****Note to users about phishing scams****

Below is the text of the email notices sent by Yahoo to users potentially affected by the issues the company disclosed on December 14, 2016. Please note that the emails from Yahoo about these issues do **not** ask you to click on any links or contain attachments and do **not** request your personal information. If an email you receive about these issues 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

NOTICE OF DATA BREACH

Dear [personalized salutation],

We are writing to inform you about a data security issue that may involve your Yahoo account information. We have taken steps to secure your account and are working closely with law enforcement.

What Happened?

Law enforcement provided Yahoo in November 2016 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. Based on further analysis of this data by the forensic experts, we believe an unauthorized third party, in August 2013, stole data associated with a broader set of user accounts, including yours. We have not been able to identify the intrusion associated with this theft. We believe this incident is likely distinct from the incident we disclosed on September 22, 2016.

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 stolen information 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

We are taking action to protect our users:

- We are requiring potentially affected users to change their passwords.

- We invalidated unencrypted security questions and answers so that they cannot be used to access an account.
- We continuously enhance our safeguards and systems that detect and prevent unauthorized access to user accounts.

What You Can Do

We encourage you to follow these 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 all of 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 Account Security Issue FAQs page available at https://yahoo.com/security-update.

Protecting your information is important to us and we work continuously to strengthen our defenses.

Sincerely,

Bob Lord
Chief Information Security Officer
Yahoo

Subject line: Important Security Information for Yahoo Users

Dear [personalized salutation],

We are writing to inform you about a data security issue that involves your Yahoo account. We have taken steps to secure your account and are working closely with law enforcement.

Our outside forensic experts have been investigating the creation of forged cookies that could allow an intruder to access users' accounts without a password. Based on the ongoing investigation, we believe a forged cookie may have been used in 2015 or 2016 to access your account. We have connected some of the cookie forging activity to the same state-sponsored actor believed to be responsible for the data theft we disclosed on September 22, 2016. Those users targeted by the state-sponsored actor were sent an additional notification like the one found here: https://help.yahoo.com/kb/SLN26995.html.

We invalidated the forged cookies and hardened our systems to secure them against similar attacks. We continuously enhance our safeguards and systems that detect and prevent unauthorized access to user accounts.

We encourage you to follow these security recommendations:

- Review all of 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 Account Security Issue FAQs page available at https://yahoo.com/security-update.

Protecting your information is important to us and we work continuously to strengthen our defenses.

Sincerely,

Bob Lord
Chief Information Security Officer
Yahoo

Subject line: Important Security Information for Yahoo Users

Dear [personalized salutation],

We are writing to inform you about a data security issue that involves your Yahoo account. We have taken steps to secure your account and are working closely with law enforcement.

Our outside forensic experts have been investigating the creation of forged cookies that could allow an intruder to access users' accounts without a password. Based on the ongoing investigation, we have found that a forged cookie was created for your account and taken from Yahoo's systems in 2015 or 2016, but we do not believe at this time that the cookie was used to access your account. We have connected some of the cookie forging activity to the same state-sponsored actor believed to be responsible for the data theft we disclosed on September 22, 2016.

We invalidated the forged cookies and hardened our systems to secure them against similar attacks. We continuously enhance our safeguards and systems that detect and prevent unauthorized access to user accounts.

We encourage you to follow these security recommendations:

- Review all of 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 Account Security Issue FAQs page available at https://yahoo.com/security-update.

Protecting your information is important to us and we work continuously to strengthen our defenses.

Sincerely,
Bob Lord
Chief Information Security Officer
Yahoo

December 14, 2016

Important Security Information for Yahoo Users

SUNNYVALE, Calif.--(BUSINESS WIRE)-- Yahoo! Inc. (NASDAQ:YHOO) has identified data security issues concerning certain Yahoo user accounts. Yahoo has taken steps to secure user accounts and is working closely with law enforcement.

As Yahoo previously disclosed in November, law enforcement provided the company with data files that a third party claimed was Yahoo user data. The company analyzed this data with the assistance of outside forensic experts and found that it appears to be Yahoo user data. Based on further analysis of this data by the forensic experts, Yahoo believes an unauthorized third party, in August 2013, stole data associated with more than one billion user accounts. The company has not been able to identify the intrusion associated with this theft. Yahoo believes this incident is likely distinct from the incident the company disclosed on September 22, 2016.

For potentially affected accounts, 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. The investigation indicates that the stolen information 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 the company believes was affected.

Yahoo is notifying potentially affected users and has taken steps to secure their accounts, including requiring users to change their passwords. Yahoo has also invalidated unencrypted security questions and answers so that they cannot be used to access an account.

Separately, Yahoo previously disclosed that its outside forensic experts were investigating the creation of forged cookies that could allow an intruder to access users' accounts without a password. Based on the ongoing investigation, the company believes an unauthorized third party accessed the company's proprietary code to learn how to forge cookies. The outside forensic experts have identified user accounts for which they believe forged cookies were taken or used. Yahoo is notifying the affected account holders, and has invalidated the forged cookies. The company has connected some of this activity to the same state-sponsored actor believed to be responsible for the data theft the company disclosed on September 22, 2016.

Yahoo encourages users to review all of their online accounts for suspicious activity and to change their passwords and security questions and answers for any other accounts on which they use the same or similar information used for their Yahoo account. The company further recommends that users avoid clicking links or downloading attachments from suspicious emails and that they be cautious of unsolicited communications that ask for personal information. Additionally, Yahoo recommends using Yahoo Account Key, a simple authentication tool that eliminates the need to use a password on Yahoo altogether.

Additional information is available on the Yahoo Account Security Issues FAQs page: https://yahoo.com/security-update.

About Yahoo

Yahoo is a guide to digital information discovery, focused on informing, connecting, and entertaining through its search, communications, and digital content products. By creating highly personalized experiences, Yahoo helps users discover the information that matters most to them around the world -- on mobile or desktop. Yahoo connects advertisers with target audiences through a streamlined advertising technology stack that combines the power of Yahoo's data, content, and technology. Yahoo is headquartered in Sunnyvale, California, and has offices located throughout the Americas, Asia Pacific (APAC) and the Europe, Middle East and Africa (EMEA) regions. For more information, visit the pressroom (pressroom.yahoo.net) or the Company's blog (yahoo.tumblr.com).

Statements in this press release regarding the findings of Yahoo's ongoing investigations involve potential risks and uncertainties. The final conclusions of the investigations may differ from the findings to date due to various factors including, but not limited to, the discovery of new or additional information and other developments that may arise during the course of the investigation. More information about potential risks and uncertainties of security breaches that could affect the Company's business and financial results is included under the caption "Risk Factors" in the Company's Quarterly Report on Form 10-Q for the quarter ended September 30, 2016, which is on file with the SEC and available on the SEC's website at www.sec.gov.

View source version on businesswire.com: http://www.businesswire.com/news/home/20161214006239/en/

Yahoo
Suzanne Philion, +1 408-349-4040
sphilion@yahoo-inc.com

Source: Yahoo! Inc.

News Provided by Acquire Media

Account Security Issues FAQs (December 14, 2016)

Yahoo has identified data security issues concerning certain Yahoo user accounts. Yahoo has taken steps to secure user accounts and is working closely with law enforcement.

Below are FAQs containing details about these issues and steps users can take to help protect their accounts.

For information about the data security issue the company disclosed on September 22, 2016, click here <link>.

1. What happened?

Law enforcement provided Yahoo in November 2016 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. Based on further analysis of this data by the forensic experts, we believe an unauthorized third party, in August 2013, stole data associated with more than one billion user accounts. Yahoo has not been able to identify the intrusion associated with this theft. We believe this incident is likely distinct from the incident we disclosed on September 22, 2016. We are notifying potentially affected users and have taken steps to secure their accounts, including requiring users to change their passwords. Yahoo has also invalidated unencrypted security questions and answers so that they cannot be used to access an account.

Separately, our outside forensic experts have been investigating the creation of forged cookies that could allow an intruder to access users' accounts without a password. Based on the ongoing investigation, the outside forensic experts have identified user accounts for which they believe forged cookies were taken or used in 2015 or 2016. The company is notifying the affected account holders, and has invalidated the forged cookies. We have connected some of this activity to the same state-sponsored actor believed to be responsible for the data theft we disclosed on September 22, 2016.

2. Was my account affected by the August 2013 incident?

We are notifying potentially affected users and posting additional information on our website. Additionally, we are taking steps to secure users' accounts, including requiring potentially affected users to change their passwords. Yahoo has also invalidated unencrypted security questions and answers so that they cannot be used to access an account.

3. Was my account affected by the cookie forging activity?

Based on the ongoing investigation, the outside forensic experts have identified user accounts for which they believe forged cookies were taken or used in 2015 or 2016. The company is notifying the affected account holders, and has invalidated the forged cookies.

4. What information was taken in the August 2013 incident?

For potentially affected accounts, 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. The investigation indicates that the stolen information 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 the company believes was affected.

5. What is a "hashed" password?

Hashing is a one-way mathematical function that converts an original string of data into a seemingly random string of characters. As such, passwords that have been hashed can't be reversed into the original plain text password. At the time of the August 2013 incident, we used MD5 to hash passwords. We began upgrading our password protection to bcrypt in the summer of 2013. Bcrypt is a password hashing mechanism that incorporates security features, including salting and multiple rounds of computation, to provide advanced protection against password cracking.

6. What information was affected by the cookie forging activity?

Forged cookies could allow an intruder to access users' accounts without a password. Based on Yahoo's ongoing investigation, we believe an unauthorized third party accessed our proprietary code to learn how to forge cookies. The outside forensic experts have identified user accounts for which they believe forged cookies were taken or used. The company is notifying the affected account holders, and has invalidated the forged cookies.

7. What is a "cookie"?

A cookie is a small piece of information stored on a computer for the purpose of identifying a web browser during interaction on websites. Websites use cookies to remember and recognize details about visitors, such as website preferences. Click here for more information on Yahoo's practices regarding cookies and similar technologies.

8. Are these incidents related to the data theft that Yahoo announced on September 22, 2016?

We believe that the August 2013 incident is likely distinct from the incident we disclosed on September 22, 2016.

We have connected some of the cookie forging activity to the same state-sponsored actor believed to be responsible for the data theft we disclosed on September 22, 2016. Those users targeted by the state-sponsored actor were sent an additional notification like the one found here.

9. I think I received one or more emails about these issues. How do I know that they are really from Yahoo?

Click here to view the content of our notices to potentially affected users. Please note that the emails from Yahoo about these issues will display the **Yahoo icon** when viewed through the Yahoo website or Yahoo Mail app. Importantly, the emails do **not** ask you to click on any links or contain attachments and do **not** request your personal information. If an email you received about these issues 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.

10. What is Yahoo doing to protect my account?

We have taken action to protect our users, including:

- We are requiring potentially affected users to change their passwords.
- We invalidated unencrypted security questions and answers so that they cannot be used to access an account.
- We invalidated the forged cookies and hardened our systems to secure them against similar attacks.
- We continuously enhance our safeguards and systems that detect and prevent unauthorized access to user accounts.

11. How do I change my password or disable security questions and answers?

You can change your Yahoo password or disable your security questions and answers by clicking here. We are requiring potentially affected users to change their passwords, and we have invalidated unencrypted security questions and answers so that they cannot be used to access an account.

12. Is there anything I can do to protect myself?

We encourage all of our users to follow these 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 all of 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.

13. What additional steps can I take to protect my information?

US/Global Version

Although the affected account information did not include passwords in clear text, payment card data, or bank account information, we encourage you to remain vigilant by reviewing your account statements and monitoring your credit reports. Below is contact information for the three nationwide consumer reporting agencies from which you can obtain a credit report.

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc.	1-888-397-3742	www.experian.com

	P.O. Box 9554 Allen, TX 75013		
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000	1-800-680-7289	www.transunion.com

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. You also may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from $5-$20 per action. Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to $10 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

For U.S. residents, you can contact the FTC to learn more about protecting your personal information. The contact information for the FTC is below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW

Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

For Rhode Island residents, you may obtain information about protecting your personal information from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401)-274-4400

EMEA Versions here

14. Are Tumblr accounts affected?

No. The systems from which the data was stolen in August 2013 contained no Tumblr user data at the time of the theft. Additionally, Yahoo has no indication that the forged cookies were used to access Tumblr accounts.

15. How can I get help with my account?

If you need further information or assistance with your account, please visit https://help.yahoo.com, where you will find the latest information and may be able to access direct customer support. DO NOT ENGAGE with any support service other than those provided by Yahoo, particularly support service providers that charge a fee for their service. Yahoo does not charge for support service for its accounts. Please note that Yahoo channels all support through https://help.yahoo.com.