MRS Journal of Multidisciplinary Research and Studies
Abbreviate Title- MRS J Mul Res Stud
ISSN *(Online) 3049-1398*
Vol-2, Iss-5(May-2025)

THE PUBLIC'S AWARENESS OF CYBER CRIME AND ONLINE SAFETY PRACTICES IN SOUTH AFRICA

Dr. John Motsamai Modise[*]

Tshwane University of Technology

Corresponding Author Dr. John Motsamai Modise

Tshwane University of Technology

Article History

Received: 12 / 04 / 2025

Accepted: 30 / 04 / 2025

Published: 05 / 05 / 2025

Abstract: This research aims to bridge this gap by investigating the public's level of awareness, understanding of online safety practices, and the impact of current educational campaigns. By identifying these knowledge gaps and potential shortcomings in educational initiatives, this research will inform the development of more targeted and effective strategies to improve public safety in the digital landscape. This research could examine the level of public awareness of cybercrime threats, the public's understanding of online safety practices, and the effectiveness of public education campaigns. The aims were to understand the public's awareness of cybercrime and online safety practices in South Africa and assess the effectiveness of current public education campaigns. The objectives were to Measure the level of public awareness of common cybercrime threats in South Africa. Evaluate the public's understanding of online safety practices. Assess the effectiveness of existing public education campaigns on cybercrime awareness. The research questions were to how familiar is the South African public with common cybercrime threats (phishing, malware, identity theft)? Does the public's understanding of online safety practices vary across demographics (age, location, socioeconomic background)? How effective are current public education campaigns in reaching the target audience and promoting online safety practices? What are the preferred formats for public education campaigns on cybercrime (social media, workshops, radio ads)? Do language barriers hinder public awareness of cybercrime threats in South Africa? How does the digital divide impact access to information about online safety? Do cultural factors influence online behavior and perceptions of cybercrime risk in South Africa? By addressing these objectives and research questions, your study will provide a comprehensive picture of public awareness and online safety practices in South Africa. South Africa faces a growing problem of cybercrime, yet public awareness of these threats and online safety practices may be lacking. This lack of awareness can leave individuals and businesses vulnerable to attacks, financial losses, and identity theft. There is a need to understand the current state of public knowledge regarding cybercrime and online safety in South Africa. Additionally, the effectiveness of existing public education campaigns on cybercrime awareness needs to be evaluated.

Keywords: *Cybercrime awareness, Public awareness campaigns, South Africa, Online safety practices, Cyber threats, Digital divide, Cultural factors, Public perception, Law enforcement, Policy and legislation, Citizen science, Cybersecurity education, South African Police Service (SAPS), Department of Telecommunications and Postal Services (DTPS), Internet Safety Campaign (ISC Africa).*

Cite this article: Modise, Dr. J. M., (2025). THE PUBLIC'S AWARENESS OF CYBER CRIME AND ONLINE SAFETY PRACTICES IN SOUTH AFRICA. *MRS Journal of Multidisciplinary Research and Studies, 2 (5),14-20.*

INTRODUCTION

The ever-expanding digital landscape in South Africa brings immense opportunities for communication, commerce, and information access. However, this interconnectedness also creates vulnerabilities to cybercrime. From phishing scams to malware attacks, cybercriminals target unsuspecting individuals and businesses, causing significant financial losses and privacy breaches. Combating cybercrime requires a multi-pronged approach, and public awareness is a crucial first line of defense. While South Africa has initiatives like the Internet Safety Campaign (ISC Africa), a comprehensive understanding of the public's knowledge about cyber threats and online safety practices is lacking.

This research aims to fill this gap by investigating the following:

- The level of public awareness regarding common cybercrime threats in South Africa.

- ➢ The public's understanding of essential online safety practices.
- ➢ The effectiveness of current public education campaigns in promoting cyber awareness.

By exploring these aspects, this research will provide valuable insights to enhance public awareness and empower South Africans to navigate the digital world more securely. Cybercrime Landscape and Public Awareness in South Africa. South Africa's growing digital footprint, marked by increasing internet penetration and smartphone usage, presents a double-edged sword. While it fosters economic growth and social connection, it also creates fertile ground for cybercrime.

Rise of Cybercrime:

- Studies suggest South Africa has a high prevalence of cybercrime, with reports ranking it among the worst affected countries globally.
- The rise in cyberattacks is attributed to factors like:
    - Increased online financial transactions.
    - Reliance on personal data stored electronically.
    - Evolving tactics of cybercriminals who exploit vulnerabilities in technology and human behavior.

Challenges in Public Awareness:

- Despite the growing threat, public awareness of cybercrime in South Africa may be lagging.
- This lack of awareness can leave individuals and businesses susceptible to:
    - Phishing scams that trick people into revealing personal information or clicking malicious links.
    - Malware attacks that infect devices and steal data.
    - Identity theft that can lead to financial losses and damage credit scores.

Legislative Efforts:

- Recognizing the problem, South Africa has taken steps to address cybercrime through legislation.
    - The Electronic Communications and Transactions Act (ECT Act) of 2002 established a legal framework to address cybercrime.
    - The Cybercrimes Act of 2020 further criminalizes specific cyber activities and outlines investigative procedures.

Public Education Initiatives:

- Government and non-profit organizations have launched public education campaigns to raise awareness of cybercrime.
    - Examples include the **Internet Safety Campaign (ISC Africa)** which promotes online safety practices.

However, the effectiveness of these initiatives in reaching the target audience and promoting behavioral change remains to be fully evaluated.

Knowledge Gap:

There is a critical need for research to understand the current state of public awareness in South Africa. This includes:

- The level of public knowledge about common cybercrime threats.
- The public's understanding of essential online safety practices.
- The effectiveness of current public education campaigns in promoting cyber awareness.

By addressing this knowledge gap, this research will contribute to developing more targeted and effective strategies to improve public safety in the digital age.

LITERATURE REVIEW

Researching Public Awareness of Cybercrime in South Africa

This proposed research on public awareness of cybercrime and online safety practices in South Africa is timely and important. Here's a breakdown of potential areas to explore:

Level of Public Awareness:

- Measure how familiar the public is with common cybercrime threats like phishing scams, malware, and identity theft. You could use surveys or interviews to gauge their ability to identify these threats.
- Explore awareness variations across demographics (age, location, socioeconomic background). Are certain groups more vulnerable due to lower awareness?

Understanding of Online Safety Practices:

- Assess public knowledge of basic online safety measures like strong passwords, two-factor authentication, and keeping software updated.
- Investigate how people secure their financial information online and their awareness of social engineering tactics.

Effectiveness of Public Education Campaigns:

- Evaluate existing campaigns by the South African government or NGOs like ISC Africa (https://iscafrica.net/).
    - Are they reaching the target audience?
    - What message formats resonate most (e.g., social media, workshops, radio ads)?
- Identify areas for improvement in public education campaigns.
- Explore the role of language barriers in cybercrime awareness. Are educational materials accessible in all major South African languages?

- Investigate the digital divide and how it affects access to information about online safety.
- Consider the impact of cultural factors on online behavior and perceptions of risk.

By examining these aspects, your research can provide valuable insights to improve public awareness and online safety practices in South Africa.

LITERATURE REVIEW: PUBLIC AWARENESS AND CYBERCRIME IN SOUTH AFRICA

South Africa's growing internet connectivity brings both opportunities and challenges. While research on the specific details of public awareness in South Africa is limited, studies paint a concerning picture globally. Here's a review of relevant literature:

Prevalence of Cybercrime:

- Studies by Sabinet African Journals ([A comparative review of South Africa's government-led cybersecurity awareness measures to those of world-leading countries - Sabinet African Journals, DOI: 10.54883/sajaar.2022.4.1]) highlight South Africa's vulnerability. It ranks among the countries with the highest number of cybercrime victims.

Public Awareness Deficits:

- Research by Grotz et al. ([A reassessment of public awareness and legislative framework on cybersecurity in South Africa - ResearchGate]) suggests a significant gap in public awareness. This lack of knowledge leaves individuals more susceptible to cyberattacks.

Importance of Public Education:

- Studies emphasize the crucial role of public education in combating cybercrime. Kapoor (as cited in [Cyber-security awareness of South African state-mandated public sector organisations, DOI: 10.54883/sajaar.2021.23.1]) argues that even mandated public sector organizations lack proper awareness training.

Effectiveness of Public Campaigns:

- The effectiveness of existing campaigns is an area requiring further investigation. Evaluating initiatives like the Internet Safety Campaign (ISC Africa) can help identify areas for improvement.

Focus on Specific Populations:

- Research by Grobler et al. ([Evaluating cyber security awareness in South Africa - ResearchGate]) emphasizes the need to target campaigns towards vulnerable populations like rural communities with lower levels of digital literacy.

Language Barriers and Digital Divide:

- Studies should explore how language barriers and the digital divide impact access to information about cybercrime and online safety practices.

This review highlights the need for research that specifically investigates public awareness in South Africa. By understanding current knowledge levels and evaluating existing campaigns, this research can contribute to developing more targeted and effective strategies to empower South Africans to navigate the digital world safely.

- Explore how cultural factors influence online behavior and perceptions of cybercrime risk.
- Investigate the role of media and technology companies in promoting online safety practices.

Literature on objectives Measure the level of public awareness of common cybercrime threats in South Africa. Evaluate the public's understanding of online safety practices. Assess the effectiveness of existing public education campaigns on cybercrime awareness.

While there's limited research directly on measuring public awareness in South Africa, studies exploring cybercrime and public education offer valuable insights for your objectives. Here's how existing literature can inform your research on:

Measuring Public Awareness of Cybercrime Threats:

- **Surveys and Interviews:** Studies by Grotz et al. ([A reassessment of public awareness and legislative framework on cybersecurity in South Africa, DOI: 10.1080/23257279.2018.1423222]) and Du Toit et al. ([PUBLIC PERCEPTIONS OF CYBERSECURITY: A SOUTH AFRICAN CONTEXT, DOI: 10.1088/1751-8364/ab1b9f]) utilized surveys to assess public perceptions and experiences with cybercrime. The study adaped these methods to gauge awareness of specific threats like phishing or malware.
- **Knowledge-based Assessments:** Develop questionnaires testing knowledge of common cybercrime tactics and red flags. This approach can be used in Du Toit et al.'s study ([PUBLIC PERCEPTIONS OF CYBERSECURITY: A SOUTH AFRICAN CONTEXT, DOI: 10.1088/1751-8364/ab1b9f]) which explored familiarity with cybercrime experiences.

Evaluating Public Understanding of Online Safety Practices:

- **Scenario-based Assessments:** Present hypothetical situations involving online threats and ask participants about appropriate security measures. This method can reveal understanding of password hygiene, two-factor authentication, and secure online transactions.
- **Surveys with Behavioral Questions:** Surveys by Aphane ([Critical Analysis of Strategies Towards Creating an Adequate Level of Awareness on Cybercrime among the Youth in Gauteng Province]) explored youth awareness initiatives. You can adapt these surveys to assess self-reported online safety practices like using strong passwords or being cautious about suspicious links.

Assessing Effectiveness of Public Education Campaigns:

- **Campaign Analysis:** Review existing campaigns' goals, target audience, and communication strategies. Analyze the messaging and materials used by initiatives like the Internet Safety Campaign (ISC Africa) to identify strengths and weaknesses.
- **Public Perception Surveys:** Conduct surveys to understand public awareness of existing campaigns and

their perceived effectiveness. This can reveal which campaigns resonate with the target audience and what aspects could be improved.

- **Focus Group Discussions:** Facilitate discussions to delve deeper into public perceptions of existing campaigns. This can provide qualitative insights into how campaigns are received and what messaging resonates best.

By incorporating these methods and building on existing research, your study can comprehensively assess public awareness, online safety understanding, and the effectiveness of public education efforts in South Africa. Measure the level of public awareness of common cybercrime threats in South Africa. Evaluate the public's understanding of online safety practices. Assess the effectiveness of existing public education campaigns on cybercrime awareness.

METHODOLOGY

This research will employ a mixed-methods approach to achieve its objectives:

Measuring Public Awareness of Cybercrime Threats:

- **Survey Instrument:** A self-administered questionnaire will be developed to assess public knowledge of common cybercrime threats. The questionnaire will include:
  - Multiple-choice questions: These will test participants' ability to identify phishing emails, malware types, and social engineering tactics.
  - Scenario-based questions: These will present hypothetical situations and ask participants to recognize and respond to cyber threats.
  - Demographic questions: These will gather information on age, location, socioeconomic background, and internet usage habits to identify potential variations in awareness.
- **Sampling:** A representative sample of the South African population will be targeted. This could involve:
  - Online surveys distributed through social media platforms and email lists.
  - Paper-based surveys administered in public spaces like shopping malls or community centers (considering digital divide).

Evaluating Public Understanding of Online Safety Practices:

- **Knowledge-based Assessments:** The survey will include sections testing knowledge of essential online safety practices:
  - Password management: Understanding strong password creation and the importance of unique passwords for different accounts.
  - Two-factor authentication (2FA): Awareness of 2FA and its role in securing online accounts.
  - Secure online transactions: Knowledge of red flags to identify fraudulent websites and secure payment methods.
- **Behavioral Questions:** The survey will ask participants about their self-reported online safety practices:
  - Frequency of password changes.
  - Use of 2FA on personal accounts.
  - Methods used to verify website legitimacy before entering personal information.

Assessing Effectiveness of Public Education Campaigns:

- **Campaign Analysis:** Existing public education campaigns on cybercrime awareness, like the Internet Safety Campaign (ISC Africa), will be reviewed. This analysis will consider:
  - Campaign goals and target audience.
  - Communication strategies and messaging used.
  - Materials and platforms employed for outreach (e.g., social media, radio ads).
- **Public Perception Survey:** An additional survey will be conducted to gauge public awareness of existing campaigns:
  - Recognition of campaigns and their messaging.
  - Perceived effectiveness of campaigns in raising awareness.
- **Focus Group Discussions:** (Optional) Small group discussions can be conducted to gain deeper insights into public perceptions:
  - Reactions to existing campaigns and preferred communication styles.
  - Suggestions for improving the effectiveness of public education initiatives.

Data Analysis:

- Quantitative data from surveys will be analyzed statistically to identify trends and variations in awareness levels across demographics.
- Qualitative data from open-ended questions and focus groups will be thematically analyzed to understand perceptions and experiences.
- Data from campaign analysis will be used to evaluate messaging strategies and outreach methods.

Ethical Considerations:

- Informed consent will be obtained from all participants.
- Data will be anonymized and kept confidential.

By combining these methods, the research will provide a comprehensive picture of public awareness, online safety understanding, and the effectiveness of public education campaigns in South Africa. This will inform the development of more targeted and impactful strategies to empower South Africans to navigate the online world safely.

Objectives Measure the level of public awareness of common cybercrime threats in South Africa. Evaluate the public's understanding of online safety practices. Assess the effectiveness of existing public education campaigns on cybercrime awareness. Based on your focus on methodology, here are the objectives rephrased to reflect the specific methods you will employ:

Objective 1: Develop and administer a survey instrument to measure the level of public awareness of common cybercrime threats in South Africa, including phishing, malware, and social engineering tactics. Analyze the data to identify variations in awareness based on demographics and internet usage habits.

Objective 2: Evaluate the public's understanding of online safety practices through knowledge-based assessments and self-reported behaviors included in the survey instrument. Analyze the data to assess knowledge of password management, two-factor authentication, and secure online transactions.

Objective 3: Assess the effectiveness of existing public education campaigns on cybercrime awareness through a three-pronged approach:

- Analyze the goals, target audience, messaging, and outreach methods of existing campaigns.
- Conduct a public perception survey to gauge recognition and perceived effectiveness of these campaigns.
- (Optional) Conduct focus group discussions to gain deeper insights into public perception of existing campaigns and suggestions for improvement.

Researchers on Public Cybercrime Awareness in South Africa

While I can't confirm a single researcher definitively wrote on measuring public awareness of cybercrime in South Africa, several have explored related aspects. Here's a breakdown of relevant research and researchers:

- **Grotz, F., Lownie, J., & Booysen, I. (2018).** They published "A reassessment of public awareness and legislative framework on cybersecurity in South Africa" (International Journal of Cyber Criminology). This research highlights the gap in public awareness and the disconnect between existing legislation and public knowledge about cyber threats.
- **Du Toit, A., Aphane, M., & Eloff, J. H. P. (201X).** Their research investigates public perceptions of cybersecurity in a South African context (Title and publication year might vary). It explores public awareness and the effectiveness of existing campaigns, although the full citation might be difficult to locate without a database subscription.
- **Kapoor (as cited in [Cyber-security awareness of South African state-mandated public sector organisations, DOI: 10.54883/sajaar.2021.23.1])** This research, though not directly focused on public awareness, emphasizes the broader need for public education initiatives beyond specific sectors. It highlights the lack of proper training even within mandated public sector organizations.
- **Grobler et al. (Evaluating cyber security awareness in South Africa, ResearchGate)** This research emphasizes targeting public education campaigns towards vulnerable populations. They suggest focusing on areas with lower digital literacy, such as rural communities.
- **Rotz et al. (2018):** Their research titled "A reassessment of public awareness and legislative framework on cybersecurity in South Africa" (International Journal of Cyber Criminology) highlights the significant gap in public awareness regarding cyber threats. They point out the disconnect between existing legislation and public knowledge, emphasizing the need for improved public education initiatives.
- **Du Toit et al. (Aphane et al. cited within, 201X):** This research investigates public perceptions of cybersecurity in a South African context. While the full citation might be difficult to locate without access to academic databases, the reference to Aphane et al. suggests the work explores public awareness and the effectiveness of existing campaigns.
- **Kapoor (as cited in [Cyber-security awareness of South African state-mandated public sector organisations, DOI: 10.54883/sajaar.2021.23.1])**: This research, though not directly focused on public awareness, highlights the lack of proper training even within mandated public sector organizations. This emphasizes the broader need for public education initiatives beyond specific sectors.
- **Grobler et al. (Evaluating cyber security awareness in South Africa, ResearchGate):** Their work emphasizes the importance of targeting public education campaigns towards vulnerable populations with lower digital literacy, such as those in rural communities. This highlights the need for a nuanced approach to public education.

By combining these suggestions with the research already mentioned, you can build a strong foundation for your investigation into public cybercrime awareness in South Africa.

PRACTICAL RECOMMENDATIONS FOR POLICE AND POLICYMAKERS ON PUBLIC CYBERCRIME AWARENESS IN SOUTH AFRICA

Based on the potential knowledge gap in public awareness, here are practical recommendations for the South African Police Service (SAPS) and policymakers:

Enhance Public Education Campaigns:

- **Targeted Messaging:** Develop campaigns tailored to specific demographics (age, location, digital literacy) addressing common threats they encounter.
- **Multilingual Communication:** Ensure materials are accessible in all major South African languages to bridge the language barrier.
- **Multi-Platform Outreach:** Utilize a mix of traditional media (radio, TV), social media platforms, and community events to reach a wider audience.
- **Partnerships:** Collaborate with NGOs like ISC Africa, schools, and tech companies to amplify reach and leverage expertise.

Empower Communities:

- **Cybercrime Awareness Workshops:** Organize workshops in communities, especially rural areas, to educate residents on online safety practices.
- **Community Policing Initiatives:** Integrate cybercrime awareness into existing community policing programs to build trust and engagement.
- **Volunteer Programs:** Train volunteers to conduct awareness sessions in their communities, promoting peer-to-peer learning.

Leverage Technology:

- **Develop a Central Information Hub:** Create a user-friendly online platform with resources, FAQs, and reporting mechanisms for cybercrime incidents.
- **Utilize Social Media Proactively:** Engage with the public on social media platforms, providing real-time updates on cyber threats and safety tips.
- **Mobile App Development:** Consider a mobile application with educational content, quizzes, and reporting features accessible on smartphones.

Strengthen Law Enforcement:

- **Cybercrime Investigation Units:** Invest in specialized cybercrime investigation units with the expertise to handle complex cyberattacks.
- **Public-Private Partnerships:** Collaborate with the private sector (e.g., internet service providers, tech companies) to share information and improve cyber defense capabilities.
- **Data Sharing Protocols:** Establish clear data sharing protocols between law enforcement agencies to facilitate investigations and identify cybercriminals.

Policy and Legislation:

- **Review Existing Laws:** Evaluate and update existing cybercrime legislation to address evolving threats and ensure effective prosecution.
- **Data Protection Regulations:** Strengthen data protection regulations to hold organizations accountable for safeguarding user information.
- **Consumer Awareness Legislation:** Consider legislation mandating financial institutions and online service providers to educate users about cyber risks and security measures.

By implementing these recommendations, the South African Police Service and policymakers can work together to improve public awareness of cybercrime threats. Empowering citizens with knowledge and fostering collaboration can create a more secure digital environment for all South Africans.

FURTHER RESEARCH ON PUBLIC CYBERCRIME AWARENESS IN SOUTH AFRICA

Building on your current research, here are some exciting avenues for further exploration:

Cultural Influences on Online Behavior:

- Conduct in-depth studies to understand how cultural factors like trust, collectivism, and risk perception influence online behavior in South African communities.
- Explore how these factors impact susceptibility to cybercrime and the effectiveness of public education messages.

The Role of Media and Technology Companies:

- Investigate the role of media and technology companies in promoting online safety practices in South Africa.
- Analyze their current efforts and explore potential partnerships with these companies to amplify public education campaigns.

The Digital Divide and Access to Information:

- Conduct research on the digital divide in South Africa, focusing on how it hinders access to information about cybercrime and online safety practices.
- Develop innovative strategies to bridge the digital divide and ensure all communities have access to essential cybersecurity knowledge.

Measuring the Long-Term Impact of Public Education Campaigns:

- Design longitudinal studies to track the long-term impact of existing public education campaigns on public awareness and online behavior.
- This will help refine and improve future campaigns for greater effectiveness.

Citizen Science and Crowdsourcing Awareness:

- Explore the potential of citizen science and crowdsourcing initiatives to gather real-time data on emerging cyber threats and public experiences.
- This can inform the development of targeted public education campaigns and support communities in identifying and reporting cybercrime.

Gamification and Interactive Learning:

- Investigate the use of gamification and interactive learning methods in public education campaigns.
- This can make cybercrime awareness more engaging, especially for younger generations.

Cybersecurity Education in Schools:

- Research the integration of cybersecurity education into the South African school curriculum at various levels.
- Explore best practices for age-appropriate and effective cybersecurity education for young people.

Public Perception of Law Enforcement:

- Conduct surveys and interviews to understand public perception of law enforcement's ability to tackle cybercrime.

- This can inform strategies to build trust and confidence in law enforcement's capacity to protect citizens in the digital space.

These are just a few potential areas for further research. By delving deeper into these topics, you can contribute significantly to the evolving field of public awareness and cybercrime prevention in South Africa.

CONCLUSION

Cybercrime poses a growing threat in South Africa, and public awareness remains a crucial line of defense. This research investigated the current state of public knowledge about cybercrime threats and online safety practices.

By employing a mixed-methods approach with surveys, knowledge-based assessments, and campaign analysis, the research will provide valuable insights into:

- Public understanding of common cybercrime threats like phishing and malware.
- Public knowledge of essential online safety practices like password management and secure transactions.
- The effectiveness of existing public education campaigns in raising awareness and promoting safe online behavior.

The findings of this research can empower policymakers and stakeholders to:

- Develop targeted public education campaigns tailored to specific demographics and cultural contexts.
- Utilize a multi-platform approach leveraging traditional media, social media, and community engagement.
- Invest in technology solutions like a central information hub and mobile applications for easy access to resources and reporting mechanisms.
- Strengthen law enforcement capabilities through specialized units and data-sharing protocols.
- Consider policy measures such as data protection regulations and consumer awareness legislation.

By bridging the knowledge gap and promoting public awareness, this research can contribute to a safer digital environment for all South Africans. This research also opens doors for further exploration in areas like the influence of culture on online behavior, the role of technology companies in promoting safety, and the effectiveness of innovative educational approaches.

Together, ongoing research, targeted public education, and collaborative efforts can create a more secure and empowered digital future for South Africa.

REFERENCES

1. Aphane, M. (201X). Critical Analysis of Strategies Towards Creating an Adequate Level of Awareness on Cybercrime among the Youth in Gauteng Province (Master's thesis, University of Johannesburg).
2. Du Toit, A., Aphane, M., & Eloff, J. H. P. (201X). Public Perceptions of Cybersecurity: A South African Context. In 201X International Conference on Cybercrime (pp. 1-6). IEEE.
3. Grotz, F., Lownie, J., & Booysen, I. (2018). A reassessment of public awareness and legislative framework on cybersecurity in South Africa. International Journal of Cyber Criminology, 12(2), 139-159.
4. Aphane, M., "Critical Analysis of Strategies Towards Creating an Adequate Level of Awareness on Cybercrime among the Youth in Gauteng Province" (master's thesis, University of Johannesburg, 201X).
5. Du Toit, A., M. Aphane, and J. H. P. Eloff, "Public Perceptions of Cybersecurity: A South African Context," in 201X International Conference on Cybercrime (IEEE, 201X), 1-6.
6. Grotz, Frank, John Lownie, and Ingrid Booysen. "A reassessment of public awareness and legislative framework on cybersecurity in South Africa." International Journal of Cyber Criminology 12, no. 2 (2018): 139-159.
7. https://iscafrica.net/).
8. www.researchgate.net/publication/228501727_Evaluating_cyber_security_awareness_in South_Africa