Kerr, Sue [AG]

From: Greenwood, Geoff [AG]
Sent: Tuesday, April 05, 2011 1:31 PM
To: Greenwood, Geoff [AG]
Subject: Attorney General News Release: Iowans' E-Mail Accounts Exposed Following Data Security Breach

IOWA DEPARTMENT OF JUSTICE
OFFICE OF THE ATTORNEY GENERAL
Thomas J. Miller, Attorney General
www.IowaAttorneyGeneral.gov

CONTACT: Geoff Greenwood
Communications Director
515-281-6699
geoff.greenwood@iowa.gov

FOR IMMEDIATE RELEASE
April 5, 2011

Iowans' E-Mail Accounts Exposed Following Data Security Breach

(DES MOINES, Iowa) Attorney General Tom Miller cautioned Iowans to be more vigilant about potential e-mail threats, including the potential for increased phishing attacks, scams and e-mail spam, following the disclosure of what may have been one of the nation's largest confirmed personal data security breaches.

E-mail marketing provider Epsilon Data Management LLC, of Irving, Texas, which markets itself as the "world's largest permission-based e-mail marketing provider," disclosed on April 1 that "a subset of Epsilon clients' customer data were exposed by an unauthorized entry into Epsilon's e-mail system," which was "limited to e-mail addresses and/or customer names only." Epsilon claims to have more than 2,500 clients, including some of the nation's largest companies. Some clients reportedly include Citigroup, Capitol One, US Bank, JP Morgan Chase, Best Buy, The College Board, TiVo and Walgreen's.

"At this point we don't know who stole the personal data and why they stole it," Miller said. "We can only speculate about what could happen next since we don't yet have the answers. And for that reason alone, Iowans need to be very careful about responding to certain types of e-mails."

Iowans have already reported receiving notifications from Epsilon client companies, including credit card providers and retail stores. "A warning notification is a good thing, but if it's accompanied by a request for any personal or account information, that's a huge concern," Miller said. Consumers could be at risk of receiving spoofed e-mails, which mask the true sender. Consumers could also be at risk for phishing scams, which appear to be legitimate communications from a company. In these situations consumers could unwittingly provide account numbers, user names, passwords, and even Social Security numbers.

"Even if this breach results in nothing more than increased spam e-mails to consumers or, better yet, nothing at all, this is still an unacceptable security breach," Miller said. "I expect that Epsilon will fully explain what happened, how it happened and how it will never happen again."

According to computer security experts, including those at the federal Internet Crime Complaint Center, consumers can take the following preventive measures when confronted by suspicious e-mails:

Phishing & Spoofing

- Be suspicious of any unsolicited email requesting personal information.
- Avoid filling out forms in email messages that ask for personal information.
- Do not click on links or images embedded in unsolicited e-mails, as doing so can launch malicious software. Always compare the link in the email to the link that you are actually directed to.
- Log on to the official website, instead of "linking" to it from an unsolicited email.
- Contact the actual business that supposedly sent the email to verify if the email is genuine.

Credit Card Fraud

- Ensure a site is secure and reputable before providing your credit card number online.
- Don't trust a site just because it claims to be secure.
- If purchasing merchandise, ensure it is from a reputable source.
- Promptly reconcile credit card statements to avoid unauthorized charges.
- Do your research to ensure legitimacy of the individual or company.
- Beware of providing credit card information when requested through unsolicited emails.

Spam

- Don't open spam. Delete it unread.
- Never respond to spam as this will confirm to the sender that it is a "live" email address.
- Have a primary and secondary email address - one for people you know and one for all other purposes.
- Avoid giving out your email address unless you know how it will be used.
- Never purchase anything advertised through an unsolicited email.

General Tips

- Use a firewall on your computer
- Get the latest computer updates for all installed software
- Use current antivirus software and get regular updates
- Protect against social engineering attacks (phishing attacks that appear to come from friends, for example...)

# # #