Web Scrapers Claim to Possess and Sell Personal Data on 1.5 Billion Facebook Users on a Hacker Forum

privacyaffairs.com/facebook-data-sold-on-hacker-forum

Miklos Zoltan

The private and personal information of over 1.5 billion Facebook users is being sold on a popular hacking-related forum, potentially enabling cybercriminals and unscrupulous advertisers to target Internet users globally.

If authentic, this may constitute one of the biggest and most significant Facebook data dump to date.

Update – 5 October: *The forum seller has today responded and denied the scam accusations, continuing to claim that the data is real. The seller commented they are willing to cooperate with administrators of the forum to prove the authenticity of the data.*

Yesterday, a number of forum posters accused the seller of not delivering the promised data after payment was made.

> **Important Clarification:** This is completely unrelated to the global Facebook outage experienced on 4 October 2021.
>
> **Several websites and Twitter accounts incorrectly attribute the 4 October Facebook outage to this alleged data leak.**
>
> **Further Clarification:** It's alleged that the data was obtained by scraping publicly available data shared by users. Several media outlets and Twitter users misinterpret this to have resulted due to a hack or data breach, which is not the case.

It is seemingly unrelated to an earlier 2021 Facebook data dump, where 500 million users were affected.

> **Highlights:**
>
> - Data scrapers are selling sensitive personal data on 1.5 billion Facebook users.
> - Data contains users': name, email, phone number, location, gender, and user ID.
> - Data appears to be authentic.
> - Personal data obtained through web scraping.
> - Data can be utilized for phishing and account takeover attacks.
> - Sold data claimed to be new from 2021.
> - Some prospective buyers claim they were scammed by the seller and no data was delivered after payment was made
> - Seller responds to scam accusations. Claims is willing to cooperate with forum administrators to prove the authenticity of the data

In late September 2021, a user of a known hacker forum posted an announcement claiming to possess the personal data of more than 1.5 billion Facebook users. The data is currently up for sale on the respective forum platform, with potential buyers having the opportunity to purchase all the data at once or in smaller quantities.

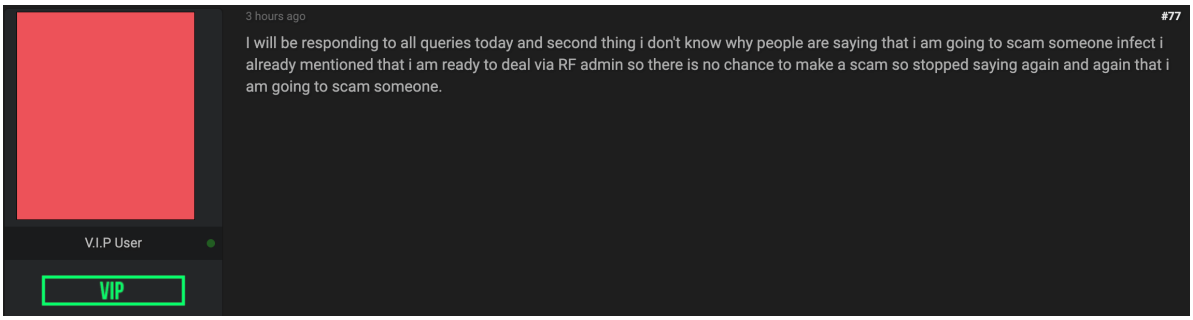
One prospective buyer claims to have been quoted $5,000 for the data of 1 million Facebook user accounts.

According to the forum poster, the data provided contains the following personal information of Facebook users:

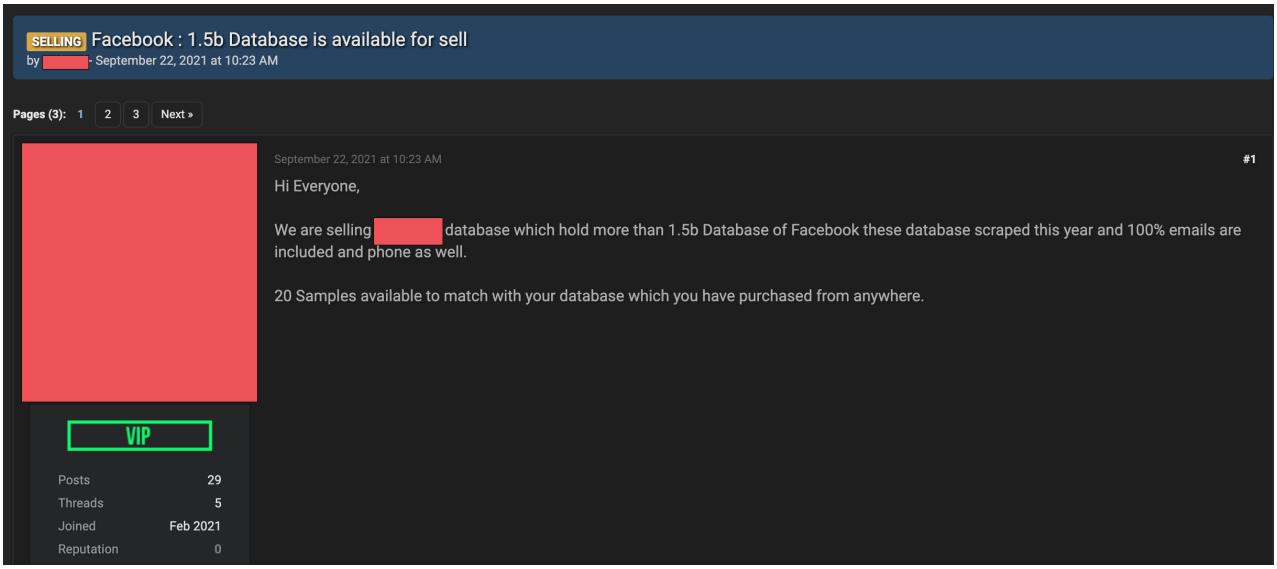
- Name
- Email
- Location
- Gender
- Phone number
- User ID

Related: *Dark Web Price Index 2021 – We looked into the prices hackers charge for items such as hacked Facebook, Instagram and LinkedIn accounts and even online banking logins on the dark web*

> **Update, 5 October:** The forum seller denies the scam accusations and claims is willing to cooperate with forum administrators to prove the authenticity of the sold data.



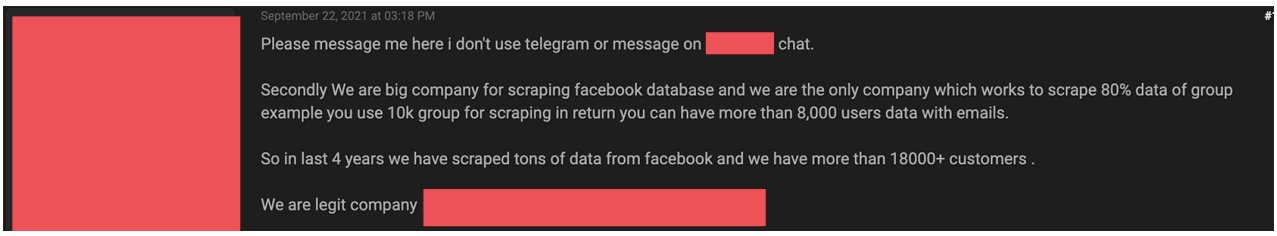
> **Update, late 4 October:** After this news was initially published, a forum user and prospective buyer claimed they paid the seller but haven't received anything in return. The seller hasn't yet responded to these accusations.
>
> All we know at this moment is that the multiple samples provided to forum users appeared to be real.



Samples presented on the forum show that the data indeed seems to be authentic.

Cross-checking them with known Facebook database leaks resulted in no matches, implying that at first glance, the sample data provided is unique and not a duplicate or re-sell of a previously known data breach or scraping.

The seller claims to represent a group of web scrapers in operation for at least four years, alleging that they've had over 18,000 clients during this time.



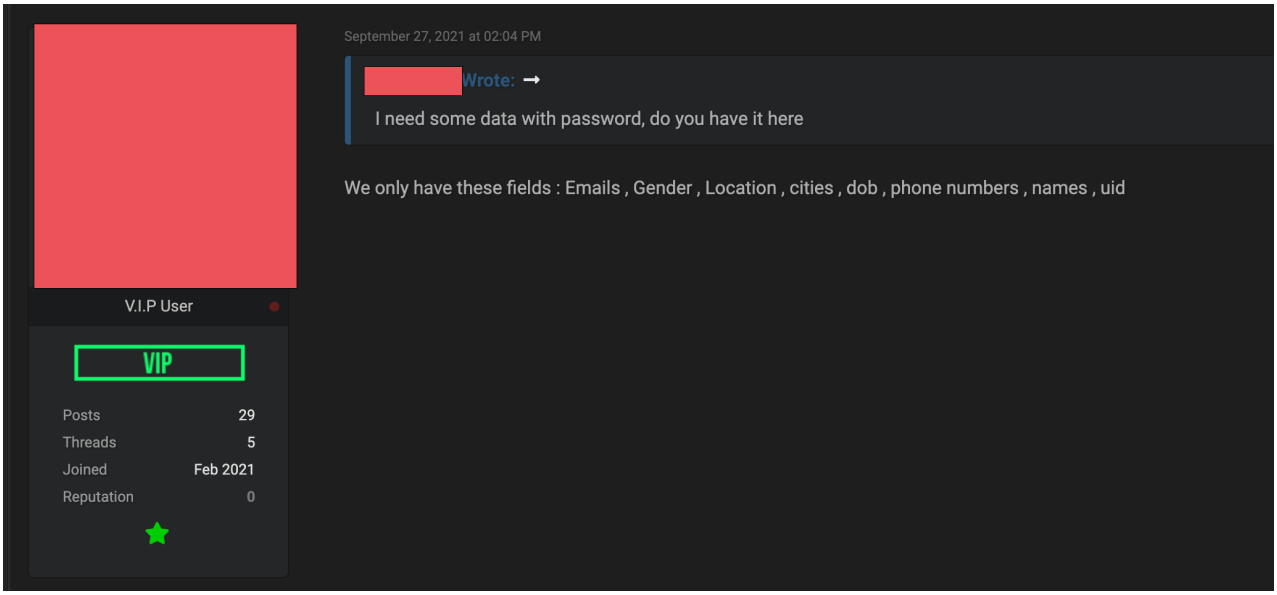
Data Obtained by Scraping

The traders claim to have obtained the data by scraping rather than hacking or compromising individual users' accounts. Scraping is a process of web data extraction or harvesting where publicly available data is accessed and organized into lists and databases.

While technically, no accounts have been compromised, this is little solace to those whose data may now end up in the hands of unscrupulous internet marketers and likely also in the hands of cybercriminals.

Unethical marketers may utilize this data to bombard specific individuals or groups of individuals with unsolicited advertising.

The fact that phone numbers, real-life location, and users' full names are included in the data is especially concerning. In addition, SMS and Push notification spam are becoming increasingly more prevalent even though most countries made these practices illegal many years ago.



Data Can be Used to Jeopardize Users' Security

For example, hackers can use the scraped data to conduct sophisticated phishing attacks or social engineering attacks.

Identifying individual users' phone numbers makes it possible for cybercriminals to send fake SMS messages to affected users pretending to be various entities such as Facebook

itself or even banks.

Users will then be invited to click on a link to either claim a prize, update their security settings, change their passwords, or do something similar.

After accessing the link, they will be redirected to a cloned version of the website the perpetrators pretend to represent. Then, if the user enters their actual current password, the cybercriminals will be able to hijack the affected account.

This is how Facebook accounts and even online banking logins are sold on the dark web for as cheap as just $10.

How is Facebook Data Scraped?

Scraping is the process of automatically collecting publicly available and accessible data online with the help of computer programs.

The majority of such data is obtained from simply scrapping Facebook profiles that have been set to “Public” by their owners. Unfortunately, the vast majority of personal information is freely shared and made available to the general public by Facebook users themselves.

Another popular – but illegal – method of data scraping is through fake Facebook surveys or quizzes.

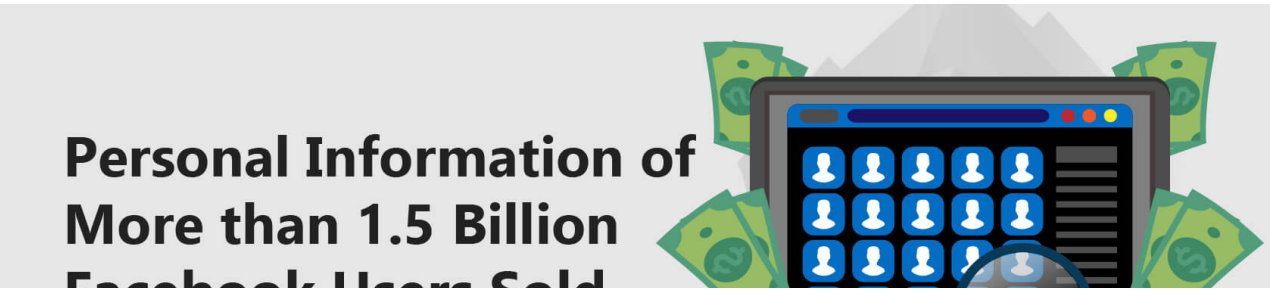
Every Facebook user has seen a post such as “Find out your Game of Thrones Lookalike with this Survey” or “Take this Quiz to Find out When you Will Get Married,” etc. Usually, these are schemes to obtain users’ personal data.

Every time someone enters one of these surveys or quizzes, they permit the creators of these games to view their personal Facebook information such as full name, email, phone number, location, gender, and more.

Facebook Users are Advised to Enhance their Security

It’s generally not recommended for Facebook users to set their accounts to be fully public.

Similarly, one should never enter random quizzes, surveys, or games on Facebook unless offered by a known and verified publisher. Almost always, these are, sadly, schemes used for data mining and scrapping.



Written by: Miklos Zoltan

Founder & CEO Privacy Affairs
Miklos Zoltan is the founder and CEO of Privacy Affairs. Miklos has long-time experience in cybersecurity and data privacy having worked with international teams for more than 10 years in projects involving penetration testing, network security and cryptography.

Miklos founded Privacy Affairs in 2018 to provide cybersecurity and data privacy education to regular audiences by translating tech-heavy and "geeky" topics into easy-to-understand guides and tutorials.