

Over half a billion Facebook users' personal information leaked

✎ by Danika Blessman ⌚ 12 April 2021

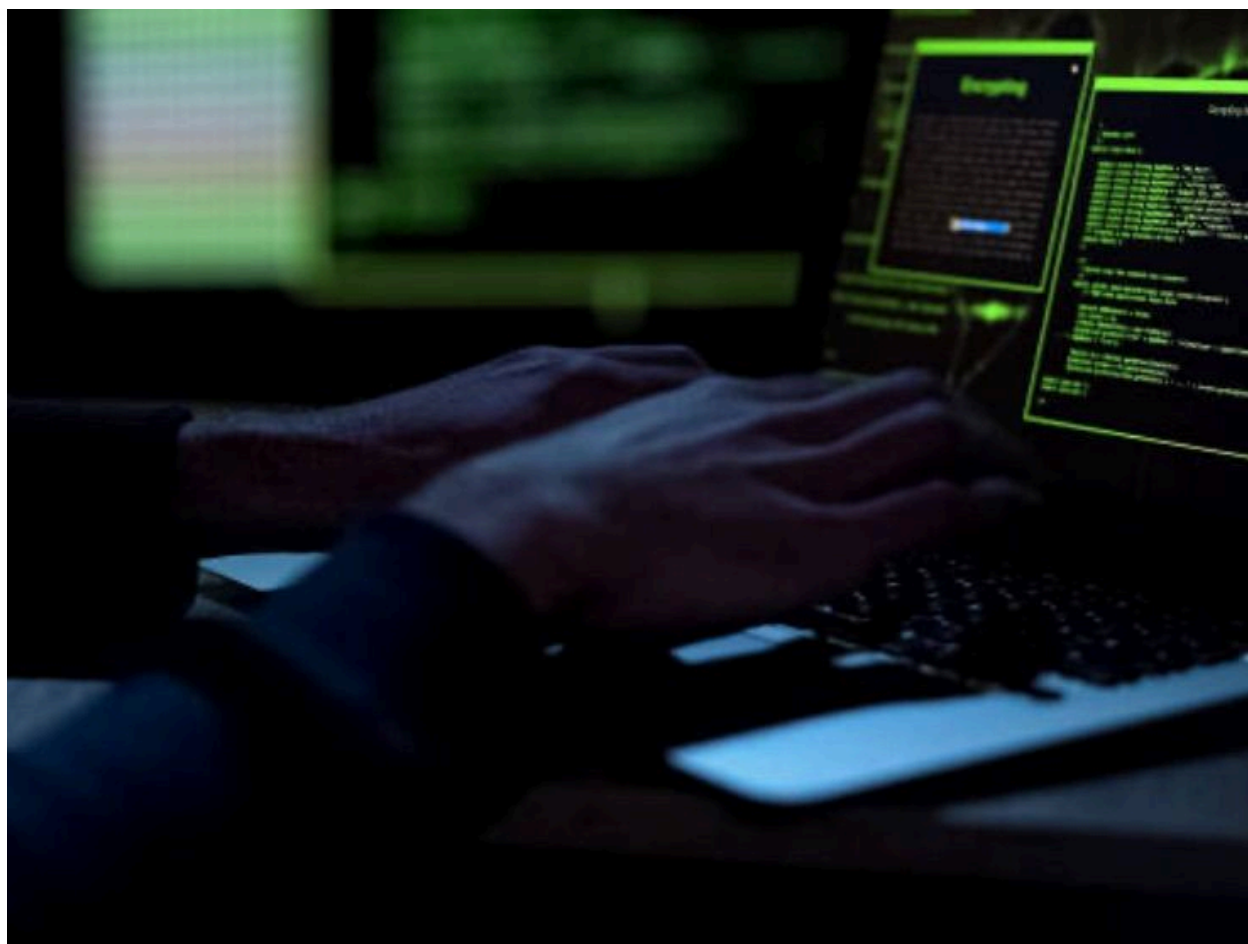


Over the Easter holiday weekend, a researcher at an Israeli cybersecurity firm discovered that the personally identifiable information (PII) – including phone numbers, birthdates, email addresses and locations – of over half a billion Facebook users had been leaked online. This leak appears to have affected users across over 100 countries; with the highest numbers of impacted users from the US (32 million), the UK (11 million), and India (6 million). Initial reporting from Business Insider revealed that over 533 million Facebook users' personal information was uploaded over the weekend to a hacking forum. Earlier this year, reports suggested that the same information was up for sale on a hacking forum.

Topics in this article

Cybersecurity

Privacy stated that the data leak was a result of “scraping” rather than a breach of the platform’s terms of service.



The leak of personally identifiable information from Facebook is likely to lead to an escalation in phishing attacks

Facebook data, leaked several years ago, is now freely available on the open web. An organization's primary asset is data, and that data is valuable to more than just your organization – or the initial threat actor (stolen data is often passed from one criminal group to another). If threat actors target a specific organization – perhaps, via a supply chain or third-party attack – simply knowing email addresses or phone numbers can easily support social engineering attacks. As Facebook is not only for individual social media use but also supports many enterprise's online digital presences, the impact can be much broader than just individual account details.

Facebook reported that the data was collected by attackers leveraging a vulnerability disclosed as early as 2016, which Facebook says was remediated in 2019. While the leaked data appears to be several years old, its age does not preclude it from being leveraged by threat actors. Many users likely haven't changed their contact information since, remaining vulnerable to potential phishing campaigns.

From a security standpoint, individuals and organizations alike need to be aware that their data is already out in the open and need to remain vigilant about the

potential for phishing or fraud. Additionally, the leak of this type of PII could lead to an uptick in robocalls or spam text messages, both of which are already significant issues, leading to the potential for affected users or organizations to reveal further information. The PII exposed in this leak isn't as valuable as credit card information or social security numbers, but is still helpful in fueling attack campaigns.

Some helpful tips for businesses:

- Ensure that data hygiene is a core part of your organization's overall security plan.
- Identity and access management solutions are crucial to successfully mitigating these types of risks.
- Digital risk monitoring programs should focus on detecting credential and data leaks and employee exposure.
- Change your password on corporate Facebook or other websites where you may have reused your password or login credentials.
- Implement multi-factor authentication to help protect assets.

References:

533 million Facebook users' phone numbers and personal data have been leaked online

Danika
Blessman

Danika Blessman

Senior Threat Intelligence Analyst, Threat Intelligence Communications Team, NTT Ltd.

INDUSTRIES

SERVICES

INSIGHTS

SOLUTIONS

ABOUT NTT DATA

CAREERS

LEGAL

 Facebook Social

 twitter social

 YouTube Social

Contact us

Terms of use

Do not sell my personal information

Sitemap

Report ethical concerns

Privacy

Cookie preferences

Unsubscribe

Careers

Copyright © 2024 NTT DATA, Inc.

