Specialised
Security Services

# PROJECT:
# QUISHING SCAMS

*The digital landscape constantly evolves, offering both convenience and new opportunities for individuals and businesses alike. With the proliferation of online activities, the emergence of new online scams has become a byproduct of this digital age.*

*As technology advances, so do the tactics of cybercriminals, who are quick to adapt and find innovative ways to exploit unsuspecting individuals. This ever-evolving landscape of online scams presents a pressing concern in today's interconnected world, as it poses threats to personal information, financial security, and overall online trust.*

*SSS addresses some of the most recent and prevalent online scams that have surfaced, shedding light on the techniques, motives, and consequences associated with these deceptive practices. Understanding these emerging scams is essential in safeguarding oneself against potential digital threats and ensuring a safer online experience.*

---

## QUISHING - QR CODE PHISHING EXPLAINED:

- Have you ever received an email urging you to scan a QR code for a Black Friday offer, only to find yourself caught in a phishing scam?
- This deceptive tactic, known as "quishing," combines QR codes and phishing to lure individuals into compromising their personal data or infecting their devices with malware.

---

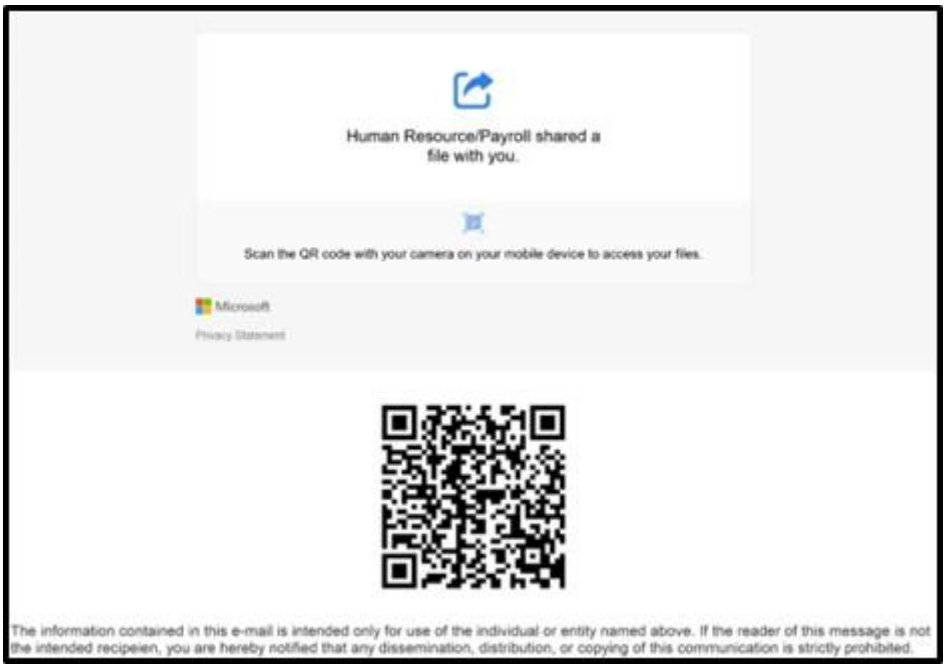
## UNDERSTANDING QUISHING:

- While the term "quishing" might not sound bad, it is a serious threat.
- This hybrid of "QR code" and "phishing" refers to the act of scamming.

---

## WHAT DOES A QUISHING HACK LOOK LIKE:

- Similar to conventional phishing emails, a quishing email is meticulously crafted to deceive recipients into becoming victims of a scam.
- These scammers aim to steal sensitive information, such as passwords or personal data, or to compromise your device with malware.
- The deceptive email often impersonates trusted senders like banks or reputable e-commerce platforms.
- It creates a sense of urgency by claiming a payment issue or a limited time offer necessitating immediate action.
- However, instead of a clickable link, a quishing email includes a QR code that recipients are instructed to scan.




---

## CONSEQUENCES OF SCANNING A QR CODE:

In a quishing email, the QR code is like a malicious link. Scanning it can lead to several adverse outcomes.

- Redirection to a phishing website.
    - Scammers can expertly mimic the appearance of legitimate organisations' websites, tricking users into entering personal information like addresses, telephone numbers, credit card details, and banking PINs.
    - This information is then exploited for financial fraud or identity theft.
- Infecting your Device with malware.

    - Scanning the QR code may automatically initiate a download, potentially containing malware, ransomware, spyware, and more.
- Stealing your Login Data
    - The QR code may present a counterfeit login window requesting your username and password.
    - For example, a quishing email might claim there's an issue with an Amazon delivery and prompt you to scan the QR code to log in.
    - Falling for this exposes your login details and allows the scammer to access your account.

---

## WHY CRIMINALS ARE TURNING TO QUISHING:

2023 shows a spike in quishing and QR code fraud as cybercriminals find new ways to exploit this technique.

- Evading awareness:
    - Most individuals are now cautious about clicking on suspicious email links and can identify safe URLs.
    - However, QR code scams are less familiar, making it easier to deceive people.
- Evading security systems:
    - QR codes, often sent as image files, may not trigger security warnings. This facilitates their passage through digital security systems.
- Mobile device vulnerabilities:
    - Scanning the QR code typically involves using a mobile device, which may have weaker antivirus and anti-phishing protections compared to computers.

---

## SAFETY MEASURES:

To protect yourself from QR code phishing, consider these 5 essential steps.

- Never scan a QR code in an email from an unfamiliar sender.
- Familiarize yourself with the signs of phishing emails, such as a sense of urgency and sender address errors, and never click on links or scan QR codes if anything seems suspicious.
- Always check the URL preview when scanning a QR code on your phone.
    - Avoid unfamiliar or shortened links and watch for minor misspellings in familiar names.

- If a QR code takes you to a page requesting login credentials, refrain from entering them.
    - Visit the company's website directly in your browser or contact the business by phone.
- Follow security practices.
    - Use strong, unique passwords for all your online accounts and keep your devices and software current.

---

## QR CODE FRAUD BEYOND EMAILS:

- In the wake of the COVID pandemic, legitimate businesses have adopted QR codes for contactless transactions.
- This trend has made people more comfortable with scanning QR codes in public places.
- Unfortunately, scammers have exploited this by deploying fraudulent QR codes on parking meters and other locations to trick individuals.

---

*Remain vigilant, stay informed, and always exercise caution when faced with suspicious QR codes.*

---

*Visit our Facebook page and our website for related and other current projects:*

- https://www.facebook.com/MikeBolhuisOfficial
- http://www.mikebolhuis.co.za

---

*Specialised Security Services is proud to invite the public to our highly anticipated WhatsApp Channel.*

*This channel is important in delivering insights into the latest crime trends, awareness, warnings and the exposure of criminals.*

## HOW TO JOIN THE MIKE BOLHUIS WHATSAPP CHANNEL:

- Simply follow the link to our dedicated channel: https://whatsapp.com/channel/0029Va9cH3n0bIdvTstlCf0t
- Hit the "FOLLOW" button to ensure you never miss our daily updates.
- Tap on the "BELL" icon to receive instant notifications whenever a new post is placed.
- Please share this with family, friends and colleagues.

---

***ALL INFORMATION RECEIVED WITH REGARD TO THE PROJECTS WILL BE TREATED IN THE STRICTEST CONFIDENTIALITY AND EVERY IDENTITY WILL BE PROTECTED.***

---

***You may forward this document.***

Regards,

Mike Bolhuis
Specialist Investigators into
Serious Violent, Serious Economic Crimes & Serious Cybercrimes
PSIRA Reg. 1590364/421949
Mobile: +27 82 447 6116
E-mail: mike@mikebolhuis.co.za
Fax: 086 585 4924
Follow us on Facebook to view our projects -
https://www.facebook.com/MikeBolhuisOfficial

**EXTREMELY IMPORTANT:** All potential clients need to be aware that owing to the nature of our work as specialist investigators there are people who have been caught on the wrong side of the law - who are trying to discredit me - Mike Bolhuis and my organisation Specialised Security Services - to get themselves off the hook.

This retaliation happens on social media and creates doubt about our integrity

and ability. Doubt created on social media platforms is both unwarranted and untrue.

We strongly recommend that you make up your minds concerning me and our organisation only after considering all the factual information - to the exclusion of hearsay and assumptions.

Furthermore, you are welcome to address your concerns directly with me should you still be unsatisfied with your conclusions. While the internet provides a lot of valuable information, it is also a platform that distributes a lot of false information. The distribution of false information, fake news, slander and hate speech constitutes a crime that can be prosecuted by law. Your own research discretion and discernment are imperative when choosing what and what not to believe.

**STANDARD RULES APPLY:** Upon appointment, we require a formal mandate with detailed instructions. Please take note that should you not make use of our services – you may not under any circumstance use my name or the name of my organisation as a means to achieve whatever end.

**POPI ACT 4 of 2013 South Africa:** Mike Bolhuis' "Specialised Security Services" falls under Section 6 of the act. Read more here: https://mikebolhuis.co.za/popi-act-4-of-2013-section-6-mike-bolhuis/

---

**SSS TASK TEAM:**
https://mikebh.link/sss-task-team

**SSS CYBERCRIME UNIT:**
https://mikebh.link/sss-cyber-team

---

Specialised Security Services

---

crimes. So that you can inform and protect your loved ones and everyone you know.

**Our mailing address is:**
Mike Bolhuis Specialised Security Services
Po Box 15075 Lynn East
Pretoria, Gauteng 0039
South Africa
Add us to your address book



---