Specialised
Security Services

PROJECT:
CORPORATE OR BUSINESS IDENTITY THEFT

SSS is on a continuous path to educate and inform the public against identity theft.

This includes individuals as well as companies or businesses. Victims are people with a business TAX number, from an individual proprietorship to a large corporation.

Corporate identity theft even includes international logos such as the Coca-Cola ribbon, Nike's tick, and the jumping athlete on Jordans.

In South Africa, criminals use longstanding businesses such as well-known Banks and SARS to sway potential victims into a sense of trust.

At the end of December 2022, the Federal Trade Commission believed that identity theft was costing the South African economy more than R1.5 billion per annum.

CORPORATE IDENTITY THEFT:

- Corporate identity is vital as the public's perception of a company builds a consumer following, thus contributing to success.
- It allows the brand to be recognisable to both its target audience and potential customers, which encourages them to select the company over its competitors.
- It creates a sense of trust with members of the public and by using longstanding names or brands of businesses, criminals can either taint a business' reputation or sway victims into paying money over to them.
- Criminals pose as owners, officers, or employees of a business to illegally transact business and establish lines of credit with banks and vendors.
- It is the unauthorised use of a business name or identity for financial gain.
- Fraudsters then use this information to make purchases, open accounts, withdraw money, and file tax returns.
- Data breaches damage reputations and cost businesses money.
- Identity theft destroys businesses, especially small and medium-sized businesses, which frequently lack the necessary security measures.
- Identity theft includes medical, criminal, financial and child identity theft.
- Businesses are especially vulnerable as they often have more significant financial resources and access to customer data.
- Data theft refers to the act of illegally obtaining digital information from an organisation for financial gain or with the intent to sabotage the business' operations.
- Criminals also use phishing emails, fake invoices, and tax filing.
- Phishing Emails:

    - Some fraudsters might email your employees or customers while pretending to be your business.
    - These emails may have a company's logo and name.
- The criminals take extreme care when falsifying emails and letterheads of the companies they target and it is not always easy to distinguish between the real documentation/electronic correspondence and the false documentation/electronic correspondence.
- Aside from income loss, other consequences associated with identity theft include late payments and fines, loss of cash flow, inability to pay employees and vendors, upholding tax obligations, or purchasing supplies.
- The business' credit score and reputation will be negatively impacted.

BUSINESS PROTECTION AGAINST IDENTITY THEFT:

- **Trademark Registration:**
    - Register your company's name, logo, and other intellectual property as trademarks.
    - This can help protect your brand identity legally and make it harder for others to impersonate your business.
- **Secure Online Presence:**
    - Ensure your website and online platforms are secure.
    - Use strong encryption, update software regularly, and employ robust authentication methods to safeguard customer data.
    - This includes firewalls, anti-virus software, spyware protection software and encryption software.
- **Educate Employees:**
    - Train your employees to recognize phishing scams and other forms of cyber threats.
    - Regular security awareness programs can help them spot and report suspicious activities.
- **Monitor Your Brand:**
    - Keep an eye on your brand's online presence and social media.
    - Watch for any unauthorized use of your company name or logo.
    - Social media listening tools can be valuable for this purpose.
- **Legal Action:**
    - If you discover someone impersonating your company, consider taking legal action to protect your brand identity.
    - Consult with a legal expert on how to proceed.

- **Two-Factor Authentication (2FA):**
  - Implement 2FA for access to critical systems and accounts.
  - This adds an extra layer of security by requiring users to provide two forms of authentication before granting access.
- **Customer Verification:**
  - Be cautious when dealing with new customers or partners, especially if they request sensitive information.
  - Verify the legitimacy of businesses before entering into any financial transactions or agreements.
- **Report Incidents:**
  - If you suspect corporate identity theft or fall victim to it, report the incident to the appropriate authorities, such as law enforcement agencies and regulatory bodies in South Africa.
  - They can investigate and take action against the perpetrators.
- **Data Privacy Compliance:**
  - Ensure your business complies with South Africa's data protection laws, such as the Protection of Personal Information Act (POPIA).
  - This can help protect customer information and reduce the risk of data breaches.
  - Businesses should use data protection software to record network activity and regularly check logging data and audit trails for suspicious activity.
  - Data breaches that expose employees' passwords and other sensitive data.
  - Data breaches are the leading causes of business identity theft.
  - The following statistics, according to ITWEB, highlight our concerns:
    - "South Africa's financial sector has experienced the highest average cost of data breaches, totalling R73.1 million, with the industrial and services sectors second and third, with R71.37 million and R58.78 million, respectively.
    - This represents an 8% increase over the last 3 years and a 73% increase since South Africa was added to the report eight years ago."
    - https://www.itweb.co.za/content/Olx4zMkazYQv56km

SSS has an extremely progressive and skilled cyberteam which focusses on the complete risk analysis of any business, the extensive protection of their information and the ongoing maintenance of the integrity of business data and protocols.

A successful identity theft attack can have severe consequences for businesses, including financial loss, reputational damage, legal ramifications, and loss of customer trust. It is, therefore, critical to take the necessary precautionary measures to protect the integrity of your business.

Visit our Facebook page and our website for similar and other current warning projects of which to be wary.

Specialised Security Services is proud to invite the public to our highly anticipated WhatsApp Channel.

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

HOW TO JOIN THE MIKE BOLHUIS WHATSAPP CHANNEL:

- Simply follow the link to our dedicated channel: https://whatsapp.com/channel/0029Va9cH3n0bIdvTstlCf0t
- Hit the "FOLLOW" button to ensure you never miss our daily updates.

- Tap on the "BELL" icon to receive instant notifications whenever a new post is placed.
- Please share this with family, friends and colleagues.

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/sss-task-team

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

Specialised Security Services

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