American Land Title Association
Protect your property rights

Tips to Identify Valid and Suspicious Email

March 10, 2016

While companies may have spam filters and antivirus software, spam and phishing emails can still slip through employee inboxes. Email recipients are the most critical element in preventing an attack. Here are some tips on how to identify the authenticity of a questionable email.

Incorrect Grammar/Spelling/Text Body

Many phishing email contain misspellings. Some of these messages have been poorly translated from other languages. Additionally, you will want to pay attention if the time or date appears in the message body of an email. If the email contains the date format of DD/MM/YY, 24-hour time or coordinated universal time (UTC,) it's likely that the email's point of origin generated outside of the United States.

Email Format/Absence of Logos/Plain Text Email

Most legitimate messages will be written with HTML. It should be a mix of text and images. A poorly constructed phishing email may show an absence of images. This includes the lack of the company's logo. If the body of an email is only an image as text, it's possible that it is illegitimate. Outlook blocks showing images by default. If the email is all plain text and looks different than what you're used to seeing from a frequent sender, you may want to contact the sender directly in a new email or phone call.

Urgent Request for Personal Information

One tactic that is commonly used by hackers is to alert you that you must provide and/or update your personal information about an account (e.g., Social Security number, bank account details, account password). Phishers will use this tactic to drive urgency for someone to click on a malicious URL or download an attachment aiming to infect the user's computer or steal their information.

Suspicious Attachments

High-risk attachments file types include: .exe, .scr, .zip, .com and .bat. Spam filters will generally do a good job of quarantining those formats. Most companies commonly send and receive .zip, .doc, .docx, .xls, .xlsx, .ppt, .pptx and .pdf. However, a malicious sender can implant devious code in those formats as well. Once the attachment is opened, the computer is already compromised. Take caution if you have sent an email that has an attachment and the sender is questionable. You will want to verify the legitimacy of the email first. Next, you will want to examine the context of why the attachment is being sent.

Links in the Email

A common practice is to avoid blindly clicking on links in an emails. Outlook allows you to hover over a link before clicking on it. If the link in the body of the email is different than what Outlook hovered preview reports, it is not legitimate. Even if it seems legitimate, open a new browser window and type the URL directly into the address bar. If you've clicked on a link, a phishing website will look identical to the original. However, your system may already be compromised. If you're work email is connected to your phone, you will want to take extra precaution.

Use Work Email for Work Purposes Only

Employees should avoid using their work email address for personal signups. These include social media websites or customer loyalty/ reward programs.

Copyright © 2004-2016 American Land Title Association. All rights reserved.

Reprinted with ALTA's permission.