
DOZIER

Domain Name Dynamics

YOUR DOMAIN IS AT RISK IN TODAY'S ENVIRONMENT

BY JOHN DOZIER

THE LAWYERS AT MY FIRM REPRESENT registrars. We also represent domain name owners. And we sometimes represent domain name thieves (yes, everyone is entitled to an attorney). Here is an insider's perspective on the new dynamics at play in domain name cybersquatting.

Most domain owners think their registrar is licensed by some governmental agency with oversight responsibilities. That's not really the case. The due diligence of ICANN and registries in approving registrars is virtually nonexistent. All it takes to become a registrar is payment of the $10,000 fee. Yet my impression is that consumers take from the registrars a false sense of comfort — as if their mere existence ensures domain names will be protected.

That assumption can get you in a lot of trouble. Recently, several registrars have failed in a highly publicized fashion:

- Some went out of business and left the domain name owners in the dark, thus exposing those domain names to cancellation and loss.
- Others encountered security problems in which either the data queries or data flows were intercepted by unscrupulous third parties during availability inquiries.
- Finally, there are cases where databases were accessed legally and then filtered for incorrect email addresses; ultimately, the domain name involved was taken over.

Couple these issues with the fact that you never really know, in many cases, who you're dealing with, and you have a recipe for disaster. The problem, of course, is that there are no established due diligence or minimum standards involved in the application process; no meaningful standards of performance that would serve as an early alert system; and no one actively overseeing the performance of the registrars.

The problem is that there are no established due diligence or minimum standards involved in the application process

All of that means your domain name is at risk in today's environment. In fact, it may already be in someone else's hands and you don't even know it because most thieves will change the ownership information (or at least the email address and password) but leave it pointing to the real owner's site until the time is right to make the getaway. It's a bit like someone surreptitiously breaking into your business one night, ripping you off, then waiting until the next morning, during normal business hours, to walk out.

How do you solve this problem? You can't. However, you can take steps to minimize the chance of losing your domain name. Make sure you house your names with a reputable and reliable registrar. Make absolutely sure your email address is correct in your registration records. On a regular basis, check the Whois information and confirm you are still listed as the owner and all of your contact information is correct (most importantly your email address). Don't assume there is no problem simply because traffic still flows to your site.

What should you do if you lose your domain name? In most instances, it's not realistic to expect ICANN's Uniform Domain Name Resolution Policy (UDRP) arbitration to help you. It is not designed to deal with stolen domain names. If the thief is foolish enough to use the name in a manner that could infringe on your registered or common law trademark, a UDRP arbitration might be successful. Unfortunately, though, these thieves are usually much too smart to do that; they will sit passively on your name and wait for you to come knocking.

At that point, you can hire a lawyer to file a lawsuit — with little hope of recovering damages, as the new owners are most often overseas con men — or you can buy your name back from them in what appears to be a legitimate business transaction.

Does all this sound like the perfect crime? It comes pretty close. ■

John Dozier is president of Dozier Internet Law, PC, a law firm representing small and mid-sized online businesses. He can be reached at jwd@cybertriallawyer.com or online at Cybertriallawyer.com.