dallasnews.com
The Dallas Morning News

Data breach at Irving-based Epsilon exposes email addresses of major firms' customers

By VICTOR GODINEZ
Staff Writer
vgodinez@dallasnews.com

Published 04 April 2011 11:56 PM

In what could be one of the largest data security breaches in history, the email addresses of potentially millions of Americans have been stolen from an Irving-based online marketing company.

The theft could enable scammers to precisely target potential victims with phony emails that appear to be from companies or organizations those Americans have done business with in the past.

The company, Epsilon, a subsidiary of Plano-based Alliance Data Systems Corp., handles email marketing campaigns for some of the biggest names in corporate America. The list of companies affected by the breach is growing by the day and includes Target Corp., Best Buy Co. and Citigroup Inc.

The hackers apparently did not steal credit card numbers or other personal info.

Rather, the pilfered names and email addresses could be used in so-called phishing scams, where a fraudulent email either entices an unwitting victim to provide account information that can be used to steal money or to click on a link to download malicious software to the user's computer.

What's more, as the broad array of banks, hotels, retailers and more send out warning emails to their customers, there's a danger that scammers could craft their own fake warning emails and use the concern over the breach to actually accelerate their attacks.

Alliance Data Systems Corp. said Monday that the breach is limited to names and email addresses.

"This incident involved nonpersonally identifiable information," said Shelley Whiddon, a spokeswoman for Alliance Data. "That is a really critical point here. We're not talking about Social Security account information, that kind of stuff."

Whiddon said Alliance Data has already identified the source of last week's attack and is working with law enforcement.

It wasn't clear what kind of financial liability Epsilon or Alliance Data might face.

Shares of Alliance Data Systems fell $1.73, or 2 percent, to close at $84.20 Monday.

Alliance Data specializes in managing private-label credit cards for retailers and loyalty programs for airlines and other companies.

But Whiddon said none of those divisions appear to have been targeted by the hackers.

Murat Kantarcioglu, an assistant professor of computer science and director of the University of Texas at Dallas' data security and privacy lab, agreed that the impact of the breach shouldn't be too severe.

"The main risk I see is that the email addresses could be used to have targeted phishing attacks," he said. "Other than that, I don't see too much risk, like identity theft, happening here."

A phishing attack generally involves a scammer sending out phony emails under the name of a legitimate business or government agency.

The email asks the recipient to provide his login information or account numbers or just click through to a simple website so the company can verify the accuracy of the numbers.

Often, the scams are easily noticed if the scammer pretends to represent a company with which a consumer has never done business.

But in the Epsilon case, the scammers can match actual customer names and emails to a particular retailer or bank or other institution.

So the phony emails might seem more legitimate as they'll appear to come from the recipient's bank or grocery store.

Kantarcioglu said the best course to prevent getting scammed is to use a system he jokingly calls “don’t trust, but verify.”

“I never click on the links I receive,” he said. “If I get an email from Chase saying, ‘Please click on this thing to verify your account,’ I close my email, I open my web browser, and I type the URL. And make sure you type it correctly. Then I log into my account.”