Social Networks, OSINT and Cybercrime -Strategies for User Protection in the Digital Age

Abereijo Tawakalitu Omobolanle
Department of Computer Systems Technology
203 Price Hall
North Carolina A & T State University
Greensboro, NC, USA 27411

ABSTRACT

The rise of social networks in the digital age has brought unparalleled opportunities for networking, collaboration and professional networking. However, these platforms have also provided fertile ground for cybercrime by sharing information openly. This paper examines the complex interplay of social networks, open source intelligence (OSINT), and cybercrime, highlighting the dual use of publicly available data Highlights the critical role of Social Media Intelligence (SOCMINT) a small OSINT team controls. Identity theft, and corporate espionage. The study examines the responsibilities of users, platforms, and law enforcement agencies in addressing cyber threats. Users should adopt best practices, such as two-factor authentication and compliance with privacy policies, while platforms should improve security measures and provide user education Regulatory frameworks and public-private partnerships are essential to address cybersecurity challenges and drive innovation. By examining blockchain-based data security and real-world case studies and identifying emerging trends, this study highlights the need for a multi-stakeholder approach to creating a thriving digital ecosystem protect the Identified Shared responsibility, user education and continued collaboration to prevent cybercrime and ensure security engagement on social networks Importance they are emphasized

Keywords: Social Networks, OSINT, SOCMINT, Cybercrime, Cybersecurity, Digital Responsibility, Phishing, Data Privacy, User Protection

CISDI Journal Reference Format
Abereijo, T.O. (2024): Social Networks, OSINT and Cybercrime -Strategies for User Protection in the Digital Age. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 15 No 4, Pp 29-36.
Available online at www.isteams.net/cisdijournal. dx.doi.org/10.22624/AIMS/CISDI/V15N1P3

1. INTRODUCTION

In the digital age, online social networks have become a cornerstone of personal and professional communication. While these systems facilitate communication and collaboration, they still expose users to cybersecurity risks. Information shared on these platforms, from personal photos to business insights, can be used for malicious purposes such as phishing, identity theft, and targeted attacks This publicly accessible area of information undertake open source intelligence (OSINT) (by Hassan et al. , 2020). A special subgroup of OSINT, Social Media Intelligence (SOCMINT), refers to the collection and analysis of information from social networks. Although originally developed for governments and law enforcement agencies, SOCMINT is increasingly being used by cybercriminals to identify and exploit vulnerabilities in users' digital footprints (Trottier & Fuchs, 2015).

This paper explores the connections between social networks, OSINT, and cybercrime, and provides insights into how collaboration between users and platforms can mitigate risk It includes an analytical, persuasive case study of LinkedIn establish functional and platform responsibilities. A multi-stakeholder approach, encompassing education, platform security audits, and regulatory oversight, is emphasized as a cornerstone for creating safe online environments

1.2 Mathematical Modeling and Algorithmic Approach

A risk assessment framework and algorithmic model are proposed to understand the risks associated with OSINT and SOCMINT. These tools assess the likelihood of a cyber threat based on user actions and actions taken on the platform.

Risk Assessment Theory

The risk of cybercrime exposure (R) can be calculated using the following formula:

$$R = P(U) \times V(D) \times C \qquad (1)$$

Where:
- P(U): Probability of user vulnerability (e.g., weak passwords, public profiles).
- V(D): Value of exposed data (e.g., personal identifiable information, corporate data).
- C: Cost or impact of exploitation (financial, reputational, operational).

1.2 Algorithm for Mitigating OSINT Risks Using Machine Learning

An algorithm leveraging machine learning can help automate threat detection on social networks:
1. Input user data, threat indicators, and platform security parameters.
2. Aggregate this data into a dataset for feature extraction.
3. Train a supervised model (e.g., Random Forest) to classify risk levels.
4. Generate risk scores and personalized recommendations based on predictions.

- Input: Public profile visibility = 70%, Password strength = Weak, Threat history = High.
- Calculation: Risk score $R_s = 0.4(0.7) + 0.3(0.3) + 0.3(0.8) = 0.58$ (Moderate Risk).
- Output: Enable two-factor authentication, reduce profile visibility, and report suspicious activities.

2. RELATED LITERATURE

This section examines existing research on the intersection of social networks, open source intelligence (OSINT), and cybercrime, focusing on key studies and theoretical frameworks The review focuses on the development of OSINT, the it means for cybersecurity,

2.1 Development of OSINT and SOCMINT

Open source intelligence (OSINT) refers to the collection and analysis of publicly available information for legitimate or malicious purposes. Hassan, Algarney, and Aldribi (2020) note that OSINT has become an important tool for organizations, governments, and cybercriminals. A key subunit of OSINT, Social Media Intelligence (SOCMINT), deals primarily with extracting data from social media platforms (Trottier & Fuchs, 2015). Originally developed for law enforcement and market research, SOCMINT is increasingly being used by malicious actors to identify weaknesses in individuals and organizations (Mann, 2021).

2.2 The Role Of Social Networks In Cybercrime

Social networks like LinkedIn, Facebook, and Twitter offer a wealth of user-generated content, making it a prime target for cybercriminals. Research by González, García-Ros, and Menéndez (2019) shows how attackers use OSINT tools such as Shodan and Maltego to gather information that can be used for phishing, identity theft, and corporate espionage Barnett (2019) explains how seemingly innocent public information or communications such as these can enable highly targeted cyberattacks.
For example, LinkedIn profiles that post employment information are often used to spear phishing emails posing as HR professionals.

2.3 Dual-Use OSINT Tools

While OSINT tools such as Maltego and FOCA have legitimate applications in cybersecurity and threat intelligence, they are equally useful for malicious Cybercriminals using these tools to simulate or target an organization's systems details (Hassan et al., 2020). This dual use of OSINT tools raises ethical and legal questions about access and accountability.

2.4 User knowledge and behaviour

User behavior greatly influences the effectiveness of cyberattacks. Many users underestimate the risks of sharing personal information online. Gonzalez et al. (2019) highlight the lack of cybersecurity awareness among social media users, leaving them vulnerable to attacks such as phishing and identity theft. Poor password usage and indiscriminate acceptance of connection requests further compound the issue.

2.5 Meeting Responsibilities

Social media platforms play an important role in ensuring security for users. The review highlights the ethical and professional responsibility of platforms to implement strong security measures. Trottier and Fuchs (2015) argue that platforms should provide user education, privacy management, and real-time threat detection systems. Mann (2021) argues that regulatory frameworks such as the General Data Protection Regulation (GDPR) are forcing platforms to adopt stricter data protection practices

2.6 Legal Collaboration Efforts

Regulatory agencies and governments play an important role in cybersecurity. Regulations such as the GDPR set the benchmark for data privacy and security, forcing platforms to align their practices with global standards (Barnett, 2021). Additionally, public-private partnerships, such as collaborations between law enforcement agencies and social media companies have proven effective in countering emerging threats.

3. METHODOLOGY

In addition to describing the research design, data collection, and analytical methods used in this study to examine the links between social networks, OSINT, and cybercrime, this sectionf presents an example data set how OSINT tools and techniques can reveal vulnerabilities in social networks.

3.1 Research design

The study used mixed methods, combining qualitative and metric methods:

1. Qualitative assessment: Articles developed in computer databases of OSint were reviewed.
2. Quantitative data: Disclosures in social networks were analyzed through simulated OSINT operations.

3.2 Summary of Information

1. Materials:
   a) Maltego: Used to map relationships and store metadata.
   b) Shodan: Analyzed proven systems and networks.
   c) Social cartographer scraped social media data available to the public.

2. Sources:
   a) Public comments on LinkedIn, Twitter and Facebook.
   b) Newsletters and event logs from cybersecurity organizations.
   c) Legal publications on data protection.

3. Ethical Considerations:
All data were collected from publicly available sources without any right of intrusion or breach of privacy.

3.3 Sample Data

Data sources

The sample data sets were collected using publicly available information obtained through tools such as Maltego and Social Mapper, and social media data were taken from anonymous LinkedIn, Twitter and Facebook profiles

Example 1: LinkedIn Data Collection

Data Point	Sample Value	Source	Potential Exploitation
Name	John Doe	LinkedIn Profile	Identity theft
Current Employer	ABC Tech	LinkedIn Profile	Phishing emails from "HR"
Job Title	Senior Software Engineer	LinkedIn Profile	Tailored attacks targeting specific tools
Connections	500+	LinkedIn Profile	Map professional networks
Public Posts	"Starting vacation tomorrow!"	LinkedIn Updates	Risk of physical theft

Example 2: Twitter Data Analysis

Metric	Result	Source	Interpretation
Followers	1,200	Twitter Profile	Indicates influence and reach
Geotags in Posts	Location: San Francisco	Twitter Geotags	Vulnerable to tracking
Topics of Interest	#Blockchain, #AI	Twitter Hashtags	Tailored phishing attacks
Engagement Metrics	500 likes, 300 retweets	Twitter Analytics	High visibility for malicious actors

Example 3: Facebook Data Insights

Profile Details	Example Value	Source	Implication
Date of Birth	Jan 15, 1990	Facebook Profile	Password recovery exploitation
Relationship Status	Married to Jane Doe	Facebook Updates	Social engineering attacks
Frequent Check-ins	CoffeeShop123, MallXYZ	Facebook Locations	Real-time location tracking

4. CONCLUSIONS AND BEST PRACTICES

This section presents research findings and suggests best practices for users, platforms, and law enforcement agencies to mitigate risks associated with social networks, OSINT, and cybercrime What the findings happen emphasizing the shared responsibility needed to respond to evolving cyber threats.

4.1 Conclusions

The study revealed several important insights into how OSINT and social networks are being used to commit cybercrime and what actions should be taken to address these vulnerabilities:

4.1.1 Weaknesses in social media platforms

a) **Access to public data**: Open profiles and posts provide more information for attackers to conduct targeted attacks such as spear phishing and identity theft
b) **Inadequate privacy settings**: Many users fail to set privacy settings, leaving sensitive information exposed.
c) **Weak authentication methods**: The lack of a strong integrity system (e.g., two-factor authentication) increases the risk of unauthorized access

4.1.2 User knowledge and behavior

a) **Over-sharing of personal information:** Users often disclose personal information such as vacation plans and work details, making them vulnerable to phishing and attacks
b) **Acceptance of unknown connections**: Many users accept connection requests from strangers, exposing their networks to potential risk.

4.1.3 Platform Challenges

a) **Balancing usability and security**: Platforms struggle to implement complex security measures without compromising the user experience.
b) **Managing data volumes**: The sheer volume of data used makes cyber threats difficult to identify and mitigate.
c) **Regulatory compliance**: Platforms find it difficult to comply with global privacy and data security regulations.

5. CHALLENGES IN CYBERSECURITY

This Section explores the multifaceted challenges that users, platforms, and law enforcement agencies face with regard to cybersecurity, particularly at the intersection of social networks, OSINT, and cybercrime

5.1 Challenges for users

Lack of insight:
Many users are still unsure of how their publicly shared information can be used. For example, geotagged posts or advanced LinkedIn profiles often provide attackers with access to exploitable data.
Surprise Threats:
Cybercriminals are now using advanced techniques such as deepfakes, social engineering and AI-powered phishing to make threats harder to detect.

Robust privacy policy:
Social media platforms often have complicated privacy policies, making it difficult for users to adequately protect their profiles.

5.2 Challenges on Platforms

Safety vs. safety. Benefits
Platforms strive for a seamless user experience, often compromising strict security measures. For example, simplifying account recovery processes can make accounts more vulnerable to attack.

The amount of data provided
Platforms control large amounts of user-generated data, and if this data is not properly protected or managed properly, it leads to significant vulnerabilities.

Rules of Compliance:
Platforms face challenges in complying with evolving global data protection regulations, such as the GDPR in the European Union or the CCPA in California where the risks of non-compliance include hefty fines and reputation a they destroy it.

5.3 Challenges for Regulatory Agencies

Authority Conflict: Cybercrime often crosses multiple countries, creating challenges in enforcement. For example, criminals in one country can use information from users in another country, bypassing local laws.

Technological Advances: Regulators are struggling to keep up with rapidly evolving technologies like AI and blockchain that are being used for both legitimate and nefarious purposes

Public Awareness Campaign:
Encouraging users to adopt safer online practices remains a challenge, requiring innovative and sustainable education strategies.

5.4 Emerging Threats

AI-driven cybercrime: AI algorithms can create fake profiles or phishing emails that are more accurate.

IoT Disadvantages: The proliferation of IoT devices connected to social platforms creates additional vulnerabilities, as seen in cases where attackers accessed networks through insecure devices

Data scraping at scale: Automated scraping tools extract large amounts of user information, which is then used for malicious activities such as mass identity theft or targeted phishing campaigns5.3 Challenges for Regulatory Agencies

Authority Conflict: Cybercrime often crosses multiple countries, creating challenges in enforcement. For example, criminals in one country can use information from users in another country, bypassing local laws.

Technological Advances: Regulators are struggling to keep up with rapidly evolving technologies like AI and blockchain that are being used for both legitimate and nefarious purposes

Public Awareness Campaign: Encouraging users to adopt safer online practices remains a challenge, requiring innovative and sustainable education strategies.

5.4 Emerging Threats

AI-driven cybercrime: AI algorithms can create fake profiles or phishing emails that are more accurate.

IoT Disadvantages: The proliferation of IoT devices connected to social platforms creates additional vulnerabilities, as seen in cases where attackers accessed networks through insecure devices

Data scraping at scale: Automated scraping tools extract large amounts of user information, which is then used for malicious activities such as mass identity theft or targeted phishing campaigns

REFERENCES

1. Barnett, A. (2021). Twitter data scraping and its risks. Cyber Security Journal, 15(3), 44–59.
2. European Data Protection Board (EDPB). (2023). Guidelines on Social Media Data Use. Available at: www.edpb.europa.eu.
3. Facebook. (2023). Public Profile Data. Available at: www.facebook.com.
4. GitHub. (2023). OSINT Tools Repository. Available at: www.github.com.
5. Kaspersky Lab. (2022). Annual Cybersecurity Report. Available at: www.kaspersky.com.
6. LinkedIn. (2023). Public Profile Information. Available at: www.linkedin.com.
7. Maltego Technologies. (2023). Maltego for OSINT Investigations. Available at: www.maltego.com.
8. Shodan. (2023). Shodan Tool Documentation. Available at: www.shodan.io.
9. Trottier, D., & Fuchs, C. (2015). Social Media, Politics, and the State. Routledge.
10. Twitter. (2023). Hashtags and Analytics. Available at: www.twitter.com.

11. Mann, M. (2021). Understanding digital privacy threats. Journal of Online Safety, 8(4), 22–37.
12. Cybersecurity Ventures. (2023). Cybercrime Trends. Available at: www.cybersecurityventures.com.