myresearchgo

myresearchgo Volume 1, October Issue 7, 2025, ISSN: 3107-3816 (Online)

LinkedIn Under Attack: A Study on Job Profile Hacking and Digital Identity Exploitation

Ms. Niya Varghese
Assistant Professor, V. K. K. Menon College, Bhandup (East)

Abstract
In today's digital age, LinkedIn has become a vital platform for professional networking and job searching. However, the rise of job profile hacking poses significant threats to user trust and platform integrity. This study draws from personal experience and broader observations to highlight how account compromises on LinkedIn can lead to unauthorized access, misuse of profiles, and fraudulent activities. Despite LinkedIn's reputation as a professional network, hacking incidents reveal vulnerabilities that undermine users' confidence in the platform's security. This paper emphasizes the importance of raising awareness about LinkedIn account hacking and advocates for stronger security measures to protect users. Ensuring trustworthiness on professional networks is essential for their continued role in career development and recruitment.

Keywords: *LinkedIn, Job Profile Hacking, Account Compromise, Cyber security, Digital Identity Theft, Professional Networking Security, Online Job Fraud, Account Recovery Challenges, Social Engineering, User Awareness.*

Introduction

LinkedIn is the world's largest professional networking platform, hosting more than 1 billion users globally. While it serves as a critical tool for recruitment, job searching and professional growth, its increasing popularity has also made it a prime target for cybercriminals.

LinkedIn is widely used by students, professionals, and recruiters to connect and explore job opportunities. Unlike typical social media platforms, LinkedIn focuses on professional identities and career development, making it a trusted environment for millions. However, despite this trust, LinkedIn accounts are increasingly being hacked, leading to serious security concerns.

These attacks go beyond simple social media hacking; cybercriminals gain unauthorized access to legitimate LinkedIn profiles and manipulate them to promote fraudulent businesses or scams. By altering profile details and business information, hackers deceive the victim's network, harming reputations and misleading potential employers or clients. Unfortunately, many users remain unaware that such threats are prevalent within professional networks like LinkedIn.

Given the platform's crucial role in the global job market, it is essential for users, recruiters, and platform providers to understand these risks. Awareness of LinkedIn account hacking and its consequences are vital to protect professional identities and maintain trust in digital job platforms.

This research paper aims to explore the rise of LinkedIn job profile hacking, investigate the methods hackers use, assess the impact on victims, and examine the challenges users face during account recovery. Through this study, the goal is to raise awareness and suggest improvements to enhance security and user protection on LinkedIn.

myresearchgo Volume 1, October Issue 7, 2025, ISSN: 3107-3816 (Online)

Literature Review

LinkedIn is the world's leading professional networking platform, extensively used for job searching, recruitment, and business networking. Due to its importance, LinkedIn accounts have become prime targets for cyber attackers seeking to gain unauthorized access. Unlike the creation of fake profiles, which involves setting up entirely fraudulent accounts, LinkedIn account hacking specifically targets genuine user profiles through methods such as phishing, credential stuffing, and social engineering. Once compromised, these accounts are exploited to conduct fraudulent business activities, spread misinformation, or scam the victim's professional network.

Several cybersecurity studies highlight the increasing frequency of account takeover attacks across social media platforms, emphasizing that compromised real accounts pose greater risks due to their established trust and connections. On LinkedIn, attackers leverage this trust to start businesses or advertise services under the victim's name, leading to reputational damage and financial loss.

LinkedIn has implemented various security measures such as multi-factor authentication and suspicious activity monitoring to protect users. However, many users remain vulnerable due to weak security practices and lack of awareness. Additionally, detection and response often depend on user reporting, causing delays in mitigating ongoing attacks.

A critical security issue identified in recent user reports involves the account recovery process. While biometric face verification can help rightful owners regain access to hacked profiles, victims frequently encounter difficulties in fully restoring control because the attacker's phone number remains linked to the account for password resets and two-factor authentication. This flaw allows hackers to maintain partial control and continue misusing the profile even after the victim regains access .This loophole highlights a significant vulnerability in LinkedIn's security infrastructure and emphasizes the need for more robust recovery mechanisms that prioritize complete restoration of account ownership.

Despite these growing concerns, academic research specifically addressing LinkedIn account hacking and the nuances of recovery challenges remains limited. Most existing studies focus on fake profile detection or general

social engineering attacks, leaving a gap in understanding the full scope and impact of compromised real profile misuse in professional networks.

This study seeks to address this gap by exploring the techniques used to hack LinkedIn accounts, the consequences of such breaches, and the challenges victims face during recovery, thereby contributing valuable insights for enhancing platform security and user protection.

Problem Solving

LinkedIn has become a vital platform for professional networking, job applications, and business visibility. However, the rise in account hacking on LinkedIn has introduced a serious threat to user security and trust. Cybercriminals are no longer just creating fake profiles they are hacking real user accounts and altering them to promote their own businesses, conduct scams, or impersonate the victim for personal gain.

This not only damages the professional image of the hacked individual but also puts their network (recruiters, clients, employers) at risk. In many cases, even after the rightful owner regains access, they are unable to change crucial security details such as passwords or linked mobile numbers, allowing hackers to maintain partial control.

The key problems addressed in this research are:

- How LinkedIn accounts are being hacked and misused.
- The lack of user awareness about these risks.
- The limitations in LinkedIn's account recovery and security systems.
- The impact of such incidents on trust, careers, and recruitment.

This study aims to provide insights into the seriousness of the issue and offer practical recommendations to improve platform safety and user awareness.

Research Methodology

To understand the issue of LinkedIn job profile hacking, a mixed-methods approach has been used, combining both qualitative and quantitative research methods.

1. Personal Case Study

This paper is inspired by a real-life experience, where the author's LinkedIn account was hacked, and suspicious activities (like messages from strangers and unauthorized changes) were discovered. This experience provides a practical context to the issue.

2. Surveys

A short questionnaire was distributed among students, working professionals, and HR recruiters to collect data on:

- Whether they've experienced or heard of LinkedIn hacking.
- Their awareness of LinkedIn's security features.
- Their trust in the platform post-incident.

3. Interviews

Short interviews with cybersecurity experts and HR professionals were conducted to gain deeper insights into:

- Common hacking methods used on LinkedIn.
- Real-world cases they've encountered.

- Suggestions for better security and awareness.

4. Online Profile Observations
A sample of public LinkedIn profiles was observed to identify suspicious patterns such as:

- Sudden changes in job roles.
- Fake business promotions.
- Engagement in unusual messaging activity.

5. Secondary Research
Existing literature, cybersecurity blogs, LinkedIn security documentation, and news articles were reviewed to support the findings and compare with broader trends.

Results & Findings

1. Discovery of Fraudulent Companies Gaining Unauthorized Access
During the course of the research, it was discovered that several fraudulent companies are exploiting LinkedIn's open networking model to gain unauthorized access to user accounts. These companies often present themselves as legitimate employers and invite users to connect or apply for jobs. Once contact is made, they somehow gain access to the user's profile (either through phishing, social engineering, or account permissions).

2. Profile Hijacking and History Deletion
A pattern was identified in which users reported that their LinkedIn work history had been deleted or replaced without their consent. In most cases, the fraudulent company added itself to the user's profile, listing the user as a Sales Executive or a similar role. This appears to be an effort to boost the fraudulent company's credibility by making it appear as though it has many employees.

3. Widespread Pattern Among Multiple Users
Multiple users were affected by the same company or group of companies. Most of the affected profiles showed:

- Sudden changes in work history
- Identical or similar job titles
- Involvement with little known companies with no online presence.

This indicates an organized and possibly automated effort to hijack LinkedIn profiles.

4. Lack of Verification and Weak Security Measures
The results show that LinkedIn lacks effective security and verification protocols to prevent such actions. Users are not immediately alerted when job history is changed, and there are minimal barriers for companies to be listed as employers on the platform.

5. User Awareness is Low
Interviews and reports from affected users show that most were unaware of what had happened until days or weeks after the change. There is a clear gap in user awareness and platform protections making it easy for these fraudulent companies to operate undetected.

Analysis

This research revealed a concerning trend on LinkedIn, where fraudulent companies exploit the platform's weak verification systems to gain unauthorized access to user profiles. These companies often alter users' professional histories deleting legitimate experience and adding fabricated roles, typically labelling users as "Sales Executives" under their own brand. This manipulation not only damages individual reputations but also raises broader questions about digital identity protection and trust in professional platforms. The findings show that many users remain unaware of such changes until after significant damage is done and LinkedIn offers minimal safeguards or alerts for unauthorized profile edits.

This matters because it exposes users to reputational harm, enables scams, and allows fake companies to falsely establish credibility. More importantly, it highlights serious flaws in platform accountability, employer verification, and user awareness.

Moving forward, there is a clear need for stronger security features on LinkedIn, including real-time alerts for profile changes, stricter employer verification, and user education on digital safety. Further research is also needed to investigate how these fraudulent entities gain access, how widespread the issue is, and what technological tools can be used to detect such activities. Collaboration between professional platforms, cybersecurity experts and users is essential to protect digital professional identities in an increasingly vulnerable online environment.

Conclusion & Future Scope

Through my experience and research, I learned that there is a specific type of hacking targeting LinkedIn profiles, which many users are unaware of. Fraudulent companies and individuals exploit vulnerabilities to manipulate profiles, often without the user's knowledge. This highlights a significant security gap on LinkedIn that can damage professional reputations and undermine trust in the platform.

Therefore, it is crucial for LinkedIn to strengthen its security measures to protect users from such attacks. Increased verification processes, real-time alerts for profile changes, and better user education about potential risks are essential steps to prevent these incidents.

For the future, further research is needed to understand the methods hackers use to access accounts and to develop advanced tools for detecting suspicious activity. Collaboration between LinkedIn, cybersecurity experts, and users will be vital to ensure a safer and more reliable professional networking environment.

References

LinkedIn Corporation. (2024). *Keeping your LinkedIn profile secure*. Retrieved August 22, 2025, from https://www.linkedin.com/help/linkedin/answer/66/keeping-your-linkedin-profile-secure

Johnson, L., & Patel, R. (2022). Hacking professional profiles: A new threat to online networking. *Cybersecurity Today*, 9(4), 110-123.