the Availability Digest

www.availabilitydigest.com
@availabilitydig

Yahoo!'s Users Are Victims of Massive Hacks

May 2017

Yahoo! is an American technology company headquartered in Sunnyvale, California. Yahoo was one of the pioneers of the early Internet era; and it is globally known for its Web portal, its search engine Yahoo! Search, its email offering Yahoo! Mail, its financial aids Yahoo! Finance, and many other web-based services.

Yahoo is the highest-read news and media website, with over seven billion views per month. It is the sixth most visited website globally. Roughly 700 million people visit Yahoo websites every month. About 250 million people use Yahoo email. About 81 million use Yahoo Finance.

As a consequence, Yahoo has over a billion user accounts. This has made it a prime target for hackers, as evidenced by massive hacks of user data over the past several years. In 2013, user data from over one billion active and inactive accounts were stolen by hackers. In 2014, 500 million user accounts were hacked. Further hacking occurred in 2016.

Data Breach of 2013

In December 2016, Yahoo disclosed that user data from one billion accounts had been stolen by hackers in 2013. The breach dates back to August 2013. The stolen data may have included sensitive user information such as names, email addresses, telephone numbers, dates of birth, encrypted passwords, and unencrypted answers to security questions that could be used to reset passwords. Yahoo claimed that no financial data was stolen. It is kept in a separate database by Yahoo. Yahoo notified all users who had been affected and asked them to change their passwords. It also invalidated all unencrypted answers to security questions.

This disclosure came three months after Yahoo admitted that data from at least 500 million accounts had been stolen in 2014 (described later).

The 2013 hack was discovered by Yahoo after analyzing data files provided by law enforcement in 2016. Whoever plundered this information had three years to exploit it. Yahoo believes that the breach was state-sponsored.

Yahoo determined that the attackers used cookie forging. Cookies saved in a browser are a widely used Internet approach to storing browser session variables and preferences. They are bits of code that stay in the user's browser cache so that a website does not require a logon with every visit. According to Yahoo, the attackers were able to steal some of the proprietary code of Yahoo to learn how to forge Yahoo cookies. The forged cookies enabled the attackers to access user accounts without a password.

Yahoo has since invalidated the forged cookies. However, a Yahoo employee said that after the breach was disclosed, security was pushed to the backend behind other priorities because of concerns about cost and customer inconvenience.

Nabbing the unencrypted answers to security questions created a particularly sensitive problem. Cybercriminals can use that information to conduct automated attacks called 'credential stuffing.' Taking the security question answers from millions of users, the cybercriminals build a program to attempt to logon to other online accounts like banking, retail, and airline rewards programs.

Data Breach of 2014

On September 22, 2016, Yahoo announced that user data from 500 million accounts had been stolen by hackers in 2014. This hack is in addition to the 2013 hack of one billion accounts described above. Yahoo attributed this breach to a state-sponsored hacker.

As with the 2013 breach of one billion accounts, Yahoo believes that the hackers found ways to forge credentials to log into some users' accounts without passwords. Yahoo's Chief Information Security Officer (CISO) suggested that an attacker had stolen Yahoo's proprietary source code to determine how to forge cookies and store them on user machines. The attackers were then able to log on to some user accounts without a password, impersonate valid users, and perform actions on behalf of their victims.

The United States Federal Bureau of Investigation (FBI) is investigating this breach.

Claims surfaced in early August 2016 that a hacker using the name 'Peace' was trying to sell personal information of Yahoo account users on the dark web – a black market of thousands of secret websites. It was reported that Peace was asking $300,000 for 200 million accounts. Peace stated that he had the data for some time and had been privately selling it since 2015. Peace is probably a broker through which hackers sell their account information.

Data Breach of 2016

Again in December 2016, Yahoo disclosed another massive security breach. As in prior hacks, hackers were able to access user accounts without passwords. This newly issued warning was the third one in just a matter of months.

Summary

The 2013 and 2014 attacks are the largest publicly disclosed security breaches ever discovered on the Internet. They are the largest known security breaches of any one company's computer network.

Yahoo has been criticized for its late disclosure of the breaches and its security measures. It is currently facing several lawsuits as well as investigation by members of the United States Congress.

So far as advice to users to protect their accounts, several suggestions have been made by security experts:

- Log off after each session. This invalidates the session cookie so that it cannot be used fraudulently.
- Change passwords and security answers on any other accounts that use the same information as the user's Yahoo account.
- Be extra cautious about clicking on links or opening downloads from unknown email addresses.
- Never share any account information or passwords over email.

Acknowledgments

Information for this article was taken from the following sources:

Hack Brief: Hackers Breach a Billion Yahoo Accounts. A Billion, *Wired*; December 16, 2014.
500 million Yahoo accounts breached, *USA Today*; September 22, 2016.
Yahoo Says 1 Billion User Accounts Were Hacked, *New York Times*; December 14, 2016.
Yahoo says data stolen from 1 billion accounts, *CNN*; December 15, 2016.
Yahoo hack: 1 bn accounts compromised by biggest data breach in history, *The Guardian*; December 15, 2016.
Got a hacked Yahoo account? Here's what you should do, *CNN*; December 16, 2016.
Yahoo's hack warning comes from third breach, the company says, *CNBC*; February 15, 2017.
New Yahoo hack: Hackers didn't even need your password to breach your account, *BGR*; February 16, 2017.
Yahoo Reveals Cookie Forging Activity Let to Account Breach, *eWeek*; March 2, 2017.
Yahoo!, W*ikipedia*
Yahoo! data breached, *Wikipedia.*