Oregon Law Practice Management
Practice Management Tips for Oregon Lawyers

LinkedIn Phishing Scam

If you receive a message entitled “LinkedIn Security Notice” informing you that your LinkedIn account has been closed for lack of activity, it is a known phishing attempt.

LinkedIn Customer Support Message

Subject: Possible Phishing Attempt

Hi Beverly,

Thank you for bringing this item to our attention.

The email you mention has been identified as a fraudulent email and was not sent out by LinkedIn or anyone associated with the company. Please be cautious in opening any attached files included in these types of malicious spoof emails as they may contain Malware which could be damaging to your system. Your privacy is our top concern. We work hard to earn and keep your trust, so we adhere to the following principles to protect your privacy:

1. We will never rent or sell your personally identifiable information to third parties for marketing purposes.
2. We will never share your contact information with another user without your consent.
3. Any personally identifiable information that you provide will be secured with all industry standard protocols and technology.

I apologize for the inconvenience the malicious sender has caused.

Sincerely,

LinkedIn Privacy Team

Original Contact:

Member Comment: Beverly Michaelis 07/14/2011 11:34

I have received two emails now entitled "LinkedIn Security Notice" from Updates@linkedin.com stating:

"This automatic message is to notify you that your account at LinkedIn has been automatically disabled due to no activity for more than 3 months. Please Follow this link to review your account.
Thank you for using LinkedIn! - The LinekdIn Team http://www.linkedin.com (then the copyright symbol), LinkedIn Corporation. See attached snag of the email.

I suspected as much and contacted LinkedIn.

If you receive a potentially fraudulent email appearing to originate from LinkedIn, DO NOT CLICK ON ANY LINKS WITHIN THE EMAIL MESSAGE. Promptly notify Customer Support. Login to your LinkedIn account, scroll to the bottom of the page, and click on Help Center. In the “Get Started Here” Search box, enter “fraudulent email.” Click on the first Search result: “Possible Fraudulent Email.” At the bottom of the page you will find a link to the Privacy Department. Click on the link to complete an online contact form. If possible, save a copy of the scam e-mail and attach it to the online contact form.

Phishing scams are nothing new. It's hard to know whether reporting them does any good, but it only takes a moment of your time.

Originally published at http://oregonlawpracticemanagement.com/2011/07/14/linkedin-phishing-scam/ on July 14, 2011.