

## **\*\*Note to users about phishing scams\*\***

Below is the text of the email notice sent by Yahoo to potentially affected users. Please note that the email from Yahoo about this issue does not ask you to click on any links or contain attachments and does not request your personal information. If an email you receive about this issue prompts you to click on a link, download an attachment, or asks you for information, the email was not sent by Yahoo and may be an attempt to steal your personal information. Avoid clicking on links or downloading attachments from such suspicious emails.

**Subject line:** Important Security Information for Yahoo Users

### **UPDATED NOTICE OF DATA BREACH**

Dear **[personalized salutation]**,

We are writing to update you about a data security issue Yahoo previously announced in December 2016. Yahoo already took certain actions in 2016, described below, to help secure your account in connection with this issue.

#### **What Happened?**

On December 14, 2016, Yahoo announced that, based on its analysis of data files provided by law enforcement, the company believed that an unauthorized party stole data associated with certain user accounts in August 2013. Yahoo notified the users it had identified at that time as potentially affected. We recently obtained additional information and, after analyzing it with the assistance of outside forensic experts, we have determined that your user account information also was likely affected.

#### **What Information Was Involved?**

The stolen user account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (using MD5) and, in some cases, encrypted or unencrypted security questions and answers. Not all of these data elements may have been present for your account. The investigation indicates that the information that was stolen did not include passwords in clear text, payment card data, or bank account information. Payment card data and bank account information are not stored in the system we believe was affected.

#### **What We Are Doing**

In connection with the December 2016 announcement, Yahoo took action to protect users (including you) beyond those identified at that time as potentially affected. Specifically:

- Yahoo required potentially affected users to change their passwords.
- Yahoo also required all other users who had not changed their passwords since the time of the theft to do so.

- Yahoo invalidated unencrypted security questions and answers so they cannot be used to access an account.

We are closely coordinating with law enforcement on this matter, and continue to enhance our systems that detect and prevent unauthorized access to user accounts.

### **What You Can Do**

While Yahoo already has taken action to help secure your account, we encourage you to consider the following account security recommendations:

- Change your passwords and security questions and answers for any other accounts on which you used the same or similar information used for your Yahoo account.
- Review your accounts for suspicious activity.
- Be cautious of any unsolicited communications that ask for your personal information or refer you to a web page asking for personal information.
- Avoid clicking on links or downloading attachments from suspicious emails.

Additionally, please consider using Yahoo Account Key, a simple authentication tool that eliminates the need to use a password on Yahoo altogether.

### **For More Information**

For more information about this issue and our security resources, please visit the Yahoo 2013 Account Security Update FAQs page available at <https://yahoo.com/security-update>. We value the trust our users place in us, and the security of our users remains a top priority.

Sincerely,  
Chris Nims  
Chief Information Security Officer