

PROJECT: BOASTING AND POSTING ON SOCIAL MEDIA

Many parents want to post the very first schooldays of their child, or the brand-new luxury vehicle or the dream holiday.

However there are several reasons why some parents choose not to post photos of their children, homes, or luxury vehicles on social media, and these concerns generally revolve around privacy, safety, and security.

INPUT BY MR MIKE BOLHUIS:

https://mikebh.link/beGjgQ

KEY REASONS NOT TO BOAST/POST ON SOCIAL MEDIA:

- Privacy and Consent:
 - Children have a right to privacy, and posting their photos without their consent infringes upon that right.
 - As they grow older, they might not appreciate having their childhood moments shared publicly.
 - Parents should be mindful of their children's digital footprint and give them the autonomy to decide what they want to share online when they are old enough.
- Online Safety:
 - Posting pictures of children on social media may expose them to potential risks.
 - Predators can use publicly available information to identify and target children.
 - There is a risk of unintended audiences viewing these photos, especially if privacy settings are not configured correctly.
- Home Security:
 - Sharing images of the interior or exterior of your home may provide potential burglars with valuable information about your living arrangements.
 - Posting pictures of high-value items, such as luxury vehicles, may make your family a target for theft.
- Digital Kidnapping:
 - There have been cases of individuals taking photos of other people's children from social media and creating false identities or narratives.
 - This is known as "digital kidnapping."
 - These images might be misused or reposted without permission, leading to potential emotional distress for the families involved.
- Identity Theft:
 - Sharing personal information about your family, including names, birthdates, and locations, could potentially be used by identity thieves to commit fraud or other malicious activities.
- Maintaining Control:
 - Once something is posted online, it is challenging to control its distribution.
 - Even if you have privacy settings, there is always a risk that images can be copied, saved, and shared without your knowledge or consent.
- Future Implications:
 - Children may feel uncomfortable or violated when they discover that their childhood moments were shared online without their say.

• This could strain the parent-child relationship in the future.

While these concerns do not apply universally, as some families choose to share their lives online responsibly, it is essential for parents to be aware of the potential risks and make informed decisions about what they share on social media.

Implementing strict privacy settings, being mindful of the content shared, and respecting the privacy of children are crucial considerations in this digital age.

SAFETY MEASURES:

Safeguarding your social media profile is crucial to protect your privacy, personal information, and online reputation.

Here are some measures to help you secure your social media accounts:

- Use Strong Passwords:
 - Create strong, unique passwords for each of your social media accounts.
 - Use a combination of letters, numbers, and symbols, and avoid easily guessable information like birthdays or names.
- Enable Two-Factor Authentication (2FA):
 - Turn on two-factor authentication wherever possible.
 - This adds an extra layer of security by requiring a second verification step, such as a code sent to your phone or email, in addition to your password.
- Review and Adjust Privacy Settings:
 - Regularly review and update your privacy settings on each social media platform.
 - Adjust who can see your posts, who can send you friend requests, and who can look you up.

- Be Selective with Friend Requests:
 - Only accept friend or connection requests from people you know and trust.
 - Be cautious about adding strangers, even if they seem to have mutual friends.
- Think Before You Share:
 - $_{\circ}~$ Be mindful of the content you share.
 - Avoid posting sensitive or personally identifiable information, such as your address, phone number, or financial details.
- Regularly Update and Monitor:
 - Keep your social media apps and devices up to date with the latest security patches and updates.
 - Regularly check your account activity for any suspicious logins or activities.
- Review Third-Party App Permissions:
 - Periodically review and revoke access for third-party applications that are connected to your social media accounts.
 - Only grant access to apps and services you trust.
- Educate Yourself about Scams:
 - Stay informed about common social media scams and phishing attempts.
 - Be sceptical of unsolicited messages or requests for personal information.
- Use a Separate Email Address:
 - Consider using a dedicated email address for your social media accounts.
 - This can help compartmentalise your online presence and reduce the risk of a security breach affecting multiple accounts.
- Manage Tags and Mentions:
 - Adjust settings to control who can tag you in posts and photos.
 - Monitor and manage tagged content to ensure it aligns with your preferences and privacy concerns.
- Regularly Audit Your Friends/Connections:
 - Periodically review your friends or connections list and remove individuals you no longer want to have access to your information.
- Report Suspicious Activity:
 - If you notice any suspicious activity or if your account is compromised, report it to the respective social media platform immediately.

By implementing these practices, you can enhance the security of your social media profiles and reduce the risk of unauthorised access or misuse of your personal information.

It is essential to stay vigilant and proactive in managing your online presence.

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

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

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: <u>https://chat.whatsapp.com/Ew1H1dbUR988qoG8gei2sE</u>
- "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.

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: <u>mike@mikebolhuis.co.za</u> Fax: 086 585 4924 Follow us on Facebook to view our projects -<u>https://www.facebook.com/MikeBolhuisOfficial</u>

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

SSS TASK TEAM:

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

SSS CYBERCRIME UNIT:

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



🕒 f 🖉 🖾

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 <u>update your preferences</u> or <u>unsubscribe from this list</u>.

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