



PROJECT:

PROTECTING YOUR DIGITAL FOOTPRINT

Your digital footprint refers to the trail of data and information that you leave behind as a result of your online activities. It is essential to be aware of the information you share online and how it contributes to your digital footprint.

Managing your online presence, adjusting privacy settings, and being cautious about the content you post can help you control and protect your digital image.

Safeguarding your digital image is essential for maintaining privacy, preventing identity theft, managing your reputation, enhancing online security, reducing the risk of harassment, and minimizing the impact of targeted advertising.

-
- We all leave digital traces every time we use the internet.
 - This includes spending habits, personal data, and other demographic characteristics.
 - Companies track this information through various means, such as when we like a post on social media, make an online purchase, or participate in surveys.
 - As we share progressively more of our lives online, keeping track of all the information being collected about us can be challenging.
 - We need to take some measures to reduce our online footprint and protect our data from cybercriminals.
 - It is crucial to protect your personal information and prevent identity theft.
 - Cybercriminals are always on the prowl and can easily target unsuspecting individuals.
 - To minimize your digital footprint, follow the steps mentioned below.
 - Delete old email accounts:
 - If a hacker gains access to an old email account of yours, they can potentially view your contacts, impersonate you with ease, search for your personal information, and attempt to use the same password on other accounts.
 - If you no longer use the email address regularly, it may take a while to notice any suspicious activity, which can lead to more damage.
 - Limit social media accounts:
 - Many people find it impractical or undesirable to delete their social media accounts.
 - However, it is possible to minimize your exposure and protect your data by limiting the posts you share with others to "friends only," disabling location data collection, and selecting options to remove your profile from public search engine results.
 - If you have social media accounts you no longer use, it is advisable to deactivate them.
 - Skip the survey:
 - It is best to avoid taking clickbait questionnaires on unknown websites, as companies may use them to gather information on you.
 - Create a spam email address:
 - Consider creating a separate email account for marketing and promotional activities like store discounts.
 - Be cautious while storing any identifying information on that email account.

- In the case of a security breach in any marketing database where your account gets compromised, you can simply delete the address to reduce the loss of digital information.
- This may also help you to significantly reduce the amount of spam in your primary email account.
- Remove yourself from people's search sites:
 - Online data brokers, also known as "people search" sites, allow anyone to access personal details like names, addresses, and phone numbers for a small fee and in just a few clicks.
 - Malicious online trolls can also use this information to harass their targets.
 - To prevent this, click the "opt-out" button while placing an order or signing up for newsletters or other communications to prevent sites from sharing your information with marketing database companies.
 - Additionally, work with online data brokers to opt out of sharing your information.
- Search for "online data brokers" to find a list of such brokers:
 - Every broker has different steps to remove your information, these include formal requests through letters or faxes.
 - Opting out and protecting your privacy is worth the effort.
- Set up stealth mode when you search:
 - Browsers offer stealth or incognito mode, allowing you to browse privately without saving data on your computer.
 - Search for instructions on how to activate it based on your preferred browser.

ADDITIONAL SAFETY MEASURES:

- Protect your passwords:
 - Creating strong passwords that are not easy for others to guess is essential.
 - It is recommended to use a combination of upper and lowercase letters, numbers, and special characters.
 - Avoid using easily guessable information such as your name, birthdate, or common words.
 - Additionally, it is crucial to update your passwords frequently to reduce the risk of them being compromised.
 - If you must write them down, ensure that you store them in a secure location.

- Use multi-factor authentication whenever possible to add an extra layer of protection to your information.
 - Keep your software up to date:
 - It is crucial to keep the software on your laptops and smartphones up to date to protect your information.
 - This includes installing the latest version of antivirus software, which makes it harder for hackers to access your systems.
 - Additionally, using protected Wi-Fi at home can reduce the risk of exposure to potential threats.
 - Be in control of your phone apps:
 - List your apps on your phone and review the terms and conditions when downloading new apps.
 - Limit permissions from apps such as location, camera, and sharing information with others.
 - Knowing how your information is shared with other sites and companies helps you manage your digital footprint.
 - Consider deleting apps you no longer use to decrease the chance of others gathering information about your digital behaviour.
 - If you have ever provided your email to a company for a one-time coupon or discount, you may receive unwanted emails from those companies.
 - To keep your email account cleaner and prevent third parties from gathering your information, it is a good idea to **un**subscribe from mailing lists.
-

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.***

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/ssb-task-team>

SSS CYBERCRIME UNIT:

<https://mikebh.link/ssb-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

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