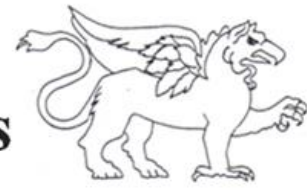




*Specialised*  
Security Services



---

## **PROJECT:** **HIGH-PROFILE** **IDENTITY THEFT**

---

*Identity theft is a pervasive and growing problem in today's digital age. It can have devastating consequences for individuals and organisations alike.*

*Even high-profile individuals can fall victim to identity theft, as illustrated by the case of Mr Mike Bolhuis, who recently discovered that his personal information was being used in fraudulent activities. This project explains that anyone is vulnerable to identity theft, especially if you have an impeccable name and reputation if you are a well-known celebrity/influencer or even an evangelist.*

*Mr Mike Bolhuis, an individual with extensive experience in cybersecurity, recently faced a disturbing situation when he learned that fraudsters were exploiting his identity.*

---

*His experienced cyber team promptly detected and responded to the issue, highlighting the importance of proactive measures in combating identity theft.*

---

**PLEASE READ OUR PREVIOUS PROJECTS FOR SIMILAR CASES AND WARNINGS:**

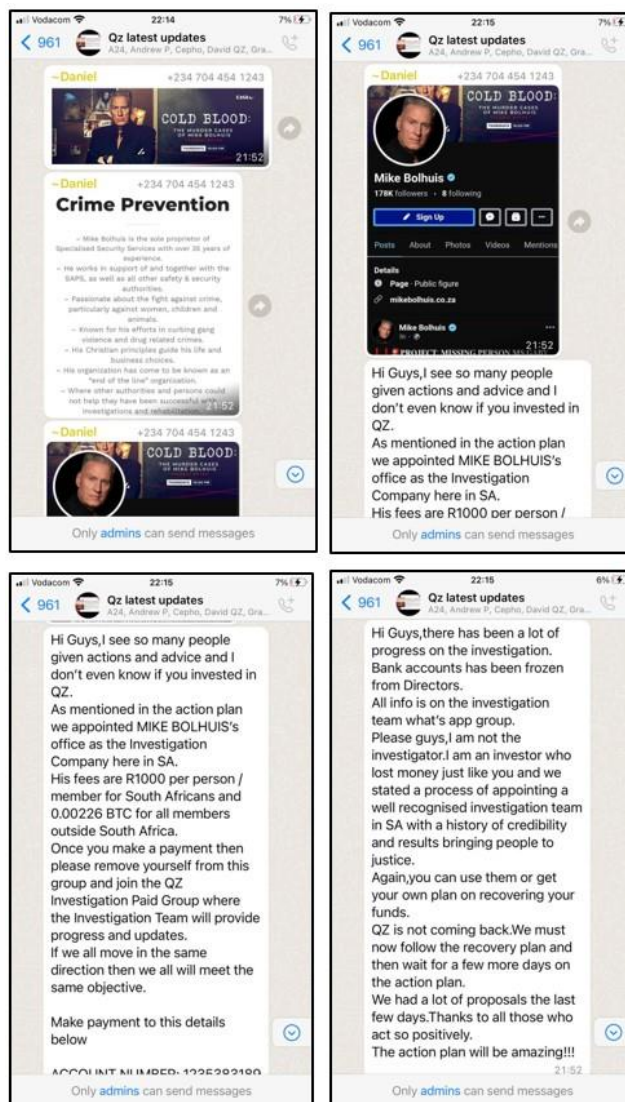
- <https://mikebh.link/HDZs6v>
  - <https://mikebh.link/ix1sEH>
  - <https://mikebh.link/dNC0ai>
  - <https://mikebh.link/Ebrh9Q>
  - <https://mikebh.link/e3yYgv>
  - <https://mikebh.link/ITSpXR>
- 

- On Tuesday 6 June 2023, Mr Bolhuis was contacted by Mr Joao Diamantino Pienaar, the head of Mr Bolhuis' SSS Johannesburg Cyber team.
  - Mr Pienaar informed Mr Bolhuis that his identity was being used to scam investors and victims in a Ponzi scheme conducted by QZ Asset Management.
  - The fraudsters had created a WhatsApp group, using Mr Bolhuis' company details - falsely linking his company to an unknown and new Capitec bank account.
  - Mr Bolhuis' experienced cyber team was quick to identify the suspicious activity.
  - They noticed discrepancies and inconsistencies in the information being used by the fraudsters.
  - Mr Pienaar, being well-versed in cyber investigations, immediately recognised the red flags and alerted Mr Bolhuis about the fraudulent scheme.
  - The team discovered that a WhatsApp group had been created with the fraudster acting as the group's administrator.
  - The scammer was using the name "Daniel" and an undisclosed second name, along with contact numbers +2348135173006 and +2347044541244, respectively.
  - Through their diligent efforts, Mr Bolhuis' cyber team was able to trace the fraudulent activities back to a Capitec bank account, account number 1235383189, under the name Constance Sindisiwe Mkhize.
  - Mr Bolhuis emphasised that he has never opened a Capitec account before and exclusively banks with Standard Bank.
  - His cyber team's swift action prevented further fraudulent activity and protected his reputation from being tarnished by the scam.
-

*Cases of high-profile identity theft are often sophisticated and challenging to detect. However, having an experienced and proactive cyber team can significantly enhance the chances of identifying and mitigating such threats.*


*Mr Bolhuis' case serves as a reminder of the importance of investing in cybersecurity measures and maintaining a vigilant approach to personal information protection.*

### WHATSAPP GROUP CREATED BY SCAMMERS:



- In recent weeks, Mr. Mike Bolhuis has gained significant attention in news articles and on television due to his new series titled "Cold Blood: The Murder Cases of Mike Bolhuis," which is currently airing nationally on DSTv.
- Unfortunately, scammers have taken advantage of Mr Bolhuis' public presence by using personal information to deceive unsuspecting members of the public.
- These scammers falsely portray themselves as representatives of a reputable investment, going so far as to claim that Mr Mike Bolhuis is involved with their organisation.
- It is crucial to emphasise that these claims are entirely false and devoid of any truth.
- In reality, Mr Bolhuis and his dedicated cyber team have been actively investigating QZ Asset Management and will soon unveil their findings, exposing the corrupt nature of this Ponzi Scheme.
- Stay tuned for more information on this upcoming project, as Mr Bolhuis and his team are determined to bring the truth to light and protect individuals from falling victim to fraudulent activities.

- If this was a legitimate endeavour initiated by Mr Bolhuis or SSS, the following would have been made clear:
  - The SSS Specialist Investigator's full and detailed credentials would have been used.
  - Each and every specialist investigator can be identified by their unique electronic business card, for example:



**Mike Bolhuis**  
 Mike Bolhuis, Pretoria, South Africa. 84,295 likes · 9,402 talking about this. Mike Bolhuis. Specialist Investigators into Serious Violent & Serious Economic Crimes.  
[www.facebook.com](http://www.facebook.com)

**SSS SPECIALIST INVESTIGATOR:**

Mr. Joao Diamantino Pienaar

Cybercrime Specialist Investigator  
 Track and Trace Expert  
 Ex SAPS Officer  
 Armed Response Expert

Mobile: 066 377 3301  
 E-mail: [jdpienaar@mikebolhuis.co.za](mailto:jdpienaar@mikebolhuis.co.za)  
 PSIRA REG: 792106

Facebook page: <https://www.facebook.com/mikebolhuisofficial>  
 Website: <https://mikebolhuis.co.za>  
 Tiktok: <https://vm.tiktok.com/ZSJSd4GGD/>  
 Instagram: <https://www.instagram.com/mikebolhuis/>  
 YouTube: <https://youtube.com/channel/UJCggRny7ADSvi7M4NaOLwhhg>

**!!! IMPORTANT – DISINFORMATION IS EXTREMELY DESTRUCTIVE !!!**

If you receive any information regarding Mr. Mike Bolhuis and or Specialised Security Services that causes you concern, contact Mr. Mike Bolhuis directly - to confirm whether the information is factual or not. Assumptions and hearsay information are NOT factual and must be examined to determine whether they are true or not.

**!!! RULES THAT APPLY !!!**

1. Upon appointment we require a formal mandate with detailed information and instructions.

- 
- The electronic business card of each specialist investigator will also show all of the criteria and the details of Mr Mike Bolhuis.
  - Each specialist investigator is verified and noted on our projects and on our official website.
  - Herewith is the link available confirming the appointed SSS Team Members: <https://mikebh.link/Task-Team-2023>
  - The bank details used by SSS will never be changed unless an official announcement is made by Mr Bolhuis personally or his Management Team.
  - SSS would never create a WhatsApp group requesting payments into any other account but our existing Standard Bank account.
  - If our organisation requests donations which is only on rare occasions, an official project will be posted on all our social media platforms.
  - If need be, the verified specialist investigator assigned to a case will be able to confirm banking details.

---

## **SAFETY MEASURES:**

To protect yourself from high-profile identity theft, consider implementing the following preventive measures:

- **Stay Informed:** Stay updated on the latest identity theft techniques and scams. Educate yourself and your team about best practices for online security and privacy.
  - **Employ Cybersecurity Measures:** Utilise robust security software, firewalls, and antivirus programs to protect your devices from malware and phishing attempts.
  - **Regularly Monitor Accounts:** Monitor your financial accounts, online presence, and credit reports for any unusual activity or unauthorized changes.
  - **Report any suspicious activity** to the relevant authorities and your financial institutions promptly.
  - **Educate Your Team:** Provide cybersecurity training to your employees or team members to enhance their awareness of potential threats and the importance of safeguarding sensitive information.
  - **Implement Multi-Factor Authentication (MFA):** Enable MFA for your online accounts wherever possible.
  - This adds an extra layer of security by requiring a second form of verification, such as a code sent to your mobile device, in addition to your password.
  - **Use Strong Passwords:** Create unique, complex passwords for each online account.
  - **Avoid using easily guessable information** and consider using a password manager to securely store.
-

## **IMPORTANT:**

- Financial institutions must take responsibility for thoroughly verifying account holders and conducting regular checks to ensure they remain in control of their accounts.
- It is crucial for banks to be proactive in flagging suspicious activities and freezing accounts once a police case is opened, proving that the account is being used for fraudulent purposes.
- This should not solely rely on requests from other banks, as it is a shared responsibility to protect innocent individuals from falling victim to identity theft.
- Email your bank/SSS a detailed account of the crime:
  - Document the incident and email all the relevant information to yourself.
  - This step ensures that you have a record of the events and the details surrounding the fraudulent activity.
- Contact your Bank:
  - Notify your bank immediately about the fraudulent transfer to the Capitec account.
  - Provide them with all the necessary information, including the Capitec account number and any other relevant details that you have discovered.
  - They will guide you on the steps to take and may initiate an investigation to recover any lost funds.
- File a Police Report:
  - Visit your local police station and open a case regarding the identity theft.
  - Provide them with all the evidence and information you have gathered.
  - This step helps initiate an official investigation and provides additional legal protection.

---

**IF YOU HAVE BEEN A VICTIM OF QZ ASSET  
MANAGEMENT OR ANY SIMILAR SCAM, CONTACT SSS'  
SPECIALIST CYBER INVESTIGATOR, MR JD PIENAAR:**

Contact number: +27 66 377 3301

Email address: [jdpienaar@mikebolhuis.co.za](mailto:jdpienaar@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  
Mobile: +27 82 447 6116  
E-mail: [mike@mikebolhuis.co.za](mailto: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/Task-Team-2023>

---



# *Specialised* Security Services



---

Copyright © 2023 Mike Bolhuis Specialised Security Services.  
All rights reserved.

You are receiving this email to inform and keep you up to date with violent and/or economic crimes. This is important to enable you to inform and protect your loved ones and everyone you know.

Our mailing address is:

[mike@mikebolhuis.co.za](mailto:mike@mikebolhuis.co.za)

Mike Bolhuis Specialised Security Services

Po Box 15075 Lynn East

Pretoria, Gauteng 0039

South Africa

Add us to your address book

Want to change how you receive these emails?

You can update your preferences or unsubscribe from this list.



---

This email was sent to [mike@mikebolhuis.co.za](mailto:mike@mikebolhuis.co.za)

[why did I get this?](#) [unsubscribe from this list](#) [update subscription preferences](#)

Mike Bolhuis Specialised Security Services · Plot 75 Leeuwfontein · Pretoria, Gauteng 0039 · South Africa