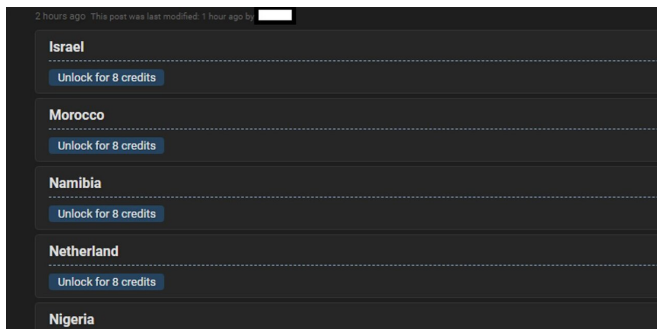


Facebook data breach: What happened and why it's hard to know if your data was leaked

6 April 2021, by Paul Haskell-Dowland

(@UnderTheBreach) [January 14, 2021](#)



Credit: Alon Gal/Twitter

Over the long weekend [reports](#) emerged of an alleged data breach, impacting half a billion Facebook users from 106 countries.

And while this figure is staggering, there's more to the story than 533 million sets of data. This breach once again highlights how many of the systems we use aren't designed to adequately protect our information from cyber criminals.

Nor is it always straightforward to figure out whether your data have been compromised in a breach or not.

In early 2020 a vulnerability that enabled seeing the phone number linked to every Facebook account was exploited, creating a database containing the information 533m users across all countries.

It was severely under-reported and today the database became much more worrisome 1/2

pic.twitter.com/ryQ5HuF1Cm

— Alon Gal (Under the Breach)

What happened?

More than [500 million Facebook users' details](#) were published online on an underground website used by cyber criminals.

It quickly became clear this was not a new data breach, but an older one which had come back to haunt Facebook and the millions of users whose data are now available to purchase online.

The data breach is believed to relate to a vulnerability which Facebook reportedly [fixed in August of 2019](#). While the exact source of the data can't be verified, it was likely acquired through the misuse of [legitimate functions in the Facebook systems](#).

Such misuses can occur when a seemingly innocent feature of a website is used for an unexpected purpose by attackers, as was the case with a PayID attack in 2019.

In the case of Facebook, criminals can mine Facebook's systems for users' personal information by using techniques which automate the process of harvesting data.

This may sound familiar. In 2018 Facebook was reeling from the [Cambridge Analytica scandal](#). This too was not a [hacking incident](#), but a misuse of a perfectly legitimate function of the Facebook platform.

While the data were initially obtained legitimately—as least, as far as Facebook's rules

were concerned—it was then passed on to a third party [without the appropriate consent](#) from users.

Were you targeted?

There's no easy way to determine if your details were breached in the recent leak. If the website concerned is acting in your best interest, you should at least receive a notification. But this isn't guaranteed.

Even a tech-savvy user would be limited to hunting for the leaked data themselves on underground websites.

The data being sold online contain plenty of key information. [According to](#) [haveibeenpwned.com](#), most of the records include names and genders, with many also including dates of birth, location, relationship status and employer.

data could be to enhance phishing and SMS-based spam attacks.

I've had a heap of queries about this. I'm looking into it and yes, if it's legit and suitable for [@haveibeenpwned](#) it'll be searchable there shortly. <https://t.co/QPLZdXATpt>

— Troy Hunt (@troyhunt) [April 3, 2021](#)

How to protect yourself

Given the nature of the leak, there is very little Facebook users could have done proactively to protect themselves from this breach. As the attack targeted Facebook's systems, the responsibility for securing the data lies entirely with Facebook.

On an individual level, while you can opt to withdraw from the platform, for many this isn't a simple option. That said, there are certain changes you can make to your social media behaviors to help reduce your risk from data breaches.

Chief technology officer of cybercrime intelligence firm Hudson Rock, Alon Gal, discovered the leaked database, posting screenshots on Twitter. Credit: Twitter

(1) Ask yourself if you need to share all your information with Facebook

There are some bits of information we inevitably have to forfeit in exchange for using Facebook, including mobile numbers for new accounts (as a security measure, ironically). But there are plenty of details you can withhold to retain a modicum of control over your data.

Although, it has been [reported](#) only a small proportion of the stolen data contained a valid email address (about 2.5 million records).

(2) Think about what you share

Apart from the leak being reported, there are plenty of other ways to harvest user data from Facebook. If you use a fake birth date on your account, you should also avoid posting birthday party photos on the real day. Even our [seemingly innocent photos](#) can reveal sensitive information.

This is important since a user's data are less valuable without the corresponding email address. It's the combination of date of birth, name, [phone number](#) and email which provides a useful starting point for [identity theft and exploitation](#).

If you're not sure why these details would be valuable to a criminal, think about how you confirm your identity over the phone with your bank, or how you last reset a password on a website.

(3) Avoid using Facebook to sign in to other websites

Haveibeenpwned.com creator and web security expert Troy Hunt has said a secondary use for the

Although the "sign-in with Facebook" feature is potentially time-saving (and reduces the number of accounts you have to maintain), it also increases [potential risk](#) to you—especially if the site you're signing into isn't a trusted one. If your Facebook account is compromised, the attacker will have automatic access to all the linked websites.

(4) Use unique passwords

Always use a different password for each online account, even if it is a pain. Installing a password manager will help with this (and this is how I have more than 400 different passwords). While it won't stop your data from ever being stolen, if your password for a site is leaked it will only work for that *one* site.

If you really want a scare, you can always download a copy of all the [data Facebook has on you](#). This is useful if you're considering leaving the platform and want a copy of your data before closing your account.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

APA citation: Facebook data breach: What happened and why it's hard to know if your data was leaked (2021, April 6) retrieved 26 September 2021 from <https://techxplore.com/news/2021-04-facebook-breach-hard-leaked.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.