The Royal Family Doesn't Need Your Bank Account: Neither Does the USPTO

By Elyzabeth Joy Holford

Assistant Executive Director

Resource Type: Risk eNews

Topic: Intellectual Property, Trademark and Copyright

The ability to spot a scam delivered via email, text, or voice message is key to protecting the mission, reputation, and assets of a community serving nonprofit. And one of the most important assets of any organization is its name.

I recently learned that trademark related scams are on the rise. In an August 19 post, the World Trade Review indicated that US Patent and Trademark Office (USPTO) trademark fraud claims have doubled. And on September 8, the Federal Trade Commission (FTC) published an online Consumer Advice Alert warning about the rise in scam trademark emails and calls, urging recipients to stay vigilant.

Sure enough, last week NRMC received several credible-looking emails indicating that our trademark protections with the USPTO were expiring… soon! Not surprisingly, there was a click through button promising quick and easy correction of that (fraudulent) problem. After all, there's nothing a fast click and some money can't solve for us, right? What was surprising is that, to be honest, it took more than a quick glance to recognize this email as a scam. Here are some tips from the USPTO, the FTC, and others with reminders of what to know and what to do.

- The USPTO assures us that no USPTO employee will ever ask for personal information or payment information over the phone, in an email, or text, and they do not require payment via wire transfer, gift cards, cash, check, or money order to third-party addresses.
- If you are filing your trademark, the USPTO recommends you hire an attorney with demonstrated trademark experience.
- Never share the password for your USPTO.gov account, even with someone who helps you file. If you do, your account may be used without your knowledge, including in applications and registrations that don't belong to you. This could result in your account being suspended.
    - If you hire an attorney to represent you, the attorney must have their own USPTO.gov account to file on your behalf. They do not need to file through your account. If they tell you otherwise, they are likely a scammer.
- In emails or calls, there is often a request for action or payment that's not due, and this is usually accompanied by a threat of losing your trademark rights if you don't pay. The requests are usually worded more like demands and often refer to urgent legal matters needing immediate attention.
    - USPTO timelines and fees are listed on the USPTO webpage.

- Take time to review the website and/or email address that you received. USPTO website addresses end in .gov, and emails directly from the USPTO end in @uspto.gov.
    - USPTO stands for the “United States Patent and Trademark Office.” Any variation is not part of the USPTO, such as “Patent and Trademark Bureau” or “Trademark Renewal Service” or USPTOrenewalervices.org.
- Don’t trust your caller ID. Your caller ID might show the name of the USPTO and even the same area code as the national or a regional office. It may even display their actual phone number, but caller ID can be faked.

Some of the scam topics commonly used in fraudulent trademark-related emails and calls include false change of email requests, wrongful appointment of attorney notices, assertions of fake owner addresses on applications, and claims of illegitimate signatures on submissions.

I know all of us are inundated with a daily barrage of emails. It is exhausting and the time it takes us to sort our electronic mail boxes is often limited. In addition, most of us use filters and firewalls, which can lull us into feeling that our inboxes are relatively safe. Yet, malicious emails still break through. In the interest of having safer emails, at NRMC we have added some recommendations to the above-noted cautionary advice.

We suggest you slow down and take more time with *any email that is from an unknown source*, a source you know but have never exchanged emails with, or an alleged government agency. Check carefully to see if the email address is from a legitimate site and if you are not sure, seek the opinion of others in your organization. In addition, we strongly suggest that if you receive what you believe to be a scam, you share that information internally using the appropriate organizational channels and report the attempt to any appropriate external agencies. The process for reporting trademark scams can be found here and the email they recommend for reaching out is TMScams@uspto.gov.

Elyzabeth Joy Holford is Assistant Director of the Nonprofit Risk Management Center. She enjoys applying a risk lens to the thorny challenges and questions posed by our Affiliate Members and consulting clients. Elyzabeth can be reached at 703-777-3504 or elyzabeth@nonprofitrisk.org.