In June 2021, data from 700 million Linked-In accounts were released onto the web in a controversial hack. The actor responsible for the hack hacked into Linkedin's api to override it's rate limit protocol in order for the hack to access as many accounts as it did. When asked why he leaked this data, the hacker explained that he simply did it for fun.

Linkedin denied that this was an actual data breach of confidential information, however the hacker certainly used the API to scrape the website for massive amounts of data in a way that was not intended at all. Because Linkedin was arguing this was a data scrape and not a breach of confidential user data, it does not appear as if they have made any changes to protect against their API's vulnerabilities. In fact, the recent hack is not the first time in 2021 that Linkedin's api was used to scrape the website for large amounts of user data. It appears as if the Linkedin api is not protecting their user's data, but instead providing a roadmap around their own security parameters for bad actors to exploit.