PUBLICATION

Leveraging Intellectual Property to Mitigate Web Spoofing, Phishing Attacks, and other Deliberate Acts of Confusion on the Internet

Authors: Benjamin West Janke, Nicole Berkowitz Riccio
July 08, 2021

While phishing has been around for years, cybercriminals continue to become more sophisticated and their fraud schemes more robust and well-orchestrated. Website spoofing – where a cybercriminal sets up a fake website that mirrors a trusted site – is often a key component of phishing attacks. The fake website domain name may be sent to victims through email, social media, or advertising efforts to entice them to visit the site. As the user interacts with the fake website, such as by entering login credentials, the attacker harvests the user's personal information. These types of attacks occur across industries, but are particularly prevalent in the banking sector, where the attacker might use the user's credentials to steal funds from their account.

There are various security measures and other precautions that businesses can take to avoid these types of attacks. Sometimes overlooked, however, is how businesses can leverage their intellectual property to take prompt action in the face of a website cloning attack. Spoofed websites are typically accompanied by a similar domain name to the genuine site. The fake domain name might be a few characters different, contain an extra hyphen or underscore, or use a different high-level domain such as ".net" instead of ".com." There are services that businesses can employ to proactively monitor domain name infringement, which can catch these types of attacks early, potentially even before the domain name is shared with any victims. Other times the infringing domain may be identified in the course of ordinary online and social media activities or after contact from confused customers.

In some instances, companies may discover that a confusingly similar version of their brand name is registered as a website domain by a third party with no legitimate connection to the brand name. Website registrations by these infringers who seek to capitalize on the brand's popularity may not necessarily be established for nefarious purposes such as collecting protected personal information, but the use of a confusingly similar domain name to drive traffic to a competitor or to intentionally deceive customers is just as dubious, and the legitimate owner of the brand can assert its superior trademark rights against the infringing registrant.

Once the infringing domain name is identified, there are multiple avenues for recourse. Many domain providers and hosting companies are receptive to takedown notices in these types of situations. In the case of fake websites, which are usually mirror images of the original, they generally contain numerous instances of trademark and copyright infringement. Under the Digital Millennium Copyright Act (DMCA), an internet service provider notified of copyright infringement must remove or disable access to the infringing content expeditiously in order to qualify for a safe harbor from liability. The infringing conduct might also violate the providers' own terms and conditions.

Another approach, which can be used in tandem with takedown notices, is to submit a complaint under the Uniform Domain-Name Dispute-Resolution Policy (UDRP). The UDRP is an international policy followed by all domain registrars that provides for expedited administrative proceedings in instances of trademark-based domain-name disputes. If successful, the complainant is transferred the disputed domain name, at which time it also gains control over the content on the website. In order to prevail in a UDRP proceeding, a complainant must establish (1) the disputed domain is identical or confusingly similar to the complainant's trademark;

(2) the domain name registrant has no rights or legitimate interests in the domain; and (3) the domain name was registered and being used in bad faith. As a result, the UDRP process is particularly useful where the spoofed website has a domain name that is confusingly similar to the complainant's registered trademark, but it can also be used where the complainant has strong common law trademark rights and/or has strong evidence of the attacker's bad faith in registering and using the domain name. Once the complaint is filed, the registrar locks the domain name and notifies the respondent of the UDRP proceeding, after which the respondent has an opportunity to respond, and a panel issues a decision on the complaint. The filing of the complaint itself may be sufficient to get the attention of the attacker and cease the attack. If seen to conclusion, resolution of a dispute under the UDRP takes approximately 45-60 days and is generally quicker and more cost-effective than litigation.

If you have any questions or would like to learn more about how to leverage your intellectual property to prevent and mitigate web spoofing and phishing attacks, please contact Ben Janke, Nicole Berkowitz, or any member of Baker Donelson's Trademark and Branding Team.