State of West Virginia
Monthly Security Tips
NEWSLETTER

May 2011 Volume 6, Issue 5

Phishing Alert – Epsilon Data Breach

From the Desk of the West Virginia Office of Information Security and Controls
Jim Richards, Chief Information Security Officer (Jim.A.Richards@wv.gov)

Information about the recent Epsilon Breach

On March 30th, Epsilon, a major e-mail marketing services provider experienced a security breach that compromised the customer data of some of the businesses that utilize Epsilon for their e-mail marketing needs. The breach affects over 90 high profile companies including but not limited to drugstore chain Walgreens, electronics chain Best Buy, communications provider Verizon, a number of financial services companies including Capital One, Citibank, JP Morgan Chase, Barclaycard, hotel chain Marriott, bookseller AbeBooks, sports apparel dealer Lacoste and retail supermarket chain Kroger. You can view the link at the end for an up to date list of companies affected.

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. There are already websites that have appeared purporting to represent Epsilon that claim to allow people to find out if they have been affected. These are fake sites and are intended to trick individuals into downloading malicious software.

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 of their data. Please note that any correspondence with affected companies should not ask to the customer to confirm or provide any information.

What can I do to be safe?

This exposure of emails and customer names may lead to a wave of phishing attacks. Phishing is a vehicle to obtain your personal data, such as credit card numbers, passwords, account data, or other information. The scam attempts 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 social security number, bank account number or credit card number, and/or it may download malicious software onto the recipient's computer. 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 are always vigilant for phishing attacks and understand how to recognize a phishing attempt and what users can do to protect yourself and minimize the likelihood of

getting phished. The tips below will help you stay safe.

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 respond to any unsolicited (spam) incoming e-mails.
- Do not open any attachments contained in suspicious emails.
- Do not respond to an email requesting personal information or that ask you to “verify your information” or to “confirm your user-id and password”.
- Beware emails that reference any consequences should you not ‘verify your information’.
- Do not enter personal information in a pop-up screen. Providing such information may compromise your identity and increase the odds of identity theft.
- If it 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.

Resources for More Information:

1) List of Companies Affected by Epsilon Breach:
www.bankinfosecurity.com/articles.php?art_id=3505
2) MS-ISAC Newsletter on Phishing:
www.msisac.org/awareness/news/2008-10.cfm
3) FTC’s Identity Theft Website:
www.ftc.gov/bcp/edu/microsites/idtheft
4) NCCIC Advisory on Targeted Phishing Attacks:
www.msisac.org/documents/NCCICPhishingAdvisory.pdf
5) AntiPhishing Work Group:
www.antiphishing.org
6) OnGuard Online:
www.onguardonline.gov/phishing.html
7) US CERT:
www.us-cert.gov/cas/tips/ST04-014.html

Brought to you by:

For more monthly cyber security newsletter tips, visit:
http://www.technology.wv.gov/security/Pages/monthlynewsletter.aspx