Defending Your Brands Against Cybersquatters

Posted on December 27, 2017

In October 2009, Michael Bosman, a California resident, registered worldwrestlingfederation.com with Melbourne IT, a domain name registrar in Australia. Three days later, he tried to sell the name to the World Wrestling Federation Entertainment Inc. (WWF) for a huge profit.

That December, The World Intellectual Property Organization (WIPO), a United Nations agency, began implementing procedures for settling domain name dispute cases specific to the misuse of existing registered trademarks. The WWF bought forth their case and the independent panelist of WIPO judged Bosman's transaction to have been made in bad faith. It was decided that "The domain name he registered is identical or confusingly similar to the trademark and service mark of the WWF, and that he has no rights or legitimate interests in the name and the domain name was taken with a malicious intent." Hence, Bosman was asked to transfer the domain name back to WWF. This was the first case of cybersquatting settled by WIPO and the beginning of hundreds & thousands more to come as businesses slowly started realizing the use of technology and started wanting to create their place in the world of the Internet.

Importance of online brand

The ease & gigantic potential that the Internet provides to businesses to expand their reach amongst their customers and tap markets that traditionally would have required way too much effort & resources is definitely remarkable. Being present on the Web via their websites has become a cornerstone for businesses to create brand awareness, showcase their products & service and also for selling their offerings directly online. And with each passing day, people are beginning to rely more and more on this virtual presence of brands and are increasingly interacting with them.

Domain names to that effect have become a very critical component for expanding and building a brand identity as well as enhancing its reputation online. And just like any valuable asset in plain sight, there are a lot of bad guys who either want to cause harm or exploit your brand’s potential for their own benefit. Which is of course not great news for you!

Cybersquatting started of being broadly defined as the practice of registering a domain name with the intention of profiting from the resale of the name. Since then until now cybersquatters have gotten only more innovative and found loopholes to make monies with domain names. Cybersquatting or domain squatting in 2017 can be classified into different types so as to draw clarity on what is legally allowed and what is not.

Typosquatting: Typosquatting is often referred to as ‘URL hijacking,’ ‘a sting site,’ and a ‘fake URL.’ A typosquatter is a person who registers domain names with common typos of major domain names to attempt to divert traffic to sites that benefit the registrant. Such mistakes include misspelling and different phrasing of a domain name. More advanced typosquatting techniques exploit the visual or sound similarities of trademarks. To trick internet users, typosquatters may also create a fake website that resembles the original by using a similar layout, color schemes, logos, and content.

Top-level domain swapping: By simply changing a .com domain name to a separate TLD domain such as .org, or .net, malicious entities try to compel legitimate website owners to buy the cybersquatted domain names, generate more web traffic, or sometimes even spread malware.

Identity theft: Cybersquatters may purchase a domain which was unintentionally not renewed by the previous owner. Cybersquatters use special software applications which allow them to monitor the expiration dates of targeted domain names easily. After registering the expired domain names they can either imitate your website to make your site’s visitors believe that the cybersquatter is you, or perhaps worse redirect them to the site or advertisements that contain your competitor’s products or services.

Name jacking: Name jacking refers to the registration of a domain name associated with the name of an individual, usually celebrities and well-known public figures. Name jackers benefit from web traffic related to the targeted individuals.

Reverse cybersquatting: This is the practice of brand owners attempting to secure a domain name legally owned by another person and who is not otherwise a cybersquatter. A brand owner may claim that they own the rights to your domain, and threaten legal action unless you transfer that domain over to them.

While anyone who is a victim to any of these case of cybersquatting can resort to legal measures to protect themselves and their trademarks, it's essential that one tries to prevent such scenarios. The solution is quite simple. Pre-empt the cybersquatter by registering as many variations of your own domain name as possible & following these simple steps before:

- Today there are many variations other than .com. So register .net, .org, .biz, and any other variation you think a cybersquatter might abuse.
- Register hyphenated variation of the domain name
- Register your domain name in both its singular and plural forms.
- Misspelling is very common. Cybersquatters will take advantage of this. So register all possible misspellings before they do.
- Pre-empt and outsmart the cybersquatters & haters by registering abuse variation before they do.

This might seem excessive and maybe even expensive. However, when you consider the costs of legal actions or the ransoms that you'll have to pay, paying some dollars for purchasing these domain names becomes a no-brainer.

Besides this, Brand and Trademark monitoring services take care of the demanding and slightly overwhelming task of protecting your brand online by preventing domain name and trademark hijacking, enforcing action against counterfeit websites and maintaining your overall brand reputation.

WhoisXmlApi has many API products such as Brand Alert API & Registrant Alert API that can help keep your brands safe. Besides that, our Domain Research Suite (DRS) provides an online web app that helps you research & monitor domains. Stay a step ahead of such nefarious entities and ensure your brand reputation is not hampered!

Do write to us at support@whoisxmlapi.com to know more about how you can safeguard your brand online.