HINSHAW

Alerts

Avoid Becoming Another Hacking Statistic: A Primer on Foreign Domain Extensions

November 8, 2018
Cyber Alert

Download a PDF of the Alert

Risk Management Question: Most of my clients and contacts are located in the United States; is there an easy way to recognize emails that originate outside the U.S.? What should I do if I receive an email from a name that I recognize but the email address appears odd or is not the sender's normal address?

The Issue: Today's law firms, irrespective of their size, geographic footprint or practice group structure have become a target of hackers. While the latest hacking exploits and vulnerabilities grab the headlines, tried and true methods like phishing and social engineering are the most likely way a hacker will gain access to your network. And the reason is simple; human beings are the weakest link in a firm's cyber defenses. Malware is growing increasingly sophisticated and we are seeing major law firms with excellent security being significantly impacted by malware infections. As a result, training to recognize these threats is more important than ever. One easy way to spot potentially malicious emails is to slow down and scrutinize emails with a foreign domain extension. An email with a foreign domain extension that purports to come from someone you know in the U.S. is likely malicious.

Risk Management Solution: We have become so used to seeing emails that end with a .com, .gov, .net, or .law domain extension that we frequently gloss over an email's domain extension. Moving too quickly, we may miss that the email ends in .co rather than .com. Every country has been assigned a top-level domain extension, and the .co domain extension is assigned to Columbia. By slowing down a bit and checking the domain extension of the sender of an email, you can recognize emails that originate outside the U.S. It's not too difficult to spot a foreign domain extension. Here are few examples:

> Bob.Smith@gmail.cn - The .cn domain extension tells you the email originated in China.
>
> Bob.Smith@gmail.ru - The .ru domain extension tells you the email originated in Russia.
>
> Bob.Smith@gmail.ee - The .ee domain extension tells you the email originated in Estonia.

Attorneys

Steven M. Puiszis

Katherine G. Schnake

Service Areas

Cyber Security for Law Firms

Law Firm Cyber Alerts

Lawyers for the Profession®

Here's a handy link to a list of foreign domain extensions to keep in your back pocket should the need arise: https://www.webopedia.com/quick_ref/topleveldomains/countrycodeA-E.asp

Technology isn't foolproof and even the best technical safeguards can be compromised. Always remember to carefully check the name and domain extension of the sender of any email you receive. Treat any email with a foreign domain extension that does not match the sender's last known location as potentially malicious. And remember our three anti-phishing rules:

1. never click on any links or attachments in an email from anyone you don't know or with whom you have not done business;

2. never click on any links or attachments you were not expecting to receive even from a known sender—call the sender first and confirm he or she sent it; and

3. if you forget the first two rules and click on something which opens a dialog box asking you to a) supply additional information, b) double click to open the attachment, or c) enable a later software version, etc.—close out immediately and consider having a scan run on your computer.

Don't become another hacking statistic. Think before you click.