Reducing Cybersquatting, Phishing

Alex Tajirian
September 26, 2009

Solutions to cybersquatting and phishing must target brand customers instead of the trademark infringers, who are in effect liars. This paper outlines why online-based traditional solutions fail, and it offers solutions to two types of lying (cybersquatting and phishing).

There's no point to trying to reduce phishing by reducing its profits. Nobody knows how much money can be made by phishing, and this includes would-be phishers; an economic-incentives solution can't work if the solution's target has no idea what his or her profits are. Meanwhile, the would-be culprits do know they face entry barriers that are negligible at best. Why not give the scam a try and see what happens?

Trying to blacklist phishing sites doesn't work either, judging by the research of Tyler Moore and Richard Clayton at Cambridge University. The problem, they argue, is that liars can manipulate crowdsourcing-based solutions (see Evaluating the Wisdom of Crowds in Assessing Phishing Websites).

A third anti-phishing tactic, that of shutting down the sites, can be countered by strategies found in a paper done by Moore (see Phishing and the Economics of E-crime). But site takedowns do get results when fighting cybersquatters, since traffic to the liar's site is through direct navigation (which can be taken down) or search engines (which take a long time to index under different domain names).

The remaining solutions, suing the violators or buying up their sites, often do more harm than good. (See "Domain Name Lessons from Napster" and "Don't Litigate, Mitigate!").

Brand owners can get better results with solutions that target brand users:

1. Increase customer recognition of fake Web sites by increasing the customization of genuine sites. Display visitor-relevant information (date of last visit, name, IP, etc.) or go further and customize the site's "look and feel" and content based on the visitor's preferences. Of course, such solutions may require new cookie technologies that are harder to reverse-

engineer, and they require an investment by the brand owner (and thereby act as barriers to entry). It should be noted that content customization is itself value-adding to the site's owner.

2. Post a public list of legitimate sites. Customers can find more online information about a company than companies realize. Why not make it even easier for them while adding value to their experience.

3. Educate customers about potential fraud. This solution is becoming more important with "vishing," which uses VOIP to target customers through automatic dialing. An automated message informs the customer that his credit card has had suspicious activity and that he should call the recorded phone number immediately. Another new technique is the bogus live chats. Education should also make "money mules" (i.e., money transfer agents) more aware of possible scams and thus make money laundering more difficult.

4. Increase the risk of buying counterfeit. Brand owners can create their own fake sites and post warnings there that the requested merchandise is a knockoff. If the customer goes through with the check out, the site sends a warning e-mail. Fake sites are traps to catch criminals after they enter their personal information, and thus deter online shoppers from buying counterfeit products as the risk of being caught increases. Moreover, being aware of lower profits deters entry of criminals. The solution does not alienate legitimate brand buyers—who should realize that if a Web site's deal is too good to be true, then it is too good to be true—and it can protect the value of genuine merchandise from dilution. In short, if you cannot beat cybersquatters, join them. ■

Key words: online crime