Targeted phishing scams could rise after Epsilon data breach

April 7 2011

Consumers may see an increase in targeted "phishing" attacks after a massive data breach at one of the world's biggest marketing services.

A wave of alert emails has been distributed over the last few days as Epsilon, one of the nation's largest marketing services, deals with what could end up being one of the largest data breaches in U.S. history. Customers of major banks, grocers, and hotel chains have been receiving notifications alerting them that their names and email addresses may have been compromised.

Consumers may see an increase in targeted "phishing" attacks after a

massive data breach at one of the world's biggest marketing services.

The good news for consumers is that there is no indication of any sensitive data, like Social Security Numbers (SSN) or bank account information, being stolen. But Indiana University's Center for Applied Cybersecurity Research encourages citizens to be aware of potential scams in the wake of this massive data breach.

"The concern here is that attackers, armed with knowledge of customer e-mail lists, could craft very convincing phishing emails to trick customers into revealing further personal information such as passwords or SSNs," said CACR Deputy Director Von Welch. "It's also plausible that attackers use other public information such as phone books to look up customers' phone numbers and make fraudulent phone calls."

"Phishing" emails are called just that because of their fraudulent intent to "fish" information from unsuspecting users. They may appear to be from your bank, social networking site, or an organization you belong to and even feature official-looking logos. Some common methods of attempting to obtain information include:

- Asking the recipient to call a number, at which point he or she is asked for personal information
- Threatening the closure of an account unless the recipient responds within a certain period of time
- "You've won a prize." Lottery scams are all too common and should be treated as phishing attempts

Legitimate companies should never ask for personal information via email. If you have doubts about the legitimacy of an email, contact the

customer service department of the organization who sent it to you using a phone number or email address you got from a trusted source like a phone book, paperwork from when you opened an account, or the back of a bank card.

Recipients may also receive emails with embedded links. The phishing email will ask the user to click on the link, which may appear legitimate at first glance. But hovering your mouse over the link may reveal a different destination, a clear sign that the link is not accurate. Another clever method uses "typo-squatting," or "cybersquatting." A user may be asked to click a link that looks legitimate, until a closer look reveals that the company name is misspelled. "Mircosoft" or "Micosoft" are common examples.

Fred H. Cate, director of CACR, said data like those stolen in the Epsilon data breach give attackers a better chance of succeeding.

"Phishing attacks aren't new and happen every day. However, having information like names and email addresses has the potential to support targeted phishing email messages, which IU research shows are far more likely to fool unsuspecting recipients than bulk phishing email," he said.

Even if a consumer hasn't received a notification that personal data may have been compromised, the CACR encourages all citizens to be actively alert for potential email scams.

Provided by Indiana University