

Keeping Up with Online Brand and Other Related Scams and Frauds

By Richard E. Peirce

There can be little doubt in today's world that the Internet offers new ways to do old things. We can now work more efficiently, conduct financial business, enjoy recreational reading, socialize and perform a host of other tasks — all online. Yet, this same Internet has provided an almost unguarded playground to allow thieves and other criminals to develop and unleash sophisticated scams and frauds on unsuspecting users.

There is almost an unlimited amount of Internet scams and frauds that are active at any one point, yet because of the nature of the Internet, it is almost impossible for a small business or a consumer to stay up to date. The scammer's arsenal is almost without limitation. He may use a well-known brand or logo to lure the user into an identity theft trap. He may attempt to play off of a recent disaster in an effort to trick the user into making a donation to a fraudulent entity disguised as a legitimate relief organization. Regardless of the tactic and motive, businesses and consumers should always be mindful that scams and frauds can appear in almost any place on the Internet — from e-mail to social-networking sites.

While it is nearly impossible to address and identify all of the scams and frauds that may be active at any one time, the short list below provides a nice overview of some of the more common ones that infect the Internet. The hope is that Internet attorneys will not only be able to recognize the scams and frauds, but also be able to recognize the characteristics of one so that he or she will be better equipped to identify other scams and frauds of today and tomorrow — and be prepared to advise their clients.

Common Scams and Frauds Involving Brands

By using a well-known brand in the scam or fraud, the scammer is able to take advantage of the good will and reputation a company has developed in that specific brand. With the amount of brand bombardment that occurs in today's marketing world, the use of a brand for fraud makes for the perfect bait.

Cybersquatting. The bad faith registration and use of domain name that is identical or confusingly similar to another party's trademark. Bad faith, while not limited to a specific behavior, commonly is done with the intent to divert Internet traffic from the mark owner, offer the domain name back to the mark owner for a price higher than the registration cost, and/or disrupt the mark owner's business.

While use of the domain name may vary, many times it is used for phishing schemes or to resolve to Web content for competing goods and services, pornography, sponsored advertising links and/or counterfeit products.

The targeted domain names go well beyond just those that are identical to the brand. For example, suppose my hypothetical company is named PeirceBev and I sell sport drinks. Some of the variations on my brand that are likely to be sought after by cybersquatters may include:

1. Plurals and hyphens (peircebevs, peircebeving, peircebev);
2. Business designations (peircebevcorp, peircebevinc, peircebevco, peircebevllc);
3. Product designations and characteristics (peircebevdrink, peircebevpop, peircebevcola, peircebevorange, peircebevsoda, peircebevthirst, peircebevdiet);
4. Geographic designations (peircebevamerica, peircebeveurope, peircebev123, peircebevphilly, peircebevjersey, peircebevusa);
5. Typosquatting and phonetics. (peircebevcom, wwwpeircebev, pearsebev);

6. Negatives and positives (peircebevsucks, peircebevstinks, peircebevlawsuits, peircebevlawyers, peircebevproblems, ihatepeircebev, ilovepeircebev); and
7. Other miscellaneous variations (mypeircebev, ourpeircebev, drink-apeircebev, peircebevforum, peirce bevchat, peircebevblog, peircebevgroup, peircebevdiscussion, peircebevmeeting, peircebevclub, peircebev1).

Fraudulent Domain Name Transfers. A scammer attempts to trick a domain name owner into transferring its domain name to the scammer. While the technique may vary, one common approach is to send a deceptive e-mail notice to the domain name owner with the hope that the owner will approve the fraudulent transfer request.

A close variation on this scam is what is called *domain name slamming*. It is the process where a competing registrar or other domain name registration entity sends out an official looking "renewal notification" notice to a domain name owner. The hope is that the domain name owner will believe that the notice is official (perhaps coming from the owner's registrar or a governmental agency), respond as requested in the notice, and as a result, have its domain names unknowingly transferred to the sender's maintenance system.

Domain Name Tasting. A domain name is registered for the purpose of evaluating its value, especially in connection with click-through advertising revenue, during the five-day add-grace period for domain name registration. If the domain name does not "perform" well during the five-day period, it is often returned for a refund. Many times, the domain names being registered through this practice consist of common misspellings (typosquatting) of brand names and marks.

Domain name kiting is where the taster engages in a pattern of registering, dropping before the end of the add-grace period, and re-registering the same domain name with the intent of never having to pay the registration fee.

Domain Name Spying. A person views or spies on another party's domain name whois/ownership searches to see what domain names are being considered for registration. The purpose is that if the domain names are not registered immediately, the spy will register them, believing that they may have some current or future value. Thereafter, the spy may "taste" and use them for click-through revenue or attempt to auction them.

Domain Name and Keyword Availability Scam. An entity sends an e-mail to a brand owner and informs it that some other third party is about to register a number of domain names and Internet keywords containing the brand owner's mark(s). The brand owner is then given the opportunity to block the registrations by having the domain names and keywords registered with the sending entity. It is the hope of the sender that the brand owner will be concerned enough over the "potential" registrations that the brand owner will authorize the sender to prevent or block the registrations — which is nothing more than the sender obtaining the brand owner's registration business through deception.

Phishing. An entity sends out an e-mail or pop-up message falsely claiming to be from a legitimate business or organization, perhaps even one that is familiar to the recipient such as a bank, ISP, or governmental agency. The purpose of the phishing attack is to trick the recipient into revealing personally identifiable information, access codes or other financial information. The e-mail or message may look very official and include the legitimate company's trademarks and logos. The sending entity's e-mail address (spoofed e-mail) may look as if it came from the legitimate company by incorporating the legitimate company's mark as part of the address. The message may include a link where the URL looks nearly identical to that of the legitimate company's URL. If the link is clicked, it may take the recipient to a Web site that looks nearly identical to the legitimate company's Web site. It is likely that at this site, the scam sender will attempt to collect its information from the victim.

A *vishing* scam is a variation on phishing where the scam e-mail states that some account (credit card, bank, eBay, PayPal, for example) has been suspended and that the recipient needs to act quickly to resolve the issue. Again, the goal of the sender is to gain access to

sensitive information like account passwords and credit card numbers. For example, it was reported recently that vishing e-mails were sent out seeking Google Calendar login information from recipients.

Pharming. A site's traffic is redirected to a fake site, usually unknown to the user, with the common purpose of conducting a phishing scam or for other identity theft purposes. These can be some of the most deceptive scams online because it may be difficult to know whether or not the site is legitimate, especially if the DNS system has been compromised in some manner.

Employment Fraud Scams. An entity reviews job posting sites and sends fraudulent messages to job seekers, holding itself out as being affiliated with a legitimate company. The job seeker then is scammed into revealing personally identifiable information as part of the application process, or is lured to a job unrelated to the legitimate company. The scam message will likely include many uses of the legitimate company's brands, including in the e-mail address. The scammer may also post a fraudulent job on a job listing site with the same intent.

Auction Scam Issues. There are many different types of scams and frauds that occur in connection with auction sites such as the sale of fake or counterfeit goods, theft of credit card information, and the use of phishing e-mails for fake auctions.

Bogus Humanitarian e-Mails and Sites. Fraudulent e-mails and sites used in an effort to trick users into making donations to a fake entity holding itself out as being related to a legitimate humanitarian organization. These types of scams usually increase in volume around well-publicized disasters and can cause great damage to a legitimate organization's efforts to get donations.

Misuse of Search Engine Keyword Purchasing. Certain search engines allow users to purchase terms, including the trademarks of others, as keywords so that when such terms are searched on the respective search engine, the user's advertisement and link will appear in a prominent position on the search engine result page. Many times, the advertiser misuses a trademark or name in the text of the advertisement or on the resulting site in an effort to create a likelihood of confusion as to the source, sponsorship or affiliation of the advertiser's goods/services.

Other Internet Concerns, Scams and Frauds

Economic Stimulus Payment Scams. According to the IRS, at least two new scams have surfaced:

1. Taxpayers receiving calls from individuals impersonating the IRS during which the caller asks the taxpayer for his/her social security and bank account numbers to complete the payment; and
2. Taxpayers receiving e-mails appearing to come from the IRS wherein it asks for bank account information for direct deposit of the refunds.

"Nigerian" Money Offer (419) Scams. e-Mails that claim to be from some wealthy business person or government official, wherein these individuals ask for assistance with getting money moved out of foreign accounts (perhaps because of some government conflict or a death) in exchange for the recipient keeping a large percentage.

Work At Home/Turn Computer Into a Money-Making Machine. The software required to do the "job" will many times contain malware, spyware, or spam generating software unknown to the victim.

Money Mule Scam. Victim takes a job where he or she will be sent money that needs to be divided up and re-sent to other parties (additional scammers). The victim is told to keep a portion of the money. Thereafter, the victim finds out that the money came from an innocent third party who thought he or she was buying something from a party (scammer) on eBay. Now the innocent third party turns to the victim for his or her product. The result is that the scammers used the victim to launder stolen money from the innocent third party.

Fraudulent Grand Jury Summons. The messages look authentic and may contain references to the court, case and jurisdiction. The recipient is then directed to click on a link to download forms that usually contains malware or spyware.

Overpayment Scam. The seller/victim has a product for sale. A potential buyer agrees to pay for more than the asking price so as to cover shipping and handling. Any difference is to be wired back to the buyer. Seller receives a check or money order, ships the product, and wires back the difference. Thereafter, the buyer's check or money order is found to be a fake and the seller is responsible for the entire amount.

Reshipping Scam. It starts out as an employment scam. Victim is "hired" to receive goods and re-ship them overseas. Victim receives the goods and does his or her job, yet the goods were likely purchased with stolen credit cards. Thereafter, the goods are fenced overseas and the victim just unknowingly participated in the process.

Suggestions for Combating

Frauds and Scams On the Internet

While the above-referenced scams and frauds differ in style and appearance, many have similar traits, such as brand abuse or requests for personal information by e-mail. Recognizing the "smell" or the characteristics of a scam or fraud will help assist the user to identifying them even before they are covered or reported on by the press or government.

In addition to recognition, the following recommendations may also be useful in combating scams and frauds on the Internet:

1. Check with applicable Internet, trademark, deceptive practice/fraud and related laws for legal options. For example, Section 1125(d) of the Lanham Act (Anticybersquatting Consumer Protection Act) and The Uniform Domain Name Dispute Resolution Policy provide legal options specific to cybersquatting;
2. Visit government sites such as the FBI, SEC, IRS and FTC for updated information on the latest frauds and scams;
3. Use foreign counsel when needed if the issue has an international element;
4. Keep clients educated on scams and frauds that target the company's brands;
5. Encourage clients to report fraudulent activities involving the company's brands;
6. Keep security software up to date;
7. Police company brands on the internet for misuse and abuse; including, but not limited to, domain names, Web content, search engine sponsored advertisements, auctions and chat rooms;
8. Form a response team to handle scams and frauds that attack the company — IT, management, privacy and legal;
9. Explore Web site take-down options when appropriate if the content is being used to perpetuate the scam or fraud;
10. Be mindful of issues that may arise in social networking sites such as Facebook and MySpace, or in virtual world sites such as SecondLife; and
11. Contact local, state and federal law enforcement when needed.