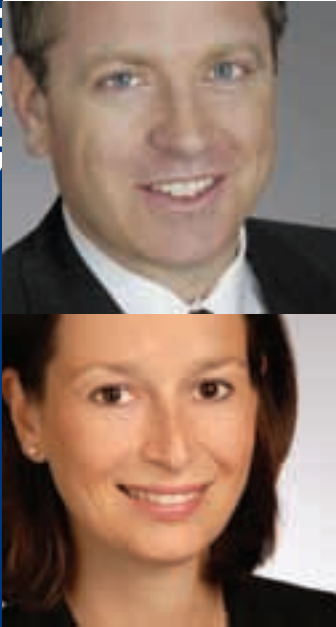


Advertising Agencies: Beware!



BY GREG SATER AND
NATASHA SHABANI

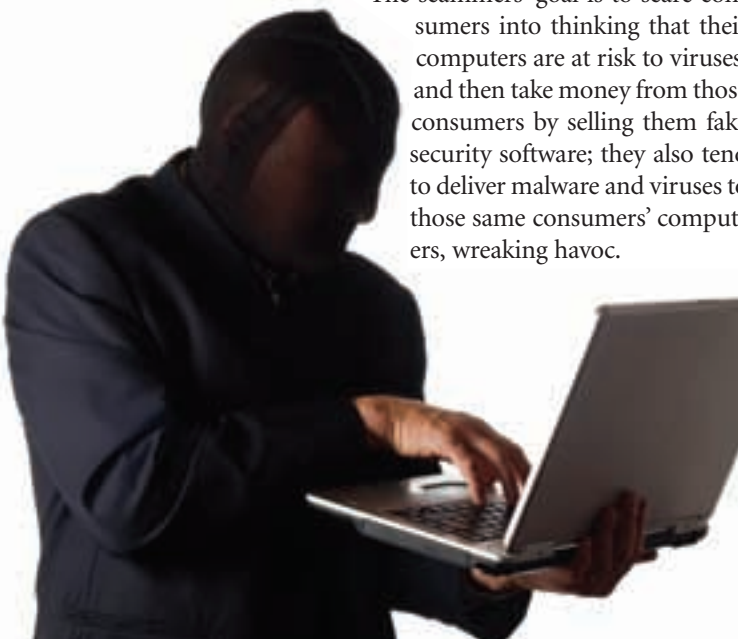
If you're a well-respected advertising agency, it's quite possible that you have been, are being, or soon will be impersonated by one or more unscrupulous third parties who pass themselves off as being you!

Why would they do this? By using your name and by pretending to be you, these scammers can get banner ads to run online (banner ads they don't have to pay for because they get credit terms extended to them by websites that mistakenly believe they're you and that you'll be paying the bill). Then, when consumers click on those banner ads, not only do they get defrauded out of their hard-earned money through "scare ware," but their computers also then get infected with malicious viruses.

You might call it "advertising agency identity theft" and unfortunately, right now it's becoming more and more common. This article explains the nature of the problem and suggests what you can do about it.

HOW THE SCAM WORKS

The scammers' goal is to scare consumers into thinking that their computers are at risk to viruses, and then take money from those consumers by selling them fake security software; they also tend to deliver malware and viruses to those same consumers' computers, wreaking havoc.



In Internet parlance, such fake software is called "malware" or "scareware," and the schemes used to distribute them are becoming more and more ingenious.

The latest is that the scammers are buying ad space, such as banner ads on trusted, popular websites. Their ads look legitimate both to the operator of the website (who agrees to run the banner ad) and to the consumer who visits the website (and who clicks on the ad). But what the ad really does is redirect that consumer to a fraudulent website that then performs a fake security scan. Next, an urgent pop-up message appears that scares the consumer into purchasing and downloading bogus antivirus software to supposedly fix the problem. In some cases, the software then actually installs viruses and malware onto that computer.

How do the scammers get their banner ads onto those legitimate websites? They pose as a legitimate advertising agency, representing a legitimate client, and use that credibility to purchase advertising space for their banner ads, on credit terms.

For example, malware recently was being distributed in this fashion by one or more scammers fraudulently impersonating Koeppel Interactive, a well-respected agency that buys online media for its clients. The scammer, who operated under the false name "Jan Koller," registered the domain name "koeppelinteractive.co.uk," which was a very slight variation on the legitimate website address. "Jan" then represented himself to third-party websites as being "director of media buying" at Koeppel Interactive, and used the e-mail address jan@koeppelinteractive.co.uk.

By passing himself off as working for Koeppel, "Jan" was able to purchase, on credit terms, a banner ad campaign, purportedly for Coors. The day after the online ad campaign launched, consumers began complaining about security warnings and

malware. The malware was redirecting consumers to fraudulent scareware websites, and some computers were being infected.

Word got back to Koeppel. "The scammers appeared to be quite sophisticated in their approach to impersonating legitimate agencies," observes Peter Koeppel, president of the agency. "Fortunately, there are web security experts who track these types of scams and they contacted us and helped shut them down."

What did Koeppel do? He and his staff went to the domain name registrar and filled out a "report abuse" form, online, resulting in the suspension of the domain name by the registry. Then, the website that had been conned into running the ad campaign shut it down and Koeppel placed a notice on the landing page of its website, warning everyone that somebody was impersonating it. Finally, our firm filed a complaint with the Federal Trade Commission on Koeppel's behalf. (At press time, the federal authorities were working on tracking down the scammers.)

ANOTHER SCAM CASE

At or about the same time, a strikingly similar situation was occurring with another well-respected advertising agency, Quigley-Simpson. A scammer fraudulently registered a URL almost identical to Quigley-Simpson's authentic homepage. This particular scammer had really done his homework, because he even took the extra step of registering his domain name under the name of the agency's CEO. He contacted media owners, purporting to be an employee of Quigley-Simpson, using the fictitious name "Craig Colbert" and an e-mail address of c.colbert@quigley-simpson.net. In case a media owner might do any due diligence on him, by going to his website at the ".net" URL, "Craig" had his URL automatically transfer all visitors to the authentic Quigley-Simpson URL. In

this manner, he was able to purchase banner ads and other media purportedly for Quigley-Simpson clients, and thereby distribute his malware and scareware.

Quigley-Simpson acted quickly when it discovered the ruse. "We found out about the false registration about two weeks after the perpetrators had set up the false link," says Gerald Bagg, Quigley-Simpson's CEO. "We immediately posted a detailed warning on our homepage

In Internet parlance, such fake software is called "malware" or "scareware," and the schemes used to distribute them are becoming more and more ingenious.

to alert anyone directed to our website from the false URL that there was an imposter out there. This quick action prevented an epidemic of false media placements from being made under our name. Then we needed to gain control of the false website, which was not only identity theft, but also an infringement of our trademark." On Quigley-Simpson's behalf, we filed a domain name arbitration complaint under the Uniform Domain Dispute Resolution Policy (UDRP) in order to recover the domain name the scammer had used.

A UDRP is a special arbitration proceeding created specifically to resolve domain name ownership disputes. It's quick and cheap. UDRPs apply to domain endings such as .biz, .com, .info, .name, .net and .org (but not foreign country code domains). The UDRP ended well: the perpetrator's domain name was transferred to Quigley-Simpson. In addition to filing the UDRP, we also reported the scam to the FTC, on behalf of the impersonated advertising agency.

These are but two examples of ad agencies being impersonated in this fashion. There have been several others in recent weeks.


WHAT TO DO

If you are an advertising agency that has been impersonated, contact the FTC right away. Also call an attorney.

The FTC works to prevent fraudulent, deceptive and unfair business practices and to provide information to help stop such practices. It commences an investigation when it has "reason to believe" that the law has been or is being violated and it appears a proceeding is "in the public interest."

Sometimes, the FTC "gets their

man." For instance, in December 2008, the FTC directed a U.S. District Court to temporarily halt a massive scareware scheme similar to those discussed above. According to the FTC, the scheme had tricked more than 1 million consumers into buying security products under names such as WinFixer, WinAntivirus, DriveCleaner, ErrorSafe and XP Antivirus by using an "elaborate ruse that duped Internet advertising networks and popular website into carrying their advertisements."

As a short-term solution, get the perpetrator's domain name suspended and/or launch a UDRP proceeding, if possible, to at least wrestle the phony URL away from the scammers. Posting a clear notice on your website is another useful step and a deterrent to further mischief involving any theft of your good name. 

Greg Sater is an attorney with Rutter Hobbs & Davidoff Inc., a law firm based in Los Angeles. He can be reached at (310) 286-1700, via e-mail or at gsater@rutterhobbs.com. Natasha Shabani is also an attorney at the law firm and can be reached at (310) 789-1858, or via e-mail at nshabani@rutterhobbs.com.