

WING TIPS

Cybersquatting – moving with the times?

Cybersquatting – the practice of registering internet domain names that are based on another entity’s brands or company name - is as prevalent as ever. As online business models have developed and converged, the cybersquatter’s methods have adapted accordingly.

Today, businesses routinely need to think about registering domain names simply to prevent others getting hold of them – in the wrong hands, a domain name can be used to divert business, confuse customers, dilute the brand and commit fraud.

It had been thought that the wide-spread use of search engines would significantly reduce the damage cybersquatting could cause, as users more commonly found websites through search and not typing in the URL. But this has not been the case - the prevalence of search engines has in fact become a useful tool in the cybersquatter’s armory.

New product? Think new domains...

Any new branded product or service launch involves considerable time and effort, with an online presence essential. Today, more than ever, businesses have to allocate at least part of that effort towards securing as many of the relevant domain names as possible before launch.

The recent press reports regarding Apple’s iPhone highlight that cybersquatting remains commonplace. In anticipation of the much publicised UK launch of the iPhone on the O2 network, it is reported that cybersquatters have rushed to register “*o2iphone.co.uk*”, “*o2iphone.net*”, “*ukiphone.co.uk*” as well as “*orangeiphone.co.uk*”, “*tmobileiphone.com*” and “*iphonenvodafone.co.uk*”.

With cybersquatting as blatant as this, Apple should have little legal difficulty in getting any hosting of the domain names as websites stopped, often by simply complaining to the relevant ISPs, and the domains subsequently transferred via one of the domain name dispute resolution bodies or the local courts. The problem is that cleaning up the issue will take a frustrating amount of time and effort.

With infinite combinations of words possible for domain names it is clearly not possible to prevent all cybersquatting. There are well over 100 million domain names registered across 19 generic top level domains (gTLDs) like .com, .org and .biz and 248 country code domains (ccTLDs) like .uk and .de. – for every domain name you register to cover your brand there will be many more you miss. Like most major brand owners, Apple will have registered many domain name variations of the iPhone brand before launch. But there will always be gaps - Apple could have registered *o2iphone.co.uk* and *ukiphone.co.uk* only to encounter problems with *iphone02.co.uk* and *iphones02.co.uk* and *ukiphones.co.uk*...and so on.

That said, making an attempt to pick up the most obvious variations (and misspellings) of brand and company names is certainly well worth the effort.

Why domains still matter

An ever increasing number of internet users rely on search engines when looking for a particular branded product or service on line. Google's market share of search continues to grow – now up to 75% of the UK search market. Why try and guess the domain name you need when Google will give you the answer just as quickly?

The problem for brand owners is that a determined cybersquatter in possession of a confusingly similar domain name can still cause great damage to your brand and your business. Some examples:

- A website with a URL that is confusingly similar to the brand name may well attract some on-line traffic with users looking for the genuine site. Cybersquatters take advantage of this, fraudulently setting up affiliate “pay-per-click” deals with the brand owner, via affiliate brokers. Once the deals are in place the cybersquatter can earn revenue by re-directing users who have stumbled onto their unlawful website towards the brand owner's genuine site.
- In a similar vein, the growth of on-line contextual advertising, such as Google's AdSense, has given cybersquatters another easy and perhaps the most important route to monetising their unlawfully registered domain names. The process is simple – register a domain name which contains, for example, a slight misspelling of a well-know brand or company. Set up a “parked” website hosted to that domain name and register it with one of the contextual advertising providers. The advertising service creates a HTML (or XML) webpage with various pay-per-click adverts which are displayed to the user visiting the parked domain. As the webpage often only has links, there is a good possibility that the users will click to navigate out of the webpage and this user activity translates to revenue when the clicked link is an advertisement. Most often it is the brand owner's own adverts that the user clicks, so the cybersquatter gets revenue from the very company it is mimicking. Frequently the more prolific cybersquatters will test out the traffic that a domain name will generate in the grace period before payment is due for registration (often called “domain tasting”); dropping the domain if the traffic is lower than expected.
- Of even greater concern is the practice known as phishing. Having registered a domain name that is confusingly similar to a brand name or company, cybersquatters can set up email accounts and send out spam emails using that domain. For example, receiving an email from offers@iPhoneUK.co.uk may confuse many people into thinking they were being contacted by an entity officially associated with Apple. The brand owner has no control over the content of these emails or the damage and confusion they can cause.
- Spam email is often used in combination with cloned sites. The recipient of the spam is invited to click on a link and visit a website, building a more convincing image of authenticity. Companies have discovered that their entire website has been copied by a cybersquatter, with all the links working as if it were the genuine site. Minor alterations might be made in copying the genuine site, for example to email and telephone contact information, so that if the user is not sure it is the real site they may call the telephone number on the website, and the deception is continued. Banks have been used to combating this practice for some time. Other companies are discovering examples of cybersquatters trying to obtain goods on credit in that company's name, using the cloned site as “proof” of identity.

So, what can you do?

Nearly all cybersquatting activities can be stopped. The law has kept up well with the issue, but the challenge is often how fast can you stop it and how much time, effort and money are you willing to put into chasing the problem? For the bigger brand owners this has become a way of life – dedicated teams track and challenge cybersquatters, trying to keep the tide of infringements at bay.

What procedures should a concerned brand owner be putting in place? Some practical thoughts:

1. Check what domain names you currently have registered. Are there any other obvious names or combinations that you would hate to find in the hands of someone else? See if you can register them and if not check to see who does own them and what they are using them for. Take action if you discover cybersquatting (see below).
2. Before launching any new branded product or service, try and register the obvious domain names and variations covering that brand – it can only enhance your ability to attract on-line traffic and reduce the number of potential cybersquatting problems. Don't forget to think about obvious misspellings or combinations of words, but bear in mind you cannot cover all the options.
3. Institute a domain name watching policy with one of the many watching services. They can provide you with regular reports on domain names that are registered which contain the word or words you want to keep an eye on. Check if the service can pick up domains with typos and misspellings.
4. If you find a website being operated by (or for) the cybersquatter under the domain name, you may be able to get the relevant ISP that is hosting the site to take it down. If successful, this can limit the financial or reputational damage being caused and buy you time to resolve the problem directly with the cybersquatter.
5. If there is clear cybersquatting, take action to recover the domain names – don't let the problem develop. Most cybersquatters will not defend their position, which often means that using one of the domain name dispute resolution systems (ICANN for gTLDs, or for example, Nominet for the .uk domains) is a formality. For more serious cases, the courts can provide a faster and more robust solution – cybersquatters have become used to getting ICANN complaints but the threat of court proceedings, costs orders and the possibility of being held in contempt of court tends to focus the mind.

Dealing with cybersquatters has become a commonplace issue for most companies. Rather than simply an on-line branded address, domain names are fast becoming more akin to registered intellectual property rights – you register them to stop others using them.

To find out more about dealing with cybersquatters, please contact Andy Moseby, Partner, andy.moseby@kemplittle.com or Paul Garland, Head of Litigation paul.garland@kemplittle.com at Kemp Little LLP