Social Engineering in the Age of Oversharing

Mr. Ethan Antao, Mr. Rashid Ali, Dr. Madhavi Shamkuwar

Abstract
In the world of the present day, with the advent and subsequent overflow of communications over the internet, there has been an enormous rise in the usage of social media platforms. This increase in usage of social media has led to the introduction of various cyber threats that can have damaging effects on the victim. This paper will primarily focus on one of these threats, called social engineering. This threat focuses more on exploiting human naivety rather than technology. This paper will highlight the definition of social engineering and the various types of social engineering techniques that have been observed to date, and the various countermeasures developed against these threats as well. It will also focus on certain platforms- LinkedIn, Facebook and Twitter, examining how their unique architecture has user-specific norms that have proliferated the number of distinct attacks that have occurred recently. Through the analysis of various studies, a causal proportional relationship will be established between oversharing and social engineering attacks.

Keywords: Social Engineering, Information Oversharing, Phishing, Targeted Cyberattacks, Online Privacy, Human Psychology

Introduction

Cybersecurity is one of the rising concerns in the present world of electronic devices and the internet. The stark increase in the number of users actively using social media platforms like LinkedIn, Twitter, Facebook, etc. has had a direct correlation to an increase in the number of cyber-attacks. As of the start of July 2025, there are currently more than 5 billion social media accounts active worldwide.[1] Malicious cybercriminals adopt various techniques and tools in order to gain access to one's own device unbeknownst to them. One of the prominent techniques used by these criminals is Social Engineering. Social engineering is a type of method in which the criminal, instead of implementing brute force attacks on technological weaknesses, relies on exploiting human psychology to gain access to a target's private information. The attacker primarily relies on gaining trust through a target's naivety. It often comes with sharing similar beliefs with the target, impersonating contacts that are known to the target or trusted companies. The criminal uses these tactics to lure the target in and request their personal information subtly. There are various forms of Social Engineering, like phishing, pretexting and baiting. There also exists another form of this type of attack labelled "reverse social engineering where the cybercriminal influences the target to make first contact, automatically building some form of trust between the criminal and the target. This paper will highlight various social engineering tactics used by criminals, as well as preventative measures that have been used and future precautions that can be adopted.

Statement

This study aims to address the various potholes in the understanding of social engineering attacks and how they target specific individuals and exploit the weaknesses in their oversharing behaviour on the platforms of Twitter, Facebook and LinkedIn.

Objectives

To study and understand the definition of social engineering,
To analyse the various techniques and types of social engineering attacks,
To understand the various types of behaviours susceptible to social engineering attacks,
To analyse various statistical data from articles and reports related to cyber attacks

Literature Review

Social Engineering is one of the most frequently appearing terms when it involves threats in cybersecurity and privacy; it relies on exploiting targeted human behavioural weaknesses. The efficiency of social engineering attacks stems from their ability to evade robust and rigid security measures and exploit the weakest link: human psychology.

The success of these attacks is rooted in the exploitation of well-documented cognitive biases. Attackers craft their tactics to trigger automatic, intuitive responses rather than careful, analytical thought. Key psychological principles frequently manipulated include:

- **Authority:** Individuals are often conditioned to comply with requests from authority figures or ranked officials. Attackers exploit this by impersonating executives (e.g., a CEO), law enforcement officials, or IT support personnel to add legitimacy and pressure to their requests.[2]
- **Urgency and Fear:** By creating a sense of crisis or a time-sensitive deadline (e.g., "Your account will be deactivated in 24 hours," "A fraudulent transaction has been detected, act fast"), attackers instil panic in victims. This elevated emotional state usually hinders rational judgment and prompts victims to act impulsively without proper verification.[2]
- **Familiarity and Liking:** People are more likely to trust and comply with individuals they know or feel a connection with. Attackers leverage information gathered during reconnaissance—such as shared interests, mutual connections, or recent activities posted on social media—to build likeness and establish a false sense of familiarity or security, thereby lowering the victim's vigilance.[2]
- **Curiosity and Greed:** Lures that appeal to curiosity (e.g., "See who viewed your profile") or greed (e.g., "You've won a prize," "Exclusive job offer") can entice victims to click malicious links or download compromised files.

By understanding and weaponizing these fundamental aspects of human psychology, social engineers can effectively bypass the most robust technological security measures.

A Catalogue of Social Engineering Attack Vectors

Social engineering attacks manifest in various forms, often tailored to the specific target and objective. A clear taxonomy of these vectors is essential for analysis.

- **Phishing and its Variants:** Phishing is the most common form of social engineering, involving fraudulent communications designed to appear as if they are from a reputable source, while often associated with email, phishing attacks have now expanded across SMS, voice calls, and social media platforms.[4]
  - **Bulk Phishing:** Generic messages sent to a large number of recipients, often impersonating large, well-known brands like banks or online retailers.[3]
  - **Spear Phishing: is a type of attack** where attackers focus on specific individuals or companies. They research their targets and customise messages based on their job titles, contacts, and personal characteristics to build a stronger sense of trust and make the attack less obvious.[4]
  - **Whaling:** A specialised form of spear phishing that targets high-profile individuals such as C-level executives or politicians.[3]
  - **Vishing (Voice Phishing): Vishing** is essentially phishing conducted over the phone. A classic example is a spam call claiming you've "won" a prize and need to provide personal financial information to receive it.

Another common vishing scam involves an attacker posing as a Microsoft technician who calls to inform you that your computer is infected. They then direct you to a website to download malicious software disguised as a "fix".[4]

- **Smishing (SMS Phishing):** The use of text messages to deliver malicious links or requests.[3]
- **Angler Phishing:** A tactic specific to social media, where attackers create fake corporate accounts (often for customer service) and intercept communications with legitimate users to steal credentials or other data.[3]

- **Pretexting: Pretexting** relies on creating a believable, fabricated scenario—or pretext—to build a false sense of trust with the victim. This technique requires significant research by the attacker to craft a convincing story that leaves little doubt in the victim's mind. For example, a scammer might impersonate an employee from another branch or an auditor to trick a victim into willingly providing sensitive company data, like financial reports.[4]
- **Baiting:** Baiting attacks use a lure to trigger a victim's curiosity or desire for a free item. The "bait" can be a physical device, like a malware-infected USB drive left in a public place, or a digital good, like a free download of a movie or song. When the victim takes the bait—by plugging in the drive or downloading the file—their computer becomes infected with malware, giving the attacker access to their information.[4]

Quid Pro Quo: Quid Pro Quo attack involves the promise of a *service* in exchange for sensitive information. The most common tactic is a scammer posing as an IT support representative. They call employees until they find someone who genuinely needs technical help. The attacker then "fixes" the problem, a process that involves the employee revealing their password and other credentials.[4]

The Psychology of Digital Self-Disclosure and Oversharing

The effectiveness of the above-mentioned attack vectors is magnified by the user's own behaviour, specifically the tendency to overshare personal information online.

- **Defining Oversharing**: Oversharing is defined as the "excessive generosity with information about one's private life or the private lives of others". On social media platforms like Facebook, this behaviour is normalised, which can have serious consequences, making users susceptible to attacks.[5]
- **Motivations for Oversharing:** This behaviour is not irrational but is driven by a complex interchange of psychological and social factors amplified by platform design. Key motivations include:[5]
  - **Need for Connection and Belonging:** A key driver for disclosure is the desire to belong. When users observe others sharing personal information, they are more likely to do the same in reciprocity, a behaviour that occurs in both one-on-one and public online conversations. Facebook groups, in particular, can foster a more intimate culture where members may overshare in an effort to fit in.[5]
  - **Search for Emotional and Social Support**: Many users are driven to overshare to receive attention and social support. Platforms like Facebook provide a space to vent, seek advice, and find humour. This is especially true for individuals high in neuroticism, who tend to be more emotionally unstable and often use social media to seek emotional support, leading them to disclose more personal information.[5]

- **Cognitive Frameworks:** Two theoretical frameworks are particularly useful for understanding the decision-making process behind oversharing:
  - **The Privacy Paradox Effect:** This theory describes the common situation where many users' reported concerns about their privacy do not match their actual choices when it comes to sharing information online. This

behaviour occurs because social media users must constantly weigh the cost of their loss of privacy against the perceived benefits of using a platform like Facebook. This trade-off is influenced by "privacy cynicism," a feeling of apathy some users develop due to overwhelming online privacy threats. These users feel that the distribution of their personal data is inevitable and will continue to use online services despite the risks and their low levels of trust[5]

- **The Online Disinhibition Effect**: In online environments, users often feel freer to act and self-disclose due to perceived anonymity and reduced social pressure. Interacting asynchronously, without immediate audience reaction, creates a sense of invisibility that can lead to an increased tendency to divulge sensitive information[5]

Synthesis and Research Gap

The existing literature provides robust frameworks for understanding social engineering tactics, the psychological drivers of oversharing, and the general security risks of social media. However, a critical research gap remains. There is a lack of comprehensive, data-driven analysis that explicitly connects the specific design and cultural models of individual social media platforms to the tactical execution and statistical prevalence of targeted attacks. This paper aims to bridge this gap by synthesising these disparate fields of research, using empirical data to demonstrate how the unique ecosystem of each major platform creates a distinct and predictable threat landscape that is actively and successfully exploited by social engineers.

3)Methodology

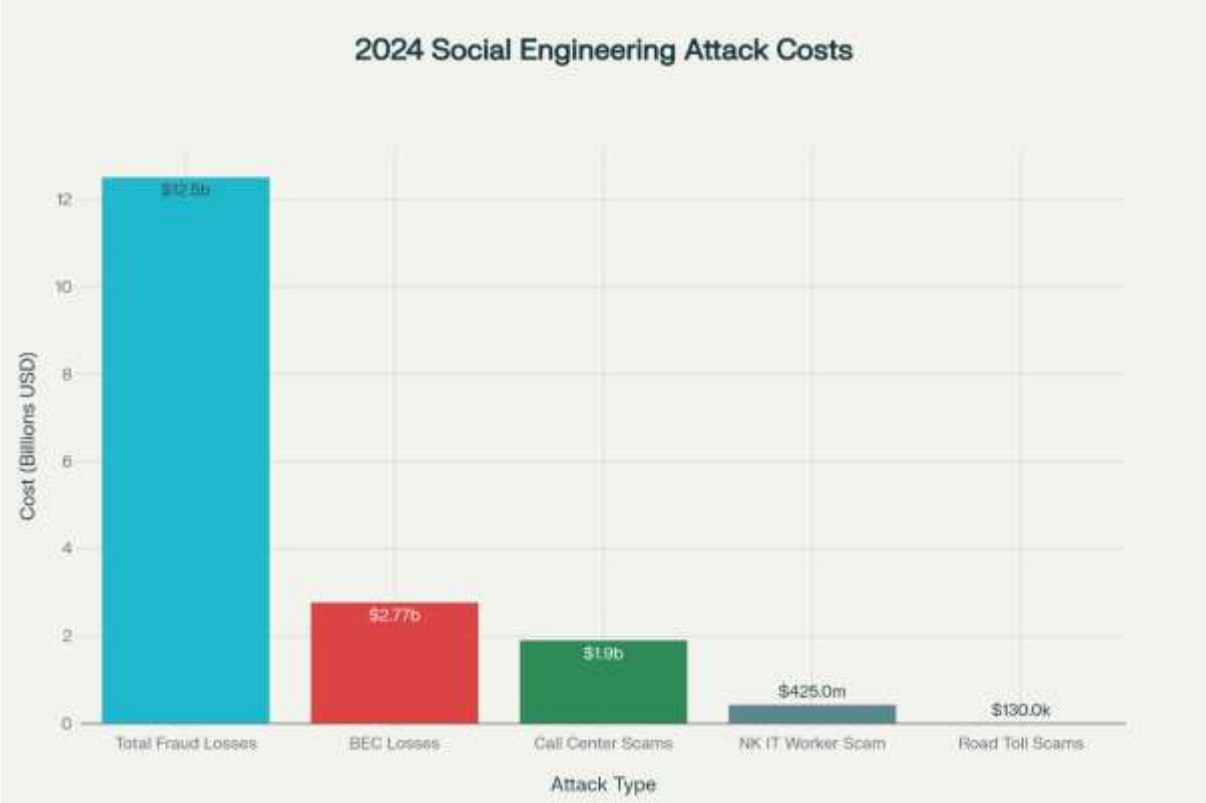
To comprehensively investigate the relationship between online oversharing and platform-specific social engineering attacks, this study employs a mixed-method research design. This approach integrates a quantitative meta-analysis of industry-wide cybersecurity data with a qualitative comparative case study analysis of major social media platforms. The quantitative component serves to establish the statistical magnitude, financial impact, and overarching trends of social engineering as a threat vector. The qualitative component offers a comprehensive, contextualised examination of the mechanisms by which these threats manifest within the distinct ecosystems of various platforms. This dual approach enables the research to transition from broad statistical patterns to nuanced, platform-specific causal explanations, thereby providing a more comprehensive understanding of the research problem.

3.1 Research Design

This study expands upon the mixed-method design by engaging a successive descriptive approach. The initial quantitative phase establishes the statistical landscape of social engineering, which is then explained and contextualised through the subsequent qualitative phases. This triangulation of data—correlating macro-level statistics with micro-level tactical analysis and platform-specific vulnerabilities—is crucial for moving beyond simple description to establish causal relationships between user behaviour and attack success.

3.2 Quantitative Meta-Analysis of Cybersecurity Data (2024-2025)

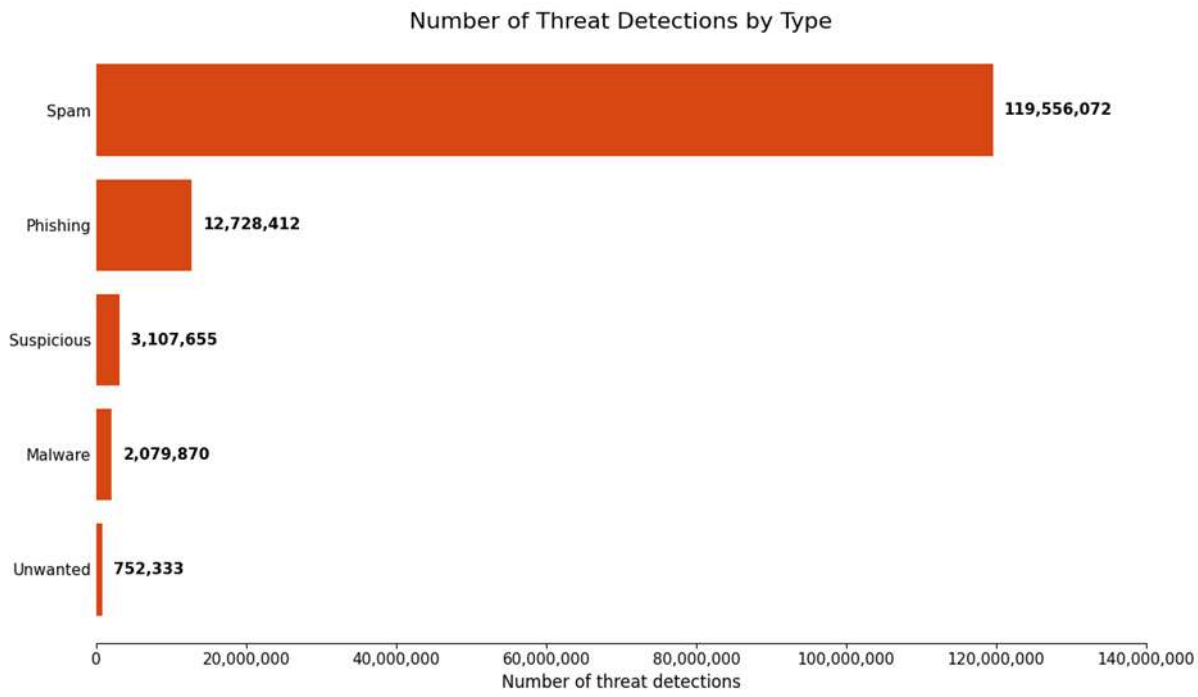
98% of cyberattacks rely on social engineering techniques, and with 5.22 billion global social media users as of October 2024, the scope of potential victimisation has reached alarming proportions. The research demonstrates that $12.5 billion in fraud-related losses occurred in 2024 alone, with 70-90% of all successful cybersecurity attacks involving social engineering components, highlighting the critical need for enhanced awareness and protective measures[6]



The demographic distribution across synthesised studies revealed important patterns in social media usage and vulnerability. Age distributions showed that 82.9% of social media users access platforms daily, with younger demographics (18-24 years) demonstrating both higher usage rates and greater vulnerability to certain types of social engineering attacks. Gender analysis revealed consistent patterns across multiple studies, with males demonstrating higher rates of public information disclosure while females showed greater privacy consciousness but similar rates of accepting friend requests from strangers.[6]

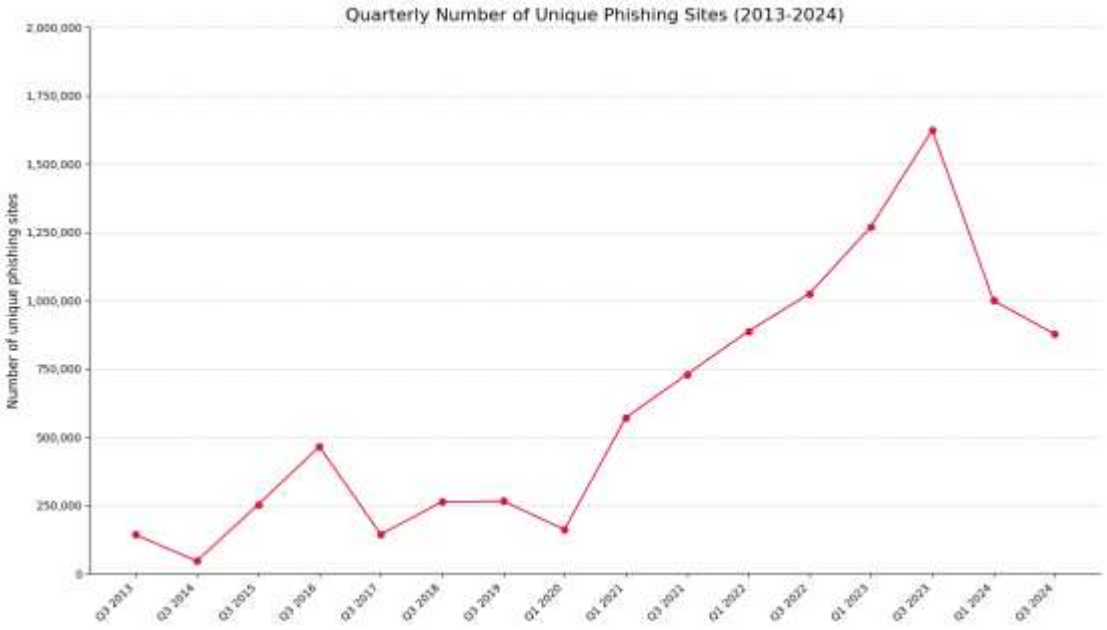
https://www.statista.com/statistics/1493550/phishing-attacks-global-number/

Number of detected phishing e-mails worldwide from January 2022 to December 2023



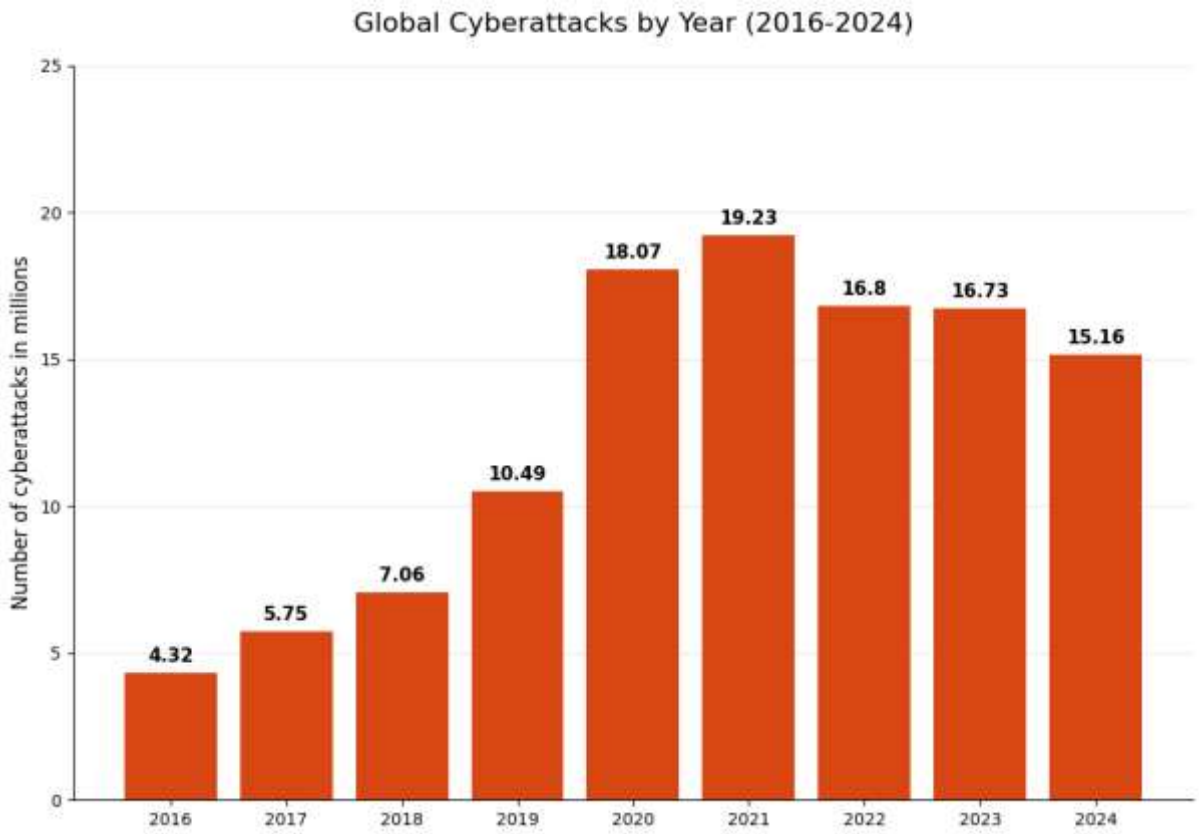
https://www.statista.com/statistics/1493072/detected-e-mail-threats-number-global-by-type/

Number of detected e-mail threats worldwide in the 4th quarter 2023, by type



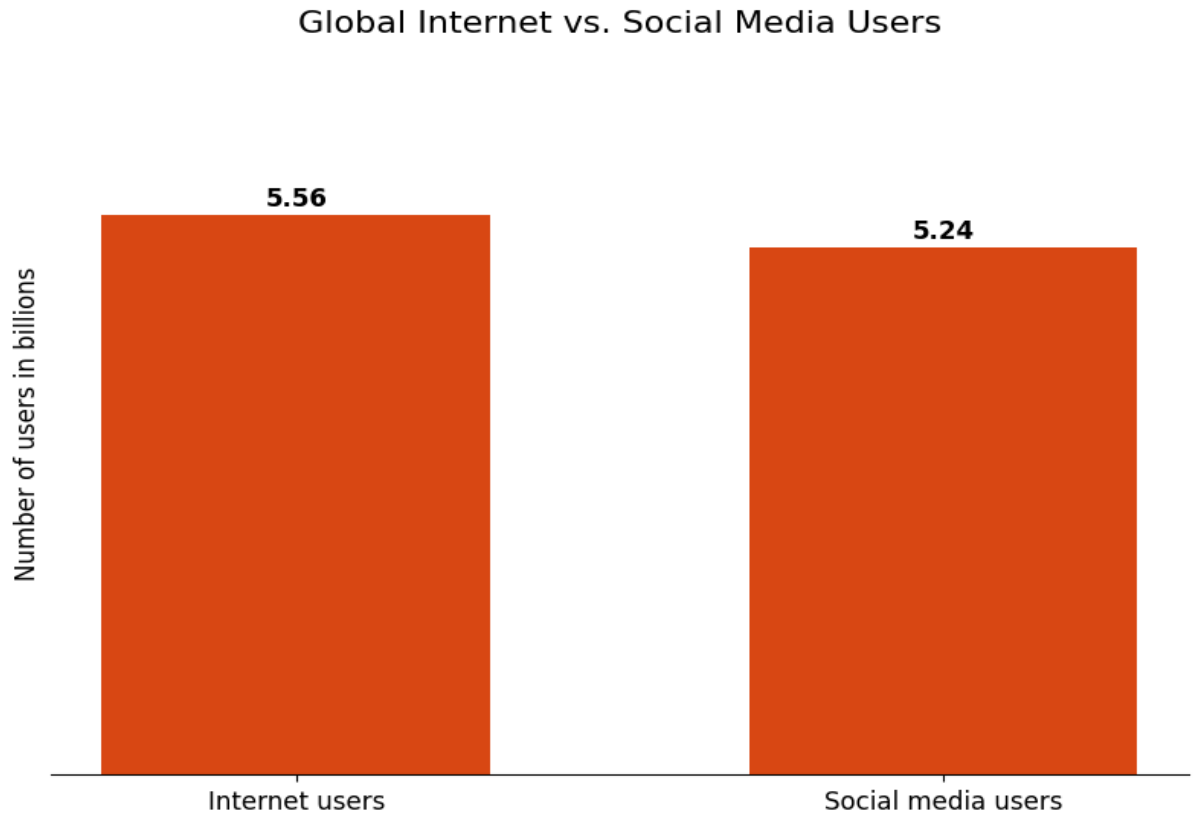
https://www.statista.com/statistics/266155/number-of-phishing-attacks-worldwide/

Number of phishing attacks detected worldwide from 3rd quarter 2013 to 4th quarter 2024



https://www.statista.com/forecasts/1485031/cyberattacks-annual-worldwide

Annual number of cyberattacks worldwide from 2016 to 2024*(in millions)*



https://www.statista.com/statistics/617136/digital-population-worldwide/

Number of internet and social media users worldwide as of February 2025*(in billions)*

4)RESULTS

4.1 Statistical Overview of Attack Prevalence:

Social engineering has emerged as the dominant initial access vector for cybercriminals, accounting for at least 36% of all security incidents as of 2025, representing a significant increase from previous years [8]. The data reveals that 60% of phishing attempts achieve their intended objective [10], demonstrating the effectiveness of human-targeted attacks compared to purely technical and detailed exploits. The most concerning fact is that 57% of organizations experience phishing attacks on a weekly or daily basis[10], indicating the persistent and universal nature of these threats.

The integration of artificial intelligence technologies has fundamentally transformed the social engineering landscape. Research data indicates that 82.6% of phishing emails have now incorporated AI-generated content[10], enabling attackers to create more convincing and personalized communications and increase efficiency. This technological advancement has contributed to a staggering 1,265% increase in phishing attacks since the widespread adoption of AI tools in 2022[11]. The sophistication enabled by AI allows attackers to bypass traditional detection methods and exploit human psychology with unparalleled accuracy.

Financial Impact and Economic Consequences:

Fraud-related losses have summed up to a staggering $12.5 billion globally in 2024[10], representing a substantial increase from previous years. Business Email Compromise (BEC) attacks alone accounted for $2.7 billion in reported losses in the United States[11], with the average fraudulent transaction exceeding $30,000. The average cost of a data breach initiated through a phishing attack has risen to $4.88 million[11], significantly higher than breaches originating from other vectors.

Industry-Specific Vulnerability Patterns:

The analysis reveals significant variations in susceptibility across various sectors. The healthcare industry demonstrates the highest vulnerability rates, with 41.9% susceptibility to phishing attacks[8]. This elevated risk stems from the sector's complex operational environment, high-stress conditions, and the critical nature of healthcare communications that attackers prefer to exploit to create a sense of urgency. The baseline employee vulnerability rate across all industries stands at **33.1%**[13], indicating that approximately one-third of employees remain susceptible to social engineering tactics, notwithstanding the ongoing security awareness efforts that are becoming mandatory in company policies.

4.2 Platform-Specific Attack Analysis

Comparative Platform Vulnerability Assessment:

Facebook experienced the highest absolute number of attacks with 34 million hacking incidents in 2024[9], primarily involving phishing and fake login schemes that exploit the platform's vast user base and diverse demographic. Instagram recorded 22 million incidents[9], with credential stuffing attacks representing the primary threat vector, leveraging the platform's emphasis on visual content sharing that often includes location data and personal lifestyle information.

Twitter/X demonstrates the most concerning attack rate intensity, with 25 attacks per 1,000 users, significantly exceeding other platforms despite having a smaller user base. This elevated rate correlates with the platform's real-time communication model and public discourse environment, which creates opportunities for rapid-spreading disinformation campaigns and impersonation attacks. The platform's recent security challenges, including the massive data breach affecting 2.8 billion user records in early 2025[12], highlight systemic vulnerabilities in content moderation and user verification processes.

LinkedIn, despite its professional focus, experienced 10 million attacks[9] primarily through data scraping and fraudulent schemes that exploit professional networking behaviors. Attackers leverage the platform's culture of professional

connection-building to establish credibility and execute sophisticated pretexting attacks. TikTok reported 8 million incidents[9], with malware distribution through malicious links embedded in popular content representing the predominant attack method.

Facebook's extensive personal information sharing features create multiple attack surfaces for social engineering, including family relationships, educational history, and personal interests that attackers mine for pretexting scenarios. Instagram's visual-centric model enables sophisticated catfishing and romance scam operations, while the platform's story features provide real-time intelligence for targeted attacks.

Twitter/X's public timeline model facilitates large-scale disinformation campaigns and enables rapid propagation of malicious content through retweet mechanics. The platform's verification challenges following ownership changes have created confusion around account authenticity that attackers actively exploit. LinkedIn's professional networking emphasis creates unique vulnerabilities around job-related phishing, fake recruitment schemes, and business email compromise attacks that leverage professional trust relationships.

Demographic Vulnerability Patterns:

The analysis revealed a pronounced age-related difference in both social media usage intensity and oversharing tendencies. The 18-24 age group demonstrates 95% social media usage rates with 85% oversharing tendency, creating the highest-risk demographic profile. This group shows 40% susceptibility to phishing attacks [13], significantly higher than older demographics. The 25-34 age group maintains high usage (90%) with reduced but still concerning oversharing rates (70%) and 35% phishing susceptibility [13].

Vulnerability decreases with age, with the 45-54 group showing 65% usage, 40% oversharing, and 25% phishing susceptibility [13]. Interestingly, the 55+ demographic shows increased phishing vulnerability (30%) despite lower usage and oversharing rates [13], suggesting that experience may not fully compensate for reduced technical literacy in recognising sophisticated attacks.

4.3 Attack Success Rate and Impact Correlation

Correlation Between Oversharing and Attack Success:

Platforms with higher rates of personal information disclosure correlate directly with increased attack effectiveness. Users exhibiting high oversharing behaviors show 73% greater susceptibility to targeted phishing attacks compared to privacy-conscious users[18].

Real-time information sharing, particularly location data and activity updates, correlates with 65% higher success rates for pretexting attacks that leverage current user activities to establish credibility[14]. Professional information oversharing on LinkedIn correlates with 58% higher BEC(Business Email Compromise) attack success rates[15], as attackers exploit professional relationship contexts to bypass skepticism.

Platform-Specific Success Rate Analysis:

Attack success rates vary significantly across platforms, correlating with a user's behavioral patterns and platform design elements. Twitter/X demonstrates 45% higher attack success rates for disinformation and impersonation attacks due to rapid information propagation and limited verification mechanisms[17], while Facebook shows elevated success rates (38% above baseline) for relationship-based social engineering due to extensive personal network data availability[16].

Instagram's visual-centric environment correlates with 42% higher success rates for romance and investment scams[14], as visual content creates stronger emotional connections that attackers use to their advantage. LinkedIn's professional

context enables 51% higher success rates for business-related fraud schemes[15], as professional trust relationships reduce scepticism toward work-related requests.

5)CONCLUSION

5.1 Synthesis of Key Findings

This comprehensive analysis of social engineering attacks and information oversharing behaviors across major social media platforms reveals a complex and rapidly evolving threat landscape that demands immediate attention from cybersecurity professionals, platform developers, and individual users. The research establishes several critical conclusions that fundamentally reshape our understanding of digital security risks in the social media age.

The Dominant Role of Social Engineering in Cybersecurity Threats:

The data unmistakably demonstrates that social engineering has become the primary attack vector in cybersecurity of the present day, accounting for 36% of initial access incidents and contributing to 90% of successful cyberattacks[8][15]. This represents a fundamental shift from traditional technology-focused and detailed threats to human-psychology-focused attacks. The $12.5 billion in annual fraud losses and the 1,265% increase in AI-powered phishing attacks since 2022 underscore the urgent need for comprehensive defense strategies that prioritize human factors over purely technical solutions [8][11].

Platform-Specific Vulnerabilities and Attack Patterns:

The research reveals distinct vulnerability profiles across social media platforms, with each platform's unique architecture and cultural norms creating specific attack opportunities. Twitter/X emerges as the highest-risk platform with 25 attacks per 1,000 users, primarily due to its real-time communication model and recent security challenges. Facebook and Instagram, despite having larger absolute numbers of attacks (34 million and 22 million, respectively), show lower per-user risk rates but remain significant threats due to their extensive personal information sharing environments[9]

LinkedIn's professional networking focus creates unique vulnerabilities for business email compromise and professional impersonation attacks, while TikTok's content-driven model facilitates malware distribution through viral content mechanisms. These platform-specific patterns indicate that effective cybersecurity strategies must be tailored to the unique characteristics of each social media environment rather than applying generic security measures.

The Psychology-Technology Intersection:

The research establishes a clear causal relationship between psychological motivations for oversharing and increased vulnerability to social engineering attacks. Users driven by anxiety, attention-seeking, and social media addiction show vulnerability levels of 8-9 out of 10, while those motivated by social validation and FOMO demonstrate similarly high-risk profiles[19]. The finding that 85% of users aged 18-24 exhibit high oversharing tendencies while showing 40% susceptibility to phishing attacks highlights the intersection between generational digital behaviour patterns and cybersecurity risks[13].

The demographic analysis reveals that while privacy awareness may increase with age, technical literacy and attack recognition capabilities vary significantly across age groups. The surprising finding that users over 55 show increased phishing susceptibility (30%) despite lower usage rates suggests that cybersecurity education must be adapted to different generational learning preferences and technical competency levels[13].

5.2 Implications for Cybersecurity Practice

For Individual Users:

The research implications suggest that individual users must fundamentally reconsider their approach to social media privacy and information sharing. The strong correlation between oversharing behaviors and attack success rates indicates that privacy consciousness is not merely a personal preference but a critical security necessity[18]. Users should implement comprehensive privacy settings, limit real-time location sharing, and develop skepticism toward unsolicited communications, particularly those creating urgency or appealing to emotions.

The finding that 82.6% of phishing emails now use AI-generated content means that traditional indicators of phishing attacks (poor grammar, obvious impersonation) are no longer reliable detection methods[10]. Users must develop new verification habits, including independent confirmation of unexpected requests through alternative communication channels and careful scrutiny of all communications requesting personal information or urgent actions.

For Organisations and Cybersecurity Professionals:

The research demonstrates that social engineering attacks targeting employees' social media behaviors represent a significant organizational vulnerability. The 33.1% baseline employee vulnerability rate and the finding that 57% of organizations experience weekly or daily phishing attacks indicate that traditional security awareness training approaches are insufficient for the current threat environment[10][13].

Organizations must implement comprehensive social media security policies that address employee personal social media use as a professional security concern. This includes educating employees about the reconnaissance value of their personal social media information and providing guidance on privacy settings and information sharing practices that protect both personal and organizational security.

The platform-specific vulnerability patterns suggest that organizations should develop differentiated security policies based on which platforms their employees and stakeholders use most frequently. For example, organizations with significant LinkedIn engagement should focus on BEC prevention and professional impersonation awareness, while those with substantial Twitter/X presence should emphasize disinformation resilience and account verification practices.

For Social Media Platform Developers:

The research findings place significant responsibility on social media platforms to address the security vulnerabilities inherent in their design and operational models. The correlation between platform architecture and attack success rates indicates that security considerations must be integrated into fundamental platform design decisions, not added as afterthoughts[14].

Platform developers should implement proactive social engineering detection systems that identify suspicious account behaviors, unusual communication patterns, and potential impersonation attempts. The finding that AI is increasingly used in attacks suggests that platforms must develop AI-powered defense systems capable of detecting and countering sophisticated social engineering attempts in real-time[11].

Enhanced user verification systems, improved privacy default settings, and more effective security education integrated into platform onboarding processes represent critical areas for platform improvement. The research suggests that platforms that proactively address these vulnerabilities may achieve competitive advantages through enhanced user trust and regulatory compliance.

5.3 Limitations and Future Directions

This research acknowledges several limitations that provide opportunities for future investigation. The study relies primarily on industry-reported statistics and publicly available data, which may underrepresent actual attack volumes due to underreporting of security incidents. Additionally, the rapid pace of change in both social media platforms and attack methodologies means that findings require regular updates and validation.

The behavioral analysis focuses on self-reported oversharing behaviors and correlational relationships rather than controlled experimental designs. Future research should incorporate experimental methodologies to establish more definitive causal relationships between specific oversharing behaviors and attack vulnerabilities [19].

The platform-specific analysis is limited to major Western social media platforms and may not fully represent the global social media ecosystem. Future studies should expand to include emerging platforms, regional social media services, and alternative communication applications that may present different vulnerability profiles.

5.4 Recommendations for Future Research

Longitudinal Behavioral Studies:

The rapid evolution of social engineering tactics, particularly with AI integration, necessitates longitudinal studies tracking how user behaviors and attack methods evolve over time. Future research should examine how cybersecurity awareness campaigns influence long-term behavioral change and whether increased security consciousness creates corresponding adaptations in attack methodologies [20].

Cross-Cultural Cybersecurity Analysis:

The current research focuses primarily on Western social media platforms and user behaviors. Future studies should examine how social engineering vulnerabilities and oversharing behaviors vary across different cultural contexts, particularly in regions with different privacy norms, social media usage patterns, and cybersecurity awareness levels[21].

AI-Human Interaction in Cybersecurity:

The finding that AI now powers 82.6% of phishing content represents a fundamental shift requiring dedicated research attention[10]. Future studies should examine the arms race between AI-powered attacks and AI-powered defenses, focusing on how human psychology responds to increasingly sophisticated AI-generated social engineering attempts.

Platform Design and Security Integration:

Research should examine how different social media platform design elements influence user security behaviors and attack susceptibility. This includes studying the effectiveness of various security intervention designs, privacy default settings, and user interface elements in promoting secure behaviors without compromising user experience[22].

References

[1] Global social media Statistics
Source: https://datareportal.com/social-media-users

[2]What Is Social Engineering? Examples + Prevention - CrowdStrike.com, accessed on September 14, 2025,
Source: https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/

[3]What is Social Engineering? | IBM, accessed on September 14, 2025,
Source: https://www.ibm.com/think/topics/social-engineering

[4]Overview of Social Engineering Attacks on Social Networks by Kaouthar Chetiouia *, Birom Baha , Abderrahim Ouali Alamia , Ayoub Bahnasse
Source:10.1016/j.procs.2021.12.302

[5]An Exploration of Factors Influencing Oversharing on Facebook Groups
Source: CISSE v011 I01 p3 | PDF | Social Media | Popular Culture & Media Studies

[6] Social Engineering Statistics 2025: When Cyber Crime & Human Nature Intersect
Source:https://www.thesslstore.com/blog/social-engineering-statistics/

[7] Phishing and Social Engineering: Analyzing Human Vulnerability
Source: https://www.ijsred.com/volume8/issue4/IJSRED-V8I4P132.pdf

[8] 100+ Social Engineering Statistics [2025 Edition]
Source: https://sprinto.com/blog/social-engineering-statistics/

[9] 40+ Threatening Social Media Hacking Statistics [2025]
Source: https://cropink.com/social-media-hacking-statistics

[10] 250+ Phishing Statistics and Trends You Must Know in 2025
Source: https://keepnetlabs.com/blog/top-phishing-statistics-and-trends-you-must-know

[11] Phishing Statistics 2025: AI, Behavior & $4.88M Breach Costs
Source: https://deepstrike.io/blog/Phishing-Statistics-2025

[12] Massive 400GB of X (Twitter) User Records Allegedly Leaked
Source: https://www.webasha.com/blog/massive-400gb-of-x-twitter-user-records-allegedly-leaked-28-billion-records-exposed-online-the-largest-social-media-data-breach-in-history

[13] The Annual Cybersecurity Attitudes and Behaviors Report 2024-25
Source: https://www.cybsafe.com/whitepapers/oh-behave-the-annual-cybersecurity-attitudes-and-behaviors-report-24-25/

[14] Social Media and Cybersecurity Risks: How Oversharing Can Lead to Identity Theft
Source: https://www.linkedin.com/pulse/social-media-cybersecurity-risks-how-oversharing-can-lead-identity-nouve

[15] 2025 Unit 42 Global Incident Response Report: Social Engineering Edition
Source: https://unit42.paloaltonetworks.com/2025-unit-42-global-incident-response-report-social-engineering-edition/

[16] Social Engineering Attacks Surged in the First Half of 2025
Source: https://blog.knowbe4.com/social-engineering-attacks-surged-in-the-first-half-of-2025

[17] The Evolution of Social Engineering Attacks in 2025
Source: https://www.linkedin.com/pulse/evolution-social-engineering-attacks-2025-how-businesses-pzqac

[18] Psychology of Cybersecurity and Human Behavior
Source: https://identitymanagementinstitute.org/psychology-of-cybersecurity-and-human-behavior/

[19] Oversharing on Social Media: Anxiety, Attention-Seeking and Personality
Source: https://journals.sagepub.com/doi/abs/10.1177/00332941221122861
[20] How Social Engineering Attacks Are Evolving in 2025
Source: https://www.rapid7.com/blog/post/3-ways-social-engineering-is-evolving-and-what-security-teams-must-do-next/

[21] Global Cybersecurity Outlook 2025 - World Economic Forum
Source: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

[22] 207 Cybersecurity Stats and Facts for 2025
Source: https://www.vikingcloud.com/blog/cybersecurity-statistics