

Yahoo Security Breach (2014)

Wayne Ricks, Jr.

Old Dominion University

Abstract

The Yahoo security breach, one of the largest breaches in history, exposed critical cybersecurity vulnerabilities that left millions of users' sensitive information compromised. The breach highlighted flaws within Yahoo's security infrastructure, which enabled the unauthorized access to user accounts. The vulnerabilities that were exploited included insufficient encryption protocols, weak password protection, and a failure towards monitoring systems. The hackers were able to capitalize on these vulnerabilities by executing sophisticated attacks such as phishing and credential stuffing. The repercussions that came following the attack were severe, ranging from compromised user accounts, financial losses, and damage to Yahoo's reputation. This incident could have been avoided if Yahoo had fortified their security measures like improved encryption algorithms, multi-factor authentication, and regular security audits.

Keywords: vulnerabilities, phishing, repercussions, security

Yahoo Security Breach

In the realm of cybersecurity, many veteran officials preach time and time again to the people of the world to avoid answering unknown or skeptical emails that are forwarded to them. Back in the beginning of 2014, Yahoo would begin its journey of unfortunate events when hackers were able to penetrate past its security measures and inflict massive amounts of damage not only to the company but to every person that was affiliated with them, including its users. Senior correspondent Marty Williams said in his article, Inside the Russian hack of Yahoo: How they did it, that the attack began with the hackers spear-phishing email sent to a number Yahoo employees (Williams 2017). These phishing attacks were designed to give the Russian hackers access to Yahoo's user database and account management tool so that they could be given access to edit these programs. The database is where all user information such as usernames, phone numbers, password recovery emails, and a unique cryptographic value for each account, while the account management tool was obtained in order to have access to edit the database. Williams also states that the hackers also left themselves a back door so that they could access this data whenever they please and that a backup copy of the database was stolen and transferred to the hacker's computer. Yahoo's lack of properly encrypting the sensitive information and poor management of data were the vulnerabilities that the hackers exploited in order to carry out their attack.

The aftermath of the attack on Yahoo's database left severe repercussions not only to the company but to all users that had an account with Yahoo. The main speculation as to why so

many accounts were compromised led to people questioning why officials took so long to detect and prevent the breach from happening. According to Ajay Kumar, a correspondent with 15 years of experience in handling information security for various companies, explains that the breach was reported once the data was up for sale on the Black Market in his article “What have we learned from the Yahoo breach” (Kumar 2016). Once Yahoo officials noticed the breach happening, they did not issue a public statement addressing the situation, but issued out a security notice on the webpage, which explains what they will do to prevent incidents like this from happening again. The financial repercussions of this breach include Yahoo agreeing to pay \$117.5 million to cover the damages done to its users and Verizon Communications spending \$306 million in order to reinforce Yahoo’s cybersecurity and quadruple their IT staff (Matthews 2019).

Yahoo officials could’ve prevented this incident from occurring had they implemented vigilant cybersecurity measures. In the article, *IOTW: Multiple Yahoo data breaches across four years result in a \$117.5 million settlement*, author Kayla Matthews covers over what CISOs should learn from an incident such as this. Matthews states, “CISOs should prepare for attacks that use social engineering just as much as brute-force attacks. This will require CISOs to provide some level of cyber security education to non-cyber security and non-tech savvy staff.” (Matthews 2019). Firstly, a measure such as enhanced encryption protocols for all sensitive data would’ve made it more challenging for hackers to exploit any vulnerabilities. The implementation of a multi-factor authentication could’ve added an extra layer of protection, by having users provide multiple forms of identification to prove who they truly are. This in turn thwarts any attempts to compromise any account using stolen credentials. Measures such as regular security audits and vulnerability tests would’ve played a crucial role in determining any

vulnerabilities that were present within the systems at the time, enabling provident mitigation measures before any exploitation from happening. Social engineering attacks could've been mitigated had Yahoo properly educated and trained all employees with cybersecurity awareness, reducing the chance of anyone falling victim to phishing and increasing the overall vigilance of the team.

References

- Kumar, A. (2016, October 11). *What have we learned from the Yahoo breach?* CSO.
Retrieved January 16, 2024,
<https://www.csoonline.com/article/558343/what-have-we-learned-from-the-yahoo-breach.html>
- Matthews, K. (2019, October 7). *IOTW: Multiple Yahoo data breaches across four years result in a \$117.5 million settlement.* Cyber Security Hub. Retrieved January 16, 2024,
<https://www.cshub.com/attacks/articles/incident-of-the-week-multiple-yahoo-data-breaches-across-4-years-result-in-a-1175-million-settlement>
- Williams, M. (2017, October 4). *Inside the Russian hack of Yahoo: How they did it.* CSO.
Retrieved January 16, 2024,
<https://www.csoonline.com/article/560623/inside-the-russian-hack-of-yahoo-how-they-did-it.html>