***Yahoo Says Hackers Stole Data on 500 Million Users in 2014***

**By**[**NICOLE PERLROTH**](http://www.nytimes.com/by/nicole-perlroth)SEPT. 22, 2016



The announcement of the breach at Yahoo comes as Verizon Communications moves forward with its $4.8 billion acquisition of the company. CreditMike Blake/Reuters

SAN FRANCISCO — [Yahoo](http://www.nytimes.com/topic/company/yahoo-inc?inline=nyt-org) announced on Thursday that the account information of at least 500 million users was stolen by hackers two years ago, in the biggest known intrusion of one company’s computer network.

In a statement, Yahoo said user information — including names, email addresses, telephone numbers, birth dates, encrypted passwords and, in some cases, security questions — was compromised in 2014 by what it believed was a “state-sponsored actor.”

While Yahoo did not name the country involved, how the company discovered the hack nearly two years after the fact offered a glimpse at the complicated and mysterious world of the underground web.

The hack of Yahoo, still one of the internet’s busiest sites with one billion monthly users, also has far-reaching implications for both consumers and one of America’s largest companies, [Verizon Communications](http://www.nytimes.com/topic/company/verizon-communications-inc?inline=nyt-org), which is in the process of [acquiring Yahoo](http://www.nytimes.com/2016/07/26/business/verizon-yahoo-sale.html) for $4.8 billion. Yahoo Mail is one of the oldest free email services, and many users have built their digital identities around it, from their bank accounts to photo albums and even medical information.

Changing Yahoo passwords will be just the start for many users. They’ll also have to comb through other services to make sure passwords used on those sites aren’t too similar to what they were using on Yahoo. And if they weren’t doing so already, they’ll have to treat everything they receive online with an abundance of suspicion, in case hackers are trying to trick them out of even more information.

The company said as much in an email to users that warned it was invalidating existing security questions — things like your mother’s maiden name or the name of the street you grew up on — and asked users to change their passwords. Yahoo also said it was working with law enforcement in their investigation and encouraged people to change up the security on other online accounts and monitor those accounts for suspicious activity as well.

“The stolen Yahoo data is critical because it not only leads to a single system but to users’ connections to their banks, social media profiles, other financial services and users’ friends and family,” said Alex Holden, the founder of Hold Security, which has been tracking the flow of stolen Yahoo credentials on the underground web. “This is one of the biggest breaches of people’s privacy and very far-reaching.”

**[How to Protect Yourself After the Yahoo Attack](http://www.nytimes.com/interactive/2016/technology/personaltech/what-to-do-if-hacked.html)**

[Simple tips to follow if you think your personal information online has been exposed to hackers.](http://www.nytimes.com/interactive/2016/technology/personaltech/what-to-do-if-hacked.html)

[[](http://www.nytimes.com/interactive/2016/technology/personaltech/what-to-do-if-hacked.html)](http://www.nytimes.com/interactive/2016/technology/personaltech/what-to-do-if-hacked.html)

The Yahoo hack also adds another miscue to what has been a troubled sale of a long-troubled company. In July, Verizon said it would acquire the internet pioneer, roughly a month before Yahoo security experts started looking into whether the site had been hacked. It is unclear what effect, if any, the breach will have on Yahoo’s sale price.

In a statement on Thursday, a Verizon spokesman, Bob Varettoni, said his company learned of the breach of Yahoo’s systems only two days ago and had “limited information and understanding of the impact.”

It is unclear whether security testing — such as a test to see if security experts could break into the Yahoo network — was performed as part of Verizon’s due diligence process before it agreed to the acquisition.

But such security is often overlooked by investors, even though breaches can result in stolen intellectual property, compromised user accounts and class-action lawsuits. To date, no law requires such security checks as part of due diligence.

“Cybersecurity can absolutely affect a valuation, and these are important questions that investors need to be asking,” said Jacob Olcott, vice president of BitSight Technologies, a security company.

Yahoo said it learned of the data breach this summer after hackers posted to underground forums and online marketplaces what they claimed was stolen Yahoo data. A Yahoo security team was unable to verify those claims. But what they eventually found was worse: a breach by what they believe was a state-sponsored actor that dated back to 2014.

A potential breach of Yahoo’s systems was first reported by the [tech news site Recode](http://www.recode.net/2016/9/22/13012836/yahoo-is-expected-to-confirm-massive-data-breach-impacting-hundreds-of-millions-of-users) early Thursday morning.

The first sign that something was amiss appeared in June, when a Russian hacker who goes by the user name Tessa88 started mentioning, in underground web forums, a new trove of stolen Yahoo data, Mr. Holden said. In July, Tessa88 supplied a sample of the stolen collection to people in the so-called underground web for authentication.

The sample contained valid Yahoo user accounts, but it was unclear whether the data was from a breach of a third-party service or Yahoo itself. And it was not clear whether it came from a recent Yahoo breach or a previous incident in 2012, when the internet service acknowledged that more than 450,000 user accounts were compromised.

Then, in August, a second hacker who goes by the alias Peace of Mind began offering a large collection of stolen Yahoo credentials — including user names, easily cracked passwords, birth dates, ZIP codes and email addresses — on a site called TheRealDeal, where hackers can buy and sell stolen data, Mr. Holden said.

TheRealDeal uses Tor, the anonymity software, and Bitcoin, the digital currency, to hide the identities of buyers, sellers and administrators who are trading attack methods and stolen data.

After looking into that data, Yahoo did not find evidence that the stolen credentials came from its own systems. But it did find evidence of a far more serious breach of its systems two years earlier.

Two years is an unusually long time to identify a hacking incident. According to the Ponemon Institute, which tracks data breaches, the average time it takes organizations to identify such an attack is 191 days, and the average time to contain a breach is 58 days after discovery.

Security experts say the breach could bring about class-action lawsuits, in addition to other costs. An annual report by the Ponemon Institute in July found that the costs to remediate a data breach is $221 per stolen record. Added up, that would top Yahoo’s $4.8 billion sale price.

Thursday afternoon, Senator Mark R. Warner, a Democrat from Virginia and former technology executive, issued a statement that said the “seriousness of this breach at Yahoo is huge.”

He weighed in with a call for a federal “breach notification standard” to replace data notification laws that vary by state. Senator Warner added that he was “most troubled” that the public was only learning of the incident two years after it happened.