Huge Email Data Breach Means Consumers Need to be Cautious - An ACCESS Fraud Alert

April 4, 2011 - Last week a company named Epsilon, a marketing corporation that works with a corporate who's-who list, began notifying its clients that its email marketing database had been breached by hackers. The breach apparently only revealed names and e-mail addresses, so identity theft is not an immediate concern even though it is potentially the largest data breach of its kind to date. What is of great concern is that even with the limited amount of information the hackers were able to gain access to, enough information was breached to allow the hackers to launch phishing scams. Consumers will need to be on their guard for the foreseeable future if they want to avoid being victimized.

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);
})();

The hack of Epsilon means that email lists of a number of large corporations were breached last week. Epsilon's client list includes companies like Best Buy, Capital One and JP Morgan Chase. In fact a number of large banks utilize the company's email marketing services along with hotel chains, grocers and other major retailers.

Last year, Epsilon sent more than 40 billion email messages out on behalf of their clients. There is a very good chance that if you belong to a hotel rewards program, a grocery store loyalty program, or bank with a major financial institution, your information was exposed in this breach.

This means that hackers now have your name and e-mail address; everything they need to send personalized e-mail messages to you. And there is a very good chance that these messages will appear to be from one or more of the companies that make up Epsilon's client list. That's where this data breach becomes dangerous.

ACCESS is urging anyone receiving commercial e-mail messages requesting personal information to either ignore them or to contact the sender by phone using a phone number that you have actually looked up yourself. Messages like this may actually be part of a phishing scam.

Do not respond to requests for updated credit card information, bank account information or any other personally identifiable information by clicking on links within email messages. This is never a good idea but in light of the Epsilon breach, it is now especially dangerous. The same advice holds true if you receive email messages stating that you've won something from one of the companies that you do business with. As tempting as it may be to respondâ€¦ after all, who doesn't like the idea of winning somethingâ€¦ you could be setting yourself up to be victimized.

The federal government is taking the breach seriously. The Secret Service is now investigating the hack. If you suspect that you have received an e-mail message as a result of this hack, you can forward it to the Secret Service at phishing-

report@us.cert.gov.

Epsilon serves more than 2,500 client companies. Some of the larger ones that may be affected include: Ameriprise Financial. Best Buy, Brookstone, Capital One, Citi, Home Shopping Network, The College Board, JP Morgan Chase, New York & Co., Kroger, Ritz-Carlton Rewards, LL Bean Visa Card, Hilton Honors, Marriott Rewards, Disney Destinations, US Bank, TiVo, McKinsey Quarterly, Walgreens and Ethan Allen. Any email messages received from these companies which solicit personal information must be viewed as suspect.

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: