Protecting Our Members

Cory Scott May 18, 2016

In 2012, LinkedIn was the victim of an unauthorized access and disclosure of some members' passwords. At the time, our immediate response included a mandatory password reset for all accounts we believed were compromised as a result of the unauthorized disclosure. Additionally, we advised all members of LinkedIn to change their passwords as a matter of best practice.

Yesterday, we became aware of an additional set of data that had just been released that claims to be email and hashed password combinations of more than 100 million LinkedIn members from that same theft in 2012. We are taking immediate steps to invalidate the passwords of the accounts impacted, and we will contact those members to reset their passwords. We have no indication that this is as a result of a new security breach.

We take the safety and security of our members' accounts seriously. For several years, we have hashed and salted every password in our database, and we have offered protection tools such as email challenges and dual factor authentication. We encourage our members to visit our safety center to learn about enabling two-step verification, and to use strong passwords in order to keep their accounts as safe as possible.

UPDATE: May 18, 5:30 p.m. PT

We're moving swiftly to address the release of additional data from a 2012 breach, specifically:

We have begun to invalidate passwords for all accounts created prior to the 2012 breach that haven't updated their password since that breach. We will be letting individual members know if they need to reset their password. However, regularly changing your password is always a good idea and you don't have to wait for the notification. Feel free to reset your password by following the directions here.

We have demanded that parties cease making stolen password data available and will evaluate potential legal action if they fail to comply. In the meantime, we are using automated tools to attempt to identify and block any suspicious activity that might occur on affected accounts.

UPDATE: May 23, 11 p.m. PT

We've finished our process of invalidating all passwords we believed were at risk. These were accounts that had not reset their passwords since the 2012 breach. We will soon be sending more information to all members that could have been affected, even if they've updated their password. If you have questions about your personal account, please contact us here.

UPDATE: June 6, 8:30 a.m. PT

Recent reports of celebrity accounts being compromised on social media have resulted in questions about connections to the 2012 LinkedIn data breach. Here are

- There is no new data breach. Several weeks ago, additional names and passwords from the original data breach in 2012 were released and we took quick action to notify our members.

- At that time, we inactivated all the passwords on LinkedIn for members that hadn't updated them since the 2012 incident and reached out to every member who had an account as of June 6, 2012 to let them know what had happened, reminding them to reset their passwords on other sites.

- All members should take care to manage and change passwords across other sites, avoid re-use, leverage advanced security features and update often.

Topics

Security

Related story
Managing Your Settings on LinkedIn is Now Easier Than Ever

Related story
LinkedIn's Transparency Report about Government Requests for Member Data: Second Half of 2015