

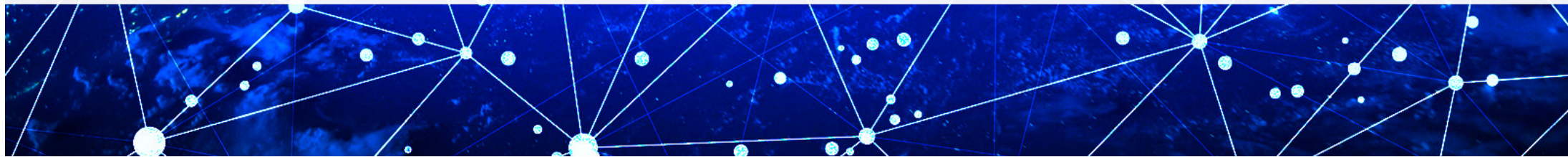
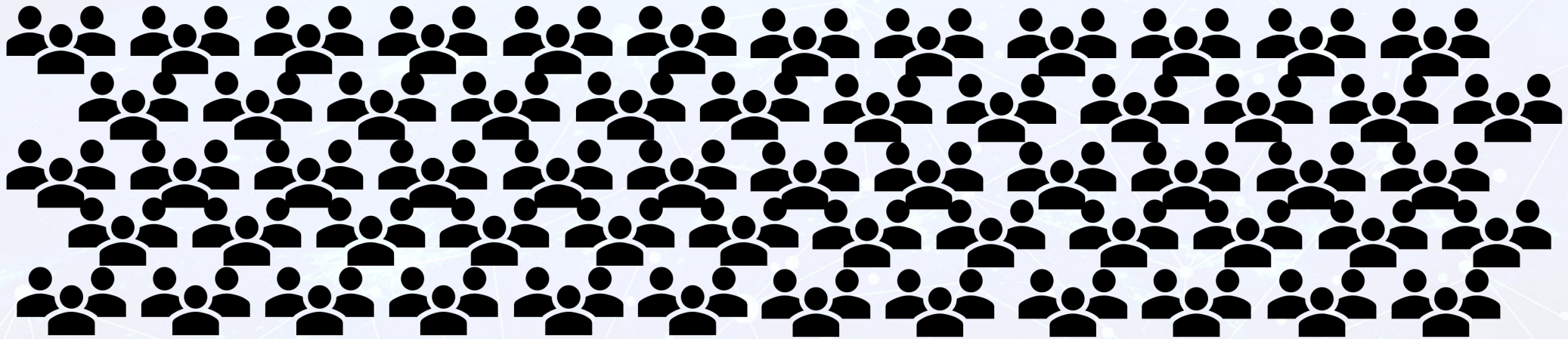
Mohammad Atieh

LinkedIn Data Breach 2021



LinkedIn Data Breach

- Date: June 2021
- Impact: 700 million users



Types of Data Affected

- User information for 90% of the users were stolen.

```
"full_name":"charlie [REDACTED]","gender":"male",  
"linkedin.com/[REDACTED]5",  
"linkedin_username":"charlie-[REDACTED]5","linkedin_id":"2:[REDACTED]3",  
"facebook_url":"facebook.com/v[REDACTED]",  
"facebook_username":"v[REDACTED]",  
"facebook_id":"1[REDACTED]5",  
"work_email":"cl[REDACTED].com",  
"mobile_phone":"+15[REDACTED]8",  
"industry":"biotechnology",  
"location_name":"cambridge, massachusetts, united states",  
"location_metro":"boston, massachusetts"  
"location_geo":"42.37,-71.10","location_last_updated":"2020-12-01",  
"linkedin_connections":120,"inferred_salary":"[REDACTED]",  
"inferred_years_experience":5,  
"summary":"I am a moti[REDACTED]  
"full_name":"mehari [REDACTED]"  
"linkedin_url":"linkedin.com/[REDACTED]",  
"linkedin_username":"mehari-[REDACTED]5",
```

Hill, M. (2021) The 15 biggest data breaches of the 21st century. *CSO Online*.

Taylor, S. (2021) New LinkedIn Data Leak Leaves 700 Million Users Exposed. Available from: <https://restoreprivacy.com/linkedin-data-leak-700-million-users/> [Accessed 12 October 2022].

Types of Data Affected

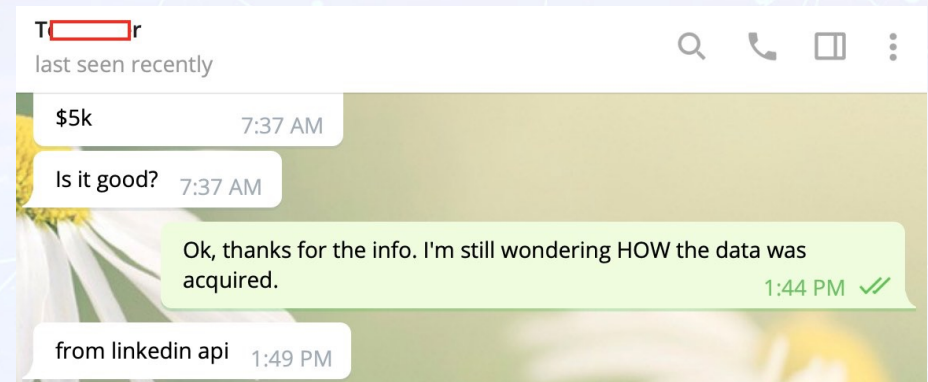
Email Addresses, Full **names**, **Phone numbers**
Physical addresses,
Geolocation records,
LinkedIn username and **profile URL**,
Personal and professional **experience/background**,
Genders,
and other **social media accounts and usernames**

Hill, M. (2021) The 15 biggest data breaches of the 21st century. *CSO Online*.

Taylor, S. (2021) New LinkedIn Data Leak Leaves 700 Million Users Exposed. Available from: <https://restoreprivacy.com/linkedin-data-leak-700-million-users/>
[Accessed 12 October 2022].

What Happened?

- User information was obtained using data scraping from LinkedIn API and other sources and offered for sale for 500\$

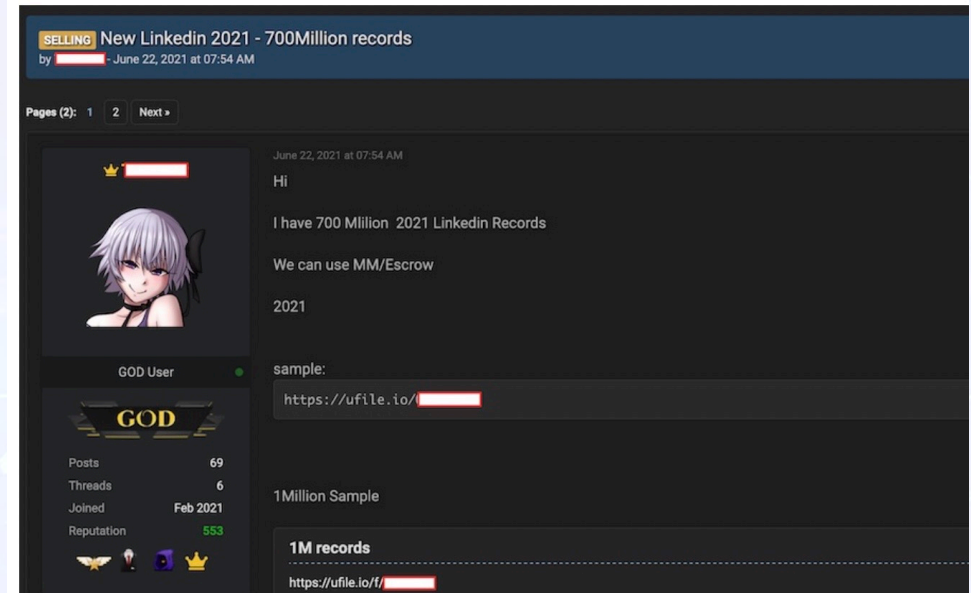


National Council on Identity Theft Protection (2022) The LinkedIn Data Breaches: What to Do and Who Was Affected - IdentityTheft.org. Available from: <https://identitytheft.org/data-breach/linkedin/> [Accessed 12 October 2022].

Taylor, S. (2021) New LinkedIn Data Leak Leaves 700 Million Users Exposed. Available from: <https://restoreprivacy.com/linkedin-data-leak-700-million-users/> [Accessed 12 October 2022].

Who was responsible?

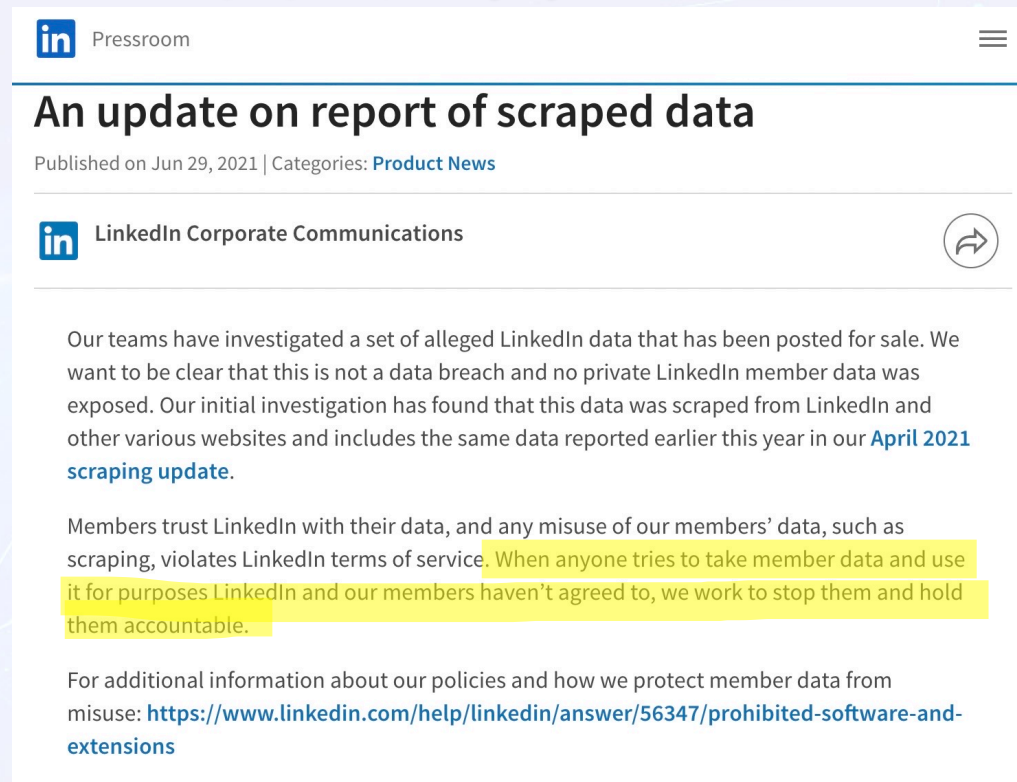
- TomLiner
- Classified as a “God” User” in the undermarket!



Taylor, S. (2021) New LinkedIn Data Leak Leaves 700 Million Users Exposed. Available from: <https://restoreprivacy.com/linkedin-data-leak-700-million-users/> [Accessed 12 October 2022].

Were any Escalation(s) Stopped - How?

- LinkedIn published as statement and a warning.



The screenshot shows a LinkedIn Pressroom article. At the top left is the LinkedIn logo and the word 'Pressroom'. At the top right is a hamburger menu icon. The main title is 'An update on report of scraped data'. Below the title is the publication date 'Published on Jun 29, 2021' and the category 'Product News'. The author is 'LinkedIn Corporate Communications' with a share icon to the right. The article text begins with: 'Our teams have investigated a set of alleged LinkedIn data that has been posted for sale. We want to be clear that this is not a data breach and no private LinkedIn member data was exposed. Our initial investigation has found that this data was scraped from LinkedIn and other various websites and includes the same data reported earlier this year in our [April 2021 scraping update](#).' The next paragraph states: 'Members trust LinkedIn with their data, and any misuse of our members' data, such as scraping, violates LinkedIn terms of service. **When anyone tries to take member data and use it for purposes LinkedIn and our members haven't agreed to, we work to stop them and hold them accountable.**' The final paragraph provides a link for more information: 'For additional information about our policies and how we protect member data from misuse: <https://www.linkedin.com/help/linkedin/answer/56347/prohibited-software-and-extensions>'

Was the Business Continuity Plan instigated?

- No



The screenshot shows a LinkedIn Pressroom article. At the top left is the LinkedIn logo and the word 'Pressroom'. To the right is a hamburger menu icon. The main title is 'An update on report of scraped data'. Below the title, it says 'Published on Jun 29, 2021 | Categories: Product News'. The author is 'LinkedIn Corporate Communications' with a share icon to the right. The main text of the article is highlighted in yellow and reads: 'Our teams have investigated a set of alleged LinkedIn data that has been posted for sale. We want to be clear that this is not a data breach and no private LinkedIn member data was exposed. Our initial investigation has found that this data was scraped from LinkedIn and other various websites and includes the same data reported earlier this year in our April 2021 scraping update.' Below this, there is a paragraph: 'Members trust LinkedIn with their data, and any misuse of our members' data, such as scraping, violates LinkedIn terms of service. When anyone tries to take member data and use it for purposes LinkedIn and our members haven't agreed to, we work to stop them and hold them accountable.' At the bottom, there is a link: 'For additional information about our policies and how we protect member data from misuse: <https://www.linkedin.com/help/linkedin/answer/56347/prohibited-software-and-extensions>'

Was the Business Continuity Plan instigated?



Edwin A. Brockner, FIP

Assisting businesses with data privacy guidance and direction || CIPP/E/US, CIPM, CIPT, CDPSE, CRISC, CISA

- Per Article 4 of GDPR, a ‘personal data breach’ is a “breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed”
- The author stated that **it was not a data breach because private data was not disclosed**. Private data was protected with OAuth 2.0 for authorization and authentication. All they did is data scraping and aggregation.

Brockner, E. A. (2021) LinkedIn's June 2021 'Breach'. Available from: <https://www.linkedin.com/pulse/linkedins-june-2021-breach-edwin-brockner-cipm> [Accessed 12 October 2022].

General Data Protection Regulation (GDPR) (2022) General Data Protection Regulation (GDPR) – Final text neatly arranged. Available from: <https://gdpr-info.eu/> [Accessed 12 Oct. 2022].

Was the ICO notified?

- It is a US company, and they posted an international statement

in Pressroom



An update on report of scraped data

Published on Jun 29, 2021 | Categories: [Product News](#)

in LinkedIn Corporate Communications



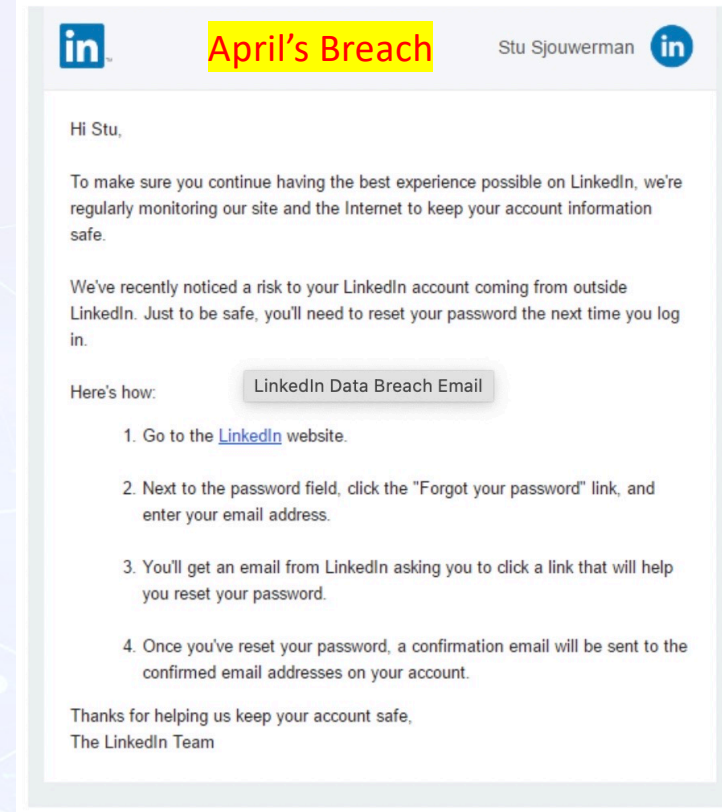
Our teams have investigated a set of alleged LinkedIn data that has been posted for sale. We want to be clear that this is not a data breach and no private LinkedIn member data was exposed. Our initial investigation has found that this data was scraped from LinkedIn and other various websites and includes the same data reported earlier this year in our [April 2021 scraping update](#).

Members trust LinkedIn with their data, and any misuse of our members' data, such as scraping, violates LinkedIn terms of service. When anyone tries to take member data and use it for purposes LinkedIn and our members haven't agreed to, we work to stop them and hold them accountable.

For additional information about our policies and how we protect member data from misuse: <https://www.linkedin.com/help/linkedin/answer/56347/prohibited-software-and-extensions>

Where the Users Notified?

- Yes, by email.



Sjouerman, S. (2022) Scam Of The Week: LinkedIn Email Change Your Password. Available from: <https://blog.knowbe4.com/scam-of-the-week-linkedin-email-change-your-password> [Accessed 12 October 2022].

What were the social, legal, and ethical implications of the decisions made?

- Risks of:
 - Identity theft
 - Phishing attempts
 - Social engineering attacks
 - Hacked accounts

Brockner, E. A. (2021) LinkedIn's June 2021 'Breach'. Available from: <https://www.linkedin.com/pulse/linkedins-june-2021-breach-edwin-brockner-cipm> [Accessed 12 October 2022].

Taylor, S. (2021) New LinkedIn Data Leak Leaves 700 Million Users Exposed. Available from: <https://restoreprivacy.com/linkedin-data-leak-700-million-users/> [Accessed 12 October 2022].

What Mitigations Would've Put had you been the ISM of the Organization

- Before the incident:
 - Enforce 2FA
 - Network traffic monitoring
- After the incident:
 - Enforce 2FA
 - Send emails warning from possible phishing attacks after the incident



Thanks!