Squatters Beware

Protecting Your Business from Cyber-Opportunists – the Modern-Day Pirates

By Mark Sableman

If your grandmother's last phone had a rotary dial, she had better study up if she wants to master her new iPhone. Technology changes, and we all need to keep up. So why then are so many otherwise savvy businesses being taken by surprise by the new tricks being used by pirates and opportunists on the Internet?

Every business that is using the Internet today should be attentive to pirates and infringers. Using a variety of techniques, some old and some new, cyber-opportunists are attacking your Internet activities:

- By registering or using domain names based on your trademarks
- By using metatags or invisible text to divert your customers to their websites
- By using your trademarks to trigger their advertisements on search engine results pages
- By using your trademarks to attract visitors to manufactured search portals, all to generate pay-per-click advertising revenue
- In some extreme cases, by using your trademarks and logos to give credibility to their Internet fraud schemes

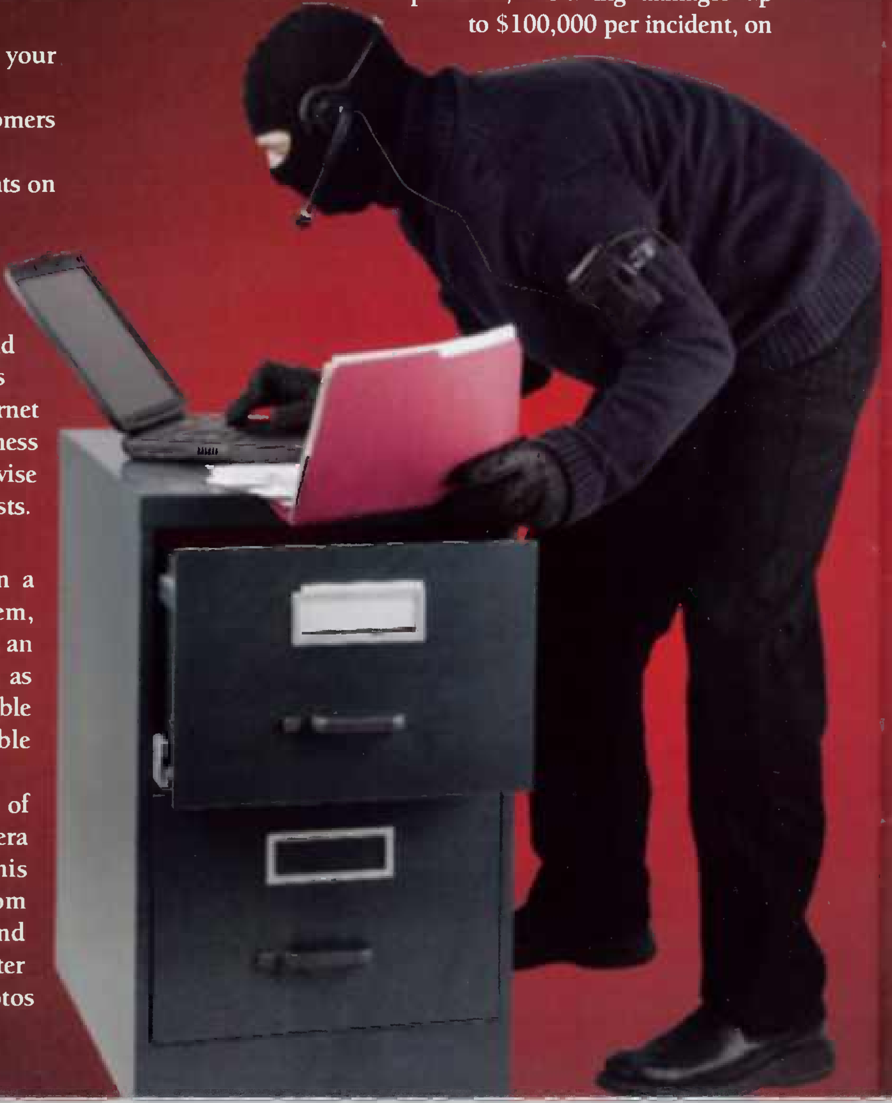
As the major marketing battleground of today, the Internet needs your attention—not just in your affirmative business efforts, but also through careful monitoring and wise enforcement activities, defending against cyber-opportunists.

Cyber-squatting

For fifteen years, Internet domain names have been a battleground for business. The domain name system, created in the 1980s by a California academic, contained an inherent bottleneck, with the dot-com top-level domain as the sole desirable business address. That led to a scramble for desirable dot-com addresses, and some inevitable cyberspace conflicts.

This Internet congestion led to the first generation of cyber-squatter—the modern equivalent of gold-rush era land squatters. Cyber-squatter pioneers like Dennis Toeppen grabbed up hundreds of desirable dot-com names, like panavision.com, unitedairlines.com, and deltaairlines.com. (In one funny episode, Toeppen, after being sued by Panavision, immediately posted aerial photos of Pana, Illinois on his panavision.com website. Of course, it only requires a tall ladder to take aerial photos of Pana, Illinois, and no one believed that that is why he registered the Panavision domain.)

Congress and ICANN (it's pronounced "I-Can"), the non-profit regulator of the Internet domain name system, took steps in 1998 to ban such blatant cybersquatting. The federal Anti-Cyber-squatting Consumer Protection Act imposed tough penalties, including damages up to $100,000 per incident, on



cyber-squatters. ICANN set up a streamlined international administrative procedure for combating cyber-squatters. Both procedures focus on bad faith conduct, shown by evidence such as unauthorized use of others' trademarks, use of fictitious names, multiple infringing registrations, and the like. As an example, if the St. Charles Candy Factory registered "hershey.com," it would probably be viewed as acting in bad faith—even more so if it also registered "m&m.com" and did so using a fictitious name.

These procedures have significantly cut back on cybersquatting, though, unfortunately, this kind of abuse continues, because of the temptations of a system where anyone can register for a few dollars a domain name that may be worth thousands or more to the right company.

Customer Diversion

Many cyber-opportunists have moved on to new abuses. Some quickly discovered the potential of playing with the hidden computer codes known as "metatags." Metatags were designed as legitimate hidden index words and phrases, ways to tell search engines and other search tools about the content of a website. But abusers found that they could exploit this technique. An adult website, for example, put the terms "playboy" and "playmate" in its own site's metatags, so that search engines would list its website high in response to a search for either term. Top search engines wised up immediately, changing their algorithms, but this abuse is still practiced at times and can still fool second-tier search services.

Courts have been willing to crack down on metatag abuse, to the tune of millions in damages in the Playboy case. Internet pirates, however, are adept at new techniques. Some have used "invisible text" to fool search engines, instead of metatags. It is a simple thing: the text is there in the website computer code, visible to all search engine robots. But because it is coded to appear on the screen in the same color as the surrounding background, users don't see it.

The federal Anti-Cyber-squatting Consumer Protection Act imposed tough penalties, including damages up to $100,000 per incident, on cyber-squatters.

The latest technique for diverting consumers is controversial and of disputed legality. It involves purchase of advertisements (sometimes called "sponsored links") on search engine results pages, keyed to a competitor's trademarks. Pepsi, for example, would pay Google so that every time someone searched for "Coca-cola," Google would place an ad or sponsored link for Pepsi on the results page. This is generally considered infringement where the resulting ad displays the search term, or is otherwise misleading.

But where the advertiser's ad or listing makes no reference to the trademarked search term or its owner, the legality of this much-used technique is currently unclear, due to conflicting cases and a paucity of evidence about actual consumer understandings. Many legitimate businesses use this technique, and just as many bristle about their competitors' use of it. On both sides, businesses are well advised to consult knowledgeable counsel.

Pay-per-click Revenue Schemes

Some recent Internet innovations have led to a new cottage industry of cyber-opportunists who exploit the cheap and easy availability of domain names, and the potential for accruing significant revenue, through pay-per-click advertising links.

In the early days of the Internet, domain name registrations cost around $80 each, forcing registrants to choose their domains carefully. Competition in the registration business has lowered the cost to just a few dollars each for mass purchasers, and many mass purchasers now exploit a quirk in the system that allows them to register a name, test it for five days, and then immediately return it without paying for it.

Pay-per-click ads have invited these schemes. Many website operators are willing to pay pennies per click to anyone who sends potential customers to their sites. So someone might place a linked ad for such an advertiser on his or her own website, and benefit from the pay-per-click revenue. But most people don't want to clutter up their own useful sites with the often seedy pay-per-click ads, nor do are they really want to send their own customers away.

The result has been the creation of many essentially phony websites. They exist for no other purpose than to display pay-per-click links and ads. Usually they display links to websites relating to certain subject areas—though, unlike a legitimate search engine results page, the links are all to paid advertising (as, of course, are the adjoining display ads).

In some cases, domain name registrars will themselves set up these sites, using "parked" domains that their customers have registered but not put in use. Many times cyber-opportunists will register domain names that they think will attract a certain type of user, often basing the domains on typographical errors in the spelling of certain words or trademarks. The advertising links will then be tailored to the expected interests of the web users who are attracted. If, for example, the domains are all based on misspellings of "Chevrolet," the linked pay-per-click ads are likely to all be auto-related.

Every week, thousands of such sites are registered and tested for five day trials; those that do not generate enough pennies are shut down and the rest remain up until someone calls the cyber-pirate to task.

Such websites designed to exploit pay-per-click advertising often run afoul of cybersquatting, trademark, and other laws. Businesses can and should carefully monitor and vigorously fight the pay-per-click opportunists who exploit their good will in these ways.

It can get even worse. In some cases, we have found fraud artists in Asia and Eastern Europe setting up websites cloaked in the legitimacy of the trademarks and logos of leading United States companies—all to deceive consumers in the few weeks before the infringing sites are discovered and shut down.

Cyber-opportunists are a sad reality of the Internet. The Internet may be one of the greatest communications and marketing media of all time, but it is also an impersonal network that extends access, and instant credibility, to almost any user. That has allowed it to be used in many improper, exploitive ways. All businesses should watch for these potential abuses, and take the necessary monitoring and enforcement steps to fight them. STOP