# Facebook Data Breach

March 16, 2021, it was [**revealed**](https://heimdalsecurity.com/blog/533-million-facebook-data-leaked-online/) that the personal information of 533 million Facebook users, approximately 20% of all accounts, was leaked online.

Although the data is 2 years old, the 2021 Facebook data breach is an extremely serious matter, since the leaked data is still valuable to cybercriminals who use people’s personal information to impersonate them or scam them into handing over login credentials.

## What Kind of Data Was Leaked and How Was It Done?

Private information of users was primarily obtained by exploiting Facebook’s contact importer feature that allows users to find friends on the social media app using their phone’s contact list.

The publicly accessible database had personal details of Facebook users with phone numbers, Facebook IDs, full names, locations, birthdates, bios, and, in some cases, email addresses. Even Facebook CEO Mark Zuckerberg’s own private credentials were reportedly leaked in the process.

Threat actors then leaked this data on the dark web. Information on users’ finance and password were not divulged.

According to Business Insider, a Facebook spokesperson confirmed that the data had been scraped due to a vulnerability that [**the company patched in 2019**](https://edition.cnn.com/2019/09/04/tech/facebook-phone-numbers-exposed). Facebook said it fixed the contact importer flaw after it discovered it was being exploited. The company said that it’s important to mention that attackers did not hack its systems by injecting malicious code that would weaken the company’s security defenses. Instead, the attackers scraped the data from its service.

Critics allege that this is nothing more than Facebook’s attempt to downplay the severity of the leak. Facebook apologized for the 2019 data loss, but never directly informed users their accounts had been compromised.

**Hudson Rock**’s Chief Technology Officer Alon Gal said that the leaked data could benefit cybercriminals who use people’s personal information to impersonate them or scam them into handing over login credentials.

Gal is the one who discovered the leak in January when a user in the same hacking forum advertised an automated bot that could provide phone numbers for hundreds of millions of Facebook users for money.

## How Is Facebook’s 2021 Leak Unique?

The personal information that was leaked online included over 32 million records on users in the U.S., 11.5 million in the U.K., and 6 million in India.

The 2021 Facebook data breach is similar to LinkedIn’s security incident where data from over 500 million users has been sold online by an unknown hacker who had dumped two million users’ data as proof.

According to Raj Samani, Chief Scientist at cybersecurity firm McAfee, in the case of LinkedIn, it was affirmed that data was scraped, meaning someone violated the terms of service to gather public profile data and data from other websites.

The information leaked is in many ways similar to the Facebook incident, but it contains other professional information that might add another layer of sensitivity, Samani says.

Facebook’s stolen data first appeared on a hacking community in June 2020 when a member began selling the Facebook data to other members, but what made the leak stand out was the fact that the data contained member information that can be scraped from public profiles and private mobile numbers associated with the accounts.

## How Can the Leaked Data Be Used?

Alon Gal confirmed that data from the 2021 Facebook data breach was now being sold on multiple groups on the cloud-based messaging app Telegram. What’s more, the data set seems to appear on various hacker forums all over the Internet.

The stolen information can be used for [**email fraud**](https://heimdalsecurity.com/blog/how-to-report-email-fraud/), [**scam phone calls**](https://heimdalsecurity.com/blog/victim-scam-phone-calls/), [**phishing attacks**](https://heimdalsecurity.com/blog/abcs-detecting-preventing-phishing/), [**SIM swapping**](https://heimdalsecurity.com/blog/what-is-sim-swapping/), and target advertising. It can be used to plot and execute various nefarious online fraud schemes. Hackers can [**impersonate users**](https://heimdalsecurity.com/blog/how-to-prevent-identity-theft-20-steps/) and make money transfers on their behalf, without their knowledge or approval.

The database of private information is available on the dark web for anyone to sift through.

All Facebook users should be wary of strange emails or texts that are requesting further information or instructing the user to click on enclosed links.

## How to Protect Your Data

Everyone is talking about the 2021 Facebook data breach and we all should take a few moments of reflection about the privacy of our data on the Internet. Users even started deleting their Facebook accounts following the leak, urging people to leave the social network, while others may be really concerned about the exploitation of personal data.

Users seeking to know whether their data has been leaked or compromised can visit [**HaveIBeenPwned.com**](https://www.haveibeenpwned.com/). The website was updated to show compromised phone numbers and emails. All they have to do is to key in their email ID and check.

If you’re among the people who were impacted by the data leak, the first thing you should do is update your password. You can use a security service like 1Password to help manage multiple, strong passwords across different apps.

Facebook also recommended that users should enable two-factor authentication on their accounts in order to access them, as a means of protection.

It is understandable that Facebook users are becoming more and more frustrated with yet another report of mismanaged data. They are tired of apologies followed by statements about how seriously the social media giant takes their privacy.

It’s worth reminding that Facebook will (still) know things about you, but at least you can limit its access to your private data.

## Final Thoughts

Facebook has a long history of failing to protect customer data and has been in the news for massive breaches that seem to be getting bigger each year.

The news about the Cambridge Analytica firm harvesting personal data taken from millions of Facebook without user consent hit the headlines back in 2015 when the third-party app developer improperly harvested data on 87 million users. The same data was used to micro-target voters in the 2016 U.S. presidential election and British Brexit voters. Facebook was **fined** by U.S. and British regulators for mishandling user data and changed its policy around the information shared with third-party app developers.

As for the 2021 Facebook data breach, Cory Doctorow of the Electronic Frontier Foundation (EFF) said dominance in the tech industry directly contributed to hacks like these.