

Subject line: Important Message Regarding Your Account Security

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.

What Happened?

A recent investigation by Yahoo has confirmed that a copy of certain user account information was stolen from our systems in late 2014 by what we believe is a state-sponsored actor. We are closely coordinating with law enforcement on this matter and working diligently to protect you.

What Information Was Involved?

The stolen user account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) 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 ongoing investigation suggests that stolen information did not include unprotected passwords, payment card data, or bank account information; payment card data and bank account information are not stored in the system that the investigation has found to be affected.

What We Are Doing

We are taking action to protect our users:

- We are asking potentially affected users to promptly change their passwords and adopt alternate means of account verification.
- We invalidated unencrypted security questions and answers so they cannot be used to access an account.
- We are recommending that all users who haven't changed their passwords since 2014 do so.
- We continue to enhance our systems that detect and prevent unauthorized access to user accounts.
- We are working closely with law enforcement on this matter.

Our investigation into this matter continues.

What You Can Do

We encourage you to follow these security recommendations:

- Change your password 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 altogether.

For More Information

For more information about this issue and our security resources, please visit the Yahoo 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 against the threats targeting our industry.

Sincerely,

Bob Lord
Chief Information Security Officer
Yahoo

Press Release

Title: An important message to Yahoo users on security

Date: 9/22

Time: 11:30 AM PT

SUNNYVALE, Calif. (BUSINESSWIRE) A recent investigation by Yahoo! Inc. (NASDAQ:YHOO) has confirmed that a copy of certain user account information was stolen from the company's network in late 2014 by what it believes is a state-sponsored actor. The account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers. The ongoing investigation suggests that stolen information did not include unprotected passwords, payment card data, or bank account information; payment card data and bank account information are not stored in the system that the investigation has found to be affected. Based on the ongoing investigation, Yahoo believes that information associated with at least 500 million user accounts was stolen and the investigation has found no evidence that the state-sponsored actor is currently in Yahoo's network. Yahoo is working closely with law enforcement on this matter.

Yahoo is notifying potentially affected users and has taken steps to secure their accounts. These steps include invalidating unencrypted security questions and answers so that they cannot be used to access an account and asking potentially affected users to change their passwords. Yahoo is also recommending that users who haven't changed their passwords since 2014 do so.

Yahoo encourages users to review their online accounts for suspicious activity and to change their password 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 on links or downloading attachments from suspicious emails and that they be cautious of unsolicited communications that ask for personal information. Additionally, Yahoo asks users to consider using [Yahoo Account Key](#), a simple authentication tool that eliminates the need to use a password altogether.

Online intrusions and thefts by state-sponsored actors have become increasingly common across the technology industry. Yahoo and other companies have launched programs to detect and notify users when a company strongly suspects that a state-sponsored actor has targeted an account. Since the inception of Yahoo's [program](#) in December 2015, independent of the recent investigation, approximately 10,000 users have received such a notice.

Additional information will be available on the Yahoo Security Issue FAQs page, <https://yahoo.com/security-update>, beginning at 11:30 am Pacific Daylight Time (PDT) on September 22, 2016.

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 investigation involve potential risks and uncertainties. The final conclusions of the investigation 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 June 30, 2016, which is on file with the SEC and available on the SEC's website at www.sec.gov.

Yahoo!, the Yahoo family of marks, and the associated logos are trademarks and/or registered trademarks of Yahoo! Inc. Other names are trademarks and/or registered trademarks of their respective owners.

Yahoo

Suzanne Philion

sphilion@yahoo-inc.com

+1 (408) 349-4040

Tumblr Post

Author: Bob Lord, CISO

Title: An Important Message About Yahoo User Security

Date: 9/22

Time: 11:35 AM PT (revised 4:30 PM PT)

Post to: yahoo.tumblr.com and security.yahoo.tumblr.com

A recent investigation by Yahoo has confirmed that a copy of certain user account information was stolen from the company's network in late 2014 by what it believes is a state-sponsored actor. The account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers. The ongoing investigation suggests that stolen information did not include unprotected passwords, payment card data, or bank account information; payment card data and bank account information are not stored in the system that the investigation has found to be affected. Based on the ongoing investigation, Yahoo believes that information associated with at least 500 million user accounts was stolen and the investigation has found no evidence that the state-sponsored actor is currently in Yahoo's network. Yahoo is working closely with law enforcement on this matter.

We are taking action to protect our users:

- We are notifying potentially affected users. The content of the email Yahoo is sending to those users will be available at <https://yahoo.com/security-notice-content> beginning at 11:30 am (PDT).
- We are asking potentially affected users to promptly change their passwords and adopt alternate means of account verification.
- We invalidated unencrypted security questions and answers so they cannot be used to access an account.
- We are recommending that all users who haven't changed their passwords since 2014 do so.
- We continue to enhance our systems that detect and prevent unauthorized access to user accounts.
- We are working closely with law enforcement on this matter.

We encourage our users to follow these [security recommendations](#):

- Change your password 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 altogether.

An increasingly connected world has come with increasingly sophisticated threats. Industry, government and users are constantly in the crosshairs of adversaries. Through strategic proactive detection initiatives and active response to unauthorized access of accounts, Yahoo will continue to strive to stay ahead of these ever-evolving online threats and to keep our users and our platforms secure.

For more information about this issue and our security resources, please visit the Yahoo Security Issue FAQs page, <https://yahoo.com/security-update>, which will be up beginning at 11:30 am (PDT). We also issued [this](#) press release.

Statements in this press release regarding the findings of Yahoo's ongoing investigation involve potential risks and uncertainties. The final conclusions of the investigation 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 June 30, 2016, which is on file with the SEC and available on the SEC's website at www.sec.gov.

We have confirmed, based on a recent investigation, that a copy of certain user account information was stolen from our network in late 2014 by what we believe is a state-sponsored actor. The account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers. The ongoing investigation suggests that stolen information did not include unprotected passwords, payment card data, or bank account information; payment card data and bank account information are not stored in the system that the investigation has found to be affected.

Below are FAQs containing details about this issue and steps that users can take to help protect their accounts.

1. What happened?

A recent investigation by Yahoo has confirmed that a copy of certain user account information was stolen from our network in late 2014 by what we believe is a state-sponsored actor. We are working closely with law enforcement authorities and notifying potentially affected users of ways they can further secure their accounts.

2. Was my account affected?

We are notifying potentially affected users by email and posting additional information to our website. Additionally, we are asking potentially affected users to promptly change their passwords and adopt alternate means of account verification.

3. Is the state-sponsored actor still in Yahoo's network?

The ongoing investigation has found no evidence that the state-sponsored actor is currently in Yahoo's network.

4. What information was stolen?

The stolen user account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers. The ongoing investigation suggests that stolen information did not include unprotected passwords, payment card data, or bank account information; payment card data and bank account information are not stored in the system that the investigation has found to be 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 converted into the original plain text password.

6. What is “bcrypt”?

Bcrypt is a password hashing mechanism that incorporates security features, including salting and multiple rounds of computation, to provide advanced protection against password cracking.

7. I think I received an email about this issue. How do I know that it is really from Yahoo?

[Click here](#) to view the content of our notice to potentially affected users. Please note that the email from Yahoo about this issue will display the Yahoo icon  when viewed through the Yahoo website or Yahoo Mail app. Importantly, the email does **not** ask you to click on any links or contain attachments and does **not** request your personal information. If the email you received 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.

8. What is Yahoo doing to protect my account?

We have taken action to protect our users, including:

- We are notifying potentially affected users.
- We are asking potentially affected users to promptly change their passwords and adopt alternate means of account verification.
- We invalidated unencrypted security questions and answers so that they cannot be used to access an account.
- We are recommending that all users who haven't changed their passwords since 2014 do so.
- We continue to enhance our systems that detect and prevent unauthorized access to user accounts.
- Our investigation into this matter continues.

9. 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](#).

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

We encourage all of our users to follow these security recommendations:

- Change your password 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's Account Key](#), a simple authentication tool that eliminates the need to use a password altogether.

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

Although the affected account information did not include unprotected passwords, 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 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. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000	1-800-680-7289	www.transunion.com

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 nationwide 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

12. Are Tumblr accounts affected?

No. The systems from which the data was stolen contained no Tumblr user data at the time of the theft.

13. 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. Please DO NOT ENGAGE with fraudulent online fee-based, toll-free-number services PRETENDING to be Yahoo support. Please note: Yahoo channels all support through <https://help.yahoo.com>.