



PROJECT:

HACKING OF

MOBILE PHONES

Mobile phone hacking poses various risks, ranging from privacy invasion to financial loss and even potential harm.

POSSIBLE DANGERS:

- Data Theft:
 - Personal Information: Hackers may steal your personal information, including contacts, emails, photos, and documents.
 - Financial Data: Bank account details, credit card information, and payment app credentials are at risk.
- Identity Theft:
 - With access to personal information, hackers can impersonate you, leading to identity theft and potential fraud.
- Privacy Invasion:
 - Unauthorised access to your camera or microphone can compromise your privacy, leading to the recording of sensitive conversations or capturing intimate moments.
- Financial Loss:
 - Hackers may use your device to make unauthorized purchases or transactions, resulting in financial losses.
- Ransom Attacks:

- Some hackers may lock you out of your device and demand payment for its release, holding your data hostage.
 - Malicious Activities:
 - Hackers may use your device for illegal activities, such as distributing malware, participating in DDoS attacks, or engaging in cybercrime.
 - DDoS Attack means "Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.
 - Spyware and Tracking:
 - Malicious software can track your location, online activities, and communications, compromising your safety and security.
-

SAFETY MEASURES:

- Use Strong Passwords:
 - Set strong, unique passwords for your devices and accounts.
 - Avoid using easily guessable information like birthdays or common words.
- Enable Two-Factor Authentication (2FA):
 - Add an extra layer of security by enabling 2FA on your accounts, especially for email, social media, and financial apps.
- Keep Software Updated:
 - Regularly update your phone's operating system and apps to patch vulnerabilities and ensure you have the latest security features.
- Be Cautious with Apps:
 - Download apps only from official app stores.
 - Avoid sideloading apps from unknown sources, as they may contain malware.
- Review App Permissions:
 - Regularly check and review the permissions granted to apps.
 - Disable unnecessary permissions to limit access to your personal information.
- Install Antivirus Software:
 - Consider installing reputable antivirus or security apps to scan for and protect against malware.
- Secure Wi-Fi Connections:
 - Avoid connecting to public Wi-Fi networks without using a virtual private network (VPN) for added security.

- Regularly Back Up Data:
 - Back up your data regularly to a secure cloud service or an external device so that you can restore your information if needed.
 - Beware of Phishing Attacks:
 - Be cautious of emails, messages, or calls asking for personal information.
 - Avoid clicking on suspicious links and verify the legitimacy of communication.
 - Remote Wipe and Lock:
 - Set up remote tracking and wipe features on your phone so that you can locate, lock, or erase your device if it's lost or stolen.
-

By implementing these security measures, you can significantly reduce the risk of your mobile phone being hacked and protect your personal information from unauthorised access.

If you believe that your mobile phone or any other device might have been compromised, do not hesitate to contact Mr Bolhuis personally.

Specialised Security Services has a highly skilled cyber unit which serves as a formidable line of defence against cyber threats, leveraging its knowledge, skills, and collaborative approach to protect sensitive information and critical infrastructure from the ever-evolving landscape of cyber threats.

Specialised Security Services invites the public to the Mike Bolhuis Daily Projects WhatsApp Group.

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

HOW TO JOIN THE MIKE BOLHUIS DAILY PROJECTS WHATSAPP GROUP:

- Simply follow the link to our dedicated WhatsApp group:
 - <https://chat.whatsapp.com/Dys4JLOFTXCBqXBdXeEvzU>
- "JOIN" to ensure you never miss our daily updates.
- You will receive automatic notifications as soon as a new project is placed.
- Please share this with family, friends and colleagues.

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

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

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:

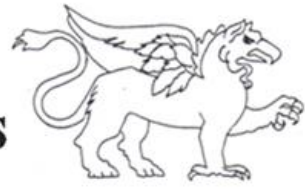
<https://mikebh.link/sss-task-team>

SSS CYBERCRIME UNIT:

<https://mikebh.link/sss-cyber-team>



Specialised Security Services



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. 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](#)

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

[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