Cyber-Identify Theft

Although the introduction of ICT and its continuous evolution brings many positive benefits to digitizing and improving our everyday lives and industries globally, it also has negative consequences, one of which been cyber-identify theft.

Cyber-Identify theft is one the most common internet-related crimes, involving the use of electronic means (e.g., use of ICT, via the Internet) to gain unauthorised access to any legal personal information or identity such as: names, addresses, social security numbers, documents, bank account information and so on, - with the intent of carrying out any form of deceitful activity, whether online or offline.

This cybercrime not only targets individuals, but also businesses and organizations, leaving victims socially, mentally and financially impacted (Close, et al., 2006).

Kenyan report, (Communications Authority of Kenya, 2022), points out how other than social media platforms been one of the hosts to cyber-identity theft and impersonation, various phishing attacks like use of emails, have also contributed to the successful theft of sensitive data. Other contributions include: social engineering techniques, accessing untrusted websites, improper disposal of documents containing personal information on them, data breaches, ignorance and lack of cybersecurity awareness, and many more.

The Kenyan government has established various investigative tools and practices to combat cybercrime. For instance, in 2018, the Cybercrime and Computer Related Crimes Bill was approved, thus establishing a legal framework for prosecuting cybercriminals (Anon, 2018). Additionally, to coordinate the country's response to cyber threats, the National Kenya Computer Incident Response Team (National KE-CIRT/CC) was formed (Communications Authority of Kenya, N.D.). However, investigating cyber-identity theft crimes can be challenging especially if the crimes are international or transnational. In numerous instances, the use of Kenyan and international investigative tools and practices may hinder the effectiveness of an investigation. Among these limitations are:

- Lack of cooperation among different law enforcement agencies, jurisdictions and legal frameworks, limits cross-border sharing of information and evidence. Since different countries are governed by different laws and legal systems, it can be difficult for the investigators to collect evidence and hold cyber criminals accountable; example it can be more challenging when criminals have different nationalities.
- Victims conceal attacks by not admitting or reporting the attack so as to protect their reputation, example when National Bank of Kenya initially denied been targeted whereby millions of shillings was stolen and client accounts tampered with (Karanja, 2017).
- Lack of expertise, capacity and resources needed to investigate the cybercrime effectively. Due to the rapid growth of technology, some countries are more up-to-speed with new technologies while other lag behind and need to improve their ways to investigating and tackling cybercrimes. Additionally, due to the complexity of cybercrimes, Kenya may experience difficulty and delays in identifying, investigating and prosecuting cybercriminals (Kahongeh, 2022).

- Poor handling of evidence that leads to the case not been inadmissible in court (Kahongeh, 2022).

Aside from the victims been financially impacted by cyber-identity theft, the cost of investigating and prosecuting this crime can be high, especially when the case is handled by: multiple countries (requiring international cooperation) or multiple jurisdictions or legal frameworks.

In conclusion, cyber-identity theft is growing rampantly resulting in financial, psychological and social consequences for victims. While international and Kenyan investigative tools and practices are in place to combat cybercrime, their effectiveness may be limited by the above-mentioned limitations, so more needs to be done to enhance effective tactics for combating cyber-identity theft.

References

Anon, 2018. *Laws of Kenya.* [Online]
Available at: http://www.kenyalaw.org/lex/actview.xql?actid=No.%205%20of%202018
[Accessed 29 April 2023].

Close, A. G., Zinkhan, G. M. & Finney, Z. R., 2006. Cyber-Identity Theft. *Encyclopedia of E-Commerce, E-Government, and Mobile Commerce,,* pp. 168-171.

Communications Authority of Kenya, 2022. *October-December Cybersecurity Report,* Nairobi: The National KE-CIRT/CC.

Communications Authority of Kenya, N.D.. *The National KE-CIRT/CC.* [Online]
Available at: https://ke-cirt.go.ke/
[Accessed 29 April 2023].

Kahongeh, J., 2022. *How legal loopholes are hurting Kenya's cybercrime fight.* [Online]
Available at: https://www.businessdailyafrica.com/bd/data-hub/how-legal-loopholes-are-hurting-kenyas-cybercrime-fight-3727058#:~:text=Legal%20and%20forensics%20experts%20now,the%20biggest%20setback%20for%20investigators.
[Accessed 29 April 2023].

Karanja, J., 2017. *Cybercrime Related Investigations in Kenya.* [Online]
Available at:
https://www.researchgate.net/publication/331431758_Cybercrime_Related_Investigations_in_Kenya
[Accessed 29 April 2023].