Domain Blocking 101

AdultBløck
Protect your brand in the adult space

ICM REGISTRY

Domain Blocking 101

You've spent years cultivating your brand.
You have a name that your customers recognise.

The time spent cultivating your image over the years has paid off. When people see your trademark, they think "integrity" and a quality product. This is a great thing. However, as it has been said, with great visibility comes great risk. The more well-known your brand, the greater your reputation, the higher the likelihood that someone may attempt to take advantage of this image.

A tremendous amount of money is made (read: lost) every year due to criminals taking advantage of public confusion. If cybercriminals believe they can gain by illicitly using your name, they will.
While in the past one only needed to worry about the dotCOM, dotNET, dotORG, and associated country level TLDs, with the creation of hundreds of new generic Top-Level Domains (gTLDs) it is now easier for someone to purchase a domain that is the same as your trademark, or similar enough to cause confusion to the public.

As a business, it is in your interest to ensure you are not impersonated. Fraud is not only bad for your customers who may get swindled but also for your company in lost revenue and reputation.

Whether or not it is technically "your fault" that someone used your name for nefarious purposes, it comes across as unprofessional that you would allow this to occur (yes, I know it's not fair, but that's just the way it goes), and your brand can suffer a hit to its reputation.

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 that involves blocking the ability to register a domain name and in turn, prevents unauthorised usage.

It 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 by manually registering a domain name that matches your trademark or a variation of your trademark across each gTLD. However, services now exist that will handle the process for you.

Domain blocking is slightly different than registering a domain as the blocked name will not resolve to a working website. Instead, it will simply prevent anyone else from registering it and thereby, protect the trademark against fraudulent use.

Why Domain Blocking Exists

In 2011, ICANN approved dotXXX for use in the adult entertainment industry. The goal was to create a sanctioned area where such sites could exist but not intrude upon traffic designed for broader audiences. However, an immediate concern arose, when a trademark could be registered in this extension. Many companies were concerned that bad actors could register well-known brand names to gain traffic, resulting in a deleterious impact on the integrity of affected trademarks. Simply registering these domains was also not considered ideal because many companies did not want to associate their brand with the adult entertainment business.

To provide a service that would prevent the creation of likely fraudulent websites using well-established trademarks, ICM Registry allowed owners of trademarks to block or opt-out of allowing the registration of their marks in the dotXXX TLD.

The need for this soon spread beyond the original dotXXX TLD. The introduction of new gTLDs, with over 1,500 domain extensions now available, created new opportunities for abuse. These range from the well-known dotCOM and dotNET domains to dotVIP, dotSEX and dotPORN. The need to make sure that these domains do not get registered by nefarious operators is paramount.

Cybercriminals use new gTLDs to their own advantage. Each month over 150 different brands are hijacked through phishing attacks.

As a result, registry operators such as ICM Registry and Donuts Inc. now provide new methods and mechanisms to help companies prevent criminals from taking advantage of these vulnerabilities. A company that signs up for the service can place a block on any new registrations for a period of time using the same trademark.

Cost of Cybercrime

Cybercriminals are becoming more and more sophisticated. Cybercrime is the only criminal enterprise with a '*help desk*!'

The pervasiveness and sophistication of cybercrime has grown exponentially in recent years. In fact, the global cost of cybercrime has now reached almost $600 billion annually. While in the past, most phishing attempts may have seemed laughable in their amateurism, this is no longer the case. Coronavirus has led to a surge in malicious campaigns as people who are desperate to protect their families visit cleverly disguised websites and fake news websites to drive their deceptive ploys.

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 dotNET and dotORG and maybe a few other TLDs however, it has become 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, that has unfortunately created a wide-open playing field for cybercriminals to register domains that look just like your meticulously built brand.

Everyone is on the same level playing field and has 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 such as the Russian Business Network.

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 at no cost. This is a huge benefit for small businesses who want to provide secure experiences to their customers however, the downside is that sites like this have no mechanism to ensure certificates are legitimate or ought to be granted. The result is that we may not even necessarily be sure that a site with SSL, and details that match the certificate, is actually a legitimate site. Hackers have misused encryption certificates to help hide malicious websites so they 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 the same character at the encoding level. While we have trained ourselves to be able to identify phishing scams with letters replaced as numbers (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 expect to see.

Let's take apple.com as an example. We see the letter "a" as part of this domain and 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 ('a'), if someone chooses to replace this character with the identical symbol in the Cyrillic alphabet, it has a Unicode entry for U+0430 ('а'). Clicking on the link would bring you to an entirely different location. This is only one example with an abundance of other substitutions that are 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 easily discern the problem if a cybercriminal were to register a domain that looks similar, or almost identical, we could easily fall prey to a phishing attack even if we are being careful.

So how do you respond?

This problem is not going to disappear as criminals continue to exploit the latest tools.

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 create a proactive strategy. A few questions that brands 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 illicit purposes.*
- *Using the same logic, which TLDs 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 terms of market reach and expense.*
- *How can you meet each of these objectives while staying within budget?*
- *If you can identify these areas, bulk domain blocking may be an ideal solution.*

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 legal 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 may have already been done by the time the problem has been resolved. There are plenty of examples of companies that ran into trouble at one time, and although they fixed the problem, in the public's mind the company is forever associated with these negative experiences (examples have been omitted out of respect for these businesses). In general, it is far better to put protection in place before a problem arises.

Another approach, as mentioned previously, is to manually register all TLDs that are associated with your brand or trademark. However, this approach is often difficult, costly and inefficient. If one were to factor in the expense of purchasing each domain name at a retail price and the amount of time it would take, the costs begin to weigh heavily against the benefits. Also, using this approach, it is very easy to miss variants or "look-alike" characters from other alphabets.

By choosing a domain blocking service all of this is handled for you. A name is registered, and any attempts to duplicate the label across different TLDs is blocked, including many variants. Additionally, domain name blocking can be used by any trademark owner. The process simplifies and consolidates blocks of names including similar names, all in one transaction. 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 have a strategy for dealing with the growing TLD landscape.

Who should use Domain Blocking?

Trademarks are extremely valuable brand assets. When making purchases or conducting 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. This is as important for smaller brands as it is for large brands. While lesser-known brands may not be targeted at the same rate that well-known international brands are, the impact of being impersonated can have devastating effects on the survival of the business. For this reason, it is absolutely crucial for companies of all sizes to consider domain blocking as a central part of their defensive marketing strategies.

The need for domain blocking also expands beyond the commercial realm. Well-known people, celebrities and politicians all trade heavily off their names. Once a person is in the public eye, it's easy for their name to become a target.

Artists, writers and other creative individuals also have a vested interest in their name or works. For this reason, it's important to consider copyright as another aspect that may need protection. This can be particularly difficult to manage if it crosses international borders. Often a trademark or copyright 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 issues for those who have a legitimate rights to the name. Domain blocking can help reduce this risk.

The right to credit written materials, names or other content remains. If someone in another country has the ability to take your name, not only can this hurt your reputation, it can directly impact sales. If you want to prevent your identity from being falsely tarnished, it's best to have a solid domain blocking plan in place.

To sum up, if you can imagine that someone would be interested in your brand, name, ideas, creative property, or more, then you are absolutely a candidate to use domain blocking.

Can you ever be fully protected?

The short and honest answer to this question is, unfortunately, no. It's not possible 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 focus on those efforts that protect ourselves and our consumers.

Theoretically, we could block every single gTLD and variant, including all homoglyphs and confusing characters. However, it is impossible to think of every possible situation where one could take advantage of consumer trust. Our approach is to limit the potential damage as long as it remains on the positive side of the cost-benefit equation.

Cyber criminals are continually evolving, requiring more effort 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, a proactive defense can alter the cost-benefit equation and push the criminals into a negative return territory. In other words, by making it more difficult, it is not worth their time and effort and instead focus on easier targets.

We can minimise risks to brands by adopting a solid domain name management strategy, through the use of effective domain blocking techniques to remove the most obvious types of phishing attacks.

Conclusions/ Recommendations

Trademark infringement is on the rise.
Cybercriminals are becoming more sophiticated in their efforts often matching the businesses and organizations they target.

Tools which have been designed to help make business easier have unfortunately, made it easier for bad actors to utilise. The benefits of the Internet to your business are precisely the same as those that entice bad actors.

However, you have 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 a brand name, trademark or reputation that needs to be maintained, domain blocking should be considered an essential component of your online strategy. It is important to understand that the more well-known your name becomes, 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 counter acting threats, it can be part of your marketing strategy. Having control over your name breeds an aura of professionalism that increases customer trust and loyalty.

By having a comprehensive domain strategy that includes all relevant (and possibly non-relevant) gTLDs, attention to homoglyphs and spellings variations of your brand, you will be in a much stronger position to protect your brands integrity online.

By taking a proactive approach, before any issues arise, you will prevent potential losses as a result of stolen identities and customers, not to mention your customer's identities! It will also save money, both in the cost of recovering, as well as time lost in fixing problems after the fact. Using pioneering technology allows you to adopt complex strategies to quickly block thousands of domains before they even enter into the minds of criminals. By securing these names, you are effectively cutting off the supply chain that cybercriminals utilize enabling you to effectively corner the market on your own trademark.

Want to know more?

For more information please visit http://adultblock.adult

Email us at support@icmregistry.com

AdultBlock
Protect your brand in the adult space

ICM REGISTRY