Facebook data leak: you should be on the lookout for scams

by Jurgita Lapienytė — 6 April 2021 in Editorial 0

Facebook data leak: you should be on the lookout for scams (c) Shutterstock

A database containing 533M Facebook users' data resurfaced on the internet, only this time for free. It means that more malicious actors can exploit data, and so you should be on the lookout for suspicious emails or messages.

If your phone number is associated with your account, name, location, marital status, phone number, or email address, then this personal information is most likely circulating for free, as well.

Facebook has been long criticized for letting third parties collect or scrape its user data, with

come as a surprise, especially for its fiercest critics who are pleading for more responsibility from a social media giant.

In Facebook's defense, we need to point out that the platform is attacked daily, and it only takes one vulnerability for a hacker to succeed. CyberNews talked to cybersecurity experts about the recent data leak. Some of them expressed harsh criticism towards the social media giant. Others weren't so fast to judge.

"Facebook gets targeted thousands of times a day from every angle. For a hacker, it only takes one vulnerability to be successful. So although they have staffed thousands of security personnel and invested billions in security, mistakes will happen. I think they are learning like any other organization but have ways to go given their size, business model, and constantly being targeted in new ways," Nick Santora, CEO at Curricula, told CyberNews.

To see if any of your online accounts were exposed in previous security breaches, use our personal data leak checker with a library of 15+ billion breached records.

Why is it free now?

The database that is offered for free now is not exactly new. It was already for sale last year. Recently, it was made available to practically any criminal who can think of ways to exploit personal data.

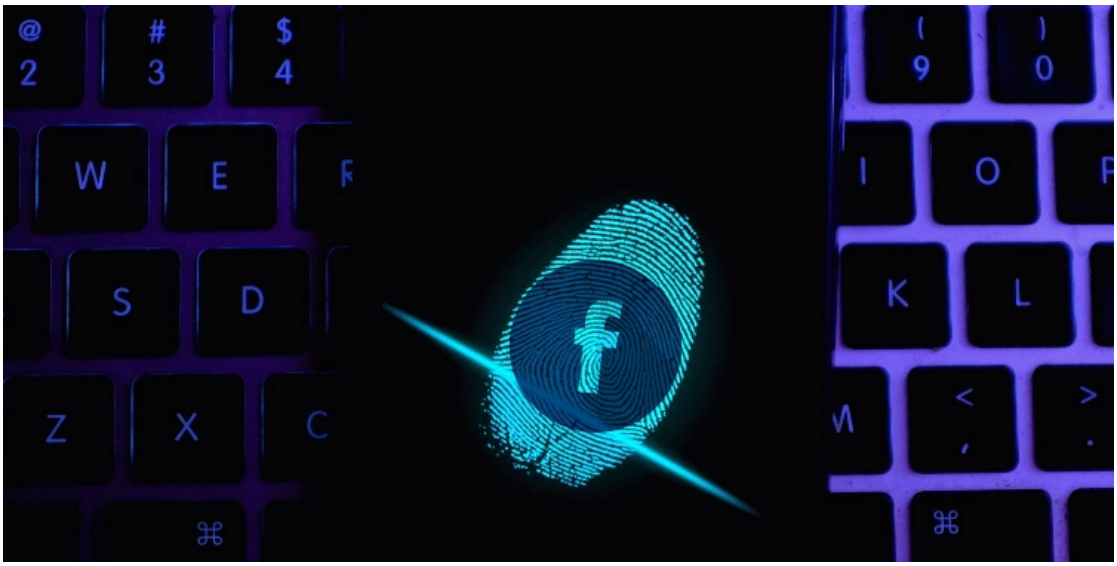
"The Facebook leak was supposedly due to an error that was exploited last June. Facebook likely fixed it fairly quickly, but the data had been extracted in the meantime. Getting all that data is not as simple as copying a file. Therefore, it is likely the reason the data does not include all 2Bn users is because Facebook closed the whole mid-stream. Another reason could be that segmentation in the database system limited the data set available to the leak. Regardless, the data leak was likely stopped fairly quickly," Stel Valavanis, the CEO of Chicago based onShore Security, told CyberNews.

What was not stopped is the dissemination of data from then on. The fact that months have passed and that the data is now made available for free means, according to Valavanis, that the criminals have made their money and don't see any way to extract more value from it.

"Putting it out for free also provides some cover should anyone try to trace the stolen data back to its source. Yet another explanation could be that a competing criminal element or other entity put

Facebook data is out there, and it is being exploited. Yet, it does not mean that Facebook has broken any laws.

“The Cambridge Analytica experience is somewhat different because it was not a leak. Facebook sold data but with a misunderstanding (or possibly deliberate misuse) of how data was accessed and used. But let’s not ignore the fact that there are criminals involved here who make no excuses. Yes, we can blame Facebook for being negligent and maybe cavalier, but this also shows the lack of policy, particularly on breach disclosure and law enforcement that normally forms the deterrent for other crimes which are, frankly, waning,” he said.



According to Mathieu Gorge, CEO, and founder of VigiTrust, the main challenge for Facebook is that they keep collecting more and more information on their users across multiple platforms (e.g. Instagram).

“It, therefore, becomes a policy issue, a technical security challenge, and mostly a major compliance headache for them. Every time they roll out new functionality or integrate a new platform, they essentially increase the risk surface and potential for security loopholes. While this explains what they are up against, it remains Facebook’s responsibility to ensure that they protect employee-, user-, the third party- and other data they are custodians of, according to applicable laws and standards,” he told CyberNews.

Facebook is acutely aware of privacy issues, as there are many lawsuits against the company around privacy.

“However, like other super enterprises, they sometimes play catch up with best practices and

“They don’t seem to care”

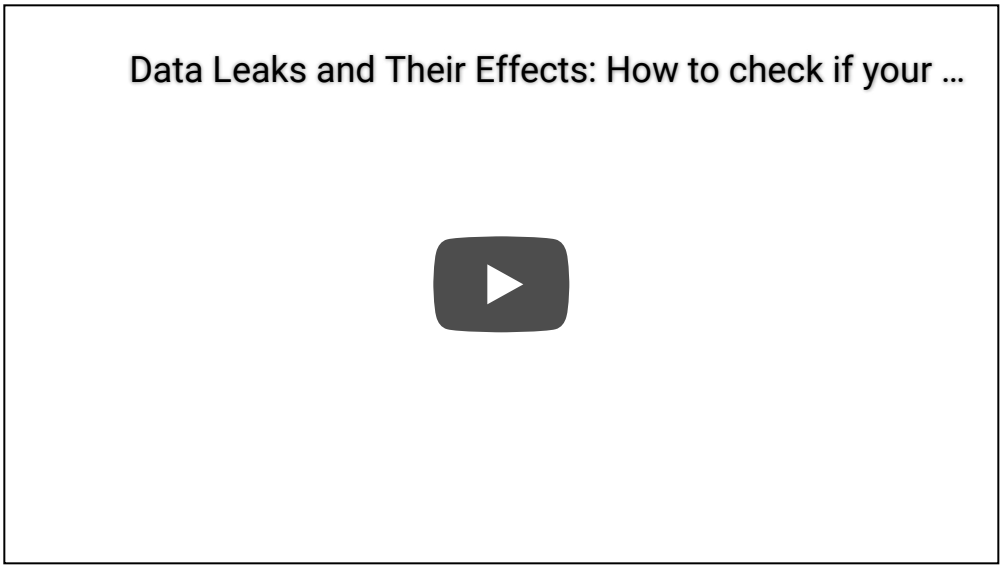
Many cybersecurity experts that CyberNews talked to expressed harsh criticism towards the social media giant. Mika Kujapelto, the CEO and founder of LaptopUnboxed, missed an immediate action from Facebook once the database resurfaced the internet.

“The lack of reaction indicates they do not seem to care about the data reveal that could put several of their users’ finances and identity at risk. It could stem from fear of significant backlash, but notifying users about potential risks would show they care about their users’ well-being,” Kujapelto said.

According to Vice, Facebook has been quick to downplay the leak; on Twitter, various Facebook executives have said that the data is from 2019 and is, therefore “old.”

George Kobakhidze, head of Enterprise Solutions at ZL Tech, believes that Facebook does not care about its users’ privacy.

“Facebook was never upset that Cambridge Analytica used Facebook data; they were embarrassed that they got caught. The truth of the matter is that companies like Facebook realized early on that user information will make them a fortune,” he told CyberNews.



A common enemy

According to Isaac Rudansky, CEO & Founder of AdVenture Media and industry expert on data sharing and user privacy, Facebook has no reasonable excuse for failing to protect its users' data. Yet, it offers a free utility and receives ad revenue in return.

For years, Facebook has been under attack from both the public and the government for not policing its content well enough, allowing hate speech and fake news to circulate, and leveraging user data to sell targeted ad inventory.

"On a more superficial level, Facebook has been forced to route an enormous amount of capital to fight these raging battles. That capital might have been allocated to strengthening their infrastructure, making it impenetrable to the low-grade hacker. But let's be honest, that's not really it, right? Facebook has a lot of money to spare. But on a deeper level, if you're repeatedly told that you're evil by the very customers you exist to serve, you'll eventually turn a blind eye to the very things, which would help exculpate you from such an ignominious moniker," he told CyberNews.

Mark Zuckerberg

Has Facebook learned anything from the public outrage caused by the Cambridge Analytica scandal? Has it done enough since then to protect privacy?

"No, I don't think Facebook learned anything from the Cambridge Analytica scandal because what happened was by design. And also no, Facebook isn't doing enough to protect user's privacy, as is evident by the most recent data breach, possibly the worst in Facebook's history," Rudansky said.

make it more expensive to steal the information than it is really worth.

“Facebook has made iterative improvements regarding its vendors, but they’re going about it in the opposite direction than what would be more secure. In cybersecurity, we practice and preach what is called the principle of least privilege. It means you don’t give access or information to anyone unless they absolutely need it. Unfortunately, for Facebook and other social network companies, that would be extremely disruptive to their business (locking out their partners), as well as impacting the functionality for the users. Can they secure the information sufficiently? Yes. Can they do it without losing billions in the process? Probably not,” he told CyberNews.

What could have Facebook done to protect people’s privacy more after the Cambridge Analytica scandal?

“I think Facebook can do a better job of educating the public on cybersecurity best practices for an end-user to operate in the public domain. The reason Facebook most likely will not do more is because it goes against their business plan. When revenue is tied to user’s posts, friends, likes, and personal interests, it is difficult to tell the end-user that they shouldn’t be sharing all of that because they are giving away a lot of private information about themselves,” Ryan O’Ramsay Barrett, CEO of ORAM Corporate Advisors, told CyberNews.

Keep data close to your chest

“Once data is out there, it’s out there. There is no turning back,” Nick Santora from Curricula told CyberNews.

Even though this database containing 533M Facebook users’ data has been circulating and resurfacing in hacker forums, this time, it is different. Previously, personal data has been for sale, and now it is being distributed practically for free.

> ***“The fact that this information is being distributed for free opens up its use by hackers that could not afford to pay for this information. The information is still valuable, as it includes phone numbers, Facebook IDs, email addresses, birthdates, and more. All of this can be used in social engineering attacks,” Chris Hauk, consumer privacy champion at Pixel Privacy, told CyberNews.***

Therefore, consumers need to make sure to keep their personal information close to their chest, change their passwords regularly, and stay alert for social engineering attacks via phone, email, and text messages.

Paul Bischoff, a privacy advocate from Comparitech, said that Facebook has left user data sitting on exposed servers, allowed app developers to abuse access to user accounts, and left bugs in code that hackers could exploit to steal data.

“On top of that, most Facebook profiles are public, which means third parties can scrape them using bots. One would hope that market sentiment would turn against Facebook, and users would leave of their own accord if they are truly concerned about data privacy and security. But we have not seen that happen on a large scale yet,” he said.

Facebook users should be on the lookout for scams and phishing messages sent by SMS or email.

> ***“Never click on links or attachments in unsolicited messages. Always verify the sender. Consider changing your phone number or use a call screening app,” Bischoff added.***

Aaron Barr, CTO at PiiQ Media, told CyberNews that every individual should be armed with a set of questions that become second nature when receiving and determining whether to open an email. Email addresses should be protected almost like passwords – you shouldn’t reuse them for everything. Of course, being skeptical about emails is crucial.

“Use proper digital hygiene. Once a month, review the information that’s available about you publicly. Do searches for your name, your email addresses, or use a service to do this for you to help understand what is publicly accessible,” he recommended.

More from CyberNews:

Protect your sensitive information and passwords with best password managers

11 million records of French users stolen from marketing platform and put for sale online

Guide to best VPN services in 2021, such as Surfshark, ProtonVPN & NordVPN