Home Depot Data Breach Included 53 Million eMail Addresses - Why You Should Care!

November 13, 2014 - Within the past week it has been revealed that the data breach at Home Depot was related to more than just credit card data. The breach of more than 50 million credit and debit cards may prove to be the largest single data breach of any retailer to date. But breach also included 53 million email addresses and that could turn a one-time data breach into an ongoing financial calamity for millions of people.

Home Depot isn't the first retailer to have an email database breached, and they certainly won't be the last. As it turns out, those stolen email addresses may prove to be more valuable than the actual credit card data that was stolen. That's because the hackers behind these retailer data breaches can do a lot of damage with nothing more than your name and your email address.

In this particular case, the hackers have the names of 53 million consumers who they know to have a relationship with Home Depot. Every single one of those people is a potential target for email phishing scams.

All the hackers have to do is create an email message that looks like it originates with Home Depot. That mail message could appear to be a flyer for a new sale, a coupon offer, or virtually anything that the hackers can dream up. Once a victim clicks on a link in one of these messages, there are a multitude of bad things that can happen. Malware and viruses can be installed on their computer. And the most creative hackers are likely try to get victims to place an order for items that they falsely advertise. This means that even those who have replaced their credit or debit cards since the original breach can be targeted a second, or a third, or even a fourth time; creating a repeating cycle of identity theft and fraud.

The worst part of this scenario is that those targeted in such a scam are not likely to be surprised when they receive an email message that looks like it came from Home Depotâ€¦ or any other company that they do business with and which has experienced a data breach. But there are some effective options that consumers can take to protect themselves.

The most important thing you can do is to make sure that your antivirus software is up to date. You should also make sure that you have installed the latest security patches for your computer's operating system.

For anyone who believes that their information may have been included in a data breach of this type, you should also establish a new email address that you only use for this type of email. Then log in to any website that you subscribe to and make sure that they are using that new email address. If you do this and continue to receive solicitations on your old email address, you can be pretty sure that those solicitations are not legitimate.
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