

{INSERT Organization}

INSERT your  
LOGO

Monthly Security Tips

# NEWSLETTER

April 2011

Volume 6, Issue 4

## Phishing Alert – Epsilon Data Breach

### Information About the Recent Epsilon Breach

On March 30, 2011, Epsilon, a major e-mail marketing services provider, experienced a security breach that compromised the customer data of businesses that use Epsilon's service for their e-mail marketing needs. The breach affected over 90 high profile companies including Walgreens, Best Buy, Verizon, Capital One, Citibank, JP Morgan Chase, Barclaycard, Marriott, AbeBooks, Lacoste and Kroger.

Epsilon reports that while customer names and email addresses have been exposed, no sensitive personal data was compromised. In the days and months ahead, it is anticipated that spammers and cyber criminals will attempt to exploit the trusted relationships customers may have with companies that use Epsilon for their email marketing needs. Affected companies are urging users to be wary of incoming emails that ask for account updates, as they may be phishing scams. A phishing scam is a vehicle to obtain your personal data, such as credit card numbers, passwords, account data, or other information.

If you conduct business with any of the impacted firms and have provided them with your email address, you should be on the lookout for communication from these businesses providing details and information about this breach. Please note that any correspondence with affected companies should not ask you to confirm or provide personal information.

### What Can I do to be Safe?

This exposure of emails and customer names may lead to a wave of phishing attacks attempting to entice email recipients into clicking on a link that takes them to a bogus website. This website may then prompt the recipient to provide personal information such as a social security number, bank account number or credit card number, and/or it may download malicious software. Both the link and website may appear authentic, however they are not legitimate. Legitimate businesses should never ask for personal or financial information via an email that is sent to you.

While targeted phishing attacks are likely to increase as a result of this breach, it is important that users remain vigilant and understand how to recognize a phishing attack.

### How Can I Avoid Becoming a Victim?

- Be cautious about all communications you receive including those purported to be from trusted entities, and be careful when clicking links contained within those messages.
- Do not click on any links contained in suspicious email messages and do not open any attachments contained in the email. Do not respond to emails requesting personal information or that ask you to "verify your information" or to "confirm your user-id and password".
- Beware of emails that reference any consequences should you not "verify your information".
- Do not enter personal information in a pop-up screen.
- If an email appears to be a phishing communication, do not respond. Delete it. You can also forward it to the Federal Trade Commission at [spam@uce.gov](mailto:spam@uce.gov).

### Resources for More Information:

List of Companies Affected by Epsilon Breach:  
[www.bankinfosecurity.com/articles.php?art\\_id=3505](http://www.bankinfosecurity.com/articles.php?art_id=3505)

OCS Phishing Newsletter:  
[www.dhSES.ny.gov/ocs/awareness-training-events/news/2008-10.cfm](http://www.dhSES.ny.gov/ocs/awareness-training-events/news/2008-10.cfm)

FTC's Identity Theft Website:  
[www.ftc.gov/bcp/edu/microsites/idtheft](http://www.ftc.gov/bcp/edu/microsites/idtheft)

NCCIC Advisory on Targeted Phishing Attacks:  
[www.msisac.org/documents/NCCICPhishingAdvisory.pdf](http://www.msisac.org/documents/NCCICPhishingAdvisory.pdf)

AntiPhishing Work Group:  
[www.antiphishing.org](http://www.antiphishing.org)

OnGuard Online:  
[www.onguardonline.gov/phishing.html](http://www.onguardonline.gov/phishing.html)

US CERT:  
[www.us-cert.gov/cas/tips/ST04-014.html](http://www.us-cert.gov/cas/tips/ST04-014.html)

For more monthly cyber security newsletter tips, visit: [www.dhSES.ny.gov/ocs/awareness-training-events/news/](http://www.dhSES.ny.gov/ocs/awareness-training-events/news/)

*The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. **Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.***

*Brought to you by:*



**MULTI-STATE**  
Information Sharing  
& Analysis Center™

A DIVISION OF  CENTER FOR  
INTERNET SECURITY