Specialised
Security Services

PROJECT:
PROTECTING PERSONAL INFORMATION WHEN NAVIGATING THE INTERNET

Specialised Security Services continuously repeats our concern regarding personal safety when navigating the internet. It might seem redundant for knowledgeable members of the public, however the number of cases we receive validates yet another confirmation of safety protocols.

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 internet connects us to a vast global community, providing unparalleled access to services and information. However, it is essential to remember that navigating the internet requires the same level of caution as any large urban environment. Protecting your personal information and financial resources from theft, and ransom demands is crucial and requires you to exercise common sense and implement technological safeguards. Proper safety measures allow you to surf, shop, play, and work online confidently and enjoy peace of mind rather than anxiety.

- Set up a VPN:
  - If you enjoy using public Wi-Fi networks in coffee shops, bars, libraries, or airport lounges, you should be aware that these networks often have weak security protocols that leave your private information vulnerable to hackers.
  - To protect your data, it is recommended that you set up a virtual private network (VPN) that can hide your IP address and encrypt your information.
  - With a VPN, you can confidently use public Wi-Fi networks without worrying about your data being hacked.
- Create strong passwords:
  - Choosing strong passwords for all your online, social media, and email accounts is important to avoid helping cyber attackers.
  - Prevent malicious AI-fuelled attacks by using passwords that are at least 12 characters long and contain a mix of uppercase and lowercase letters, numbers, and special symbols.
  - Your passwords should not be based on your personal information, and each one should be unique.
  - You may consider using a password manager to help generate and keep track of your passwords.
- Do not reveal too much personal information about yourself on social media:
  - It might seem harmless to participate in social media quizzes that determine what kind of farm animal you are based on your high school.
  - However, it is crucial to exercise caution when sharing any information online.

    - Cybercriminals can exploit this information to access sensitive data like bank accounts.
    - Therefore, thinking twice before sharing personal information or photos on social media is best.
    - Review each account's privacy settings to ensure your information is secure.
- Use anti-virus software:
    - Efficient anti-virus software, kept up to date, can provide strong protection from viruses, malware spyware, Trojans, phishing attacks, spam attacks, and other unwanted programs that can enter your computer and other connected devices and cause real harm.
    - Anti-virus software can eliminate existing viruses and prevent new ones from infiltrating your network.
    - Besides using third-party packages, you can also use the existing security protections in your operating system.
    - For example, if you have Windows 10 or 11, you can rely on Microsoft's built-in antivirus software, Microsoft Defender.
- Go incognito:
    - When browsing the internet, your web browser stores information such as browsing history, temporary internet files, and cookies.
    - To reduce this exposure, use a private browsing mode, such as InPrivate Browsing in Internet Explorer, Incognito in Chrome, Private Browsing in Firefox, or Private mode in Safari.
    - While this does offer a degree of privacy, it is not entirely foolproof.
    - If you are using a company computer, the websites you visit, your internet service provider, and your employer can still see what you're doing online.
- Think twice before clicking any link:
    - It is essential to be cautious of clickbait and phishing scams.
    - Always think twice before clicking on a link from an unknown or disguised sender in an email, text message, social media post, or website that may look familiar.
    - The website could be compromised and infect your device with malware.
    - To protect yourself from phishing, you can use a combination of technological solutions, such as anti-virus software, and common-sense measures, such as avoiding clicking on links from unknown sources, double-checking suspicious messages from known sources, verifying the URL's validity, and making sure the URL has the "https" prefix which indicates that the site is secure.
- Keep mobile devices secure:

    - When it comes to protecting yourself from data breaches, it is crucial to think about your computer and Android or iOS smartphone.
    - It is critical to keep your phone secure, and one of the best ways to do that is to accept and install patches, particularly security patches, as soon as they become available.
    - Even if your phone has a biometric feature, setting a difficult-to-guess passcode is still recommended as an additional security measure.
    - Additionally, it is a good idea to set up Find My Device or Find My iPhone to track your phone in case it gets stolen and remotely wipe your data if necessary.
- Pay with a smartphone app:
    - When shopping online, using your credit card is less secure than employing your smartphone with mobile payment apps.
    - Choose smart wallet methods, including Microsoft Pay, Apple Pay, Circle Pay, Facebook Pay, Google Pay, PayPal, Cash App, and Zelle.
    - Paying with a smartphone app protects you from the data theft dangers of credit card skimmers.
    - These transactions also generate a one-use authentication code, so if data is stolen, it does not help the scammer pilfer funds.
- Encrypt your computer:
    - If your computer is stolen, a knowledgeable hacker can access its files even if password protected.
    - With encryption, you get a hard-to-penetrate layer of security, with your information only accessible by a password and security.
    - It is gibberish without these.
    - Encrypt individual files, folders, volumes, and hard disks.
    - There are a variety of third-party encryption packages and built-in system solutions, such as Microsoft BitLocker and Apple FileVault.
- Stay as secret as possible:
    - When shopping online, being cautious with the information you share is essential.
    - A general rule to follow is only to provide the minimum amount of personal data needed to complete a transaction.
    - Stick to reputable sites you know and trust, like Amazon and eBay, to reduce the likelihood of fraud or identity theft.
    - Even so, remember that even large retail websites can be vulnerable to hacking, so it is best to limit the amount of personal information you provide as much as possible.
- Create different email accounts:

    - People often use the same email, username, and password for all their different correspondence, which may make them more easily targeted by scammers.
    - However, if you set up different emails for different uses, you would know that the bank alert for suspicious account activity received in your email account dedicated to social media was false.
    - It is suggested that one should have at least four different email accounts:
        - One for sensitive accounts, like banking and financial applications.
        - One for personal correspondence.
        - One for junk mail or shopping.
        - Another for any emails associated with work or interactions with different levels of government.
- Post with caution:
    - 67% of employers screen job applicants' social media accounts before hiring.
    - That means the pictures of you intoxicated, indecently exposed or those out-on-the-fringe political opinions may haunt you.
    - So, as you post on Facebook, Twitter, or elsewhere, ask yourself how it would play with a potential or current employer, and keep in mind that once a post is out there, it is challenging to take it down.
    - Even if you have strict privacy settings on a social media feed, a potential employer still might demand access.
- Download apps from reliable sources:
    - Be cautious when downloading apps or browser extensions from unreliable sources, as they can threaten your device's security.
    - Such apps may contain hidden malware that can compromise your personal information.
    - To stay safe, always download apps from official app stores like Google Play and the App Store and from reputable software makers.
    - It is also recommended that you remove any apps you no longer use.
    - Moreover, apps should only allow access to your location and personal data if necessary.
    - For example, a word processing program doesn't require access to your location, so it is best to deny such apps access to your data.
- Control your internet of things:
    - The Internet of Things (IoT) is becoming more integrated into our daily lives by introducing smartwatches, internet-connected home security systems, voice-activated smart lighting, and AI assistants like Amazon Echo and Google Home.

    - However, these devices can also pose a security risk if they are not adequately protected.
    - To ensure your safety, it is essential to set strong passwords for all your devices and keep your device firmware and router software up to date.
    - Additionally, you may want to consider creating a separate network for these devices to insulate their functions from your personal information and protect your privacy.
- Use multi-factor authentication:
    - Besides using complex passwords for different accounts, you should use two-factor or multi-factor authentication when permitted.
    - These provide extra security for bank accounts, social media accounts, and other accounts involving a password, a smartphone to receive verifications, and, more recently, biometric checks with scans of fingerprints or faces.
    - While this may seem like a lot of trouble, the added security can prevent disastrous data breaches.
- Be careful with free Wi-Fi:
    - It is essential to be cautious when using public Wi-Fi networks, especially when logging into your internet banking account.
    - Although using the free Wi-Fi offered in shopping malls, internet café or other public places may be convenient, it can put your confidential data at risk.
    - If your data is transferred over an insecure network, you could become vulnerable to identity fraud or theft of your financial information.
    - To protect yourself, turn off your automatic Wi-Fi connection, use a Virtual Private Network (VPN), and avoid conducting sensitive or private business in public.
- Use anti-virus software:
    - Protecting your computer and personal security is crucial.
    - One of the most effective ways to do this is by purchasing and installing anti-virus software.
    - While it may seem like an additional expense, investing in anti-virus software can help protect your device and prevent possible security threats.
    - Efficient anti-virus software, kept up to date, can provide strong protection from viruses, malware spyware, Trojans, phishing attacks, spam attacks, and other unwanted programs that can enter your computer and other connected devices and cause real harm.
    - Anti-virus software can eliminate existing viruses and prevent new ones from infiltrating your network.
    - Besides using third-party packages, you can also use the existing security protections in your operating system.

    - For example, if you have Windows 10 or 11, you can rely on Microsoft's built-in antivirus software, Microsoft Defender.
- Log out from services:
    - It is essential to always log out and close the browser after you are done with your online banking or sending emails.
    - This is especially crucial when you are using public Wi-Fi, as it prevents unauthorised access to your accounts.
    - Even if you think your accounts are safe, it is still a good idea to log out regularly, perhaps once a month, and check to ensure that you are the only one using them.
- Check to see if a link is secure:
    - It can be tempting to click on links you receive from an old college friend whom you have not talked to in years.
    - However, ensuring that the links are legitimate and not something more nefarious is essential.
    - Learning to check if links are secure is a must to protect yourself and your device.
    - Some of these insecure links are a form of data mining called phishing.
    - In such cases, the target is scammed into giving sensitive information or downloading malware.
    - Double-checking the URL, typing the URL by hand, and using a link verification service are your best bets to browse smartly.
- Clear your cache:
    - Clearing your cache is good for your "tech hygiene", helps websites load faster, and troubleshoots app issues.
    - A cache is a storage location that temporarily saves data to help websites load quickly.
    - By regularly deleting your browser history, you can safeguard your privacy and prevent any sensitive information from falling into the wrong hands.
    - Most desktop and mobile browsers offer the option to delete browser history and cookies, clear cached images and files, and remove saved passwords in the settings.

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/sss-task-team

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

Specialised Security Services

---

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
