Subject: Important: Account security alert and instructions for securing your account

Notice of data breach

Dear _____,

As one of our registered users, we are writing to share important information with you about a security incident which is related to your MyHeritage account, as well as steps we have taken in response to the incident and recommended actions you may wish to take.

What Happened?

On June 4, 2018, at 1 pm EST, we became aware of a data breach involving the email addresses and hashed passwords (these are not actual passwords) of 92.3 million MyHeritage users.

We learned about the breach when MyHeritage's Chief Information Security Officer received a message from a security researcher, which stated that the researcher had found a file named myheritage containing email addresses and hashed passwords located on a private server outside of MyHeritage. Our Information Security Team received the file from the security researcher, reviewed it, and confirmed that its contents originated from MyHeritage and included all the email addresses of users who signed up to MyHeritage up to October 26, 2017, as well as their hashed passwords. We made a public announcement about the breach within 8 hours of learning about it (https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident/).

What Information Was Involved?

Accessible information included your email address. The password associated with your account also was accessible but hashed using a cryptographic process, which like other hashing techniques converts plain text into a string of numbers and characters. MyHeritage does not store user passwords, but rather a one-way hash of each password, in which the hash key differs for each customer.

Immediately upon receipt of the file, MyHeritage's Information Security Team analyzed the file and began an investigation to determine how its contents were obtained and to identify any potential exploitation of the MyHeritage system. We determined that the file was legitimate and included the email addresses and hashed passwords of 92,283,889 users who had signed up to MyHeritage up to, and including, October 26, 2017, which was the date of the breach.

The security researcher reported that no other data related to MyHeritage was found on the private server. There has been no evidence that the data in the file was ever used by the perpetrators. Furthermore, we have not seen any activity indicating that any MyHeritage accounts had been compromised between October 26, 2017 (the date of the breach) and the present.

We believe the intrusion is limited to the user email addresses and hashed passwords. We have no reason to believe that any other MyHeritage systems were compromised. For example, credit card information is not stored on MyHeritage, but only on trusted third-party billing providers (e.g., BlueSnap, PayPal) utilized by MyHeritage. Other types of sensitive data such as family trees and DNA data are stored by MyHeritage on segregated systems, separate from those that store the email addresses, and they include added layers of security. We have no reason to believe those systems have been compromised.

What We Are Doing

- Immediately upon learning about the incident, we set up an Information Security Incident Response Team to investigate the incident. We have engaged a leading, independent cybersecurity firm to conduct comprehensive forensic reviews to determine the scope of the intrusion; and to conduct an assessment and provide recommendations on steps that can be taken to help prevent such an incident from occurring in the future.
- We have notified relevant authorities as per GDPR.
- We set up a 24/7 security customer support team to assist customers who have concerns or questions about the incident.
- We expired all passwords on MyHeritage, requiring our users to set a new password. You can read more about this in the follow up announcement we issued on June 5, 2018 (https://blog.myheritage.com/2018/06/cybersecurity-incident-june-5-6-update/).
- We added the option of Two-Factor Authentication for user accounts.

What You Can Do

1. **Change your password on MyHeritage.**

   We have protected your account by expiring your former password and requiring a password reset. Visit the MyHeritage website and log in. You will be prompted to set a new password. If you are not prompted, change your password as described in our FAQ article here: (https://www.myheritage.com/how-to-change-your-password). If you are using our mobile app or the Family Tree Builder genealogy software, first change the password on the website and then set the same new password on the mobile app and/or Family Tree Builder.

   Changing your password is a prudent and recommended practice. After doing this, you will be safer, because even if someone else has your password, they will not be able to access your MyHeritage account.

   We recommend you change your password on every other site where you used the same password. The most secure passwords are those that are difficult to guess and are used on only one website.

2. **Add Two-Factor Authentication (optional).**

   Two-Factor Authentication is an extra layer of security for your account, designed to ensure that you're the only person who can access your account, even if someone knows your password. Two-Factor Authentication allows you to authenticate yourself using a mobile phone in addition to a password, which further hardens your MyHeritage account against illegitimate access. For more details, see our blog post (https://blog.myheritage.com/2018/06/new-myheritage-adds-two-factor-authentication-2fa-to-secure-your-account/).

3. **Review Your Account.**

   Regularly review your account and report any suspicious or unrecognized activity immediately. Be vigilant and report any suspected incidents of fraud to us.

4. **Protect Your Data.**

   Never confirm or provide personal information such as passwords or account information to anyone contacting you. MyHeritage will never send you any unsolicited emails asking for your password.

For More Information

For more information listing additional steps you may wish to consider taking at any time if you ever suspect that you may have been the victim of identity theft, please go to this page: www.myheritage.com/protecting-your-identity

If you have questions or concerns, you can contact our security customer support team via email on privacy@myheritage.com or by phone via the toll-free number (USA) +1 888 672 2875, available 24/7 in English. For our customer support phone numbers in other countries, see our Contact Page (https://www.myheritage.com/contact-us) and when calling, pick option 5 in the menu (privacy). If asked by our staff, note that your account ID on MyHeritage is _____.

As always, your privacy and the security of your data are our highest priority. We continually assess our procedures and policies and seek new ways to improve our approach to security. We understand the importance of our role as custodians of your information and work every day to earn your trust.

Thank you for your understanding.
The MyHeritage Team

Important Identity Theft Information: Additional Steps You Can Take to Protect Your Identity

The following are additional steps you may wish to take to protect your identity.

Review Your Accounts and Credit Reports

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies.

You may obtain a free copy of your credit report online at www.annualcreditreport.com by calling toll free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service. P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241. 1.800.685.1111. www.equifax.com

Experian, P.O. Box 9532, Allen, TX 75013, 1.888.397.3742. www.experian.com

TransUnion, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016. 1.800.916.8800. www.transunion.com

Consider Placing a Fraud Alert

You may wish to consider contacting the fraud department of the three major credit bureaus to request that a “fraud alert” be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

Equifax:
Report Fraud:
1.888.766.0008Experian:
Report Fraud:
1.888.397.3742

TransUnion:
Report Fraud:
1.800.916.8800

Security Freeze for Credit Reporting Agencies

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com by calling toll free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service. P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348

Experian Security Freeze, P.O. Box 9554, Allen, TX 75013

TransUnion Security Freeze, Fraud Victim Assistance Department, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016

To request a security freeze, you will need to provide the following:

Your full name (including middle initial, Jr., Sr., Roman numerals, etc.)

Social Security number

Date of birth

Address(es) where you have lived over the prior five years

Proof of current address such as a current utility bill

A photocopy of a government-issued ID card

If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Don’t send cash through the mail.

The credit reporting agencies have three business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include (1) proper identification (name, address, and Social Security number), (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze all together, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three business days after receiving your request to remove the security freeze.

You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute

incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Suggestions If You Are a Victim of Identity Theft

File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1.877.IDTHEFT (1.877.438.4338); online at http://www.ftc.gov/idtheft; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf.

Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

Take Steps to Avoid Identity Theft

Further information can be obtained from the FTC about steps to take to avoid identity theft through the following paths: http://www.ftc.gov/idtheft; calling 1.877.IDTHEFT (1.877.438.4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at http://www.oag.state.md.us/idtheft/index.htm, calling the Identity Theft Unit at 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

Massachusetts residents are reminded that 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 $5 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. 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.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above and you have rights under the Fair Credit Reporting Act as described above.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, calling 1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (503) 378-4400 or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

Rhode Island residents are reminded that 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 small fee 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. 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. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1.410.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at http://www.atg.state.vt.us.