The LinkedIn Data Breach and What you Need to Know

June 8, 2012 - This week, it was announced that a data breach involving more than 6 million LinkedIn users had been discovered. For the unindoctrinated, LinkedIn is largest social network dedicated to business to business communications. It has millions of users; everyone from corporate executives in Fortune 500 companies to college students seeking their first real jobs. And the platform hosts some of the most valuable business contact information that you can find. So it is no real surprise that the company has been targeted by hackers.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

LinkedIn has been targeted before by scam artists but this latest attack is a little different. More than 6 million user names and password were discovered in a posting on a Russian website.

This breach isn't likely to lead to too many privacy issues for the people whose accounts have been hacked into. The fact of the matter is that user profiles on LinkedIn are, for the most part, publically available. People who post their information on LinkedIn actually want to be found. They are looking to have recruiters read their resumes or have potential clients read about their company's products and services.

Nor is this data breach very likely to result in identity theft. Most, but not all, LinkedIn users have free accounts. For those who fit into the "free" category, they don't have to worry about having any credit card information stolen. Even so, the breach could cause real problems for users by exposing all of the contact information of every single direct contact they have. NOTE: It is not clear that any credit card data has been exposed on paid LinkedIn account but if you do have an account on LinkedIn that has been breached, and you use a credit card in conjunction with that account, you should probably contact your bank and have them issue a new card. In my opinion, you should at the very least contact LinkedIn and ask them if any credit card data was compromised in the breach.

Once someone hacks into your LinkedIn account, they can send messages to every contact you have through the LinkedIn platform. They can also download a list of your contacts, complete with e-mail addresses. This makes it possible for someone to pose as you when they are sending out e-mail. And if the person receiving the mail message is a trusted business associate, friend, client or colleague, they are susceptible to various forms of fraud or to having their computers infected with malware or computer viruses. Those trusted contacts may not want to have anything to do with you after an experience like that. Even worse, you could lose business from existing clients.

As if this data breach isn't bad enough, some hackers have apparently decided to rub some additional salt into LinkedIn's wounds. Using the mantra, "never let a crisis go to waste," some hackers are now sending out e-mail messages that

appear to come from LinkedIn asking users verify certain information about their accounts. The mail messages provide a link. If the person receiving the message clicks on the link, they are taken to an online pharmacy. Other variations similar attacks have been know to infect the end user's computer with malware and capture data associated with their accounts. There is no reason to believe that this attack won't progress in that direction.

These messages may be especially harmful right now as LinkedIn is actively contacting the people whose account information was breached and telling them that they need to reset their passwords. The actual e-mail message that LinkedIn is sending out does not contain a link. Users need to navigate to the site manually.

LinkedIn has frozen the accounts of those who have had their data leaked. The only way to take the freeze off of your account is to setup a new password. According to a report on KNX news radion, LinkedIn has also said that they can't guarantee that the hackers who stole this user information have actually been locked out of their system yet. This means that the company could have to tell user to reset their passwords again in just a few days. In the mean time, if you are thinking about purchasing any service through the company, in my opinion you might want to hold off on giving them your credit card information until the company can make assurances that their system is hacker-free. Until that time, if you absolutely need to make a purchase through LinkedIn, you may want to check with your credit card company to see if they can issue you a one-time-use credit card number in association with your existing credit account. This will insure that even if one of these crooks gets their hands on your credit information, it will be totally useless to them.

byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS