wiley

NEWSLETTER

COVID-19 Internet Scams Are On the Rise, But Intellectual Property Rights Provide a Tool to Fight Back

May 2020

Organizations trying to navigate the unprecedented conditions caused by the global coronavirus (COVID-19) pandemic have one more thing to worry about: a barrage of opportunistic online scams seeking to exploit fears about the virus and take advantage of IT vulnerabilities related to the rapid transition many have made to teleworking and online shopping. In recent weeks, we have seen a substantial uptick in scams targeting household corporate names that have long been targets of such scams, but also targeting foundations and associations that are seeking to help members and consumers during the pandemic. The COVID-19 Internet scams generally fall into three categories: (1) email phishing scams using COVID-19 as a call to action; (2) unauthorized use of the trademarks of respected brands to provide legitimacy to fake coronavirus cures; and (3) attempts to deceive the increasing number of online shoppers into downloading viruses and malware onto their devices.

Organizations must remain vigilant in these times to protect their employees, members, and customers from becoming victims to these scams. Fortunately, there are steps that organizations can take to guard against such scams including asserting trademark and copyright claims as a means to disable the scams. And, in a bit of welcome positive news, we have noticed an increasing willingness by technical service providers to protect consumers by disabling their services when used by Internet scam artists.

The Anatomy of a COVID-19 Internet Scam

Authors

David E. Weslow
Partner
202.719.7525
dweslow@wiley.law

Ari Meltzer
Partner
202.719.7467
ameltzer@wiley.law

Practice Areas

Election Law & Government Ethics
Intellectual Property

In the first scam category, perpetrators are sending phishing emails that prey on persons seeking information about the virus or programs intended to provide assistance during the pandemic. One form of these emails purports to disseminate information about the virus from the Centers for Disease Control and Prevention and the World Health Organization, information about stimulus benefits from the U.S. Department of Treasury or the Internal Revenue Service. Emails purporting to originate from corporate managers, IT departments, or even legitimate service providers such as foundations and financial institutions will ask users to provide sensitive information, to download software, or login to an online resource to facilitate remote operations or remote access to an account. These scams can be particularly effective when the perpetrators send the emails from a typosquatted domain name that is only a letter two off from the company's legitimate domain name (e.g., "compony.com" or "conpony.com" instead of "company.com").

The second category of scam involves the use of well-known and respected brands to sell herbs, oils, and other unregulated home therapy products with vague promises of "virus defense" or worse, yet, actual purported cures and treatments for the coronavirus. These scams begin by distributing links through email and social media to fake news websites that purport to tout the benefits of the product at issue as a potential remedy for the virus. In other instances, fraudsters are claiming to sell hand sanitizer, masks, wipes, and other products—often under the guise of coming from a name brand—all designed either to steal a consumer's billing information or to enroll the consumer in a recurring charge program for fake and unreliable products. Although this scam targets consumers more than businesses, the reputational risk to companies whose marks are used to perpetuate the scams should be a concern.

The third scam category involves a proliferation of fake coupon sites that seek to capitalize on the shift from in-person to online commerce during the coronavirus response. These sites claim to offer discount codes for e-commerce, but in actuality provide links to download viruses or malware.

Tools for Monitoring for Scams and Disabling Scams

Brand abuse monitoring tools are available via subscription from specialized vendors, but free and inexpensive tools are also available online to obtain alerts for unauthorized brand uses (e.g., www.google.com/alerts) and domain name registrations (e.g., www.domaintools.com/resources/user-guides/monitors#brand-monitor). If you find that your company's name and/or trademarks are being used as part of an illicit online scam, the first step is to identify the company hosting the online content or registering the domain name at issue (in most cases, these companies merely provide hosting, registration or other services to third parties and may not be responsible for the content of the site). There are a number of free online sites, including www.whoishostingthis.com/ and www.hostingchecker.com, that will identify the host provider for any website. For domain names, the ICANN Domain Name Registration Data Lookup at https://lookup.icann.org/ will provide the name and contact information for the domain name registrar.

The next step is to file an abuse report with the hosting provider and/or domain name registrar. Although some service providers have in the past been reluctant to act in response to reports of abuse, we have found many service providers to be more responsive in recent weeks to address coronavirus-related scams.

If you have any questions or require assistance responding to an online scam, please contact one of the authors of this alert or the Wiley attorney who regularly handles your intellectual property matters.