DORSEY
DORSEY+WHITNEY LLP

Forestall Phishing Forays with Sophisticated Domain Name Watching

December 9, 2022 – The TMCA
by Breanne Wernars and Jamie Nafziger

With the holiday season upon us and online goods and services flying off the virtual shelves, companies should not lose sight of the increased risk of phishing and cyberattacks. Society's reliance on online commerce means businesses are under immense pressure to ensure their website domain names provide a safe destination for customers. To do so, they must prevent attacks on themselves and their customers. Sophisticated domain name watching can provide an early warning of phishing attacks about to happen.

According to a 2021 study from IRONSCALES, 81% of organizations around the world have experienced an increase in email phishing attacks since March 2020.[1] Further, domain name registry Identity Digital recently reported that 92.9% of all of its abuse claims for Q2 2022 were related to phishing attacks.[2]

Due to advancing technology and the expansion of allowable characters which can be used in domain names, cyber attackers are now running sophisticated phishing schemes which are not only focused on the technologically-illiterate. See The Top 5 Phishing Scams of all Time - Check Point Software.

Domain name fraud is being used to trick employees, customers, and business owners alike.

1. Cybersquatting

Cybersquatting occurs when an attacker purchases a domain name featuring a brand's name and/or trademark and uses it for illegitimate purposes.

Related People

- Breanne Wernars

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

1. Typosquatting

Typosquatting is a form of cybersquatting in which an attacker purchases a domain name which contains typos or slight discrepancies from a legitimate brand.

Ex: D0rsey.com; Dorseylawfirm.com

1. Homoglyph Attacks

Homoglyph (sometimes referred to as Homograph) attacks occur when an attacker takes advantage of the similarity between certain characters in Latin and non-Latin alphabets (such as Cyrillic and Greek) to register domain names which appear identical or very similar to the domain name of the legitimate brand.

Ex: example.com vs. exɑmple.com

Once these fraudulent domain names are registered, attackers can set up fake websites and/or email addresses to impersonate brands and fool customers into trusting them. Often these fraudulent emails are used to entice unsuspecting users to transfer funds or interact with links which can result in data breaches or malware attacks.

To proactively halt these attacks before they happen, companies can implement domain name watch services (including typosquatting and homoglyph watches) to alert them when a domain name is registered which may be of concern.

For further information regarding how brand owners can implement good domain name practices to protect their brands, please see Jamie Nafziger's article, Deepfakes, Fake News & Viral Hoaxes: How Good Domain Name Practices Can Help Prevent Truth Decay.