COWAN LIEBOWITZ & LATMAN

ON MY MIND BLOG

What to Do When the Mail Smells Phishy: Spotting and Stopping a Domain Name Scam in its Tracks

By Eric J. Shimanoff and Raphael S. Nemes

You're checking your mail and discover an official-looking notice from a "domain registration" company, notifying you that your domain name is about to expire. If that occurs, says the notice, you could lose your domain and your customers.

The notice then provides you with reassuring instructions: to keep your domain name active, simply pay a fee to the sender of the notice for a transfer or renewal of your domain. You don't recognize the name of the company that sent the notice, and wonder what to do next.

This hypothetical communication is representative of a renewal scam that appears to be increasing in frequency. How can you spot the scam? First, many domain registrars send renewal notices by email, not mail. Second, a legitimate domain renewal notice would originate from the actual domain registrar, not some unknown third party offering to renew or transfer your domain.

If you do not know the name of your registrar, you should search a Whois database for the information, or ask your web developer or attorney to find it for you. Even if a renewal notice does arrive by email and appears to be from your actual registrar, it is best practice to go directly to your registrar's authorized website to pay the renewal fee, rather than clicking on a link contained in the email.

Unfortunately, the renewal scam is not specific to domain names. We've previously written about trademark solicitation scams, in which trademark owners receive official- looking notices requesting payment for trademark monitoring services, "registration" with a private registry, recordation with U.S. Customs and Border Protection, or renewal of the trademark registration. Such notices are likely scams unless they are sent by your attorney, originate from the United States Patent and Trademark Office from its domain "uspto.gov," or originate from an official agency in another country.

One final point: be on the lookout for notices warning that a third party is about to register your trademark as a domain in another country—for example: [YourTrademark].cn—and offering you the opportunity to buy the domain first. That is usually a scam. For more information, see William M. Borchard's prior blog post regarding Chinese domain registration scams.

For further information on a domain notice that seems fishy (or phishy), please contact Eric J. Shimanoff, Raphael S. Nemes, or your CLL attorney.

Eric J. Shimanoff

Partner

Email | 212.790.9226

Eric advises on and litigates complex intellectual property matters concerning trademarks, copyrights, unfair competition, counterfeiting, domain names, false advertising, trade secrets, publicity rights, patents, the Internet, websites, social media platforms, mobile apps, content clearance, licensing and other agreements.

Raphael S. Nemes

Associate

Email | 212.790.9248

Rafi's practice focuses on intellectual property litigation and enforcement matters. He also prosecutes trademark matters before the U.S. Patent and Trademark Office.