**Hackers stole personal data from 1 billion Yahoo user accounts**

Yahoo says it believes hackers stole personal data from more than one billion user accounts in a [cyberattack](https://www.newscientist.com/article-topic/hacking/) that happened in 2013.

The technology giant says the data affected included “names, email addresses, telephone numbers, dates of birth, hashed passwords”, as well as security questions and answers, but it claims financial information such as card details was not compromised.

|  |
| --- |
| “Yahoo has identified data security issues concerning certain Yahoo user accounts,” the firm said in a statement. “Yahoo has taken steps to secure user accounts and is working closely with law enforcement.” |

**A second attack**

The company, which is currently being taken over by US telecoms company Verizon, believes the attack is “distinct” from another cyberattack the company reported in September this year, which involved around 500 million accounts and was said to have been carried out by a “state-sponsored actor” in late 2014.

The newly-disclosed attack was discovered as part of an investigation after law enforcement provided the company with data files that a third party claimed was Yahoo user data.

“We analyzed this data with the assistance of outside forensic experts and found that it appears to be Yahoo user data,” the company said. “Based on further analysis of this data by the forensic experts, Yahoo believes an unauthorised third party, in August 2013, stole data associated with more than one billion user accounts.”

Yahoo users are advised to change their passwords and [security answers](https://www.newscientist.com/article/dn18469-email-accounts-at-risk-from-not-so-secret-questions/) and look out for any suspicious activity on their accounts. They should also change passwords and security answers for any other services if they have[re-used the same credentials](https://www.newscientist.com/blogs/shortsharpscience/2009/03/why-computer-hacking-is-childs.html).

Yahoo also says that users should avoid clicking links or downloading attachments if they think an email is suspicious and that they should be “cautious of unsolicited communications that ask for personal information.”