International Journal of Social Science Research and Review

http://ijssrr.com
editor@ijssrr.com
Volume 7, Issue 5
May, 2024
Pages: 191-202

An Exploration of the Use of Software Technology to Combat Identify Theft in South Africa

Debra Claire Pheiffer [1]; Charl Johannes Naude [2]

[1] Doctor, Department of Safety and Security Management, Tshwane University of Technology, Soshanguve, South Africa
ORCID: https://orcid.org/0000-0001-6650-8446

[2] Industrial Development Cooperation, Sandton, South Africa
ORCID: https://orcid.org/0009-0004-3464-7811

E-mail: PheifferDC@tut.ac.za ; charljnaude@gmail.com

http://dx.doi.org/10.47814/ijssrr.v7i5.2043

Abstract

In the contemporary information age, individuals grapple with a myriad of challenges impeding the effective safeguarding of personal information, thereby exerting profound ramifications on both consumers and businesses. A notable obstacle in this milieu is the pervasive occurrence of identity theft, a formidable adversary that not only infringes upon the privacy of victims but also poses a potential menace to their financial stability, by instigating emotional distress. The principal objective of this study was to assess extant software technology and delve into prospective innovations capable of mitigating identity theft within the context of South Africa. Anticipated outcomes encompass the provision of valuable insights into existing software technologies dedicated to prevent identity theft, and by furnishing entities with information essential for well-informed decision-making. The research findings substantially influenced this study's conclusions when formulating recommendations for preventive software technology. This study fervently advocates for the efficacious deployment of software technology as an indispensable instrument in the concerted effort to combat identity theft. Within the dynamic landscape of technology, the cultivation of vigilance, continuous information assimilation, and adaptability emerge as imperative prerequisites to outmanoeuvre individuals seeking to exploit vulnerabilities in the digital identities. The envisaged contribution of this research was to promulgate the notion that the establishment of a robust framework, actively minimising the threat of identity theft, necessitates prioritisation of proactive measures, ongoing educational initiatives, and strict adherence to data protection regulations. Negotiating the intricate terrain of an increasingly digital landscape mandates the incorporation of precautionary technologies by consumers, to ensure a safer and more secure online environment.

Keywords: *Identity Theft; Software Technology; Crime Prevention; Fraud; Personal Data*

Introduction

It is imperative to underscore the role of technologies designed to secure personal data, forestall instances of identity theft, and actively engage in its prevention.

Recent technological advancements have facilitated expeditious detection and thwarting of such criminal activities. Liu, Fang and Guo (2016) elaborate that software technology involves realising resources into products or services, encompassing knowledge and resources to achieve established goals. Slyter (2019) defines software technology as an application that tackles business or organisational challenges on an extensive scale. The adequate protection and security of personal information are hindered by numerous challenges in the contemporary information landscape, impacting both consumers and businesses. A notable manifestation of these challenges is observable in the domain of identity theft, compelling victims to navigate the emotional distress stemming from privacy invasion and the consequential jeopardy of their financial stability. Identifying technological solutions that can safeguard personal data and prevent identity theft are essential to prevent it. According to Cassim (2015), many individuals and companies have fallen victim to identity theft. It causes financial loss to consumers, creditors, financial institutions, and the economy as a whole. It has been reported by the credit bureau Compuscan that identity theft costs the South African economy about R1 billion a year. Identity theft is a significant and ongoing issue in the South Africa (SA). Consumers must acknowledge that the responsibility for providing evidence lies with them. Even though there are safeguards in governmental and private institutions, individuals still have to prove the involvement of an organisation in financial losses caused by identity theft.

Nagtegaal (2015) describes identity theft in SA as the illegal acquisition of personal data by perpetrators for personal gain. The perpetrator commits fraud by exploiting the victim's identity to obtain credit, loans, or other advantages in their name, often resulting in substantial indebtedness. Beyond financial gains, wrongdoers frequently appropriate others' identities to conceal their own. In order to obtain employment as a foreign national, claim social grants, avoid criminal prosecution, and secure life insurance policy benefits, a new identity is utilised. Therefore, it was vital to investigate the potential of software technology to prevent identity theft. If criminals can get hold of someone’s name, address, phone number or banking details, they can then use this information to steal that person’s identity and commit fraud. Perpetrators may be able to gather a large amount of this information from bank statements or paper documents, but increasingly the easier way for them to gain access to this priceless data is by going online (MacKay, 2024). The aim of this study was to evaluate current software technology and explore possible innovations that can prevent identity theft in SA. Consequently, this article explores best practices in dealing with consumer data and identity theft prevention, which could benefit individuals and the business community as a whole.

Literature Review

A thorough literature review was conducted to evaluate the feasibility of using software technology to prevent identity theft in SA. A thorough examination of both primary and secondary sources pertaining to the subject matter of this paper was undertaken, as elaborated upon below.

Overview of the Significance of the Use of Technology to Prevent Identity Theft

The importance of protecting personal information against identity theft cannot be overstated in the digital age, where technology is intricately integrated into our lives. The critical examination of the significance of using technology as a proactive measure in preventing identity theft reveals its multiple roles in securing our digital identities. A perpetrator can obtain unauthorised access to a financial account by collecting enough personal information about an individual to impersonate them. Victims of identity theft can face significant consequences, as they may not be aware of when or how their information was

stolen. Therefore, it is advisable to proactively safeguard personal details and information from potential fraudsters before they exploit them (Popa, 2023).

Although technology unquestionably enhances our daily lives, it also negatively affects modern society. The increase in cybercrime, the rise in addiction problems, and the decrease in face-to-face human interactions are major drawbacks (Nwokiki, 2022). A deeper understanding of user behaviour is a key element in preventing identity theft. Patterns and anomalies are leveraged by technological tools, such as behavioural analytics and predictive technologies, to identify potential threats before they materialise. Beyond technological prowess, educating individuals about the intricacies of identity theft and fostering awareness is integral. Using technology to prevent identity theft goes beyond just deploying security measures. It involves educating users about potential threats and fostering awareness about safe online practices. Regarding cybersecurity education, technology plays a dual role as both a protector and an informant (Nwokiki,2022). The significance of using technology for prevention cannot be overstated in the face of the increasing challenges of identity theft, discovered important diverse aspects, encompassing everything from advanced authentication protocols to machine learning and encryption. In the ongoing fight against identity theft is not just an option but a proactive necessity to comprehend and utilise the potential of technology navigated as an increasingly interconnected digital landscape.

The Use of Software Technology to Protect Personal Data

Identity theft has become one of the fastest growing white-collar crimes in the world. It occurs when an individual's personal information such as *inter alia* his or her name, date of birth or credit card details is used by another individual to commit identity fraud. Identity theft can be committed via physical means or online. The increased use of the Internet for business and financial transactions, social networking and the storage of personal information has facilitated the work of identity thieves. Identity theft has an impact on the personal finances and emotional well-being of victims, and on the financial institutions and economies of countries. The use of new technologies has resulted in increased opportunities for criminals to steal and illegally use personal information to commit identity theft crimes. It is submitted that identity theft is increasingly challenging law enforcement agencies and governments around the world (Cassim, 2015). At the forefront of preventive software technology lies its ability to fortify digital ramparts. Through robust encryption mechanisms, firewalls, and intrusion detection systems, personal data is shielded from unauthorised access and potential breaches. The software acts as a sentinel, vigilantly monitoring and repelling any malicious attempts to compromise sensitive information. Due to technological advancements, the operational paradigms of various industries have undergone a transformative shift, as suggested by Watts (2022). These technologies aim to enhance workflow efficiency, automate critical processes, and promote better team collaboration.

The pervasive influence of technology in our daily lives is exemplified by Rana (2023), as society is constantly exposed to novel devices and software designed to streamline routine tasks. One of the striking applications of preventive software technology is its integration of behavioural analytics. By scrutinising user behaviour patterns, the software can identify anomalies that may signal a potential security threat. This dynamic defence mechanism allows real-time adjustments and heightened security protocols to thwart nefarious activities. Technology's significant advantages must be acknowledged and addressed, even though there are potential drawbacks. The general agreement that technology is essential in protecting personal information and mitigating the dangers of identity theft is supported by this insight. In addition, empirical evidence indicated that technology is crucial in proactively preventing identity theft. The importance of technology in fortifying the security of personal information and effectively mitigating the risks associated with identity theft is underscored. As personal data remains a prime target for cyber threats, preventive software technology becomes increasingly indispensable. This comprehensive exploration underscores the multifaceted applications of such technology, depicting it as a dynamic and adaptive guardian of personal information.

In the ever-expanding digital landscape, embracing and leveraging preventive software technology is not just a choice but a necessity in the relentless pursuit of securing personal data.

Technology That Can Prevent Identity Theft

The onset of the information age has brought about a new breed of criminal activity: identity theft. By exploiting this, criminals gather extensive personal information about their targets, allowing illegal access to their financial accounts. Often, victims are left unaware of the when or how of their information's theft, potentially leading to dire consequences. Consequently, proactive safeguarding of personal information against fraudsters becomes imperative to prevent misuse (Popa, 2023). While technology unquestionably enriches our daily lives, it also adversely affects contemporary society. Cybercrime rates are increasing, addiction issues related to technology are increasing, and face-to-face human interactions are diminishing (Nwokiki, 2022). As the prevalence of identity theft continues, companies are increasingly adopting advanced technologies to safeguard consumer information. Essential precautions for consumers and the collective efforts to combat this crime effectively are important to explore. While advanced technology plays a crucial role in combating identity theft, consumers must actively contribute to protecting their private information. In addition, there are several additional measures individuals can take:

- Use strong and unique passwords for online accounts and enable two-factor authentication whenever possible;
- Be cautious of phishing attempts and avoid clicking on suspicious links or providing personal information through unsecured channels;
- Regularly monitor credit reports and bank statements for any signs of fraudulent activity;
- Safeguard physical documents containing sensitive information by storing them in a lockbox or using secure document disposal methods, such as shredding;
- Utilise secured websites when making online purchases or financial transactions, ensuring the presence of “https” and a padlock symbol in the browser address bar; and
- Stay informed about emerging threats and security best practices to adapt and strengthen personal security measures (Press Room, 2024).

Identity theft and cybersecurity measures can be thwarted and enhanced due to technological advancements. Biometric authentication stands out among these innovations, leveraging unique biological traits like fingerprints, facial recognition, or iris scans to verify individuals' identities. By adding an extra layer of security, biometric authentication significantly complicates perpetrators' attempts to impersonate others. Furthermore, machine learning algorithms can scrutinise user behaviour patterns and flag anomalies indicative of fraudulent activity, thereby issuing early warnings of potential identity theft. Encryption techniques and blockchain technology provide secure methods for storing and transmitting sensitive personal information, reducing the risk of unauthorised access and data breaches (Nwokiki, 2022). By harnessing these cutting-edge technologies alongside robust security protocols, organisations and individuals can fortify their defences against identity theft and protect personal information in an increasingly digital landscape.

Challenges in Implementation Preventative Technology

Deploying technology is always a challenge, but those who boldly embrace innovation instead of merely following it will be able to conquer new territories and dismantle established barriers (Scalzo, 2019). Cybersecurity, which encompasses the use of technology, entails safeguarding internet-connected devices and services against malicious assaults orchestrated by hackers, spammers, and cybercriminals (Kelly, 2023).

Implementing preventative technology to combat identity theft presents numerous challenges for organisations and individuals. The issue of cost and resource allocation is the first thing to consider (Scalzo, 2019). One must have substantial financial resources and expertise to invest in advanced security measures like biometric authentication, machine learning algorithms, encryption techniques, and blockchain technology. Smaller businesses and individuals, in particular, may need help affording or implementing these technologies effectively. Secondly, there are concerns about usability and convenience. While advanced security measures can strengthen protection against identity theft, they may also introduce complexities that hinder user experience (Valasseri, 2022).

Biometric authentication may not always be reliable or accessible for all users, leading to frustration and resistance to adoption. It is crucial to balance security and user convenience to ensure the acceptance and effective utilisation of preventative technologies. Additionally, there are regulatory and compliance concerns that need to be addressed. Data privacy laws, industry regulations, and compliance standards mandate requirements for collecting, storing, and processing personal information. Preventative technology implementation must align with these legal frameworks to avoid potential legal consequences and liabilities. Furthermore, the constant evolution of cyber threats demands constant adaptation. As technology progresses, so do the tactics and techniques employed by cybercriminals. Preventative measures must remain agile and adaptable to address emerging threats effectively. Finally, socio-cultural factors must be considered. Establishing trust and awareness among users is paramount for successfully adopting preventative technology. Educating individuals about the significance of Cybersecurity and the perils of identity theft can cultivate a culture of vigilance and proactive protection (Valasseri, 2022; Patel, 2023; and Olmstead, 2022).

Patel (2023) identified the following challenges in the implementation of technology, namely – budget limitations; lack of professional training; poor network infrastructure; resistance to change; no systems in place to utilise technology in the curriculum; unreliable devices and software; administrators do not see the need for money technology; and learn how to embrace education technology with our experts. Choosing the right system and procedures, poor compatibility with legacy systems, and inadequate training are three technology risks (Atias, 2019). In conclusion, while preventative technology holds significant promise in combating identity theft, its implementation is challenging. Overcoming these obstacles requires concerted efforts from organisations, policymakers, and individuals to protect personal information effectively in an increasingly digital era.

Research Methodology

The purpose of research methodology is to collect, analyse, and interpret data in a scientific and structured manner to answer research questions or test hypotheses. It includes the data collection and analysis methods, the research design, and the overall framework of the study (Streekumar, 2023).

Research Design and Method

This study was empirical in nature and adhered to an exploratory research design. Empirical research design is based on observation or experience rather than theory. It is defined as the active process of leaving one's workspace, going outside intentionally, and actively seeking knowledge from outside sources (Denscombe, 2014). This design was utilised to obtain credible data from participants through observation, survey, and one-on-one interview strategy. The exploratory design was used to update information regarding the problem. Exploratory research is a type of research design where the researcher is trying to understand a subject (Cobanoglu, 2023). This research adopted a mixed-method approach.

Creswell and Clark (2017) define mixed methods as a methodology encompassing philosophical assumptions guiding the direction of data collection and analysis, involving a blend of qualitative and

quantitative approaches across various phases of the research process. Data was collected using a combination of methods, including literature study, questionnaires, and interview schedules. Internationally conducted, this research delved into the assessment of available technologies aimed at preventing identity theft and their practical applications within the context of SA. Empirical research was carried out through interviews with participants who are predominantly engaged in the field of identity theft prevention technology. The collected data consisted of various sampling methods, such as simple random sampling as a probability method; and purposive sampling as a non-probability sampling.

Simple random sampling is a technique in which each member of a population has an equal chance of being chosen through an unbiased selection method (Simkus, 2023). Purposive sampling is a technique used in qualitative research to select a specific group of individuals, participants are chosen on purpose (Heath, 2023). The sample comprised individuals in leadership roles such as Head/Partner, Senior Managers, and Managers, all of whom are involved in the development or sale of technology designed to prevent identity theft. The participants/ respondents for this study came from a variety of geographical locations, such as SA, the United States of America (USA), the United Kingdom (UK), Australia, and Namibia. Twenty participants were interviewed and 147 respondents completed the questionnaires.

Data Analysis

Data analysis involves systematically organising and categorising raw or verbal data. This process aims to convert the data into implicit and explicit measurements, constructing meaningful interpretations based on the patterns or frequencies observed during the translation or conversion of such raw data (Ary, Jacobs, Sorensen & Walker, 2019). A mixed analysis combined with quantitative and qualitative data analysis techniques was integral to this study. The mixed-methods analysis was employed to derive the study outcomes. This involved the utilisation of MS Word (2016) for graphical representations and MS Excel (2016), aligning the results with data obtained from both the questionnaire survey and interviews. Using tables and a narrative or storytelling approach allowed for integrating reviewed literature, survey questionnaires, and interview schedules. Participant feedback was presented in a narrative format and illustrated through MS Word 3D 100% stacked bar graphs, highlighting common themes and characteristics within the sampled population for enhanced visual comprehension. The interpretation of the data emphasises providing clear explanations based on the data analysis.

According to Yin (2016), the interpretation phase constitutes the key analytical part of the research report. Data were analysed, interpreted, compared, and integrated as they had been collected through different observations and fields of study. Descriptive analysis was used to analyse the data with regard to the quantitative approach to the research. This was done through a spreadsheet program, namely Microsoft Excel and Forms. Inclusive of the mixed methodology, the questionnaires consisted of qualitative components. The interview schedule questions were coded to guarantee the reliability of the answers. Similarly, before distributing to the respondents, all questions in the questionnaire survey were coded and recorded using MS Word tables. During the results capture phase, answers were grouped by combining sub-questions from the survey questionnaire, thus reinforcing the reliability of the data.

Findings and Discussions

Technology's accessibility in people’s daily lives has made everyday tasks much more accessible by introducing new devices and software. While technology offers significant advantages, it is imperative to acknowledge and understand its potential drawbacks. This study found that technology is crucial in preventing identity theft and is indispensable for the protection of personal information. According to Popa (2023), the advent of the information age has ushered in a new form of criminal activity: identity theft. This occurs when a perpetrator collects sufficient personal information about an individual to

impersonate them and gain unauthorised access to their financial accounts. The repercussions of identity theft can be severe for victims, who may remain unaware of when or how their information was pilfered. Therefore, it is advisable to proactively safeguard personal details and information from potential fraudsters before they exploit them. Despite the undeniable positive impact of technology, it also brings about adverse effects on contemporary society, including increased instances of cybercrime, addiction issues, and a decline in face-to-face human interactions (Nwokiki, 2022).

Watts (2022) states that various industries have undergone a transformation due to the impact of technologies, which have changed the way they operate. The goal of these technologies is to enhance workflow productivity, automate crucial processes, and enhance team collaboration. The significance of technology in the daily lives of people is emphasised by Rana (2023), as society being constantly exposed to new devices and software that make everyday tasks easier. While technology has major advantages, it is important to know its potential drawbacks. These statistics underscore the prevailing consensus regarding the significance of technology in protecting personal information and mitigating the risks associated with identity theft. Similarly, it was discovered that technology plays a crucial role in preventing identity theft. The importance of technology in safeguarding personal information and mitigating the risks associated with identity theft was determined. Also, that technology is indispensable for preventing identity theft.

Nevertheless, this research further recognised that technologies like TransUnion, Experian, and Biometrics could effectively prevent identity theft. The findings underscore the substantial influence of technology on identity theft, with South African participants and survey respondents identifying data breaches and an overreliance on technology as primary risks. In the USA, the most critical risks were associated with data breaches and system downtime, while in the UK, data breaches and technological malfunctions were predominant concerns. Namibia expressed apprehension about data breaches and quality as potential risks in employing technology for identity theft prevention. This research highlighted that data breaches are the primary concern when utilising technology to combat identity theft. In the context of individuals daily interactions with technology, ranging from essential devices like portable computers and smartphones, this study revealed the widespread importance of Multi-factor Authentication (MFA) in safeguarding against identity theft across various technological contexts.

Recommendations

Due to technology's dynamic nature, it is important to remain adaptable and vigilant, which necessitates continuous education and awareness. Individuals can strengthen their defences against technology-related identity theft and reduce the associated risks by implementing suggested best practices when using software technology. Practical guidelines and procedures that can be used to prevent identity theft through software technology are summarised below:

❖ Use Strong and Unique Passwords
- Creating complex passwords that include a mix of uppercase, lowercase, numbers, and symbols is a best practice. Avoid disclosing information that can be easily guessed, like birthdays; and
- To ensure security, use a trustworthy password manager to create and store strong, distinct passwords for every online account.

❖ Make sure Multi-Factor Authentication (MFA) is enabled
- To add an extra layer of security beyond passwords, enabling MFA wherever available is a best practice; and
- Enhance authentication and protect against unauthorised access by implementing MFA for email, banking, and other critical accounts.

❖ Update software and operating systems on a regular basis
- It is important to keep software, applications, and operating systems up to date to patch security vulnerabilities; and
- Implementation involves turning on automatic updates when possible and regularly checking for updates and applying them promptly.

❖ Secure Wi-Fi Practices
- Ensure that you use secure Wi-Fi networks and avoid public Wi-Fi for sensitive activities; and
- Make sure to set a secure Wi-Fi password, enable WPA3 encryption, and use a virtual private networks (VPN) to increase security when connecting to public networks.

❖ Implement Encryption for Sensitive Data
- To protect sensitive data from unauthorised access, it is recommended to encrypt it during transmission and storage; and
- Using encryption tools for communication channels, encrypting files that contain sensitive information, and enabling device encryption are all necessary steps.

❖ Exercise caution with emails and links
- When opening emails from unknown senders, it is best to be cautious and avoid clicking on suspicious links; and
- To implement this, make sure to use email filtering tools, verify email sender addresses, and hover over links to preview the URL before clicking.

❖ Monitor Financial Statements Regularly
- To avoid unauthorised transactions, it's advisable to regularly review your bank and credit card statements; and
- Create account alerts for unusual activities and immediately notify your financial institution if there are any discrepancies.

❖ Configure Privacy Settings on Social Media
- To prevent personal information from being visible, it's important to review and adjust privacy settings on social media platforms; and
- Ensure that personal details are not shared publicly and be cautious when accepting friend/connection requests.

❖ Education and training
- To increase awareness of identity theft risks, it is best practice to offer identity theft training to employees; and
- Regularly conduct training sessions, simulate phishing exercises, and ensure that employees comprehend and adhere to security protocols.

❖ Implement endpoint security solutions
- It is best practice to ensure that endpoint security solutions, such as antivirus and anti-malware software, are installed and updated regularly; and
- To protect individual devices from various cybersecurity threats, and implement reputable security software.

❖ Multi-factor authentication (MFA)
- Implement MFA solutions that require users to provide a variety of identification methods, including passwords, biometrics, and one-time codes to enhance security.

❖ Encryption tools
- Encryption technologies can be utilised to secure sensitive data while it is transmitted and stored, making it hard for unauthorised individuals to interpret it.

❖ Secure communication platforms
- To safeguard sensitive information while communicating digitally, opt for encrypted communication channels, secure messaging apps, and email services with built-in encryption.

❖ Machine learning and artificial intelligence
- Use algorithms based on AI and machine learning to detect patterns, anomalies, and potential identity theft threats in real time, which enhances proactive threat detection.

❖ Behavioural analytics
- Use behavioural analytics tools to monitor and analyse user behaviour, identifying any deviations that could be indicative of unauthorised access or suspicious activity.

❖ Backup data regularly
- To avoid losing important data in the event of a security incident, it is important to regularly back up important data; and
- Ensure that automated backup solutions are implemented, and backups are stored in secure, off-site locations or cloud services.

❖ Minimise the availability of personal data
- It is recommended to minimise the sharing of personal information online and be cautious about the details shared on public platforms; and
- It is important to be aware of the information included in online profiles and avoid oversharing.

❖ Stay up to date on identity theft threats
- It's best to keep up to date on the latest identity theft threats and trends; and
- Make sure to follow trustworthy identity theft sources, subscribe to security newsletters, and actively seek out information about emerging threats.

❖ Biometric Authentication
- Enhance user authentication and prevent unauthorised access by using technologies such as fingerprint recognition, facial recognition, and iris scanning.

❖ Encryption Tools
- Encryption technologies can be utilised to secure sensitive data while it is transmitted and stored, making it hard for unauthorised individuals to interpret it.

❖ Identity Theft Protection Services
- Incorporate identity theft protection services that use advanced algorithms to monitor and alert users to potential threats, including unauthorised access or changes to personal information.

❖ Blockchain for Identity Verification
- Explore the use of blockchain technology to verify identity in a secure and decentralised way, which reduces the risk of centralised databases being compromised.

❖ Password Management Tools
- Encourage the use of password management tools that generate and store complex, unique passwords for every online account, as this can reduce the risk of identity theft related to passwords.

❖ Mobile Security Apps
- Protect against identity theft when your device is lost or stolen by using mobile security apps that have features like remote tracking, data wiping, and secure access controls.

❖ Regular Software Updates
- Regularly updating software, operating systems, and security applications is necessary to patch vulnerabilities and prevent exploitation.

❖ Privacy-focused Browsers and VPNs
- Ensure that online activities and communications are protected from potential eavesdropping by using privacy-focused browsers and VPNs.

❖ Digital Identity Solutions
- Explore digital identity solutions that offer secure and verifiable ways to establish and authenticate online identities, reducing the risk of identity theft.

❖ Regulatory compliance tools
- Use tools to ensure compliance with data protection regulations, which reduces the risk of legal consequences associated with mishandling personal information (Naude, 2024).

These recommended technologies can help individuals strengthen their defences against identity theft, leading to a more resilient and secure digital environment. This research confirms that it is crucial to use above mentioned multi-layered approaches that incorporates various technologies, to address the diverse nature of identity theft threats.

Conclusion

This research has significantly contributed to understanding the use of preventative software technology to combat identity theft which includes the following – To educate the South African society, which includes consumers and businesses, on the availability of preventative software technology that can help to prevent identity theft; to empower and educate investigators on identity theft and how preventative software technology can help to prevent identity theft; universities will have access to the newly acquired knowledge, and to pioneer new knowledge, improve theory and motivate further research which the academic community in general will have access to. Furthermore, the South African Police Service (SAPS) will benefit from the new knowledge that has been created with respect to preventative software technology that can be used to prevent identity theft. This could assist in improving and enhancing current SAPS training curricula to ensure that investigators are more knowledgeable and better equipped to investigate identity theft; and prospective clients, including individuals and businesses, will be informed of this study's findings to safeguard consumer data. This comprehensive study of identity theft and its preventive measures emphasises the crucial need of the use of software technology to safeguard individuals. The recommendations provided are a strategic guide for enhancing defences and reducing the risks related to identity theft. Using multiple approaches, such as biometric authentication, encryption, and advanced monitoring tools, users can create strong barriers against unauthorised access and malicious activities.

In order to hamper the persistent threat of identity theft, it is crucial to implement abovementioned technological measures in the digital realm. By embracing these suggestions, individuals can empower themselves to navigate the digital landscape with confidence and resilience, ensuring the protection of sensitive information and maintaining the integrity of personal and organisational identities. As technology evolves, by remaining vigilant, educated, and adaptable will be crucial to staying ahead of those looking to exploit vulnerabilities in our digital identities.

A resilient framework that significantly reduces the risk of identity theft was established by focusing on proactive measures, ongoing education, and compliance with data protection regulations, as summarised above. Navigating an increasingly digital landscape requires of a person to incorporate effective software technologies, which ensure a safer and more secure online environment for individuals.

References

Ary, D., Jacobs, C.L., Sorensen, C.K. & Walker, D.A. 2019. Introduction to research in education. 10th edition. Boston: Cangage.

Atias, Y. 2019. Overcoming challenges in Implementing technology systems for customers. Retrieved from: https://m51.co/blog/overcoming-challenges-in-implementing-technology-systems-for-customers/.

Cassim, F. 2015. Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves. Retrieved from: http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1727-37812015000200003.

Cobanoglu, D. 2023. What is exploratory research, definition, types and examples. Retrieved from: https://forms.app/en/blog/exploratory-research.

Creswell, J.W. & Clark, V.L.P. 2017. Designing and Conducting Mixed Methods Research, 3rdedition. Sage Publications, Thousand Oaks, CA.

Denscombe, M. 2014. The good research guide: For small-scale social research projects. 5th edition.Maidenhead, UK: Open University Press.

Heath, C. 2023. What is purposive sampling. Retrieved from https://dovetail.com/research/purposive-sampling/.

Kelly, K. 2023. What is Cybersecurity and Why It is Important? Retrieved from: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security.

Liu, S, Fang, Z. & Guo, B. 2016. Theory of science and technology transfer and applications. London: CRC Press.

MacKay, J. 2024. Eight ways to prevent identity theft. Retrieved from: https://www.metacompliance.com/blog/cyber-security-awareness/8-ways-to-prevent-identity-theft.

Nagtegaal, J. 2015. Identity theft in SA: fact or fiction. Retrieved from: https://www.lawforall.co.za/consumer-rights/identity-theft-south-africa-law/.

Naude, C. J. 2024. An exploration of the use of software technology to prevent identity theft in South Africa. PhD Thesis, unpublished. Pretoria: UNISA.

Nwokiki, F. 2022. Security and Identity Theft: The Pros and Cons of Technology in Our Era.Retrieved from: https://thetotalentrepreneurs.com/security-and-identity-theft-the-pros-andcons-of-technology-in-our-era/.

Olmstead, L. 2022. 11 Critical Digital Transformation Challenges To Overcome (2024) Available at: https://whatfix.com/blog/digital-transformation-challenges/.

Patel, H. 2023. The 7 Greatest Challenges Facing Education Technology Today. Retrieved from: https://wpgc.io/blog/the-7-greatest-challenges-facing-education-technology-today/.

Popa, M.2023. How to Prevent Identity Theft with 20 Essential Steps. Retrieved from: https://heimdalsecurity.com/blog/how-to-prevent-identity-theft-20-steps/.

Press Room. 2024. Ways Technology Prevents Identity Theft. Retrieved from: https://www.towerfast.com/press-room/ways-technology-prevents-identity-theft.

Rana, K. 2023. Importance of Technology. Retrieved from: https://www.towerfast.com/pressroom/ways-technology-prevents-identity-theft.

Scalzo, C. 2019. Challenges of implementing new technology and how to address them. Retrieved from: https://www.onlinecomputers.com/2019/01/challenges-of implementingnewtechnology-and-how-to-address-them/.

Simkus, J. 2023. Simple Random Sampling Method: Definition & Example. Retrieved from: https://www.simplypsychology.org/simple-random-sampling.html.

Slyter, K. 2019. What is Information Technology? A Beginners Guide to the World of IT. Retrieved from: https://www.scribd.com/document/522652716/Course.

Streekumar, D. 2023. What is Research Methodology? Definition, Types, and Examples. Retrieved from: https://paperpal.com/blog/academic-writing-guides/what-is-research Methodology.

Valasseri, I. 2022. Tackling Top 10 Technology Challenges of Small Businesses. Available at: https://www.infince.com/blog/top-technology-challenges-faced-by-small businesses.

Watts, A. 2022. Why is Technology Important in the Workplace. Retrieved from: https://www.edume.com/blog/importance-of-technology-in-the-workplace.

Yin, R.K. 2016. Qualitative Research: From start to finish. 2nd edition. New York: The Guilford Press.

Copyrights