the Availability Digest

www.availabilitydigest.com
@availabilitydig

eBay's Slow Response to Data Hack

July 2014

eBay.com is an online auction and shopping website through which a wide variety of goods and services are sold by its 145 million users. It handles the financial transactions associated with each sale through its subsidiary, PayPal. In 2013, eBay handled $215 billion in sales with PayPal.

The eBay Attack

In early May, 2014, eBay discovered that its user database had been hacked sometime between late February and early March. In the two intervening months, the hackers had potentially stolen the personal information of eBay's 145 million users. This information included customer names, encrypted passwords, email addresses, physical addresses, telephone numbers, and dates of birth.

eBay claimed that no confidential financial data was compromised. All user financial data is kept in the PayPal databases, which are on a separate secured network. All financial data is encrypted as a further protection against hacking.

The breach was made possible by the hackers obtaining the log-in credentials of a small number of eBay employees. Log-in credentials were presumably obtained by a spear-phishing campaign in which employees were asked to provide this information via official-looking emails. Once the hackers had a small number of log-in names and passwords, they could get into the eBay systems and access the eBay databases.

This data breach exceeded the Target breach of magnetic-stripe data from 110 million customer payment cards during the 2013 holiday season; and it was second only to the October, 2013, Adobe hack of 152 million user accounts. This breach is a further example of the vulnerability of even the biggest and most prepared companies. In April, AOL reported that its email services had been breached; and the attackers were using AOL customer accounts to send out spam.

eBay's Laid-Back Response to the Attack

eBay's response to the data breach was, in a word, disappointing. It took no overt action to notify its users of the breach for two weeks. During this time, there was no notice on its home page, no cautionary emails were sent to its users, and no notice was given to users as they logged on to their accounts. eBay's first notice was posted on its little-seen corporate website, ebayinc.com.

eBay did post a message on its PayPal site in which the title of the message indicated that users should change their passwords. However, the text of the message simply read "place holder text."

Finally, two weeks after discovering the breach, eBay sent emails to its users informing them of the breach. It listed the information that was potentially compromised, including the encrypted passwords.

There was no detail on the level of encryption so that it was not possible to determine the probability that the encrypted passwords could be decrypted. eBay urged users to change their passwords.

However, many users who went to their accounts to change their passwords were met with a “page not found” message. eBay said that this was due to excessive volume of requests for that service and that they were working on an upgraded password reset process.

eBay is working with law enforcement and security experts on the breach. It has hired FireEye’s Mandiant forensics division to help investigate the hack. Mandiant is the firm that published a February, 2013, report that described a Shanghai-based hacking group linked to the People’s Liberation Army

The Effects of the Breach

eBay has stressed that no confidential financial information was stolen. It continues to verify that it has seen no fraudulent activity of its PayPal accounts, nor has it seen any indication of rising fraud in its auction marketplace. Money movements would require control of an eBay or PayPal account

However, with the potential loss of email addresses, eBay has advised its users to expect an increase in phishing emails. Users should not click on any email links unless they are certain that the email is from a trusted source.

In addition, while hackers may not be taking money or goods out of eBay, they may be using personal information to target other sites.

Criminals are improving their ability to decrypt encrypted passwords. If users are using the same password on other sites, especially for banking applications, it is important that they change all of these passwords.

Summary

It is bad enough to lose information of 145 million users. It is a far greater disaster to not inform them of the loss immediately so that they can take action. eBay failed in its obligation to its users to do so with the two-week delay from the discovery of the breach to the notification of the breach.

Acknowledgements

Information for this article was taken from the following resources:

EBay Discloses Cyberattack, Working with Law Enforcement, *The Street*; May 21, 2014.
eBay buries its own advisory to change passwords following database hack, *Ars Technica*; May 21, 2014.
eBay Breach: 145 Million Users Notified, *Bank Info Security*; May 21, 2014.
Hackers raid eBay in historic breach, access 145 million records, *Reuters*; May 22, 2014.
Hackers Hit eBay; Millions Warned, *USA Today*; May 22, 2014.
EBay Demonstrates How Not to Respond to a Huge Data Breach, *Wired*; May 23, 2014.
eBay admits it kept massive cyber attack secret because it thought customer data was safe – but will STILL not say how long it knew data of 145m users was compromised, *Daily Mail*; May 23, 2014.