The LinkedIn Breach

Mary-Laurence Lelina-Ford

Old Dominion University

In 2021 one of the most notable cybersecurity breaches took place with LinkedIn. Google (2023) LinkedIn is a business and employment-focused social media platform that works through websites and mobile apps. According to LinkedIn, the breach was committed first in April of 2021 and again in June of the same year. User information such as full name, e-mail address, phone numbers, geological location, and links to their social media were posted on the dark web. The hacker, whose name is Tomliner (Baek, 2023) or God User (Tunggal, 2023) , tried to sell the information for thousands of dollars or for Bitcoin.

Identity Theft (2023), an online article, shows that LinkedIn has been hacked more than once for many years, which shows a network vulnerability. Its application programming interface (API) was weak on more than one occasion, so the hacker was able to easily scrape data from the system. A human-induced threat using malware exploited the network vulnerability.

Baek (2023) none of the user’s confidential information, such as payment information, was disclosed. Regardless, the repercussions could still be a danger to the affected users. Some users have their LinkedIn accounts linked to their social media profiles. Social media, such as Facebook, contains more personal information such as pictures of loved ones, birthdays, family members, etc. Another repercussion is some users use the same credentials for their social media like Facebook and LinkedIn accounts. Identity theft is another repercussion. Another person could create a profile posing as the rightful person based on the exposed information. Phishing is another repercussion. One of the pieces of information that the hacker was able to obtain was an electronic mail address. Someone could use e-mail for personal gain.

I have had a personal unpleasant experience with LinkedIn where a former boss sent me a message via LinkedIn. His message included a link to a “potential job” he was supposedly helping me with. It turned out that his account was hacked. The link asked me to enter my basic information, like name and address. Two days later, I received a check in the mail for something I had never heard of. I researched the check, and it turned out that if I had deposited the check into my account, hackers would have been able to trace it and wipe my bank. I believe that is a great example of phishing within the LinkedIn network. I thought the message was actually sent by my former boss when it was not.

I believe even if LinkedIn required users to use long, complicated passwords and change them often, the network would still not prevent the event from happening. The network has been hacked multiple times, which only shows that LinkedIn needs to use more proper security controls. I also think another layer of security for the Application Programming Interface API could have been taken to mitigate the consequences.

**References:**

Tunggal, A. (2023, November 14). *The 72 Biggest Data Breaches of All Time [Updated 2023].*

Upguard. <https://www.upguard.com/blog/biggest-data-breaches>

Baek, D. (2023, December 10). *LikedIn Data Breach (700 Million) in 2021.*

LinkedIn. h<ttps://www.linkedin.com/pulse/linkedin-data-breach-700m-2021-david-sehyeon-b>aek--ex85c

CyberNews. (2023, November). *Scraped Data of 500 Million LinkedIn Users Being Sold Online, 2 Million Records Leaked as Proof.*

<https://cybernews.com/news/stolen-data-of-500-million-linkedin-users-being-sold-online-2->million-leaked-as-proof-2/

Identity Theft. (2023). *The LinkedIn Data Breaches: What to Do and Who was Affected.*

https://identitytheft.org/data-breach/linkedin/