BOOK CHAPTER | Social Media Data Privacy

Keyword and Hashtag Search On Facebook Content: Reflections On Social Media User Data Privacy

Ayodele Oluwakemi Sade (PhD) & Owoeye Folusho Olayinka
Department of Computer Science,
Kogi State Polytechnic, Lokoja
E-mail: kemtemmy2009@gmail.com
Phone: +2348069804373

Abstract

The adoption of Facebook as a platform for social interaction has contributed to the exponential growth in user-generated content. Recently, there is a rising concern over user behaviours that mitigate data privacy on social media. This chapter conducted keywords and hashtags search on Facebook posts to understand social media user behaviour and content that constitute a threat to data privacy. The result established a correlation between personal data accessible on Facebook, identity theft, stalking, and social engineering attacks such as smishing and vishing. Data privacy literacy, privacy settings, and prioritizing privacy above influencer complex are amongst solutions proffered for social media user data privacy.

Keywords: Hashtag, Search, Facebook, Privacy, Social media, User, Data, -19, Security, Scam

Introduction

Social media user-generated data privacy entails individuals and corporate entities using the networking site to exercise control and be selective with personal or sensitive information being shared. Conversely, as social media such as Facebook encourages engagement there are instances of personal and sensitive data disclosure on networking sites which can be attributed to various reasons. The users' perception of privacy, fear of missing out and trust on social media platforms have been identified as reasons social networking site users overlook data privacy when posting content (Parker & Flowerday, 2021; Bright et. al., 2021; Schäwe et. al, 2021). Recently, a high rate of cyber-attacks such as social engineering has been attributed to interactions and personal data accessible on social media platforms (Banire et.al., 2021). To understand the dynamics of user data and social media content that affect privacy or empower cyber thieves, this chapter explores keywords and hashtags on Facebook. The insight gained reveals the consequences of user data privacy violations and the potential way forward.

Citation: Ayodele Oluwakemi Sade (PhD) & Owoeye Folusho Olayinka (2022).

Case Studies

The case studies present scenarios where Facebook users divulge data that poses a high risk to data privacy.

Case 1: Financial Details

Giveaways, soliciting for financial help, and payment for goods or services are common instances when Facebook users publicly disclose financial details which include: full name, account number, and bank name. A social media influencer, group administrator, or public figure announces a giveaway contest stating criteria such as random selection and requests interested participants to comment with valid bank details. Similarly, a common trend of disclosing back account details and phone numbers are noticeable amongst individual seeking financial assistance to offset medical bills and online vendors.

Case 2: Trending Facebook Group Member Data Challenge

Facebook groups are created to bring people from diverse backgrounds with an interest in a common cause. Hashtag search reveals challenges in Facebook groups which visibility is set public where members disclose biodata, hobbies, nickname, pet, and other data as deemed fit. The posts generated high engagement such as likes, emojis, and comments.

This created an avenue for members to increase friendship, online followers, and visibility. Also, the platform avail opportunities for online vendors to market, brand, and advertise a business. The concern here is, it is easy for participants to cross the data privacy threshold and give-up sensitive data to increase likes and comments.

Case 3: Facebook Quizzes and Games Hint on Security Answers for Password Recovery

Content is crucial driving engagements. Entertaining content such as quizzes and games on Facebook generates high comments. The keyword search showed some of the seemly harmless games and quizzes ask personal and historical questions. Sample search output shows these:

"*Where you met your partner/spouse*?" "*Favourite food/colour/teacher/pet*" etc.

Online criminals can harvest these responses to decode security answers for e-mail and social media account recovery, mobile bank app settings, and other online profile accounts.

Implication of Data Privacy Violations

Smishing and Vishing Attacks

A smishing attack occurs when a compelling Short Message Service (SMS) from a supposedly trusted source is sent to trick the receiver to release sensitive information while a vishing attack occurs over a phone call. In this chapter, we compared recorded imposter scam phone calls masquerading as representatives of Nigerian bank customer service officers and bank account details posted on Facebook.

A common trend in phone calls is the imposter trying to gain the confidence of the potential victim by giving out bank details and information associated with the receiver. Thus bank account details, phone numbers, and other personal data in the public domain such as Facebook empower imposters with data, increase the likelihood of successful psychological manipulation, and make the individual prone to social engineering threats.

Similarly, unsolicited text messages masked to have originated from government or financial institution has the potential to leverage personal data on social media platforms to perpetuate smishing.

SMISHING
Phishing gets two new neighbours, and they are just as deadly
VISHING

Fig. 1: Smishing & Vishing Attacks
Source: https://blog.logix.in/vishing-smishing/

Identity Theft

Social media challenge where participants churn out personal data is a lucrative opportunity for criminals to harvest data. The thieves either use the collected data to hijack the victim's account or create a fake profile for mischievous purposes.

Stalking and Fraudulent Appeals

The keyword search revealed personal and meta tags on social media equip stalkers and inform criminals of the right perspective to present fraudulent appeals. The appeal could be linked to a family member tagged on the targeted victim's timeline at a location shared alongside the content.

Fig 2: Cyber Stalking and Its Components
Source: https://cyberbullying.org/cyberstalking

Use Social Media Without Losing Data Privacy

Data Privacy Literacy

Over the years cyber security training is being tailored for people in formal education and organisation (Banire et.al., 2021). Netizens are comprised of people from diverse backgrounds and orientations. Hence, this necessitates every internet user to be data privacy literate irrespective of social status.

Data privacy skills should be incorporated into the education curriculum for all students from primary schools to tertiary institutions to inculcate ethics and etiquette. Furthermore, language, social class and age-appropriate data privacy awareness are needed to orientate social media users.

Explore Social Media Privacy Settings

Social media platforms such as Facebook privacy features are usually found under the app settings. Users can explore this feature to regulate access to data available in their profile and timeline.

Prioritize Data Privacy Above Influencer Complex

The drive for likes, comments, and online followership is a factor that influences posts and comments on social media. It is pertinent for individuals and social media groups to reflect on the possible consequences of content being posted through the social media profile.

Timeline and Content Clean-up

Peradventure, user-content on Facebook and other social media handles includes sensitive and personal data that compromise data privacy.

Conclusion

In conclusion, this chapter has underlined the importance of social users being data privacy-conscious. Understanding possible data privacy vulnerabilities cyber thieves can exploit helps in developing countermeasures and building cyber smart web surfers.

References

1. Banire, B., Al Thani, D., & Yang, Y. (2021). Investigating the experience of social engineering victims: Exploratory and user testing study. *Electronics (Switzerland)*, *10*(21). https://doi.org/10.3390/electronics10212709
2. Bright, L. F., Lim, H. S., & Logan, K. (2021). “Should I Post or Ghost?”: Examining how privacy concerns impact social media engagement in US consumers. *Psychology and Marketing*, *38*(10), 1712–1722. https://doi.org/10.1002/mar.21499
3. Parker, H. J., & Flowerday, S. (2021). Understanding the disclosure of personal data online. *Information and Computer Security*, *29*(3), 413–434. https://doi.org/10.1108/ICS-10-2020-0168
4. Schäwel, J., Frener, R., & Trepte, S. (2021). Political microtargeting and online privacy: A theoretical approach to understanding users’ privacy behaviors. *Media and Communication*, *9*(4), 158–169. https://doi.org/10.17645/mac.v9i4.4085