



**SPECIALISED
SECURITY SERVICES
MIKE BOLHUIS**



**PROJECT:
KNOCKS AND SCAMS
WARNING!**

As soon as people are educated regarding the latest knocks and scams, the perpetrators of these crimes think of new and more advanced ways to profit from unsuspecting victims.

Here are some of the more recent knocks and scams.



PHISHING TECHNIQUES:

- Embedding a link in an email that redirects an unsuspecting victim to an unsecure website that requests sensitive information
- Installing a Trojan via a malicious email attachment or ad which will allow the intruder to exploit loopholes and obtain sensitive information
- Spoofing the sender address in an email to appear as a reputable source and request sensitive information
- Attempting to obtain company information over the phone by impersonating a known company employee.

And there are three main categories of phishing, these are:

SPEAR PHISHING:

- Phishing attacks that are targeted at specific individuals, companies or organisations are known as spear phishing.
- Cyber criminals who conduct these attacks usually spend time gathering and using the personal information about their targets to increase the probability of success.
- It is often intended to steal data for malicious purposes and cybercriminals may also intend to install malware on a targeted user's computer.

CLONE PHISHING:

- A more sophisticated type of phishing, this method is more difficult to identify and often tricks users into believing an email is legitimate.
- In clone phishing, an email is a clone of an email which has been previously delivered, this way, the victim is less likely to be suspicious of the email because it appears to be coming from a real sender.

WHALING:

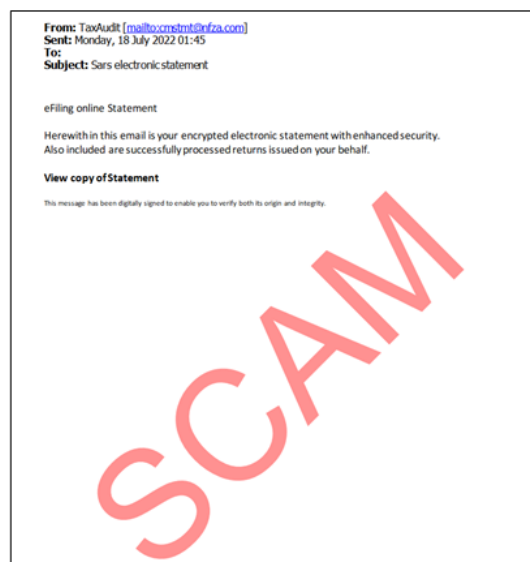
- Whaling is a form where the attacks are directed specifically at individuals who are in positions of power, high profile people, senior executives, etc.

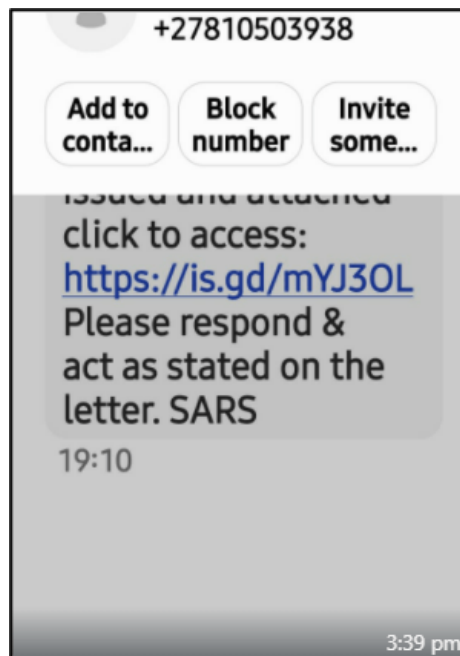
- In the case of whaling, the content of the malicious emails will be tailored to target an upper manager or person of interest.
- The content will usually include things that are more likely to get their attention such as subpoenas or complaints.

EXAMPLES

SARS:

- SARS are warning the public against spoofing or false emails, asking for taxpayers' personal details, bank details, tax details and eFiling information.
- Email addresses used are meant to look similar to those of SARS email addresses.
- Be on the lookout for:
 - returns@sars.co.za.
 - refunds@sars.co.za.
- Such misleading email addresses might have unsuspecting victims think that they are eligible to receive tax refunds.
- These emails contain dangerous links to false forms and fake websites created to look like the actual and verified SARS documents and website.





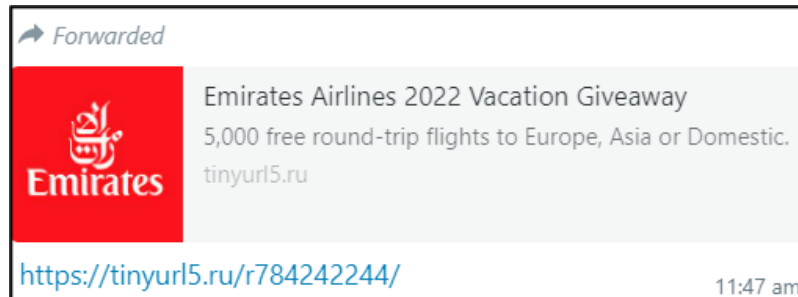
GENERAL SAFETY AND PREVENTATIVE INSTRUCTIONS:

- Do not open or respond to emails from unknown sources.
- Beware of emails that ask for personal, tax, banking and eFiling details (login credentials, passwords, pins, credit/debit card information, etc.).
- Legitimate organisations such as major banks, corporates or SARS will never request personal banking details in any communication that you receive via post, email, or SMS.
- They might however, for the purpose of telephonic engagement and authentication purposes, verify your personal details (name, date of birth, address, etc but *never* passwords or bank details.)
- Importantly, they will not send you any hyperlinks to other websites.
- Beware of false SMSs.

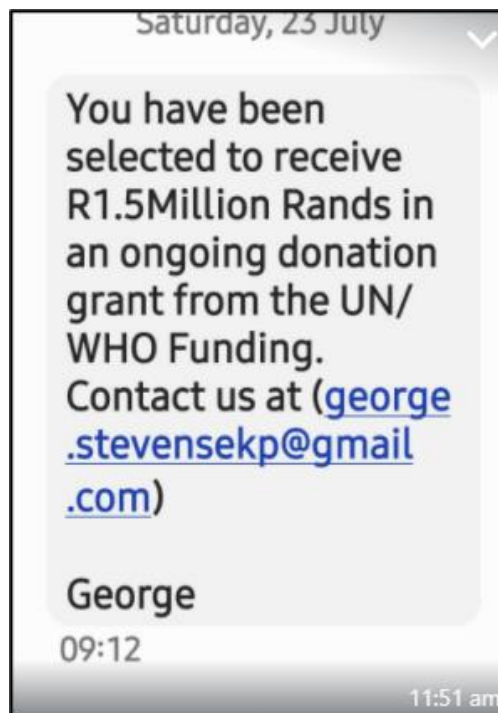
- They will not send *.htm or *.html attachments.
- They will never ask for credit card details.

MORE EXAMPLES TO OTHER PHISHING SCAMS TO BE AWARE OF:

1.

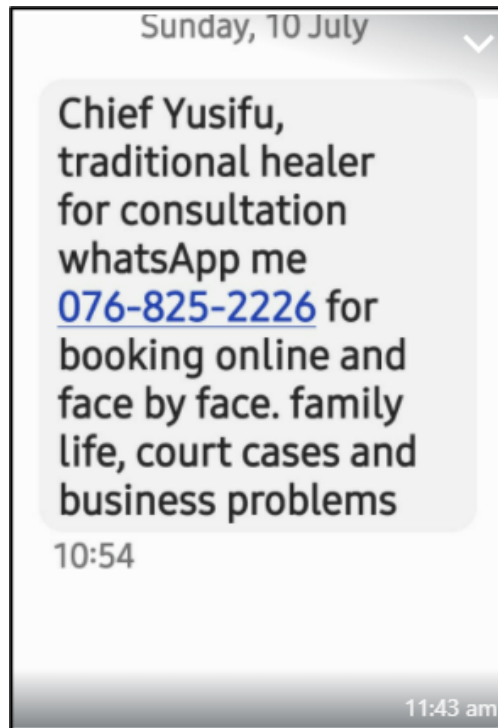


2.

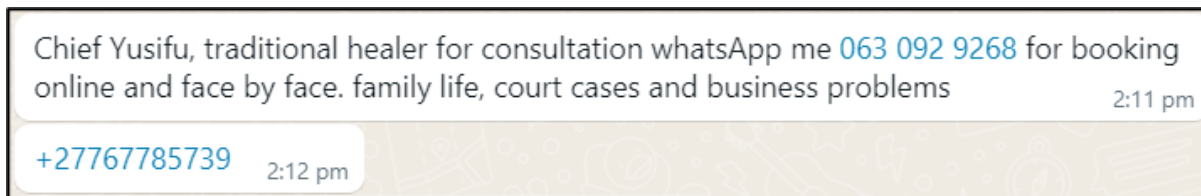


- The number from where this message was sent: +27 76 357 2352.

3.

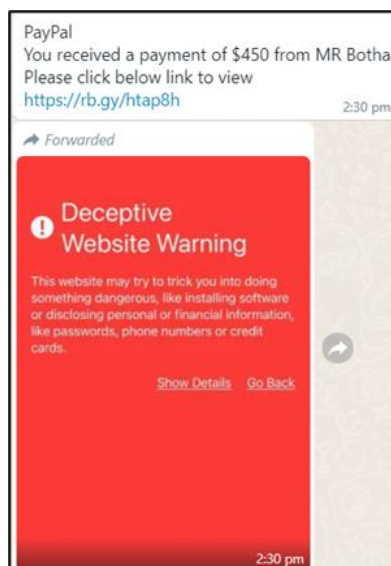


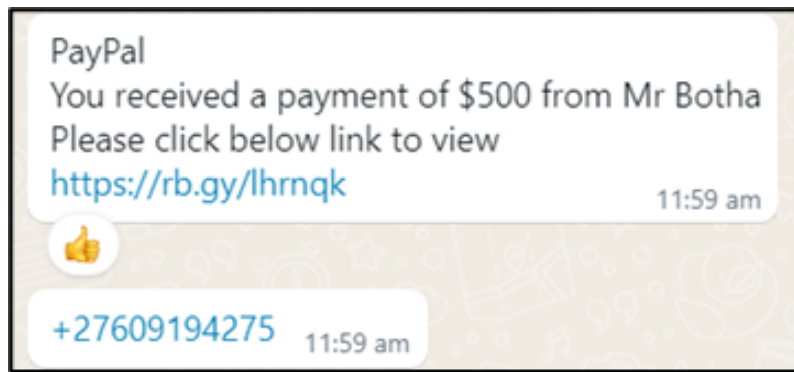
- The number from which this message was sent: +27 81 844 5006.



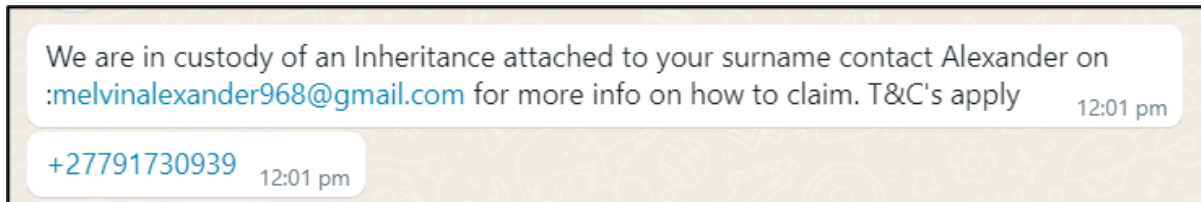
- Another number used: +27 76 778 5739.

4.

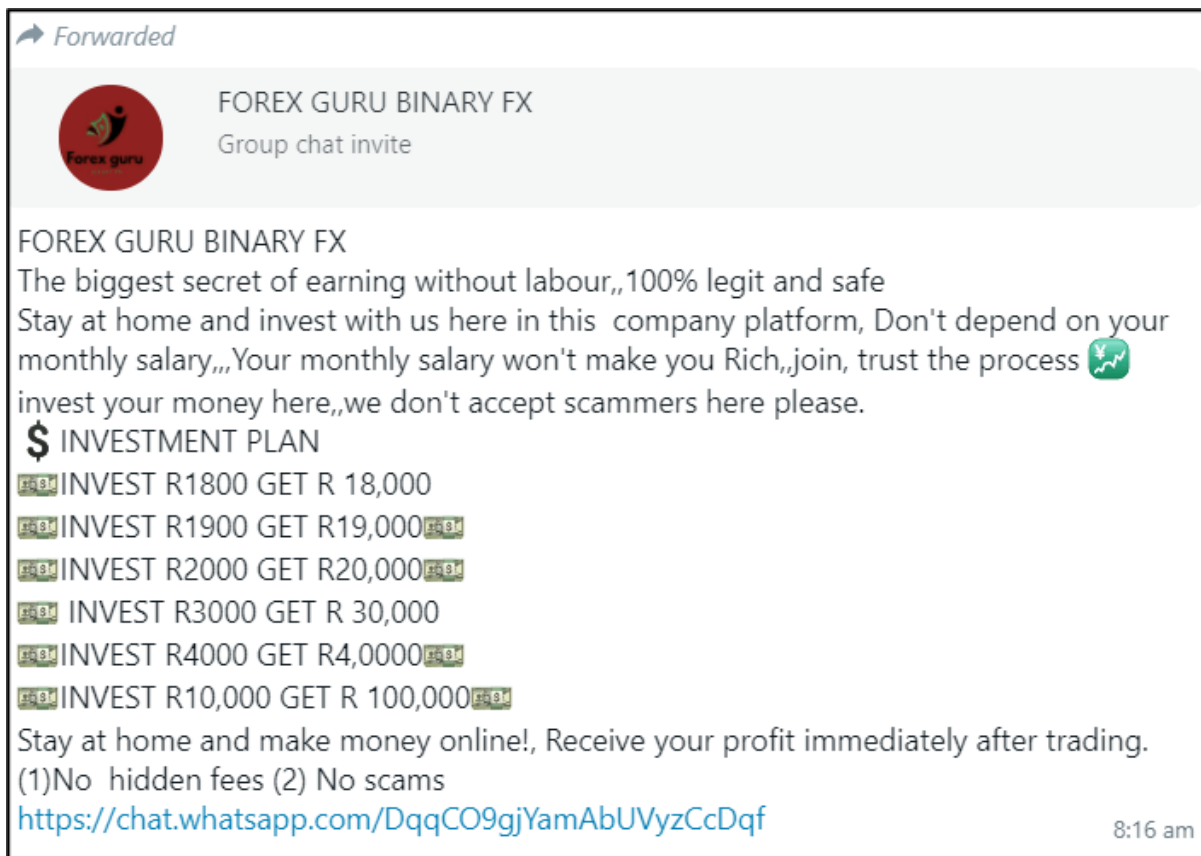




5.



6.



ANTI-PHISHING TECHNIQUES:

NEVER CLICK ON ANY SUSPICIOUS LINKS:

- Most phishing scams are successful because the emails contain very convincing links.
- The scam emails motivate people to act by impersonating institutions and threatening to close down important accounts because of inactivity.
- If you get one of these emails, don't click on the links provided in the emails.
- Instead, it is recommended that a user opens up a tab in your browser and types in the domain name him or herself.
- Once logged in, a user can then check to see if the request is authentic.
- If it is, they can take action on the legitimate website.

NEVER OPEN UNKNOWN FILES OR ATTACHMENTS:

- Opening malware files is how computer systems and networks can get infected.
- It is important to double check the attachments and files that you are receiving from emails.
- Some emails automatically send infected emails to your spam folder or delete them entirely, but it can be the case that an email bypasses that filter and ends up in your inbox.

USE A REPUTABLE ISP (INTERNET SERVICE PROVIDER):

- Implement strong anti-spam and anti-phishing technologies and policies.
- Users can check with their respective ISPs for more information about the anti-spam and anti-phishing services that are available.

SOFTWARE:

- Keep all your software and applications up to date, including your anti-virus software.
 - Updates keep you safe from known security vulnerabilities which hackers exploit for their malicious intents.
-

Education and awareness are one of the best lines of defence against cybercrime and especially phishing.

Never believe, act or click on a link unless you are absolutely convinced that you have done the necessary vetting to ensure its validity.

*Always remember:
if it seems as if it is too good to be true, it usually is.*

**IF YOU ARE UNSURE IN ANY WAY, CONTACT OUR
SPECIALIST CYBERCRIME INVESTIGATOR,
MR DEWALDT HUYSAMEN FOR MORE INFORMATION:**

Contact number: +27 61 800 0020

Email address: dewaldt@mikebolhuis.co.za

**CONTACT MR MIKE BOLHUIS FOR ADVICE,
RECOMMENDATIONS, SECURITY, PROTECTION
OR AN INVESTIGATION IF NEEDED.**

**ALL INFORMATION WILL BE TREATED WITH THE UTMOST
PRIVACY AND CONFIDENTIALITY.**

FORWARD THIS DOCUMENT TO EVERYBODY.

Regards,

Mike Bolhuis

Specialist Investigators into

Serious Violent & Serious Economic Crimes

PSIRA Reg. 1590364/421949

PSIRA Certificate: <https://mikebh.link/PSIRA>

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 to 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.

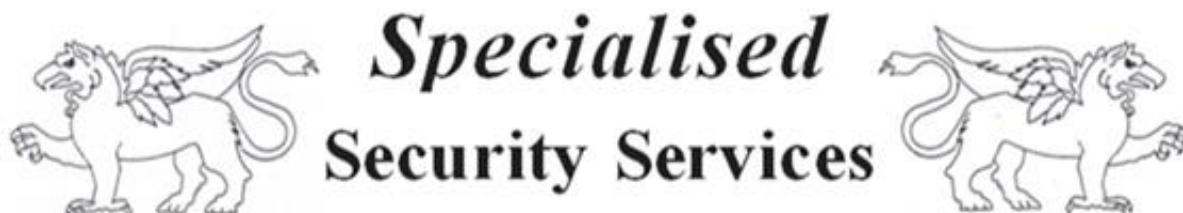
POPI ACT 4 of 2013 South Africa: Mike Bolhuis' "Specialised Security Services" falls under Section 6 of the act. Read more here: <https://mikebolhuis.co.za/popi-act-4-of-2013-section-6-mike-bolhuis/>

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.

SSS TASK TEAM:

<https://mikebh.link/taskteam>



You have received this email because you have subscribed to [Mike Bolhuis](#) as mike@mikebolhuis.co.za. If you no longer wish to receive emails please [unsubscribe](#).

[webversion](#) - [unsubscribe](#) - [update profile](#)

75 Wapad Leeuwfontein Roodeplaat Pretoria South Africa 0186

© 2022 Mike Bolhuis, All rights reserved.