

# 1-The New York Times-Yahoo

Yahoo Says 1 Billion User Accounts Were Hacked

Send any friend a story

As a subscriber, you have 10 gift articles to give each month. Anyone can read what you share.

Give this article

Read in app

Video

Will Donaldson, chief executive of the data security service nomx, said more problems with cloud data security were likely to surface.CreditCredit... Victor J. Blue/Bloomberg

[Worry]

By Vindu Goel and Nicole Perlroth

Dec. 14, 2016

SAN FRANCISCO — Yahoo, already reeling from its September disclosure that 500 million user accounts had been hacked in 2014, disclosed Wednesday that a different attack in 2013 compromised more than 1 billion accounts.

The two attacks are the largest known security breaches of one company's computer network.

The newly disclosed 2013 attack involved sensitive user information, including names, telephone numbers, dates of birth, encrypted passwords and unencrypted security questions that could be used to reset a password.

Yahoo said it is forcing all of the affected users to change their passwords and it is invalidating unencrypted security questions *[Rebuild]* — steps that it declined to take in September.

*[Disappointment]*

It is unclear how many Yahoo users were affected by both attacks. The internet company has more than 1 billion active users, but it is not clear how many inactive accounts were hacked.

Yahoo said it discovered the larger hacking after analyzing data files, provided by law enforcement, that an unnamed third party had claimed contained Yahoo information.

Simple tips to follow if you think your personal information online has been exposed to hackers.

Security has taken a back seat at Yahoo in recent years *[Disappointment]*, compared to Silicon Valley competitors like Google and Facebook. Yahoo's security team clashed with top executives, including the chief executive, Marissa Mayer, over the cost and customer inconvenience of proposed security measures *[Disappointment]*.

And critics say the company was slow to adopt aggressive security measures, even after a breach of over 450,000 accounts in 2012 and series of spam attacks — a mass mailing of unwanted messages — the following year.

*[Disappointment]*

“What’s most troubling is that this occurred so long ago, in August 2013, and no one saw any indication of a breach occurring until law enforcement came forward *[Disappointment, Legal Action]*,” said Jay Kaplan, the chief executive of Synack, a security company. “Yahoo has a long way to go to catch up to these threats.”

*[Disappointment]*

Yahoo has made a steady trickle of disclosures about the 2014 hacking, which it has been investigating with the help of federal authorities. The company said Wednesday that it now believes the attacker in that breach, which it says was sponsored by a government, found a way to forge credentials to log into some users' accounts without a password.

Bob Lord, Yahoo's chief information security officer, said in a statement that the state-sponsored actor in the 2014 attack had stolen Yahoo's proprietary source code. Outside forensics experts working with Yahoo believe that the state-sponsored hackers used Yahoo's code to access user accounts without their passwords by creating forged "cookies," short bits of text that a website can store on a user's machine. By forging these cookies, attackers were able to impersonate valid users, gaining information and performing actions on behalf of their victims. The company has not disclosed who it believes was behind the attack.

Find out which parts of your identity may have been stolen in major hacking attacks over the last several years.

In July, Yahoo agreed to sell its core businesses to Verizon Communications for \$4.8 billion. Verizon said in October that it might seek to renegotiate the terms of the transaction because of the hacking, which had not been disclosed to Verizon during the original deal talks.

*[Legal Action, Deny]*

After the latest disclosure Wednesday, a Verizon spokesman, Bob Varettoni, essentially repeated that position.

*[Legal Action]*

What to Know About Ransomware Attacks

Card 1 of 5

What are ransomware attacks? This form of cybercrime involves hackers breaking into computer networks and locking digital information until the victim pays for its release. Recent high-profile attacks have cast a spotlight

on this rapidly expanding criminal industry, which is based primarily in Russia .

Why are they becoming more common? Experts say ransomware is attractive to criminals because the attacks take place mostly anonymously online, minimizing the chances of getting caught. The Treasury Department has estimated that Americans have paid \$1.6 billion in ransoms since 2011.

Is there any connection to the rise of cryptocurrencies? The criminal industry's growth has been abetted by cryptocurrencies , like Bitcoin, which allow hackers to transact with victims anonymously, though experts see virtual currency exchanges as a weak point for ransomware gangs.

What is being done about these attacks? The U.S. military has taken offensive measures against ransomware groups, and the Biden administration has taken legal and economic action. Recent attacks have propelled ransomware to the top of President Biden's national security agenda .

Why is the government getting involved? The attacks, which were mostly directed at individuals a few years ago, have dramatically escalated as hackers have begun targeting critical infrastructure in the U.S. , including a major gasoline pipeline and meat processing plants .

“As we've said all along, we will evaluate the situation as Yahoo continues its investigation,” he said. “We will review the impact of this new development before reaching any final conclusions.”

Mr. Lord said Yahoo had taken steps to strengthen Yahoo's systems after the attacks [Rebuild]. The company encouraged its users to change passwords associated with their Yahoo account and any other digital accounts tied to their Yahoo email and account.

[Rebuild]

In the hacking disclosed Wednesday, Mr. Lord said Yahoo believed an “unauthorized third party” managed to steal data from one billion Yahoo user accounts. Mr. Lord said that Yahoo had not been able to identify how

the hackers breached Yahoo's systems, but that the company believed the attack occurred in August 2013.

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

Yahoo recommended that its customers use Yahoo Account Key , an authentication tool that verifies a user's identity using a mobile phone and eliminates the need to use a password on Yahoo altogether.

[Rebuild]

Security experts say the latest discovery of a breach that happened so long ago is another black mark for the company [Disappointment]. "It's not just one sophisticated adversary that gets in," said Ben Johnson, co-founder and chief security strategist at Carbon Black, a security company. "Typically companies get compromised multiple times due to the same vulnerability or employee culture."

Mr. Johnson added that the scale of the breaches is only increasing as companies store more and more troves of information in similar databases. "When you have these huge databases of information, it's millions — and now billions — of accounts lost," he said.

Advertisement