Yahoo Hack Sets a Record – 500 Million Accounts

September 2016

On September 22, 2016, Yahoo announced it had discovered that the details of 500 million of its user accounts were stolen. This is by far the largest corporate breach ever reported. It is ahead of the 2013 MySpace hack of 300 million user accounts.

Yahoo

Yahoo has one billion users around the globe using the variety of services that it offers:

- About 250 million use Yahoo email.
- Flickr has 113 million users.
- Tumblr has several hundred million users (Flickr and Tumblr are Yahoo-owned businesses).
- 81 million people use Yahoo finance services.
- Tens of millions of people use Yahoo Fantasy Sports.

The Hack

Though the breach occurred in late 2014, Yahoo did not discover it until recently and did not report it until September 22, 2016. It is not clear when Yahoo discovered the attack. Their announcement simply said that "a recent investigation … has confirmed the attack."

The stolen data showed up for sale on the dark web this past August. On August 1, a hacker named "Peace" claimed to have breached 200 million Yahoo usernames and passwords back in 2012 and offered to sell them on the dark web. In a June interview with *Wired*, Peace identified himself or herself as a former member of a team of Russian hackers who had breached and sold credentials from several major online services in 2012 and 2013.

It was Peace's allegations that prompted Yahoo to initiate an internal investigation. While Yahoo found no evidence to substantiate Peace's claim, this is when it found indications that the larger breach had occurred. User credentials were out in the open on the dark web for nearly two months before Yahoo confirmed the breach.

The hack affected predominantly users in the United States. However, users in Japan, the Philippines, Taiwan, and Hong Kong were also possibly compromised.

Yahoo claims that evidence points to a state-sponsored hacker. Though it did not name a suspect, likely culprits are China, Russia, and North Korea. (There is a common saying in the security industry: "There are only two kinds of companies – those who know they have been hacked by China, and those who don't know they have been hacked by China.")

Federal and state investigators will likely launch investigations and may possibly demand fines or penalties from the company.

What Was Stolen

The hackers obtained consumer names, email addresses, phone numbers, and birthdates. They also obtained passwords, but Yahoo claims that the passwords were protected by a complex hashing algorithm, brcrypt. Hackers also obtained security questions in the clear (What was your mother's maiden name?). The stolen data did not include payment card data or bank account information.

It would take tremendous computing resources to determine the actual passwords from the hashed versions. However, out of 500 million stolen passwords, it is likely that some of them will be deciphered, especially if they are of the form "password" or "12345." If the hackers were successful in decoding only 1% of the passwords, they would still have access to five million passwords.

Cybercriminals know that consumers use the same passwords across websites and applications. This is why millions of leaked password credentials coupled with their user names are so useful for perpetrating fraud.

Facebook co-founder Mark Zuckerberg's Twitter account was hacked using a similar method after the passwords of more than 100 million LinkedIn members were leaked

How to Protect Yourself

Yahoo will be contacting affected uses and asking them to supply "alternate means of account verification." Affected users can set up a "Yahoo Account Key" that sends a code by text anytime a user tries to log on to an email account. The code is received on the user's mobile phone and must be entered during the logon process in order to access the account.

Yahoo users should change their Yahoo passwords and security questions. Users should also be on guard for spam emails that might include malware, scams, or phishing attempts.

The Verizon Merger

Yahoo is in the process of being acquired by Verizon for $4.8 billion USD. Verizon was just recently notified of the breach.

Studies have shown that 97% of Americans lose trust in companies like Yahoo following a massive data breach. It is not yet clear whether this breach will affect the pending Verizon acquisition.

Summary

The Yahoo hack shows the importance of maintaining appropriate security precautions surrounding corporate data. Not only should facilities be in place to prevent intrusion from malicious outsiders, but monitoring systems should be employed to immediately detect any suspected intrusion.

Acknowledgements

Information for this article was taken from the following sources:

Yahoo Has Been Hacked: What You Need to Know; *Fortune*; undated.
Yahoo hit in worst hack ever, 500 million accounts swiped, *CNet*; September 22, 2016.
More Than Half a Billion Yahoo Accounts Have Been Hacked, Yahoo Confirms, *Slate*; September 22, 2016.
Yahoo Hack: Who Got Hit, Where, and How to Protect Yourself, *VOA News*; September 23, 2016.
Yahoo faces questions after hack of half a billion accounts, *The Guardian*; September 23, 2106.
Yahoo hack: what to do to protect your account, *The Guardian*; September 23, 2106.