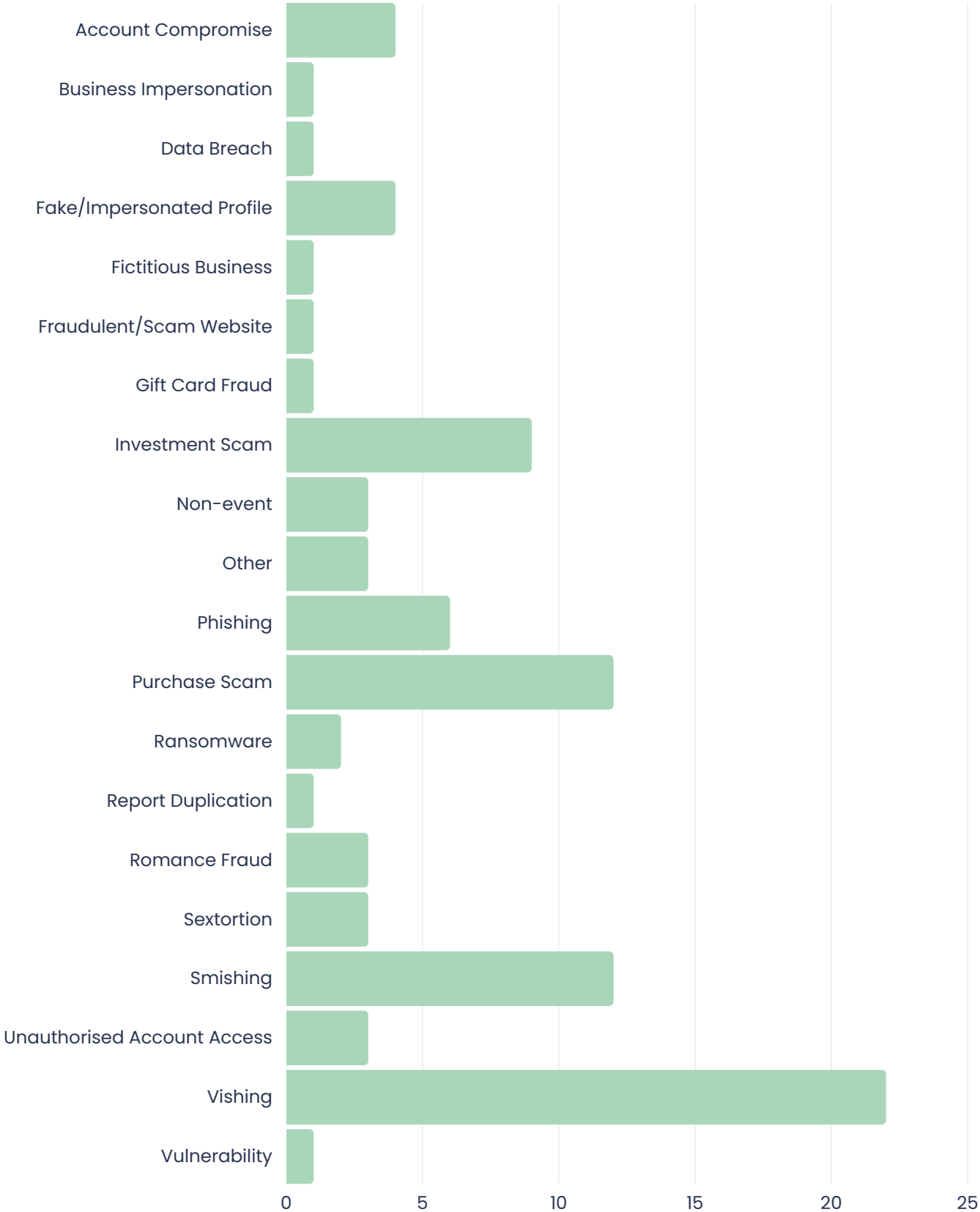
93 REPORTED

in July and August

Detail

The chart (on page 4) shows a breakdown of cyber concerns reported to us over July and August. Smishing and Vishing are once again the most widely reported forms of scams, however, we've seen a significant increase in the number of investments scams (as a percentage of total reported scams).

Cyber Concerns May & June



ISLE OF MAN THREAT COMMENTARY

BUSINESS IMPERSONATION

FALSE HOLDING COMPANY

In the period, we received a report about a local company, GEL Holdings Limited, that was falsely listed as the operating company behind the scam investment website, protradingai.com. The website, who had been taking investors' money and not returning funds, used the name of the company to add legitimacy to their criminal operations.

Before reporting to us, the website was reported to the Financial Services Authority (FSA) which published a public warning notice. After this, we were engaged and a report was received to our office, detailing the real life impacts this business impersonation was having.

We took action to contact the National Cyber Security Centre (NCSC) as well as contacting to the webhost and domain registrar providing evidence, where appropriate. From this, we were able to have the website quickly taken down.

INVESTMENT SCAMS

CRYPTOCURRENCY

Investments, in particular cryptocurrency scams, continue to be highly problematic. The cost-of-living crisis together with false promises of quick financial returns makes it easier for criminals to prey on people who are looking for extra income. We've received a number of reports on crypto scams over the period. These frauds typically start with the victim contacting the criminals after seeing adverts or posts on social media promising significant returns on small investments.

Once the victims reach out to the criminals, they are then assigned a so-called broker who will manage their initial investment. From here techniques vary, some scam-brokers encourage victims to register an account on a legitimate-looking website and deposit money, whilst others encourage victims to download additional software, with some even going as far as to get victims to download remote access software such as Anydesk and then install 'bespoke trading software' on the victim's behalf.

From this, victims are then shown a dashboard when significant gains from their investment. From reports received at OCSIA, we have observed the following patterns of these scams:

- The victim wishes to withdraw but is informed they must invest more before doing so.
- Alternatively, to dissuade the request, the victim is told that fees would be applied for any withdrawal;
- The victim is harassed by phone calls, cajoling the victim to invest more whilst dispelling any doubt about the scheme's legitimacy.

The majority of cases always involve significant dialogue between the broker and victim, this is to maximise the amount of money the criminals receive before the victim realises that this is a scam.

Any notification of significant gains, particularly coming from a broker or software should be taken with a pinch of salt. As with any exchange of money online, we recommend that residents undertake research before making any form of payment.

ACCOUNT COMPROMISE

LOCAL ESTATE AGENT

During the period we received a report of a local estate agent who had a breach of their business email account. From this, correspondence with customers was 'hijacked' and requests for additional payments were sent out. In this case the criminals attempted to make the correspondence seem legitimate using a technique called 'email chain hijacking'. The criminal uses genuine email correspondence and inserts their phishing email into the conversation.

Fortunately, no customers made payment or lost money. The estate agent contacted their technology provider who secured the account and placed enhanced-security protections such as multi-factor authentication on the account. Bank details were passed on to the police and to the Financial Intelligence Unit (FIU) for further action.

Business email account compromise presents a significant risk, not only to customers and the potential for the loss of funds, but also as a reputational risk. With access to an email account, customers will reasonably assume that they are communicating directly with the legitimate business. In this case, the prompt action of the affected company likely saved customers from being scammed.

Th CSC strongly recommends use of MFA to protect business information on devices, especially those used in a mobile or remote situation.

RANSOMWARE

We were made aware of a local company which was hit by a ransomware attack. The attack, which happened in August, utilised the well-known Lockbit ransomware and has had an impact on the company's operations and its customers with the cyber criminals asking for a significant, six-figure payment to restore services.

OCSIA were advised of the situation and have offered help and support, and with guidance on incident management considerations for the affected organisation.

We treat all reports in the strictest of confidence and therefore any information that may be potentially identifiable has been removed.

VISHING

This month saw vishing as the most reported threat, with just under a quarter of reports in the period being this common scam method. Some of the vishing calls reported to us include:

- Diesel Emission scam
- IOM Gas scam call
- Energy for Life scam call
- Debt Collection
- HSBC 'Fraud Squad'
- Timeshare scam calls
- HM Inland Revenue
- Sky

In a number of cases, recipients of these calls have ignored warnings shown on their phone advising them that the call is a possible scam. Whilst never full-proof, messages such as these should be taken seriously and appear because the caller is using a number widely reported for scams. This is why scammers often resort to spoofing a number, concealing its real identity to mask the fact they are make hundreds of scam calls per day.

From the list above, it is evident scammers are using current affairs and popular news stories to add legitimacy to their calls. Whilst slightly outdated, the diesel emissions scam relies on recipients having seen the news about Volkswagens forged emissions results, and the resulting compensation to those who were mis sold vehicles.

Vishing is still widely used, and is a highly effective method of targeting the more vulnerable members of society, who may be spending more time home alone without the guidance of someone who may be more aware of these types of scams.

THREAT FEATURE:
QUISHING

Quick-response codes, often known as QR codes, are square barcodes easily readable by mobile device cameras. These codes have been in widespread use since the year 2000, and their popularity has surged, especially with the advent of smartphones. Nowadays, QR codes are nearly everywhere, offering a quick and efficient way to access websites, make phone calls, send text messages, or even facilitate digital payments.

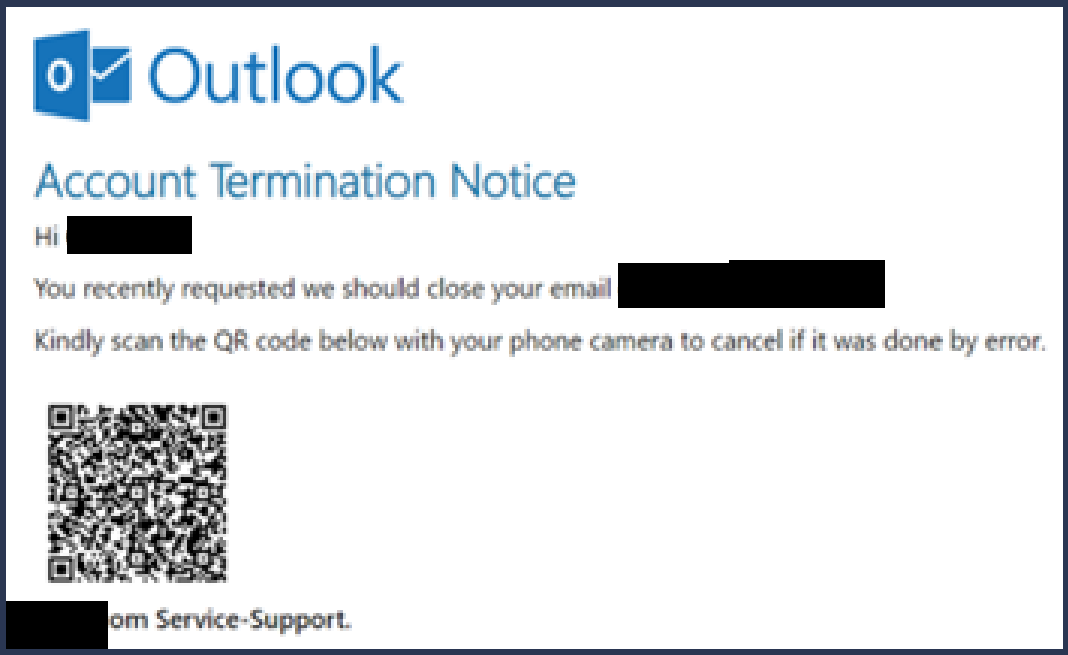
However, as with many technological advancements, there's a darker side to this convenience. With the increase in legitimate organisations using QR codes for low-contact transactions, especially during the COVID-19 pandemic, a novel threat has emerged: Quishing.

At its core, quishing is a type of social engineering attack whereby cybercriminals trick users into scanning deceptive QR codes. These codes then redirect the unsuspecting victim to fraudulent websites that may download malware or solicit sensitive information. Such an attack mechanism is comparable to traditional phishing, where attackers use poisoned attachments or misleading links. The difference with quishing is the bait: a QR code leading victims directly to their malicious trap.One of the fundamental features of QR codes is that they obscure the destination URL. Attackers capitalise on this by making it hard for users to recognise they're being redirected to a malicious website until it's too late.

But it's essential to remember that, while QR codes offer a convenient gateway to the digital world, they also open potential doors for scammers. When used responsibly, they can simplify our lives. Yet, when tampered with these same codes can become a tool for exploitation. As with any technological tool, it's crucial to approach QR codes with a balance of trust and caution.

Cyber-criminals use various tactics to deceive their targets. Here are some of the most common quishing techniques:

- Cyber-criminals often pair their malicious QR codes with compelling stories or urgent messages. For instance, a QR code might be accompanied by a message claiming the user has won a prize and needs to scan the code to claim it.
- Scammers can send emails to promote fake events, workshops, or webinars, luring victims with a QR code to scan for a ticket or an exclusive pass. Scanning the code can lead to malicious sites that solicit payment or personal information.
- Businesses often ask customers to scan QR codes to provide feedback or complete a survey. Attackers can mimic this approach, leading victims to fake feedback forms that capture personal information or credentials.
- Quishing campaigns might direct victims to counterfeit login pages of popular services (like email, banking, or social media). Once users input their login details, attackers can capture these credentials for unauthorised access or other malicious activities.



Example of quishing email courtesy of Kurt Schrauwen, Director at Riela Group

EXTERNAL THREAT COMMENTARY

MAJOR US ENERGY FIRM TARGETED IN INNOVATIVE QR CODE PHISHING CAMPAIGN

In August, a notable American energy corporation fell victim to a phishing scheme employing QR codes as a vehicle for delivering harmful emails and side-stepping security safeguards. Out of the 1,000 emails exposed in this operation, nearly a third were directed at the energy company, while various other sectors including manufacturing, insurance, technology, and financial services also experienced targeting. The cybersecurity company Cofense, which detected the campaign, refrains from disclosing the precise identity of the targeted energy firm but characterises it as a prominent U.S.-based entity.

The attackers dispatched phishing emails instructing recipients to update their Microsoft 365 account configurations by scanning a QR code attached either as a PNG or PDF file. To instill a sense of urgency, these emails stipulated that the task had to be completed within a span of 2-3 days. This innovative tactic allowed the attackers to circumvent email security tools typically employed to scan messages for known malicious links.

Although QR codes have featured in previous phishing endeavours, this marks the first instance of their widespread use, suggesting that cybercriminals may be gauging their effectiveness as an attack vector. Despite their capacity to bypass security measures, QR codes necessitate the victim's active engagement, a crucial mitigating factor for well-trained personnel. Most contemporary smartphones prompt users to verify the destination URL before launching the browser, thereby adding an additional layer of protection. Cofense recommends that organisations incorporate image recognition tools into their phishing defence strategies, although it is important to note that these tools may not guarantee the detection of all QR code-related threats.

As underscored in our Threat Focus, the incorporation of QR codes into phishing campaigns poses a growing hazard to both the general public and organisations alike. Previously, scammers have employed QR codes to redirect individuals to malicious websites with the intention of stealing finances or personal data. In January 2022, the FBI cautioned that cybercriminals were increasingly using QR codes to steal credentials and financial information. Given the persistent innovation by cybercriminals and their ongoing exploration of new technological exploits, it is imperative for individuals and organisations to maintain a high-level of vigilance, educate their personnel, and implement robust security measures to counteract these ever-evolving threats.

INTERNATIONAL OPERATION 'DUCK HUNT' DISMANTLES QAKBOT MALWARE INFRASTRUCTURE

In August, an extensive multinational operation, meticulously coordinated by international law enforcement agencies led by Europol and the FBI, has achieved the successful dismantling of the Qakbot malware infrastructure and the confiscation of nearly €8 million worth of cryptocurrencies. This collaborative operation enlisted the participation of law enforcement and judicial authorities hailing from several nations, including but not limited to France, Germany, Latvia, the Netherlands, Romania, the United Kingdom, and the United States. Qakbot, which also goes by aliases like QBot or Pinkslipbot, was a malevolent software tool operated by a network of organised cybercriminals with global reach. Its primary objectives encompassed targeting critical infrastructure and businesses across the globe, with a track record of activities such as stealing financial data and login credentials, and engaging in activities like ransomware attacks, fraud, and various other forms of cybercrime.

Qakbot had been in operation since 2007, infecting upwards of 700,000 computer systems worldwide. Its mode of infiltration frequently involved the dissemination of malicious attachments or hyperlinks within spam emails, which facilitated secondary infections with additional malicious payloads like ransomware. This turned the compromised computers into unwitting components of a botnet under the control of the cybercriminal group. The principal focus of this malware was the extraction of financial data and login credentials from web browsers. Multiple ransomware collectives deployed Qakbot to execute ransomware campaigns against critical infrastructure and corporate entities. The operators of the botnet offered access to the compromised networks to interested parties for a fee, amassing nearly €54 million in ransom payments between October 2021 and April 2023.

Termed 'Duck Hunt,' this extensive operation was spearheaded by the FBI and entailed collaboration with numerous international partner agencies.

As part of the operation, the FBI managed to infiltrate segments of the botnet's infrastructure, including a computer employed by a Qakbot administrator, and redirected Qakbot traffic toward servers under the agency's control. This strategic manoeuvre granted the FBI the necessary access to deploy an uninstaller on infected devices worldwide, effectively eradicating the infection and pre-empting further deployment of malicious payloads. To aid in the restoration process, the FBI also reached out to victims by utilising IP addresses and routing data gleaned from their computers during the removal tool's deployment.

Consequently, the operation culminated in the seizure of nearly $9 million worth of cryptocurrency from the Qakbot cybercriminal organisation. These seized assets will subsequently be allocated to benefit the victims, as articulated by U.S. Attorney Martin Estrada. This operation bears resemblance to a previous action in May, when cybersecurity and intelligence agencies representing all member nations of the Five Eyes alliance collaborated to dismantle the Snake peer-to-peer botnet, which was operated by Russia's Federal Security Service (FSB) and linked to the notorious Turla hacking group.

SURGE IN LINKEDIN ACCOUNT HACKS LEAVES USERS LOCKED OUT AND RANSOMED

In August, an increase in security issues has been observed among users of a popular professional networking platform, with reported incidents of account breaches leading to lockouts and unauthorised takeovers. These findings have been reported by a cybersecurity entity operating under the alias Cyberint. Over the past several months, there has been a remarkable 5,000% increase in searches on Google Trends for phrases such as 'LinkedIn account compromised' and 'LinkedIn account retrieval,' indicating the prevalence of this issue. A concerning aspect is that numerous victims have struggled to find resolution through the official LinkedIn support channels, with some resorting to paying a ransom in exchange for regaining control over their compromised accounts.

The attackers responsible for these breaches employ various tactics, including the use of leaked login credentials and brute force techniques to gain unauthorised access to accounts. Once inside, they rapidly modify associated email addresses and passwords, occasionally setting up two-factor authentication (2FA) to heighten the complexity of account recovery. Disturbingly, certain victims have received extortion messages, while others have seen their accounts obliterated altogether.

Experts researching this situation speculate that the perpetrators have ulterior motives, such as engaging in social engineering, phishing endeavours, blackmail, data harvesting, or the dissemination of harmful content through the compromised accounts. To reduce the risk of falling prey to these attacks, users are strongly advised to regularly monitor their account access, be vigilant for notifications from the platform regarding changes to the primary email address linked to their account, employ robust and unique passwords, and activate 2FA (abbreviated as two-factor authentication) for an added layer of security. Despite the widespread nature of this issue, the platform in question has yet to issue an official statement or response addressing the matter.

OPENAI CREDENTIALS TARGETED BY CYBERCRIMINALS FOR SOPHISTICATED PHISHING ATTACKS

Cybercriminals are increasingly targeting OpenAI credentials to create convincing phishing emails and gain access to confidential information. Threat actors have shown a growing interest in generative artificial intelligence tools, as evidenced by the sale of hundreds of thousands of OpenAI credentials on the dark web and the creation of a malicious alternative to ChatGPT, called WormGPT. This malicious tool, can generate strategically cunning and persuasive messages, enabling even less-skilled attackers to conduct phishing and business email compromise (BEC) attacks.

Security researchers have discovered over 200,000 compromised OpenAI credentials on the dark web, which could allow buyers to access premium features of ChatGPT and confidential information such as trade secrets, source code, and business plans. These credentials were stolen using various malware variants and traded on dark web marketplaces. OpenAI clarified that the compromised credentials were not due to a data breach but were harvested by way of commodity malware-based log harvesting.

Experts warn that with access to compromised OpenAI credentials, cybercriminals can create hyper-customised phishing scams and execute cyber-attacks at scale. Therefore, it is crucial for individuals and companies to take necessary precautions to protect their information and systems from such emerging threats. Businesses and organisations are recommended to train employees to verify urgent messages, especially those involving financial queries or transactions, and to improve email verification processes.

UK ELECTORAL COMMISSION HIT BY CYBER-ATTACK THAT EXPOSES 40 MILLION VOTERS' DATA

In early August, UK Electoral Commission publicly apologised after revealing that it was targeted by a sophisticated cyber-attack that may have affected the data of around 40 million voters. The breach, discovered last October but only recently disclosed to the public, involved unauthorised access to copies of electoral registers, emails, and control systems. The commission, unable to confirm which files were accessed, noted that the data held did not present a high risk to individuals, but it could potentially be combined with other public information for profiling.

Despite confidence that the cyber-attack did not affect any elections or registration statuses, concerns about the integrity of the UK's electoral system have been raised. Officials stated that the delay in public disclosure was necessary to remove the hackers' access, assess the incident, liaise with cybersecurity agencies, and implement additional security measures. Shaun McNally, the commission's CEO, expressed regret for the lack of sufficient protections and assured that significant steps had been taken to enhance the security and reliability of their IT systems.

The Information Commissioner's Office (ICO) is urgently investigating the incident, while security experts and politicians call for a thorough investigation to understand the motives behind the attack and to strengthen the cyber-resilience of the electoral system. This incident highlights the ongoing challenges faced by organisations in safeguarding sensitive data and maintaining public trust in democratic processes.

This breach was discover at the same time as a number of other high-profile incidents. With the Metropolitan police being subject to a third-party supply chain attack, as well as data breaches for both PSNI, and the loss of data by West Yorkshire Constabulary.

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

CYBERISLE 2023

The full programme for this year's cybersecurity conference is now available online. On the day there will be 16 panels and presentations including 'Apollo 13 and the art of cybersecurity', 'Minds and Machines', and '5 things your small business can do to stay secure'.

Now in its 5th year, the conference will feature speakers from a wide range of organisations from the Isle of Man, Jersey, and the UK.
The presentations cover practical advice for small businesses, Artificial Intelligence, and deception techniques used by criminals.

Speakers include Martin Smith MBE (Chairman and Founder of Security Awareness Special Interest Group), a representative from the UK National Cyber Security Centre, Dave Cartwright (Chief Information Security Officer CISO and Head of IT Risk and Operations at Santander International).

Lee Williamson (CISO, EIP Limited) will also be part of the conference, as will Dr Francis Gaffney (Senior Director at Mimecast), Peter Allwright (Head of Suntera Forensics) and Kurt Schrauwen (Director at Riela Group).

The event is free to attend, with tickets and the full agenda available on the CYBERISLE website.

Networking Dinner

Join us for an exciting evening of networking and delicious food at the CYBERISLE Networking Dinner! This in-person event will take place on Tuesday 3rd of October 2023 at 7pm.

A three-course meal with wine will complement presentations by Martin Smith MBE of The Security Awareness Special Interest Group (SASIG) and a representative from the National Cyber Security Centre (NCSC).

The dress code for the dinner is business attire, with individual tickets or tables of 10 available for purchase. Welcome glasses of prosecco and orange juice will be served with the meal starting at 7:30pm. Tickets are available here.

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

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