



# Digital brand protection hazards blog post

*Author: Stéphane Bréaz*



*Feedgenic, the content management intelligence company*

## DIGITAL BRAND PROTECTION HAZARDS BLOG POST

Author: Stéphane Brélaz

### Table of content

- ⇒ Do you want to stay in business?
- ⇒ Online ad and brand protection
- ⇒ Cybersquatting
- ⇒ Typosquatting
- ⇒ The hazards of spoofing and phishing
- ⇒ Trademarks and domain names
- ⇒ Sunrise and trademarks
- ⇒ Strategies regarding Asia
- ⇒ Image certificates and digital brand protection
- ⇒ Developers around the globe
- ⇒ An efficient brand and fraud protection program
- ⇒ Comprehensive communication policy
- ⇒ Preventive monitoring
- ⇒ Monitoring the digital world
- ⇒ When too much protection damages the business
- ⇒ In a few words...



[www.feedgenic.com/blog](http://www.feedgenic.com/blog)

### Do you want to stay in business?

Are any of you worried about the diluting value of far-away digital brand fraudsters and the havoc they can cause with your company's value brand?

What do we all strive for in business, whether it is on TV, radio, film, and of course now the Internet? I'll tell you, we WANT that consumer (customer) to have a burning desire for our product, a "must-have" item, that gives them status in the real world, and they can show off to all their friends. Whether it is digital phones, I Pods, the latest hot musical group, business is driven by the hot commodities.

But, what happens when digital fraudsters come between you and your brand? Your company presence on the Internet – your unique product. Frankly, the miracle of the Internet is far-reaching and overwhelmingly valuable, but are your customers ever confused during their attempts to reach you?

I'd like to discuss some issues that are now common with the Internet, and the inevitable cyber opportunists, and how they will affect your all-important brand. Being aware of these issues will help you sail above these problems, and keep the paychecks and profits flowing.

When it comes to brand protection, you cannot be careful enough, many usurpers want to rise up and steal your good name, your customers, and your livelihood. How to protect against this? I recommend that you take fast action to prevent the cyber cheaters from diluting your brand value.

Here's some of the methods these cheaters will use to hurt your company:



[www.feedgenic.com/blog](http://www.feedgenic.com/blog)

## **Online ads & brand protection**

Sponsored e-positioning with keyword based ad networks like Google Adwords, Yahoo! Search Marketing or Microsoft Ad Centre has given rise to a common practice where some players, usually smaller ones, are using the market leader's well recognised brand names and trademarks as keywords for their own Cost Per Click (CPC) campaigns - driving potential customers to their own website. The geo-localization features of the modern digital advertising platforms offer the advertiser the possibility to limit the ad display to specific countries, languages or even city areas making it increasingly complex to monitor such behavior.

With this technique, competitors in the same industry are attempting to capture part of the market leader's revenue by selling similar services or products or by selling or promoting fake copies or low quality versions of the same type of products. It is easy to find some examples of this just by googling well known company names or brands.

Competitors in different industries are also attempting to use well recognised brands & trademarks to drive traffic to their own website. This practice is commonly used by, but is not limited to, the porn industry. I have recently seen that one of the largest car manufacturers in Europe has its name associated to domain names including porn related keywords.



## Cybersquatting

Cybersquatting is probably the most well known and established issue applying to digital brand protection. This is when business entities or individuals purchasing country level domains (feedgenic.ch) and global top level domain names (feedgenic.com) corresponding to well known brands & trademarks. They do this for the possibility of riches, with some websites selling for millions, especially during the dot com boom years.

Some are “entrepreneurs” who, somewhat ahead of the curve, purchase domain names that they know or guess will become valuable in the future. The intention is to keep the domain name parked or published with a single page indicating that it is for sale (they hope for a significantly increased price) --sometimes going for upwards of one million dollars).

[www.feedgenic.com/blog](http://www.feedgenic.com/blog)

## Typosquatting

How many times have you quickly typed an URL, only to actually end up in a website specifically designed to capture your mistake and your attention, deliberately slowing you down.

Typosquatters take advantage of this kind of situation by purchasing Internet domain names equivalent to well- known brands but with a typo in the spelling. Not all typos are equals, the most valuable ones being those being done by people typing too fast on their keyboard or repeating famous spelling or grammar mistakes. Some cheaters plan for this occurrence by duplicating the product that the site close to their name sells, and the customer ends up buying something that is quite similar, but not what they set out to buy. Customer confusion results when the goods or services a customer set out to buy are different than what they end up with. Also leading to a lack of trust, which hinders the business world in general from benefiting from increased transactions.

Addressing this problem requires case-by-case evaluation with numerous criteria. You can proactively register domain names with common typos, but remember that typosquatters can behave

like cybersquatters. Goggle.com or gogle.com are examples of "typosquatted" domain names, the first one does not belong to Google when the second one does...

Cyber "cheaters" looking after such "opportunities" are using research taken from the most famous ad centers in order to identify the most frequently typed " typo sites".

With these statistics in hand typosquatters can estimate how many visits a given domain name could potentially drive to their website! And cause you to lose customers/market share/ jobs and revenue.

We all have experienced typing our favorite website into a search engine online, only to end up at a site you really didn't want to visit, but someone wanted you to visit on your way to the better known site. Nothing is really more frustrating to someone in a hurry, today, no-one has any time, and these internet « cheaters » definitely are time wasters for us all, the businesses that they are « cheating » by trying to divert potential customers, and the customers that just want their answer/price asap, and move on to the next item in their list.

[www.feedgenic.com/blog](http://www.feedgenic.com/blog)

## **The hazards of spoofing and phishing**

In some cases you will have to deal with real criminals not only attempting to relay on your notoriety to promote their own business but to people spoofing your identity, pretending to be your company to communicate with your potential customers on the same market. Technically speaking we can efficiently monitor any domain names registration close or identical to your brand spelling but it is another challenge, if not almost impossible, to get notified when someone sends an email using one of these domain names.

In today's sophisticated online world, companies are threatened from invisible intruders, many of whom operate from opposite ends of the world. There are many ways a new company can hijack the success of a larger more successful rival...

Proceed at your own risk:



A serious case of corporate identity fraud can force a business to shut down. These internet « cheaters » will hijack your good name for their selfish and sometimes randomly perverse purposes. It boggles the mind when you think about identify spoofing as an international sport, whose players spread across the globe.

I can give as an example one of my customers, a multinational organization:

They had an unfortunate experience when cyber-criminals in Russia registered a domain name in India that was identical to the company's name, but they added "-russia".com as a suffix. Whois.net (a website dedicated to listing ownership of domain names) data indicated my customer's company name and address in Switzerland with standard Admin., Technical and Billing contact. Everything looked legit except there was a typo in the Admin contact email address and another typo with the company phone number. Typos like this are an easy cheat designed to hide the real owner's identity. Thanks to a suspicious customer the trickery was quickly discovered and we were able to take fast action with our registrar to have this domain name added to the company's portfolio (thus preventing any serious damage).

[www.feedgenic.com/blog](http://www.feedgenic.com/blog)

This brings me to the reason for this video today, and a discussion of company brand. Your brand is your company's calling card, it says who you are, what you do, who you are targeting as customers-- with most companies extending huge efforts and oftentimes money to establish their identity.

This quote from Shakespeare explains quite a bit:

Who steals my purse steals trash; 'tis something, nothing;

'Twas mine, 'tis his, and has been slave to thousands;

But he that filches from me my good name

Robs me of that which not enriches him,

And makes me poor indeed.

— Williams Shakespeare, Othello (III iii 157–159)



Timeless Shakespeare, could he have known about how much things would change in this world, yet remain the same? Unfortunately owning a trademark isn't enough to protect you unequivocally from others attempting to use that name. In rare cases, a company may win its court against imposters, but may cost \$\$\$.

## Trademarks and domain names

Some companies persist in the outdated belief that owning a given trademark means that they are the only ones entitled to purchase the corresponding domain name. Hard-won wisdom dictates you should never assume that being the legal owner of a registered trademark automatically grants you the exclusive right to purchase and activate the corresponding domain name.



[www.feedgenic.com/blog](http://www.feedgenic.com/blog)

Today's reality shows that a third party having registered the same brand as yours either acting in a different industry either in a region not covered by your original registration has the same rights to purchase the same domain name. The famous "first arrived first served" principle is especially true for the global top level domain names like .com .net .org etc.. At local level things can vary on a case-by-case basis depending on national or regional regulations.

Many brands, and sometimes amongst the most famous one, correspond to a family name or a city name, which can also be known in the business world as a well-established company. For example, the city Zurich exists in Switzerland, but is also a large insurance company. Paris is the French capital city but is also the name of a famous celebrity.

Thus cities and people are legally entitled to purchase and use the corresponding domain name for their own purposes, even if a company legally exists and transacting business. These actions may not amount to cybersquatting as such, but the consequences for your company are similar - the loss of traffic for your website and eventually damage done to your online reputation can be very expensive compared to the domain name price. To protect against abuse, some countries have ordered the court to deny some individual rights to continue using such domain names. However these decisions do not prevent new domain names from being registered and used in the future.

## Sunrise & Trademarks

Nowadays when a new top level domain is made available to the Internet community the authorities establish a Sunrise period to safeguard the intellectual property rights of the professionals located in a specific geographical region or acting in a specific industry. This was the case for the launch of the .EU the European Union top level domain: To purchase a domain name during the sunrise period you had to comply with some strictly defined and controlled rules set by Price Waters Coopers. Documentation had to prove that your company, based in the EU, is the legal registrant of this trademark in one or more EU countries. For the launch of the .MOBI top level domain name, the rules changed, the intention being to restrict the first domain names to the established professionals in the mobile industry and not be available to all companies. Sunrise periods are unique and valuable opportunities for your company to protect your trademarks against cybersquatters; when applicable to your business do not miss it!



[www.feedgenic.com/blog](http://www.feedgenic.com/blog)

## Strategies regarding Asia

Companies who are and will be successful in this dynamic market have first had their brand translated by a linguist, then registered in local languages. Neglecting to do this will hurt you in the future as it opens the door to cheaters and competitors. Some cheaters will purchase your domain name to drive traffic to their own business and some competitors will use it to promote their own business. While knowing how difficult it can be in some countries to sue third parties abusing your trademarks and copyright it pays to take the right steps preventively.

But it comes back to business plan, and your company cannot function without one. An increasingly important facet of this plan is a domain name policy with regards to your internet presence. Being proactive in this regard will pay off for many years to come.

Not all domain names are created equal. Gone are the days when the grungy- IT guy would setup the company's domain name from his basement apartment. Now these strategies are more likely to be discussed in a swish corner office over latte's and sushi – with an eye to flamboyant attention-seeking in order to link to important revenue and recognition in the business world.



## Image certificates and digital brand protection

What you see is not necessarily what you get when it comes to certification logos which are supposed to assure viewers that the website they are looking at is legitimate.

Existing companies and domain name owners cannot afford to be lazy and let their certificates expire or become obsolete because someone is probably looking over their virtual shoulder and conspiring how to take advantage of a lapse in security.

In today's fast-moving business environment this policy will lead to almost certain death. Others will bank on your recognition and brand "cache" earned through hard work and dedication. They will piggy-back on your success, laughing all the way to the bank...

[www.feedgenic.com/blog](http://www.feedgenic.com/blog)

Despite the technical solutions available to protect image file copyright and secure logo authenticity, most companies are still using simple image files--putting the credibility of their business at risk. Nothing is simpler than googling any image certificate and re-using it. For example, there are companies on the Internet without proper certification who take a trademark logo from another website—this is just an image file—and publish it on their own website, faking compliance with quality standards. These fake certificates reduce the value of the real thing and damage the entire industry's credibility.

Another problem to address is corporate employees using their hotmail account to conduct company business. This unprofessional behavior damages company image and creates problems in terms of information control and information ownership.

## Developers around the globe

Sometimes web development strays so far that the individuals are not aware of policies necessary to protect the company, their market share, and indirectly their jobs. Within multinational groups there are often multiple levels of programmers / developers located around the globe. It is imperative that all developers and project managers get informed of the identity guidelines document ensuring that any new web development project is developed in accordance with the company's identity in the digital world.



## **An efficient brand & fraud protection program**

Human resources, monitoring solutions, and counterfeiting plans, depending on your budget. When considering the value of your Intellectual Property assets take the first step: Setting-up a domain name policy.

A domain name policy defines domain names acquisition & management rules, intellectual property ownership, authorized partners, impacted brands. It exhaustively set the geographical scope, the syntax variation to apply in case the domain name is already taken, the authorized registrant and the prohibited one— Just about everything! All possible cases should be covered by your domain name policy, and if not, go ahead and amend the plan accordingly.

[www.feedgenic.com/blog](http://www.feedgenic.com/blog)

Setting up a domain name policy is the first step in moving forward with online brand protection. It is a first attempt to efficiently and rationally define the type, scope and level of protection you wish to set-up. Purchasing domain names can rapidly become an expensive game; it's not worth registering absolutely every possible domain name corresponding to your brand(s). Without any doubt there are markets and regions where you are very unlikely to move into. There are regional sub-division of country domain names that are not worth purchasing, as well as top level domains like .NAME that are unlikely to be really interesting,...

While defining what must be registered, and therefore what must not be registered, your domain name policy is limiting the scope of what needs to be protected and watched out for the valuable & strategic part of your business. Brand monitoring solutions and software licensing model are often very sensitive to the number of domain names, brands, and Internet scope while keeping the brand protection budget within reason.

The domain name policy must state who is authorized to register domain names in your company and who is prohibited from doing so. Intellectual property is essential; Whois data must show the name of the company owning the domain name and not of an employee's own private email account! In the past this was the accepted way of business, but it is not a professional way to proceed, and not legal anyway. If you have assigned the domain name portfolio management to a third party company the whois must still indicate your company's name & contact at least in the admin and technical contacts.



## Comprehensive communication policy

Protect against threats coming from all over the world.

A cohesive corporate communication policy is very important to your brand protection. When you standardize the various aspects of digital communication your company participates in, the external world is made perfectly aware of what your official identity is, and when anything too close to your domain is registered, it becomes immediately more suspicious. Ruling which domain names are authorized for company communication and for which purpose will help to facilitate clear email communication as well as website promotion.

[www.feedgenic.com/blog](http://www.feedgenic.com/blog)

A digital brand protection program will register domain names either with the intention of activating them for communication purposes or to reserve for brand protection, a very important part of being proactive. However, even though you may own a significant domain name portfolio, be advised that if you activate them and redirect the traffic to existing websites this will be banned by all major search engines and endanger your organic e-positioning visibility, i.e. your visibility “at no cost” in search engines, the “non-sponsored” results in Google.

Dangers to your company's name or trademark domain names when acquired or used by third parties:

- \* Stealing your business
- \* Damage your online reputation
- \* Hackers masquerading as your company
- \* Legal department fees – time and cost for domain name resolution

## Preventive Monitoring

Today we have sophisticated mechanisms designed to help your company maintain its valuable intellectual property (or corporate identity), and help you breath easier.

Each company has a different level of need, yours for instance may not need BMW-level for protection, but maybe just a well-tuned Ford may provide the correct amount.

Nowadays a woman wearing a designer bag does not have the same cache as say 10 years ago, when her « bag » stood a better chance of being the real deal. Not only the Devil Wears Prada these days !

Let's drown out the faker's message and bring out the real deal- let your brand shine for the world to see. In order to do this, preventive monitoring must occur.



[www.feedgenic.com/blog](http://www.feedgenic.com/blog)

## **Monitoring the digital world**

There are various tools available to monitor how your brand is used on the Internet. Some include keywords which automatically monitor where and in which context the brand is used. These query meta and blog search engines, meta-tags, social media, and these tools can often provide you with a visual map of your brand notoriety and context usage together with the related topics most commonly associated. Other solutions specific to domain names notify the brand manager of any registration which is identical or too close to your trademarks. Some engines are able to detect logos or image certificates shown in any image file—being especially useful in detecting which third party websites have fake certificates. Other systems are specialized in the sponsored advertising networks reporting competitors using your trademark as advertising keywords.

Obviously the cost of a monitoring solution eventually associated with counterfeiting actions is to be balanced against the value of the brand itself. Due to the vast immensity of the Internet, the cost of such implementation can be prohibitive even for large companies-- this is why it is important to adjust the monitoring effort to

1) the current and potential value of the brand AND

2) to the current and potential threat the company is facing.

Your budget for this protection could be compared to taking an aspirin to fight a broken leg, or surgery to repair a cold. You can choose which level makes the most sense.

Most important is to focus on the brand credibility. A company facing a very limited number of brand attacks each year should not necessarily invest a six digits amount in a real time brand protection and counterfeiting program but should more ensure that the situation does not become difficult:

- \* Avoid worst-case scenario - taking time to time pictures
- \* Suing cheaters in court
- \* Looking for usurpers to your domain name



[www.feedgenic.com/blog](http://www.feedgenic.com/blog)

Instead, take the time to set up a domain name and communication policies and enforce it. On the opposite hand, a company which has completely lost the control of its most valuable brand in the digital world, should react quickly and, at least the first year, very strongly to correct the situation.

The digital world has something in common with the real world in a way that once your brand credibility suffers its effects last for a long time. Even hundreds of years ago, in Shakespeare's time, a man's name was the most valuable thing he owned, and today the same can be translated to your brand.

How about the proliferation of "fake" luxury goods these days? It's hard to tell if a woman's bag she is carrying is the real thing, or a "knockoff". Think of the financial impact to the company known for making the most fashionable and expensive hand bags for women and suit cases for travelers. This brand is one of the most copied in the world, and why? It's a cheap and easy way to capitalize from the "cache" generated by the name, from generations of haute couture, and exclusive availability (in the past).

Now, if you see someone with this bag, you are prone to thinking it is a fake unless said lady is driving a Ferrari. Brand credibility contributes to brand value, if you do not want your product lacking customer trust at a critical juncture, protect your brand before it's too late.

## **When too much protection damages the business**

Companies commercializing products through retailers or extended supply chain must walk the line between too much digital brand protection and inadequate protection. For instance, Microsoft or Sony would not want to prevent retailers from advertising the Xbox360 or the PS3 trademarks, which would surely impact their sales. The best thing to do is look at brand protection on a case-by-case basis.



[www.feedgenic.com/blog](http://www.feedgenic.com/blog)

Then again, if you protect too strongly, no-one will know or see your brand at all (visibility). An unknown rock star is a financially challenged rock star. You'd rather get your name and product out there to shine and attract more business, not hide your light under a rock.

## **In a few words...**

I hope that I have conveyed the fact that brand protection is in reality far more complex than simply registering domain names or subscribing to keyword monitoring services from third party vendors. I wish you the very best in your efforts to secure your domain name, identity and cohesive brand on the Internet.