

Yahoo Data Breach (2013-2016)

When it comes to data breaches regarding Yahoo, the company has reported having user accounts being compromised as far back as 2013. Most of the explanations given behind these earlier breaches involved forged cookies that allowed hackers to access user information. Whatever information the hackers hijacked was primarily to profit off of stolen information by selling the data via the dark web. "The full breadth of the incident still has to be assessed, but the information that was copied included full names, phone numbers, birth dates, email addresses, and even security question-and-answer pairs created by the user to authenticate the account. A large majority of passwords were encrypted and thus may still be protected, however even 1% of billions of users is still a considerable number of accounts." (Bitchkei) But the main focus of this essay will be on the recent reported breaches from 2016, which has reportedly been the worst one the company has faced. Around, or at least anyway, 500 million user accounts were confirmed compromised after an investigation was done on a breach back in 2014 (Lord et al.). Further investigation was conducted which pushed the originally 500 million accounts up to approximately 1 billion. The situation simply became worse.

How was Yahoo breached that allowed for this to occur? The simple answer: a phishing email was opened that created an entrance for hackers. Bob Lord explains in-depth: "The hackers used "forged 'cookies'" – bits of code that stay in the user's browser cache so that a website doesn't require a login with every visit... The cookies "could allow an intruder to access users' accounts without a password" by misidentifying anyone using them as the owner of an email account. The breach may be related to [the] theft of Yahoo's proprietary code." (Thielman) This rabbit hole only goes deeper, and it ends up leading to Russia. Russian hackers being hired by Russian intelligence FSB (Russian Federal Security Service), to be more precise.

As far as measures being taken by Yahoo in the aftermath of this breach, the company has reached out to users to simply change their passwords and user information via emails. "Commentators note that the breach was initially discovered in 2014. At the moment, Mayer refused to force an automatic reset of all user passwords, a fundamental action following a data breach." (Bitchkei) The timing with reporting these breaches has drawn a lot of criticism from the press, one the least including the purported negligence of Marissa Mayer to properly prioritize security of the data, according to an anonymous former employee. (Bitchkei) In this author's opinion, this is not a very good look for a company founded as a competitor to Google. With all of this data being compromised, it's no wonder Verizon had second thoughts about purchasing Yahoo if the security of the company was thwarted this badly. In fact, Craig Silliman (one of Verizon's lawyers) stated "I think we have a reasonable basis to believe right now that the impact is material and we're looking to Yahoo to demonstrate to us the full impact," when interviewed for The Guardian. "If they believe that it's not, then they'll need to show us that." (Thielman) As of May 3, 2021, Verizon has sold Verizon (along with AOL) to Apollo for \$5 billion, with Guru Gowrappan ("Verizon sells media businesses including Yahoo and AOL to Apollo for \$5 billion").