1-BankInfoSecurity-eBay

Credit Eligible

Get Permission

eBay is urging its 145 million customers to change their passwords following a cyber-attack that compromised encrypted passwords and other personal information. *[Rebuild]*

See Also: Live Webinar | Making the Case for Managed Endpoint Detection and Response

The attack, which occurred between late February and early March, originated after a small number of employee log-in credentials were compromised, which enabled cyber-attackers to gain access to eBay's corporate network, eBay says in an FAQ . "We are working with law enforcement and leading security experts to aggressively investigate the matter," the company says. *[Rebuild]*

The company says it's notifying all of its active users about the breach, and the need to change their passwords, by e-mail, site communications and other marketing channels. *[Rebuild]*

Compromised information includes encrypted passwords, customer names, e-mail addresses, mailing addresses, phone numbers and dates of birth, eBay says. The database that was exposed in the breach did not contain financial information, according to the company. *[Diminish]*

eBay detected the compromised employee log-in credentials approximately two weeks ago. So far, the company says there's no evidence of unauthorized activity for eBay users. The company also says it has no evidence of unauthorized access or compromises to personal or financial information for PayPal users. PayPal data is stored separately on a secure network, and all PayPal financial information is encrypted, eBay says.

“eBay regrets any inconvenience or concern that this password reset may cause our customers,” the company says. “We know our customers trust us with their information, and we take seriously our commitment to maintaining a safe, secure and trusted global marketplace.” *[Rebuild]*

Analyzing the Breach

Tyler Shields, a security analyst at Forrester Research, says the amount of time attackers had in the eBay network is concerning, because the company discovered the breach two weeks ago, yet the attackers apparently first accessed the system in late February or early March. *[Worry]*

“That’s a long time for an attacker to be in your network,” he says. “I’d be very concerned about the continued [presence] of the attacker and what else they may have taken.” *[Worry]*

Even though financial information wasn’t exposed, Shields says there was enough sensitive information potentially accessed to enable criminals to commit fraud. “Lots of attack scenarios can be devised when you know the e-mail address, home phone number and home address for 145 million people,” he says. *[Worry]*

Al Pascual , senior fraud and security analyst at Javelin Strategy and Research, says the compromise likely originated from a spear phishing campaign that resulted in the compromised employee credentials. “I guess that’s a major lesson here - the system is only as secure as its weakest link, and that is very often its people,” he says. *[Disappointment]*

Andreas Baumhof , CTO at security firm ThreatMetrix, says that although the exposed passwords were encrypted, criminals are improving their ability to crack hashed passwords. He says account takeover will be the biggest issue going forward. “We’ll see phishing sites pop up asking you to change your eBay password,” he predicts.

The attack also highlights that all companies, no matter how strong their security is, are susceptible to attack. “Even the best-run security companies have been hacked,” Baumhof says. “It’s not the question of whether you get hacked, but when.” *[Positive]*

Shields says that, with enough time, a dedicated attacker can compromise the best security. “There is an asymmetry of warfare going on where an attacker need only find one hole and defenders have to secure every point of entry,” he says.

Regarding the company advising its customers to change their passwords, Pascual says that the messaging doesn’t do enough to quench concerns. “I’d rather hear about the type of encryption used on the password list so we can determine the likelihood that it will be decrypted and misused by criminals,” he says *[Disappointment]*. “The more that a consumer uses a password across multiple accounts, the higher their rate of fraud - and we all reuse passwords far more often than we should. The breach of user credentials anywhere can result in fraud everywhere.” *[Worry]*