Assessing the Relationship Between Digital Footprints and Identity Theft on Social Networks in Ireland

Student: Olayera Oladele, Supervisor: James Egan

School of Computing, South East Technological University, Ireland

Abstract

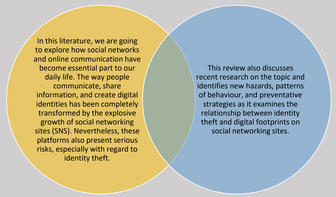
The correlation between identity theft on Irish social networks and digital footprints is researched in this dissertation. As online platforms grown in popularity, worries about data security, digital privacy, and the possibility of cybercriminals abusing personal data have grown. Irish users' understanding of internet security, the effectiveness of current security measures, and the degree to which digital footprints contribute to identity theft are all examined in this study.

According to the report, a sizable percentage of Irish users are not entirely aware of the consequences of their digital footprint, despite the fact that they are active on social media. Even with GDPR in place, the study also identifies weaknesses in Ireland's legal system for preventing identity theft. Case studies also highlight the serious financial and reputational harm that excessive online sharing has caused to people. Suggestions for increased user knowledge, more stringent laws, and cutting-edge cybersecurity techniques to reduce dangers are made in the dissertation's conclusion.

Introduction

When people interact online, they leave behind traces, such as social media activity, website visits, and digital transactions. These are known as digital footprints. Understanding who we are online is essential in protecting user representation. It is crucial to take a step back and obtain a thorough understanding of general personal methods after examining a wide range of dissimilar issues. It is crucial to explicitly question consumers about their intentions and the implications of their digital footprints in general.

Literature Review



Methodology

A mixed method approach will be used for the research. Analysis of information gathered from many sources and conclusions (using both qualitative and quantitative methods). This will be carried out using some Interview techniques, survey and secondary data

Research Questions

1. In what ways can digital footprints make people more susceptible to identity theft?
2. Which kind of identity theft are most prevalent in Ireland?
3. How well do the security mechanisms in place now prevent identity theft?
4. Which legislative frameworks are in place in Ireland to combat digital fraud, and what is their level of effectiveness?

Early Study

Numerous investigations have looked into the connection between identity theft and digital footprints (Tolulope, 2020). These results offer insightful information, even though they are not just focused on Ireland. Having read about identity theft from a number of perspectives, including research on computer security and privacy, online behaviours that increase or decrease the risk of identity theft, and the objectives and tactics of automated identity theft attacks. Initiatives like digital certificate authorisation, biometrics authentication, public key infrastructure, and digital identity management systems aim to protect data, including identity information. However, a comprehensive, structured framework for addressing identity theft detection difficulties has not yet been established.

Study Areas

Target Population: The study looks at young adults and older people in Ireland who use social media and conduct digital transactions.

includes information from identity theft victims, legal experts, and cybersecurity specialists.

Conclusion

Despite being an inevitable aspect of online life, digital footprints put people at risk for fraud, identity theft, and privacy invasion. People need to be vigilant in safeguarding their online presence as hackers create increasingly complex methods to take advantage of personal information.

Recommendation

Personal vigilance, strong privacy settings, legislative protections, and knowledge of new cyberthreats are all part of Ireland's defense against identity theft through social media. People may better protect their digital footprint and stop identity theft by using cybersecurity best practices including turning on two-factor authentication, keeping an eye on online activities, and keeping up with emerging threats.

References

Tolulope, K. A. V. O. L. A. O. s. N. O., 2020. Social Media and Identity Theft Implications on Nigerian Victims and International Economy. pp. 823-836.

https://www.bing.com/images/search?q=Social+Media+Logos+Transparent&form=RESTAB&first=1

Clea A Machold, G. J. A. M. J. E. A. M. M. E. R., n.d. Social networking patterns/hazards among Irish teenagers..

Available at: https://typeset.io/papers/social-networking-patterns-hazards-among-irish-teenagers-1keiaOv3r6

Walsh, M. J., & Baker, S. A. (2022). Avoiding conflict and minimising exposure: Face-work on Twitter. Convergence, 28(3), 664-680. https://doi.org/10.1177/13548565211036797