

5-Business Insider-Cyber Thieves

Cyber Thieves Took Data On 145 Million eBay Customers By Hacking 3 Corporate Employees

Jim Finkle and Deepa Seetharaman

2014-05-27T10:02:00Z

How ebay sees the future of commerce

Glassdoor/eBay

BOSTON/SAN FRANCISCO (Reuters) - eBay Inc initially believed that its customers' data was safe as forensic investigators reviewed a network security breach discovered in early May and made public this week, a senior executive told Reuters on Friday. *[Deny]*

eBay has come under fire over its handling of the cyberattack *[Disappointment]*, in which hackers accessed personal data of all 145 million users, ranking it among the biggest such attacks launched on a corporation to date.

"For a very long period of time we did not believe that there was any eBay customer data compromised," global marketplaces chief Devin Wenig *[Deny]* said, in the first comments by a top eBay executive since the e-commerce company disclosed the breach on Wednesday.

eBay moved "swiftly to disclose" the breach after it realized customer data was involved, he said. *[Rebuild]*

Wenig would not say when the company first realized that the cyberattackers accessed customer data, nor how long it took to prepare Wednesday's announcement. *[Deny]*

He said hackers got in using the credentials of three corporate employees, eventually making their way to the user database.

Hackers accessed email addresses and encrypted passwords belonging to all eBay users. “Millions” of users have since reset their passwords and the company had begun notifying users [Rebuild], though it would take some time to complete that task, Wenig said.

“You would imagine that anyone who has ever touched eBay is a large number,” he said. “So we’re going to send all of them an email [Rebuild], but sending that number all at once is not operationally possible.”

At least three U.S. states are investigating the company’s security practices [Legal Action]. Customers have complained on social media about delayed notification emails [Disappointment]. And New York’s attorney general called on eBay to provide free credit monitoring services to users.

But the Internet retail giant has no plans to compensate customers or offer free credit monitoring [Disappointment] for now because it had detected no financial fraud, Wenig said.

Wenig declined comment when asked if he thought eBay had good security prior to the breach [Deny]. He said the company would now bolster its security systems, and has mobilized senior executives in a subsequent investigation of the attack. [Rebuild]

“We want to make sure it doesn’t happen again so we’re going to continue to look our procedures, harden our operational environment and add levels of security where it’s appropriate.” [Rebuild]

The breach marked the latest headache for eBay this year. In January, it crossed swords publicly with activist investor Carl Icahn , who mounted a campaign to get it to spin out PayPal. Then in April, the e-commerce company disappointed investors with a weak second-quarter outlook, pressuring its shares.

AVOIDING BACK DOORS

Buying and selling activity on eBay remained “fairly normal” [Hope] though eBay is still working out the cost of the breach, which included hiring a number of security firms [Rebuild]. Wenig, who was previously a senior executive at Thomson Reuters Corp, declined to comment on whether the cost could be material to eBay’s results [Deny].

Wenig’s revelation that the company initially believed that no customer data had been compromised might take some of the heat off eBay’s executive team. [Positive]

Cyber forensics experts said it’s not uncommon for large companies to take weeks to grasp the full impact of an attack, because hackers are often able to steal data without leaving obvious clues.

“In some cases you go in and find the smoking gun immediately. Other times, it takes a few days or even a few weeks,” said Kevin Johnson , a cyber-forensics expert who was not involved in the eBay investigation but has worked for other Fortune 500 companies.

Daniel Clemens , a forensics expert and CEO of Packet Ninjas , said investigators often ask companies to hold off on disclosure until they believe they understand the full extent of an attack. Otherwise, they risk tipping off attackers who might cover their tracks or leave “back doors” so they can return after the investigators complete their probe.

On Wednesday, the e-commerce company announced that hackers raided its network between late February and early March. The company said financial information was not compromised and its payments unit PayPal was not affected.

When eBay first discovered the network breach in early May, the senior team was immediately involved and held multiple daily calls on the issue [Reinforce]. EBay staff have been working around the clock since Wednesday [Reinforce].

Wenig said he could not provide much more detail about what happened in the attack beyond the scant information given out so far. He declined to provide further specifics, citing ongoing investigations by the Federal

Bureau of Investigation and several forensics firms including FireEye Inc's Mandiant division *[Deny]*.

(Editing by Edwin Chan, Lisa Shumaker and Andrew Hay)

Sign up for notifications from Insider! Stay up to date with what you want to know.

Subscribe to push notifications

An icon in the shape of a lightning bolt.

Keep reading

Get a daily selection of our top stories based on your reading preferences.

Loading

Something is loading.

Email address

By clicking 'Sign up', you agree to receive marketing emails from Insider as well as other partner offers and accept our Terms of Service and Privacy Policy .

More: Reuters

Close icon

Two crossed lines that form an 'X'. It indicates a way to close an interaction, or dismiss a notification.

Recommended Video

Follow us on:

* Copyright © 2022 Insider Inc. All rights reserved.

Registration on or use of this site constitutes acceptance of our