RootsWeb Security Update

Posted by Tony Blackman on December 23, 2017 in Website

We want to share an important security update with you.

Last Wednesday, December 20, Ancestry's Information Security Team received a message from a security researcher indicating that he had found a file containing email addresses/username and password combinations as well as user names from a RootsWeb.com server. Our Information Security Team reviewed the details of this file, and confirmed that it contains information related to users of Rootsweb's surname list information, a service we retired earlier this year. For those of you who are unfamiliar, RootsWeb is a free community-driven collection of tools that are used by some people to host and share genealogical information. Ancestry has been hosting dedicated RootsWeb servers as a favor to the community since 2000. Importantly, RootsWeb does not host sensitive information like credit card numbers or social security numbers, and is not supported by the same infrastructure as Ancestry's other brands. We are in the process of informing all impacted customers and will also be working with regulators and law enforcement as appropriate.

We also reviewed the RootsWeb file to see if any of the account information overlapped with existing accounts on Ancestry sites. We did confirm that a very small number of accounts – less than one percent of our total customer group – used the same account credentials on both Rootsweb and an Ancestry commercial site. We are currently contacting these customers.

In all cases, any user whose account had its associated email/username and password included on the file has had their accounts locked and will need to create a new password the next time they visit.

What Happened

Immediately after receiving the file containing the RootsWeb surname list user data, the Ancestry Information Security Team commenced its analysis of the file and its contents, and started a forensic investigation of RootsWeb's systems to determine the source of the data and identify any potential active exploitation of the RootsWeb system.

As a result of that analysis, we determined that the file was legitimate, although the majority of the information was old. Though the file contained 300,000 email/usernames and passwords, through our analysis we were able to determine that only approximately 55,000 of these were used both on RootsWeb and one of the Ancestry sites, and the vast majority of those were from free trial or currently unused accounts. Additionally, we found that about 7,000 of those password and email address combinations matched credentials for active Ancestry customers. As part of our investigation, our team also uncovered other usernames that were present on the RootsWeb server that, though not on the file shared with us, we reasonably believe could have been exposed externally. We are taking the additional step of informing those users as well.

We believe the intrusion was limited to the RootsWeb surname list, where someone was able to create the file of older RootsWeb usernames and passwords as a direct result of how part of this open community was set up, an issue we are working to rectify. We have no reason to believe that any Ancestry systems were compromised. Further, we have not seen any activity indicating the compromise of any individual Ancestry accounts.

What We've Done

As a result of this discovery, we have taken two immediate corrective actions.

First, for the approximately 55,000 customers who used the same credentials at RootsWeb's surname list and Ancestry – whether currently active or not – we have locked their Ancestry accounts and will require that they create a new password the next time they visit. We have also sent them emails to alert them to the situation. Though we have seen no activity that indicates these accounts have been compromised, we believe taking this additional measure is the right step to ensure the security of these customers. If you have not received an email or a notice requiring you to change your password, you have not been affected. Again, this issue involves less than one percent of our users, so there is a very good chance your account wasn't involved.

Second, we have temporarily taken RootsWeb offline, and are working to ensure that all data is saved and preserved to the best of our ability. As RootsWeb is a free and open community that has been largely built by its users, we may not be able to salvage everything as we work to resolve this issue and enhance the RootsWeb infrastructure.

What You Should Do

If you are a customer whose account was impacted, you will receive an email telling you that you need to change your password. In that case, you will be required to create a new password the next time you visit Ancestry.

For the vast majority of customers who are not impacted by this, there is nothing you need to do as a result of this incident. However, we always recommend that you take the time to evaluate your own security settings. Please, never use the same username and password for multiple services or sites. And it's generally good practice to use longer passwords and to change them regularly.

What We're Doing from Here

As always, your privacy and the security of the data you share with us are our highest priority. We are continually assessing our policy and procedures and always seeking ways to improve our approach to security. We understand the importance of our role as stewards of your information and work every day to earn your trust.

We are doing a deep analysis of RootsWeb, its design and how we might be able to help the community enhance the site and its services. It is our desire to continue to host these tools for the community with appropriate safeguards in place.

Please let us know if you have any questions at Support Center, and thank you for your understanding.

Share Tweet Share Pin Email

Tony Blackman (https://blogs.ancestry.com/ancestry/author/tblackman/)

Tony Blackham is Chief Information Security Officer at Ancestry
might

Subject: Important message to RootsWeb users
Date: Saturday, December 23, 2017 at 11:25:34 AM Pacific Standard Time
From: RootsWeb Notifications
To: Kathryn Davidson

rootsweb.com

Dear RootsWeb user,

We want to share an important security update with you.

What Happened

This past Wednesday, December 20, Ancestry’s Security Team became aware of a potential risk to an email address and password associated with a service offered on RootsWeb. A security researcher informed our Security Team that he had found a file containing username (email address in some cases) and password combinations from a RootsWeb server. After analysis, we were able to confirm that the file was legitimate, and did contain some RootsWeb username/password combinations, specifically related to the RootsWeb’s surname list, a service we retired earlier this year.

What Information Was Involved

The file contained only email/usernames and passwords related to RootsWeb. It is important to note, RootsWeb **does not** host sensitive information like credit card or social security numbers. However, your name could also have been obtained

What Are We Doing?

In order to help safeguard our customers’ information, we have temporarily restricted access to the RootsWeb site while we investigate and resolve security gaps associated with this incident.

What You Can Do

As an extra safety precaution, if you use the same username and password from RootsWeb on other websites, we recommend that you change your password on those sites immediately. We also recommend you remain alert for phishing emails that look like they might be from RootsWeb. You can contact Ancestry Member Services here:
https://support.ancestry.com/s/phonesupport

For More Information

To learn more about this incident, please read our **blog post**. We will notify you when the site is back online. We hope it will only take a few weeks to resolve. In the meantime, if you subscribe to mailing lists on RootsWeb.com, you will continue to receive those communications.

Thank you,
Ancestry Information Security Team

Your privacy is important to us. View our **Privacy Statement** for more information.

Use of RootsWeb.com is subject to our **Terms and Conditions**.

Ancestry.com Operations Inc. 1300 W Traverse Parkway, Lehi, UT 84043, USA

Subject: Important message to RootsWeb users
Date: Saturday, December 23, 2017 at 11:27:33 AM Pacific Standard Time
From: Ancestry
To: Kathryn Davidson

ancestry

We want to share an important security update with you. You are receiving this email because we believe you used the same login information on both RootsWeb and an Ancestry site.

What Happened

This past Wednesday, December 20, Ancestry became aware of a potential risk an email address and password associated with a service offered on RootsWeb. A security researcher indicated that he had found a file containing username (email address in some cases) and password combinations from a RootsWeb server. After analysis, we were able to confirm that the file was legitimate, and did contain some RootsWeb username/password combinations, specifically related to the RootsWeb's surname list, a service we retired earlier this year.

What Information Is Involved

The file contained email/usernames and passwords related to RootsWeb. However, in our analysis, we note that your Ancestry account used the same login credentials. As a result, your Ancestry account was also at risk. It is important to note, RootsWeb **does not** host sensitive information like credit card numbers or social security numbers, and we have no indication that this incident involved any Ancestry system or account. However, your name could also have been obtained.

What Are We Doing?

In order to help safeguard our customers' information, we have temporarily restricted access to the RootsWeb site while we investigate and resolve security gaps associated with this incident. We have also temporarily locked your Ancestry account and require that you update your password upon your next visit to Ancestry. **Click here** to create a new password on Ancestry now.

What Can You Do?

In addition to changing your login for Ancestry, as an extra safety precaution, if you also use this login information on other websites, we recommend that you change your password on those sites immediately as well. We also recommend you remain alert for phishing emails that look like they might be from RootsWeb. You can contact Ancestry Member Services here: **https://support.ancestry.com/s/phonesupport**

For More Information

To learn more about this incident, please read our **blog post**. We apologize for any inconvenience this may cause you. We'll notify you when the RootsWeb site is available. We hope it will only take a few weeks to resolve. In the meantime, if you subscribe to mailing lists on Rootsweb, you will continue to receive those communications.

Thank you,
Ancestry Information Security Team

Contact Us **Online Help**

Please add Ancestry@ancestry.com to your address book to make sure you don't miss an email.

You are receiving this email because you have registered with Ancestry using the email address **kdavidson@ancestry.com**.

Your privacy is important to us. View our **Privacy Statement** for more information.

Use of Ancestry.com is subject to our **Terms and Conditions**.

Ancestry.com Operations Inc. 1300 W Traverse Parkway, Lehi, UT 84043, USA

Subject: [Test] Important message to RootsWeb users
Date: Saturday, December 23, 2017 at 12:21:14 PM Pacific Standard Time
From: Fold3.com
To: thammond@footnote.com

We want to share an important security update with you. You are receiving this email because we believe you used the same login information on both RootsWeb and an Ancestry site.

What Happened

This past Wednesday, December 20, Ancestry became aware of a potential risk an email address and password associated with a service offered on RootsWeb. A security researcher indicated that he had found a file containing username (email address in some cases) and password combinations from a RootsWeb server. After analysis, we were able to confirm that the file was legitimate, and did contain some RootsWeb username/password combinations, specifically related to the RootsWeb's surname list, a service we retired earlier this year.

What Information Is Involved

The file contained email/usernames and passwords related to RootsWeb. However, in our analysis, we note that your Fold3 account used the same login credentials. As a result, your Fold3 account was also at risk. It is important to note, RootsWeb **does not** host sensitive information like credit card numbers or social security numbers, and we have no indication that this incident involved any Fold3 system or account. However, your name could also have been obtained.

What Are We Doing?

In order to help safeguard our customers' information, we have temporarily restricted access to the RootsWeb site while we investigate and resolve security gaps associated with this incident. We have also temporarily locked your Fold3 account and require that you update your password upon your next visit to Fold3. Click here to create a new password on Fold3 now.

What Can You Do?

In addition to changing your login for Fold3, as an extra safety precaution, if you also use this login information on other websites, we recommend that you change your password on those sites immediately as well. We also recommend you remain alert for phishing emails that look like they might be from RootsWeb. You can contact Ancestry Member Services here: https://support.ancestry.com/s/phonesupport

For More Information

To learn more about this incident, please read our blog post. We apologize for any inconvenience this may cause you. We'll notify you when the RootsWeb site is available. We hope it will only take a few weeks to resolve. In the meantime, if you subscribe to mailing lists on Rootsweb, you will continue to receive those communications.

Thank you,
Ancestry Information Security Team

Please add **team@fold3.com** to your address book to make sure you don’t miss an email.

You are receiving this email because you have registered with Fold3 using the email address **thammond@footnote.com**.

Help Center

Privacy Statement • Terms & Conditions

Subject: [Test] Important message to RootsWeb users
Date: Saturday, December 23, 2017 at 12:16:17 PM Pacific Standard Time
From: Newspapers.com
To: thammond@fold3.com

Newspapers.com

We want to share an important security update with you. You are receiving this email because we believe you used the same login information on both RootsWeb and an Ancestry site.

What Happened

This past Wednesday, December 20, Ancestry became aware of a potential risk an email address and password associated with a service offered on RootsWeb. A security researcher indicated that he had found a file containing username (email address in some cases) and password combinations from a RootsWeb server. After analysis, we were able to confirm that the file was legitimate, and did contain some RootsWeb username/password combinations, specifically related to the RootsWeb's surname list, a service we retired earlier this year.

What Information Is Involved

The file contained email/usernames and passwords related to RootsWeb. However, in our analysis, we note that your Newspapers.com account used the same login credentials. As a result, your Newspapers.com account was also at risk. It is important to note, RootsWeb **does not** host sensitive information like credit card numbers or social security numbers, and we have no indication that this incident involved any Newspapers.com system or account. However, your name could also have been obtained.

What Are We Doing?

In order to help safeguard our customers' information, we have temporarily restricted access to the RootsWeb site while we investigate and resolve security gaps associated with this incident. We have also temporarily locked your Newspapers.com account and require that you update your password upon your next visit to Newspapers.com. Click here to create a new password on Newspapers.com now.

What Can You Do?

In addition to changing your login for Newspapers.com, as an extra safety precaution, if you also use this login information on other websites, we recommend that you change your password on those sites immediately as well. We also recommend you remain alert for phishing emails that look like they might be from RootsWeb. You can contact Ancestry Member Services here: https://support.ancestry.com/s/phonesupport

For More Information

To learn more about this incident, please read our blog post. We apologize for any inconvenience this may cause you. We'll notify you when the RootsWeb site is available. We hope it will only take a few weeks to resolve. In the meantime, if you subscribe to mailing lists on Rootsweb, you will continue to receive those communications.

Thank you,
Ancestry Information Security Team

1300 W Traverse Parkway, Lehi, UT 84043 USA

Help Center