

7-Reuters-EBay asks 145 million

By Jim Finkle , Soham Chatterjee , Lehar Maan

6 Min Read

BOSTON/BANGALORE (Reuters) - EBay Inc said on Wednesday that a cyber attack carried out three months ago has compromised customer data, and the company urged 145 million users of its online commerce platform to change their passwords.

John Donahoe, chief executive of eBay, speaks at the Reuters Global Technology Summit in San Francisco, June 17, 2013. REUTERS/Stephen Lam

The company said unknown hackers stole email addresses, encrypted passwords, birth dates, mailing addresses and other information in an attack carried out between late February and early March. The files did not contain financial information.

An eBay spokeswoman said a large number of accounts may have been compromised, but declined to say how many *[Deny]*. EBay said it found no evidence of unauthorized access to financial or credit card information at its PayPal payments subsidiary, which encrypts and stores its data separately.

EBay shares were down 0.2 percent late Wednesday afternoon *[Disappointment]*, compared with a 0.9 percent rise in the Nasdaq Composite Index.

The e-commerce company's stock has steadily fallen since late March *[Disappointment]* as part of a broader slide in technology shares. Last month, eBay reached an accord with activist investor Carl Icahn, who had been calling for the company to spin out PayPal, which is growing quickly.

FRAUD ALERT

Security experts advised EBay customers to be on the alert for fraud, especially if they used the same passwords for other accounts.

“This is not a breach that only hurts EBay. This is a breach that hurts all websites,” *[Disappointment]* said Michael Coates, director of product security with Shape Security.

He said that companies typically only ask users to change passwords if they believes there is a reasonable chance attackers may unscramble encrypted passwords *[Worry]*.

Once the passwords are unscrambled, attackers could use automated software that seeks to log into thousands of popular services, including Facebook, Twitter, popular email services and online banking sites, he said.

EBay spokeswoman Amanda Miller said the company was making the request “out of an abundance of caution” *[Diminish, Rebuild]* and that it used “sophisticated,” proprietary hashing and salting technology to protect the passwords. *[Reinforce]*

Related Coverage

EBay says client information stolen in hacking attack

Amit Yoran, senior vice president of EMC Corp’s RSA security division, said that cyber criminals sometimes take data from multiple breaches, combining them into detailed portfolios that fraudsters can use for scams.

“We are seeing a level of sophistication in the cybercrime world where they are able to pull data from multiple exploits to create stronger profiles of individuals,” Yoran said. “The more detailed information fraudsters have, the better their ability to successfully perpetrate fraud.” *[Worry]*

NO SIGNS OF FRAUD

EBay said its investigation of the breach is ongoing, with assistance from law enforcement.

“For the time being, we cannot comment on the specific number of accounts impacted,” *[Deny]* eBay spokeswoman Kari Ramirez said. “However, we believe there may be a large number of accounts involved.”

The company said it had not seen any indication of increased fraudulent activity on eBay and that there was no evidence its PayPal online payment service had been breached.

eBay provided little information about how the hackers got in. It said they obtained login credentials for “a small number” of employees, allowing them to access eBay’s corporate network.

It said it discovered the breach in early May and immediately brought in security experts and law enforcement to investigate.

“We worked aggressively and as quickly as possible to insure accurate and thorough disclosure of the nature and extent of the compromise *[Reinforce]*,” Miller said when asked why the company had not immediately notified users.

When asked who was behind the attack, she said: “We will not speculate on who is responsible at this time.”

ASSESSING RESPONSIBILITY

Research analysts said there was not enough information available to assess whether eBay had been negligent *[Neutral]*.

“The real key question going forward will be if any money has been stolen, or any unauthorized activity been performed, *[Worry]*” Wedbush Securities analyst Gil Luria said. “As long as this is not the case, this thing will come and go and will not be an issue for eBay.” *[Hope]*

Security experts say that virtually every major corporation, government agency and other organization has been hacked at one time.

[Neutral]

They say it is almost impossible to prevent hackers from getting into networks using social engineering techniques such as sending carefully crafted phishing emails that lure targets to tainted websites or entice them to click on malicious links. In some cases they infect websites frequented by their targets, such as the sandwich shop of a local restaurant or professional organizations.

EBay's shares fell as low as \$50.30 in early trading on the Nasdaq before recovering to \$51.83 in late afternoon *[Hope]*.

EBay has been attacked before. In February, the Syrian Electronic Army hacking group breached and defaced websites belonging to PayPal UK and eBay.

One of the biggest breaches at a U.S. company was at retailer Target Corp, where hackers last year stole some 40 million credit card numbers and another 70 million customer records.

Last month, U.S. web media company AOL Inc urged its tens of millions of email account holders to change their passwords and security questions, saying a cyber attack compromised about 2 percent of its accounts.

Additional reporting by Deepa Seetharaman in San Francisco and Saqib Iqbal Ahmed in Bangalore; Editing by Rodney Joyce, Savio D'Souza, Robin Paxton and Dan Grebler