Safenames

Domain Blocking 101

What is Domain Blocking?

Luckily, a new method of protecting your brand has arisen, known as “Domain Blocking.” Domain Blocking is a new form of brand protection which involves registering dormant domain names in order to prevent anyone else from registering or using them.

Domain Blocking is a defensive measure which businesses can use to protect a trademark from abuse. Domain blocking itself is a very simple concept. Theoretically you could do something similar manually by registering a copy of your trademark, or variation of your trademark across each gTLD, however many services exist which will handle most of the process for you at the moment you register your brand. Domain blocking is slightly different than registering a domain, as it will not resolve to a site, but instead will simply block anyone else from registering it, thereby protecting against its fraudulent use

Why Domain Blocking Exists

In 2011, ICANN approved the use of the .xxx gTLD for the adult entertainment industry. The goal of this was to create a clear sanctioned area where such sites could exist but not intrude upon traffic designed for broader audiences. However, an immediate concern arose, as it became apparent that it could be possible to register any brand with this extension. Many companies were concerned that pornographic websites could attempt to register well-known brand names so as to gain traffic but resulting in a deleterious impact on the integrity of these trademarks.

Simply registering these domains themselves was also not considered ideal, because many companies really did not want to have ownership in anything related to the adult entertainment business.

To provide a service to prevent popular brands from having (likely fraudulent) sites crop up with well-established trademarks, the ICM registry allowed owners of trademarks to opt out having one of these TLDs.

The need for this soon spread beyond the original .xxx gTLD. The growth of new gTLDs with a large variety of extensions created a wide new frontier for abuse. There are now more than 1500 different domain extensions available. These range from the well known .com and .net domains, to .biz, .ninja, .guitar, to .lol. The need to make sure that these domains do not get registered by nefarious operators is complex and great. Cybercriminals have and will take advantage of these gTLDs to their own advantage. Each month, over 150 different brands are hijacked through phishing attacks.

As a result, beyond ICM, many registry operators (RO) such as Uniregistry and Enom now provide new methods and mechanisms to help companies prevent criminals to take advantage of these vulnerabilities, and will now provide this or a similar service for a wide range of different TLDs. By registering a domain with one TLD, a company can place a block on any new registrations for a period of time with that same trademark.

Cost of Cybercrime

The pervasiveness and sophistication of cybercrime has grown exponentially in recent years. The global cost of cybercrime has now reached as much as $600 billion annually. While in the past most phishing attempts may have seemed laughable in their amateurism, this is no longer the case.

Individuals and businesses are being taken advantage of at a record pace, and the nature of these phishing attempts are getting harder to detect, even for professionals. Spoofing legitimate domains used to be protectable by registering the .net and .org and maybe a few other TLDs, however it has gotten considerably more complicated.

ICANN has recently introduced over 1,500 new gTLDs, while this is a huge boon for many businesses looking to carve out a niche, this unfortunately also creates a wide open playing field for cybercriminals to register domains that look just like your meticulously built brand.

Cybercriminals are becoming more and more sophisticated Cyber crime is the only criminal enterprise with a 'help desk!'

Because everyone is using the same playing field, we all have access to the same tools. If we have a problem, we can simply contact our ISP to solve it. Unfortunately, so can a criminal.

On top of it, there are a number of organizations that cater specifically to criminal operations.

With more sophisticated phishing attacks, even experienced professionals are being taken in. Due to the open nature of HTML and CSS, it is easy for criminals to create sites and emails that not only look similar to official sites, but that look *identical*, even including legitimate links.

It has now even become common for fraudulent sites to hold legitimate security certificates. Providers such as Let's Encrypt make it possible to get SSL certificates for no cost. This is a huge benefit for small businesses who wish to be able to participate online, and to provide secure experiences to their customers However the downside is that sites like this have no mechanism to check if certificates are legitimate or should be given. The result is that we may not even necessarily be sure that a site which is fully set up with SSL, and where everything matches the certificate, is actually a legitimate site. Hackers have misused Let's Encrypt certificates to help hide malicious websites to make them appear as if they are affiliated with legitimate companies such as Apple, Google, and PayPal. In fact, recent research has shown that up to half of all phishing sites now have the "secure lock" symbol that people associate with a safe site.

Homoglyphs, Homograph Attacks, and Confusable Characters

Further complicating this problem is the introduction of Internationalised Domain Names, or IDNs. IDNs can serve the positive purpose of making a brand accessible in non-standard character sets. While we may be used to using a standard western (Latin) library, many of the characters we use are not easily accessible to users who use a different alphabet. For this reason a need was addressed by allowing characters from non-western libraries to be used as domain names.
However, many letters in different alphabets may look similar but are not, in fact the same character at the encoding level. While we have trained ourselves to be able to identify phishing scams with numbers replaced as letters (O and 0), it can be very difficult to identify differences in some alphabets. In many cases, the symbol appears virtually identical to letters we already expecting to see.

Let's take apple.com as an example. We see the letter "a" as part of this domain, and of course, we believe that by looking at this on a page, or in a link in an email we are going to be taken to Apple's website. However, while this character has a Unicode entry for U+0061 in the Latin alphabet, if someone chooses to replace this character with the identical symbol in the Cyrillic alphabet, it has a Unicode entry for U+0430. Clicking on a link for this would bring you to an entirely different location. This is only one example, and there are a ton of substitutions that could be made that would be invisible to the naked eye.

Due to the creation of IDNs, it is now possible to register domains in pretty much any character set that exists. You can see the problem here: if a cybercriminal were to register a domain which looks similar, or in some cases identical, even if we are being careful, it could be very easy to fall for a phishing attack.

Safenames

So How Do You Respond?

This problem is not going to go away, and as new tools become available for criminals they will be used. Companies and brands are now starting to take a holistic approach to mitigate the risks associated with domain name infringement, and are now innovating to provide protection for consumers at the forefront of those their plans for maintaining customer trust and loyalty. It can be difficult for companies to navigate the landscape of possible domains and parameters to consider. Before getting too deep into details, it's often helpful to take a high-level approach to begin to create a strategy. Here are a few questions that brands can/should consider:

- What is the best way to maximise impact and reach of your domain portfolio? Do you want to consider international factors?
- Of the new gTLDs available, which are worth registering? Which are most relevant to your brand? Think about which target markets might be interested in your products. Remember, if you don't anticipate this, someone else might step in and use your name for their own purposes.
- Similarly, using the same logic, which TLDs may have the greatest potential risk for abuse?
- Is there a way you can think of these as categories, or groupings of areas of interest? You may wish to consolidate your portfolio to ensure it meets your objectives in an effective way, both for market reach and for expense.
- How can you meet each of these objectives while staying within budget? If you can identify these areas, bulk domain purchasing/blocking may be an ideal solution.

Who Should Use Domain Blocking?

Trademarks are extremely valuable brand assets. When making purchases or doing business, we have associations with specific brands as being reliable or trustworthy. Maintaining control of that image is absolutely crucial for any business with any sort of brand recognition. Losing control of this can be disastrous. While we can think of may examples of brand names that are synonymous with a product, beyond its original ownership (e.g. Coke, Kleenex, Xerox, Aspirin), we can also think of names that are synonymous with poor quality or disasters (e.g. Edsel).

While of course some of this is controlled only by public opinion, much of this association is controlled by the company itself. For this reason, it is extremely important to make sure that our trademarks do not get into the hands of those who do not have our best interests at heart.

While we may think of this as obvious for official brands, this can expand beyond the commercial realm. Well-known people, celebrities, and politicians all trade heavily off their names. Once one gets into the public eye, it's easy for one's name to become smeared.

Often a trademark may be limited to one particular country – if someone gets ahold of it in a country that does not adhere to the same rules of commerce, this can cause problems for those who have a legitimate right to the name.

Copyright is something else that may need enforcement. This can be particularly difficult to manage if this crosses national borders, however the right to credit for written materials, names or other content remains.

We also use domain blocking for other important events such as treaties and statutes (remember that cybercriminals will go after just about anything that the public might search for).

Alternatives to Domain Blocking

There are a few other approaches one could take instead of adopting domain blocking services; however, each comes with its own drawbacks.

One could theoretically do nothing. After all, at least within most western countries there are agreements regarding trademarks. Unfortunately, enforcement after the fact can be extremely problematic. Entering UDRP and URS proceedings each time a trademark is violated can be costly and time consuming. Also, due to the nature of the way that brands work, and are registered in people's minds, the damage could have already been done by the time the problem has been resolved. We can think of many examples of companies that ran into trouble at one time, and though they fixed the problems, in the public mind this company is forever associated with these negative experiences (I won't go into examples here out of respect for these businesses). In general, it is far better to put the expense and protection in before a problem arises.

Another approach, as we have mentioned before, it is that it is always possible to manually register all TLDs that are associated with your brand or trademark. However, this can have the drawback of being both painstakingly difficult, costly and inefficient. If one were to factor in the expense of purchasing each domain at retail price and the amount of time it would take, the cost begins to weigh heavily on the benefit. Also, by using this approach it is very easy to miss variants or "lookalike" characters from other alphabets.

Add to this fact that with the next round of ICANN's new gTLD programs, you would need to anticipate gTLDs that don't even exist yet, which is, of course, a virtual impossibility. By choosing Domain Blocking as a service, all of this is handled for you. A name is registered, and any attempts to duplicate this across different TLDs gets blocked, including many variants.

Domain name blocking can be used for any brand or trademark owners. The process simplifies and consolidate blocks of names and similar names, to make it easier to understand and purchase. Whether we like it or not, most new TLDs have open registration policies, meaning that anyone can register a domain without proof of ownership. By choosing Domain Blocking, brand owners can be prepared and can adapt strategies for dealing with the growing TLD landscape.

Safenames

Can You Ever Be Fully Protected?

The short and honest answer to this question is, unfortunately, no, or not if we want to continue to live in an open society where business itself is possible. However, from the perspective of domain infringement, we can make a good faith effort to mostly protecting ourselves and our consumers.

Theoretically, we could block every single gTLD and variant, including all homoglyphs or confusable characters, however, it is of course impossible to think of every possible situation one could take advantage of consumer trust. Our approach is instead that we make every step to limit potential damage, so long as it remains on the positive side of the cost-benefit equation.

Cyber criminals are continually evolving, and we will always be playing some sort of cat and mouse game to stay ahead or at least keep up. We are often behind in these battles, as it is impossible to go after a criminal until after a crime has been committed. However, if we focus on defense, we can anticipate many ways that someone might try to take advantage, and bend the cost-benefit for the criminals into negative territory. In other words, we can make it so difficult for them that it is not worth their while to try most attacks.

We can minimise any risks to our brand assets by adopting a solid domain name management strategy, through the use of efficient and effect domain blocking techniques, and to remove at least the most obvious types of phishing attacks on our brands.

Conclusions/Recommendations

Trademark infringement is on the rise. Cybercriminals are reaching levels of sophistication which match many of the businesses and organizations they target. Tools which have been designed to make business easier have unfortunately made it easier for bad actors to take advantage of them. The features of the web that make it so appealing to you as a business are precisely the same as those that drive bad actors to try and take advantage of your name.

However, you are not without the ability to fight back. To do so requires the adoption of domain blocking strategies, not just as a luxury, but as an absolute necessity. If you have any sort of brand name or trademark or reputation that needs to be maintained, domain blocking should be considered a necessary component of your online strategies. It is important to understand that the more well-known your name, the more valuable it is, the more likely it will be attacked, and therefore the greater the importance of protecting it.

Guarding your brand is also not just about acting proactively to counter threats, it can be part of your marketing strategy. Being in control over your name breeds an aura of professionalism which will in turn increase customer trust and loyalty.

If you have the right tools in place, including a careful domain blocking strategy which includes all relevant (and possibly non-relevant) gTLDs, a recognition and control over homoglyph, lookalike and other possible variations and spellings of your brand, you will be in a much stronger place in maintaining your integrity.

By taking care of this proactively, before any problems occur, you will save both any potential losses as a result of stolen identity and customers (not to mention your customer's identities!) but will also save money, both in the cost of obtaining these TLDs, as well as any time that could be lost in trying to fix problems after the fact. Using pioneering technology, you can adopt complex strategies to quickly block domains in the thousands before they are even in the mind of a criminal. By securing these names, you are cutting off the supply chain that cybercriminals would use; you effectively corner the market on your own trademark.

Safenames