



PROJECT:
THE DANGERS
LURKING IN OLD CELL
PHONES
PROTECTING YOUR DATA

In our fast-paced digital age, upgrading to the latest cell phone model has become a routine.

But what happens to our old devices once they're replaced? Many end up forgotten in drawers, sold second-hand, or worse, discarded without a second thought.

However, these seemingly harmless actions can pose significant dangers, especially when old cell phones fall into the wrong hands – the hands of cybercriminals.

**THIS PUBLIC DOCUMENT IS
INTENDED TO BE SHARED.**

PLEASE DO SO.

**THE OBJECTIVE OF SSS IS TO
SHARE INFORMATION, TO EDUCATE
AND FOREWARN THE PUBLIC.**

THE RISKS:

- Access to Personal Data:
 - Old cell phones often contain a treasure trove of personal information, including contacts, messages, photos, and even login credentials for various apps and accounts.
 - Cybercriminals can exploit this data for identity theft, financial fraud, or other malicious activities.
 - Banking App Vulnerabilities:
 - One of the most concerning risks is the access cybercriminals gain to banking apps installed on old devices.
 - Even if you have deleted the app before discarding or selling the phone, sensitive information such as your IMEI (International Mobile Equipment Identity) number may still be stored on the device.
 - This information can be exploited by hackers to access your banking accounts and carry out unauthorised transactions.
 - Social Media and Online Accounts:
 - Similarly, your old cell phone may still be linked to your social media accounts, email addresses, and other online platforms.
 - Cybercriminals can leverage this access to impersonate you, spread malware, or perpetrate scams targeting your contacts.
-

SAFE DISPOSAL PRACTICES:

- Factory Reset:
 - Before discarding or selling your old cell phone, perform a factory reset to erase all data stored on the device.
 - This helps minimise the risk of unauthorised access to your personal information.

- Remove SIM Card and Memory Card:
 - Ensure to remove both the SIM card and memory card from the device before disposing of it.
 - These cards may contain sensitive data and should be securely wiped or destroyed if no longer needed.
 - Use Encryption:
 - Consider encrypting your data before performing a factory reset.
 - This adds an extra layer of security by scrambling the information stored on the device, making it harder for cybercriminals to retrieve.
 - Physical Destruction:
 - For an added measure of security, physically destroy the old cell phone beyond repair.
 - This could involve shredding, smashing, or even melting the device to render it completely unusable.
-

PROTECTING YOUR IMEI:

- Your IMEI number is a unique identifier linked to your cell phone and can be used by banks and other services to verify your device's identity.
 - Even if you delete your banking app, the IMEI number associated with your phone may still be registered with the bank or other institutions.
 - To mitigate the risk of unauthorised access:
 - Contact your bank or service provider to update or unlink your old device's IMEI number from your accounts.
 - Regularly monitor your bank statements and online accounts for any suspicious activity, especially after discarding an old cell phone.
 - Consider using two-factor authentication or biometric security measures to further protect your accounts from unauthorised access.
-

The dangers posed by old or discarded cell phones cannot be overstated.

By following safe disposal practices and taking proactive steps to protect your personal data, you can mitigate the risks of cybercrime and safeguard your digital identity.

Remember, your data's security is in your hands, even after you have bid farewell to your old device.

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/Dys4JLOFTXCBgXBdXeEvzU>
- "JOIN" to ensure you never miss our daily updates.
- You will receive automatic notifications as soon as a new project is placed.

CONTACT MR MIKE BOLHUIS FOR SAFETY AND SECURITY MEASURES, PROTECTION, OR AN INVESTIGATION IF NEEDED.

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

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/ssb-task-team>

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



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

[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