Facebook Says It's Your Fault That Hackers Got Half a Billion User Phone Numbers

vice.com/en/article/88awzp/facebook-says-its-your-fault-that-hackers-got-half-a-billion-user-phone-numbers

A database containing the phone numbers of more than half a billion Facebook users is being freely traded online, and Facebook is trying to pin the blame on everyone but themselves.

A blog post titled "The Facts on News Reports About Facebook Data," published Tuesday evening, is designed to silence the growing criticism the company is facing for failing to protect the phone numbers and other personal information of 533 million users after a database containing that information was shared for free in low level hacking forums over the weekend, as first reported by Business Insider.

Facebook initially dismissed the reports as irrelevant, claiming the data was leaked years ago and so the fact it had all been collected into one uber database containing one in every 15 people on the planet—and was now being given away for free—didn't really matter.

Facebook has become accustomed to dealing with multiple massive privacy breaches in recent years, and data belonging to hundreds of millions of its users has been leaked or stolen by hackers.

But, instead of owning up to its latest failure to protect user data, Facebook is pulling from a familiar playbook: just like it did during the Cambridge Analytica scandal in 2018, it's attempting to reframe the security failure as merely a breach of its terms of service.

So instead of apologizing for failing to keep users' data secure, Facebook's product management director Mike Clark began his blog post by making a semantic point about how the data was leaked.

"It is important to understand that malicious actors obtained this data not through hacking our systems but by scraping it from our platform prior to September 2019," Clark wrote.

This is the identical excuse given in 2018, when it was revealed that Facebook had given Cambridge Analytica the data of 87 million users without their permission, for use in political ads.

Clark goes on to explain that the people who collected this data—sorry, “scraped” this data—did so by using a feature designed to help new users find their friends on the platform.

“This feature was designed to help people easily find their friends to connect with on our services using their contact lists,” Clark explains.

The contact importer feature allowed new users to upload their contact lists and match those numbers against the numbers stored on people’s profiles. But like most of Facebook’s best features, the company left it wide open to abuse by hackers.

“Effectively, the attacker created an address book with every phone number on the planet and then asked Facebook if his ’friends’ are on Facebook,” security expert Mikko Hypponen explained in a tweet.

Clark’s blog post doesn’t say when the “scraping” took place or how many times the vulnerability was exploited, just that Facebook fixed the issue in August 2019. Clark also failed to mention that Facebook was informed of this vulnerability way back in 2017, when Inti De Ceukelaire, an ethical hacker from Belgium, disclosed the problem to the company.

> They also claim to have 'found' the issue in 2019 - which is a blatant lie. I reported the issue to them in 2017 - they said "we might tweak rate limits in the future" and blamed users for not understanding their kafkaesque privacy settings.https://t.co/0xLpXvbonw pic.twitter.com/57yHrmYViJ
>
> — Inti De Ceukelaire (@intidc) April 6, 2021

And, the company hasn’t explained why a number of users who have deleted their accounts long before 2018 have seen their phone numbers turn up in this database.

> My #Facebook account is closed and removed since 2015 but my phone number is part a data breach fixed in 2019.
>
> This is fucking scary. #privacy #breach pic.twitter.com/zglSOYUm4v
>
> — Pierre Abi-aad (@abiaad) April 6, 2021

Facebook has been collecting users’ phone numbers for a decade, initially claiming that it was part of the platform’s security protocols. But in reality, Facebook was simply using that data to help it sell more ads and target more users — a breach of users’ trust that the Federal Trade Commission (FTC) decided was worth a $5 billion fine in 2019.

But for users whose phone numbers were being traded freely online, possibly the most aggravating part of Clark's post is when he puts the onus on users to protect the data that Facebook itself required users to hand over in the name of "security."

"While we addressed the issue identified in 2019, it's always good for everyone to make sure that their settings align with what they want to be sharing publicly," Clark wrote.

"In this case, updating the 'How People Find and Contact You' control could be helpful. We also recommend people do regular privacy checkups to make sure that their settings are in the right place, including who can see certain information on their profile and enabling two-factor authentication."

It's an audacious move for a company worth over $300 billion, with $61 billion cash on hand, to ask its users to secure their own information, especially considering how byzantine and complex the company's settings menus can be.

Thankfully for the half a billion Facebook users who've been impacted by the breach, there's a more practical way to get help. Troy Hunt, a cyber security consultant and founder of Have I Been Pwned has uploaded the entire leaked database to his website that allows anyone to check whether their phone number is listed in the leaked database.

While Facebook is attempting to downplay the seriousness of the leak, the decision about how serious this is does not lie with the company alone.

In Ireland, the Data Protection Commissioner (DPC)—which has the power to levy a fine of up to 4% of global turnover or around $3.5 billion—has slammed the company for failing to inform it of the breach.

"The DPC attempted over the weekend to establish the full facts and is continuing to do so. It received no proactive communication from Facebook. Through a number of channels, it sought contact and answers from Facebook," a spokesperson said in a statement issued on Tuesday.

The data breach is likely covered by Europe's strict new privacy rules, known as General Data Protection Regulation (GDPR), which came into effect in May 2018. The attackers had the ability to collect data from Facebook until at least June 5, 2019 according to experts analysing the leak.

A source at the DPC told VICE News that the agency is now engaging with Facebook but didn't offer any further details.

And it may also be in trouble in the U.S for failing to report the data breach at the time it happened, as Ashkan Soltani, the former chief technology officer for the FTC, points out. The last date analysts have confirmed hackers had access to the data—June 5, 2019—was just a week before Facebook's record-breaking $5 billion settlement with the agency.

> Not only is @Facebook past the indemnification period of the FTC settlement (June 12 2019), they also may have violated the terms of the settlement requiring them to report breaches of covered information (ht @JustinBrookman) https://t.co/182LEf4rNO pic.twitter.com/utCnQ4USHI
>
> — ashkan soltani (@ashk4n) April 7, 2021

But maybe everyone whose number is listed in the leaked database should follow Facebook founder and CEO Mark Zuckerberg's lead: Zuckerberg uses the highly secure messaging app Signal, which isn't owned by Facebook.

> In another turn of events, Mark Zuckerberg also respects his own privacy, by using a chat app that has end-to-end encryption and isn't owned by @facebook
>
> This is the number associated with his account from the recent facebook leak. https://t.co/AXbXrF4ZxE
>
> — Dave Walker (@Daviey) April 4, 2021

Get the latest from VICE News in your inbox. Sign up right here.