LINKEDIN: A PLATFORM OF OPPORTUNITIES OR A BREACH OF TRUST

[1]] Sivani P ,VTU25297, vtu25297@veltech.edu.in ,
[2] Dr.Priya .P. Sajan, Senior Project Engineer, C-DAC Thiruvananthapuram, priyasajan@cdac.in

***Abstract*—LinkedIn is a profound professional networking platform. But it is facing security challenges like fake profiles, recruitment frauds, trustable ground for making phishing attacks, with more than one billion users. This case study looks around current security frameworks pointing out the limitations, and propose sophisticated, scalable solutions for more elastic and reliable ecosystems.**

***Index Terms*—LinkedIn, Fake Profiles, Social Engineering**

I. INTRODUCTION

FOund in 2003 and currently owned by Microsoft, LinkedIn has evolved into a dynamic digital platform where professionals can build their careers. In opposition to traditional social media, the primary focus is on career development, corporate branding, making it crucial tool in global labor market. Individuals use the platform to build personal brands while using companies for marketing and talent. Social engineering and phishing attacks. This case study examines the dual identity of LinkedIns. This is a tool for enhancing other exams by experts and other users that reveal potentially harmful weaknesses. Addresses the system of using LinkedIn for user trust and security, assesses limitations and proposes demanding, scalable solutions to ensure a more resistant and reliable ecosystem.

II. LITERATURE SURVEY

Various research and incident reports show that LinkedIn often aims for threats. According to Kaspersky's 2021 security bulletin, LinkedIn is one of the most popular sites used in phishing attacks. This is primarily due to its professional user base and visibility of personal contact information.

Analysis of Socket 2023 North Korea's cybersurgery, Infectious Interview Campaign, showed that attacker LinkedIn used it on recruiters. These imitators show that developers are cloned with malware that appears to be legally legitimate coding tasks and traumatize the system with reliable social engineering tactics.

A checkpoint and Ciscotatos-by-Checkpoints have verified that the number of phony profiles has increased. These profiles straight-up copy real recruits and experts, who's legit and who's just some sketchy scammer. It is getting much harder to pick the fakes from the real.

The current reactive approach and moderation system on LinkedIn is frequently abandoned when sophisticated attacks are detected, emphasizing the need for proactive and flexible solutions.

III. EXISTING SYSTEM

To encourage a safe network environment, LinkedIn has put up a number of fundamental security measures and policies. This includes reporting equipment intended to contain dissemination of malicious activity, content mitigation, and user authentication.

3.1 Authentication and Privacy Controls: LinkedIn supports two-factor authentication (2FA) for user protection for their accounts. Additionally, data protection settings to manage who can view their emails, phone numbers and activities on the platform. However, these controls are optional and not robustly advertised among new users.

3.2 Reporting and Blocking Mechanisms: Users have the option to report spam, dubious accounts, or inconsistent content. LinkedIn's security teams check contents and profiles for possible misconduct. Users can limit the commitment of unnecessary profiles by using blocking features.

3.3 Platform Moderation and Machine Learning: The platform uses automated systems to identify mass messaging patterns, inappropriate keywords, and spam-like behavior. Some machine learning model flags flag accounts that quickly add connections or engage in public relations. Nevertheless, these systems often lack depth in analyzing behavioral contexts.

3.4 Limitations: In spite of these resources, LinkedIn is an ongoing challenge.

- Slow reaction to fraud or imitation reports.
- Lack of verified identity badges for professionals and recruiters.

Minimum protection against social engineering via personalized messaging. These flaws indicate that existing systems are much more responsive than prevention, and in many cases, user reports indicate that they are solely related to threats.

IV. PROPOSED SYSTEM

To effectively tackle the trust and security concerns on LinkedIn, a more comprehensive and intelligent system is needed. This proposed system combines verification protocols, real-time threat detection, and user-centric safety features to create a proactive defense model.

4.1 Verified Identity Badges

Verified Identity Badges LinkedIn must implement a badge-based verification system similar to other platforms. These badges are issued according to a document-based KYC check for individual professionals.

Domain-based email reviews for recruiters and company representatives.

This allows users to quickly identify trustworthy profiles and reduce imitation-based fraud.

4.2 AI-Powered Scam Detection

- A sudden spike in connection enquiries or commitments from new accounts.
- Genuine indicators like work history and time management consistency.
- Such a system will reduce reliance on manual reporting and improve early detection of malicious actors

4.3 Profile Trust Score

Each profile can be assigned to a trust score, such as calculations using factors:

- Verified identity
- Account age and activity stability
- Community engagement
- No history of report or flagged material

It is decided to connect with a profile when score can serve as a metric for users.

4.4 Interactive Security Dashboard

A spontaneous user should provide dashboard:

- Login behavior, privacy preferences, and a visual review of previous alerts.
- Security suggestions (eg, enabling 2FA or reviewing unfamiliar login).
- Quick tools to report or block possible hazards.

4.5 User Awareness Campaigns

LinkedIn must conduct awareness drives to educate users regularly:

- Latest scam
- How to verify the recruiters
- Safe networking habits

These campaigns can be embedded within the app through banners, emails and tutorials.

V. CONCLUSION

The development of LinkedIn's global professional network has created an opportunity-rich digital environment. But his openness and scaling make it the goal of abuse. Although platform security is based on current systems, there is the lack of depth and adaptability required to combat highly socially designed threats.

This case study concludes that the current model of LinkedIn must move from reactive moderation to aggressive protection. The proposed system includes validated identity, Behavior -KI, and user-focused tools, including structured paths to restore and maintain trust. It's important, not only to support platforms like LinkedIn when digital beings often form real careers.

VI. REFERENCES

[1] Socket, "North Korea-linked Supply Chain Attack Targets Developers with 35 Malicious npm Packages," Socket Security Blog, June 25, 2025 (references 2023 campaign). [Online]. Available: https://thehackernews.com/2025/06/north-korea-linked-supply-chain-attack.html (This is a news article referencing Socket's findings on the 2023 campaign, as a direct 2023 Socket report may not be a standalone document with that exact title).

[2] Kaspersky, "Spam and phishing in 2021," Securelist, 2021. [Online]. Available: https://securelist.com/spam-and-phishing-in-2021/105713/. [Accessed: July 2, 2025].

[3] Check Point Research, "Fake Recruiters on LinkedIn: Threat Trends, 2022." (This may be part of a broader report or a specific blog post. A common reference that cites Check Point's findings is provided below as an example, as a direct link to the exact report title wasn't immediately available for 2022). [Online]. Available: https://blog.checkpoint.com/research/ (You would need to search their research blog for specific 2022 reports on LinkedIn/recruitment fraud.)

[4] LinkedIn Trust and Safety Center, "Community Report," About LinkedIn, 2024. [Online]. Available: https://about.linkedin.com/transparency/community-report. [Accessed: July 2, 2025].

[5] Microsoft Security Blog, "Improving Trust on LinkedIn Through AI, 2023." (A direct link to a blog post with this exact title from 2023 was not immediately available. This would typically be a blog post from Microsoft's official security or engineering blogs related to LinkedIn). [Online]. Available: https://www.microsoft.com/security/blog/ (You would need to search their blog for articles related to "LinkedIn AI trust" around 2023).

[6] Cisco Talos, "The New Face of Digital Impersonation," Talos Blog, Oct. 26, 2023. [Online]. Available: https://blog.talosintelligence.com/digital-impersonation/. [Accessed: July 2, 2025].