HINSHAW

Alerts

Watch Your Domain Extensions (Who does that email REALLY come from?)

April 18, 2019
Cyber Alert

Download of PDF of the alert

Risk Management Question

How can you tell if an email—which appears to be from within a firm's own messaging system, advising the recipient that his or her information has expired or needs to be updated, and directing the recipient to click on a link to update their information—is genuine?

The Issue

Recently, several lawyers and secretaries of a law firm received an email purportedly from the firm's own "Messaging System" claiming that the recipient's email was out of date and instructing the recipient to click on a box to update his or her email.

The email was malicious. A few tell-tale signs that the message was bogus included the fact that the firm's email addresses do not go out of date. Only passwords can expire, and the firm's system was set up to alert attorneys and employees of the firm that their password was set to expire several weeks before expiration occurred. Further, the firm did not have a "Messaging System" and the email was designated as an "External email" by the firm's server.

But the real give-away was the domain extension of the sender of the email. The sender of the email in this case was located in Germany. You could tell this by looking at the sender's domain extension—in this case, .de is the domain extension used in Germany.

Risk Management Solutions

- Always check the domain extension of the sender of an email. If you move too fast you may think the extension is .com when it's really .cn which indicates the email originates in China. Be wary of anything that doesn't end in .com, .gov, .us, .law or a state domain extension like .az (for Arizona) for instance. Here is a list of foreign domain extensions to check if you ever don't recognize an extension: https://www.webopedia.com/quick_ref/topleveldomains/countrycodeA-E.asp

Attorneys

Steven M. Puiszis

Service Areas

Law Firm Cyber Alerts

Lawyers for the Profession®

- Set up your email system so that email coming from outside of the firm is tagged as "External email" and instruct employees to be cautious of all external email. In the example above, if the email had actually come from an internal "Messaging System" it would not have been designated as "External email."
- Send suspicious emails to your firm's breach inbox to have them evaluated and have the sender(s) blocked firm wide.
- As always, if you receive an email out of the blue, never click on a link or attachment. Also, if you receive an email from someone you know, but it includes an attachment you were not expecting to receive, call the sender to confirm it came from the sender and not a hacker.

Remember, let's be careful out there.