March 19, 2020

Businesses Face Increased Risk of Cybersquatting and Fraudulent Websites Exploiting the COVID-19 Pandemic

Companies across all industries worldwide are currently being forced to examine their internal infrastructures and adjust to the ever-changing landscape created by the spread of the novel coronavirus. Under normal circumstances, cybersecurity, data protection and financial crimes are the subject of extensive defensive measures. However, as businesses adapt to the current state of affairs and employees of all levels are focused on remote work capabilities and business continuity, the opportunity is ripe for scams, fraudulent activity and phishing schemes to take advantage of unsuspecting individuals who may have let their guard down.

It is crucial to ensure that businesses remain vigilant of these ever-present risks, such as fraudulent domain name registrations and phishing schemes perpetrated from email addresses associated with these domains.

What to Watch For

A major issue is the potential for cybersquatting. Cybersquatting is the practice of registering a third party's name or trademark as a domain name to force the rightful owner to pay for the right to secure that domain name. Beyond simple pecuniary gain, cybersquatting can enable online scammers to engage in phishing schemes. In such cases, the offending party uses the deceptive domain registration to trick users into believing that a webpage connected to the domain at issue is a trusted extension of the company being impersonated. This could lead to the company's consumers falling victim to fraud, data theft or other harms, potentially exposing the company to liability or, at minimum, loss of goodwill.

Separately, and potentially more concerning, is the possibility of a company employee clicking on a link provided in an e-mail that is masked to appear as though it originated internally, exposing the company's systems to viruses or access by a third-party bad actor.

What You Can Do

Businesses must be on the lookout for these nefarious practices and alert their employees and customers to the increased risk of fraudulent websites operating under the guise of an authentic company website. Areas likely to be exploited include health and benefits information, tech support, new "virtual" service offerings, and corporate communications relating to the coronavirus pandemic.

Businesses also should monitor activity online to learn quickly of any potentially infringing domain names, using internal resources or a trademark watch service.

Should such a scheme target your business, there are steps you can take to protect your company and employees. If you learn that a third party has registered a domain containing any of your proprietary trademarks and generic terms relating to the current environment (e.g., CORONAVIRUS, COVID19, VACCINE, PANDEMIC, EMERGENCY), or you receive e-mails from such domains, the first step is to instruct employees not to reply to the e-mails or click on any links provided therein.

A reasonable next step would be to contact that domain's Internet service providers (ISPs), including the registrar or host server. A demand letter to the ISP would set forth your company's existing brand rights, request that the ISP take down any infringing content on a resulting webpage, and terminate service to any e-mail addresses associated with the offending registration.

Lastly, it may be necessary to file a complaint through the Uniform Domain-Name Dispute-Resolution Policy (UDRP), seeking transfer of the offending domain if there is evidence that the registrant registered and used it in bad faith.

Going Forward

As industries continue to adapt to rapidly changing conditions and shift focus to other pressing concerns, we are committed to monitoring the situation for noteworthy developments that may affect our clients. We recommend that companies remain watchful for any fraudulent behavior, and consult with counsel immediately upon discovery to take necessary action to prevent further harm. We are also pleased to discuss defensive measures – such as advance registration of domain names and trademark watch services – that businesses may wish to take now to preempt any fraudulent action occurring from these offending domains.

Legal extern Adam Weisman, University of New Hampshire School of Law 2020, contributed to this alert.

For more Day Pitney alerts and articles related to the impact of COVID-19, as well as information from other reliable sources, please visit our COVID-19 Resource Center.

COVID-19 DISCLAIMER: As you are aware, as a result of the COVID-19 pandemic, things are changing quickly and the effect, enforceability and interpretation of laws may be affected by future events. The material set forth in this document is not an unequivocal statement of law, but instead represents our best interpretation of where things stand as of the date of first publication. We have not attempted to address the potential impacts of all local, state and federal orders that may have been issued in response to the COVID-19 pandemic.

Authors

Alex P. Garens

Partner

Boston, MA | (617) 345-4872

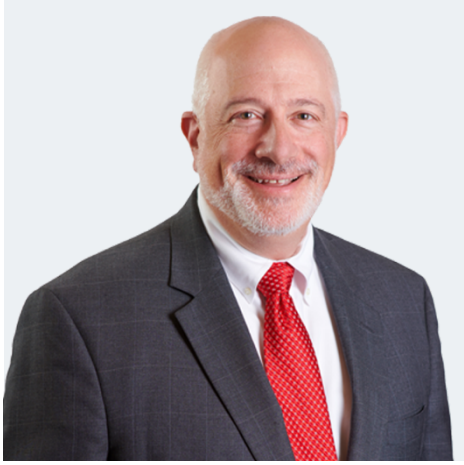
agarens@daypitney.com

Carrie Webb Olson

Partner

Boston, MA | (617) 345-4767

colson@daypitney.com



Richard D. Harris

Partner

Hartford, CT | (860) 275-0294

New Haven, CT | (203) 752-5094

rdharris@daypitney.com