

Facebook admits storing passwords in plain text (Update)

March 21 2019, by Glenn Chapman



Facebook says its employees had access to millions of user passwords

Facebook on Thursday admitted that millions of passwords were stored in plain text on its internal servers, a security slip that left them readable by the social networking platform's employees.

"To be clear, these passwords were never visible to anyone outside of Facebook and we have found no evidence to date that anyone internally abused or improperly accessed them," Pedro Canahuati, the company's vice president of engineering, security, and privacy, said in a blog post.

The blunder was uncovered during a routine security review early this year, according to Canahuati, and comes after a series of controversies centered on whether Facebook properly safeguards the privacy and data of its users.

Canahuati said that the Silicon Valley company expected to notify hundreds of millions of Facebook Lite users, tens of millions of other Facebook users, and tens of thousands of Instagram users whose passwords may have been vulnerable to prying eyes.

The California firm reaches an estimated 2.7 billion people with its core social network, Instagram and messaging applications.

Worldwide probes

Brian Krebs, of security news website KrebsOnSecurity.com, cited an unnamed Facebook source as saying the internal investigation had so far indicated that as many as 600 million users of the social network had account passwords stored in plain text files searchable by more than 20,000 employees.

The exact number had yet to be determined, but archives with unencrypted user passwords were found dating back to the year 2012, according to Krebs.

Facebook's admission of the faux pas came after the report by Krebs.

"We have fixed these issues and as a precaution we will be notifying

everyone whose passwords we have found were stored in this way," Canahuati said.

Facebook's practice is to mask people's passwords by replacing them with random characters and then tucking away software keys needed to make sense of the jumble, according to Canahuati.

The technique allows Facebook's system to recognize valid passwords when users log in, without storing the information in plain text that employees or hackers could read.

Facebook said that social network users could harden security by updating to complex passwords and opting to require a second piece of data such as a texted code to access accounts.

Dinged data defense

Regulators, investigators and elected officials around the world have already been digging into the data sharing practices of Facebook which has more than two billion users.

The social network's handling of user data has been a flashpoint for controversy since it admitted last year that Cambridge Analytica, a political consultancy, used an app that may have hijacked the private details of 87 million users.

Facebook has announced a series of moves to tighten handling of data, including eliminating most of its data-sharing partnerships with outside companies.

Last week the social network announced that its chief product officer Chris Cox was leaving, becoming the highest-ranking executive to depart amid the turmoil at the leading social network.

Cox made his announcement on his Facebook page, saying he was leaving "with great sadness" after 13 years.

While Cox gave no specific reason for his move, he noted that Facebook chief Mark Zuckerberg has unveiled a new direction away from being the "digital town square" to focus on smaller-scale, private interactions.

"As Mark has outlined, we are turning a new page in our product direction, focused on an encrypted, interoperable, messaging network," Cox wrote.

"This will be a big project and we will need leaders who are excited to see the new direction through."

© 2019 AFP

Citation: Facebook admits storing passwords in plain text (Update) (2019, March 21) retrieved 20 September 2024 from <https://phys.org/news/2019-03-facebook-passwords-plain-text.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.