Hahn Loeser & Parks LLP

Domain Name Scams

By: Amanda H. Wilcox, Esq.

A company's domain name is one of its most valuable assets. Business could be brought to a halt if that domain name was suddenly lost. Unscrupulous parties registering similar-sounding domains, or country-code specific versions of the company's main domain name, can also be damaging to a company. Since companies realize the value of their domains and are protective of these assets, they can sometimes be easy targets for domain name scammers.

"Another company is trying to register your domain name or keywords."

One of the most prevalent domain name scams begins when a company contacts you claiming that someone is trying to register a version of your domain name in a foreign country. Most often, these inquiries are from China or the European Union, but they can be from anywhere in the world. Sometimes these inquiries are made by phone, and other times they are in the form of an e-mail from an official-sounding domain name registrar. The company will offer you the chance to register that domain name, (at a much higher price), to prevent registration by the third party. Usually a decision must be made on-the-spot, or within a very short time frame of 24 hours or less.

The companies will usually tell you that they cannot release the name of the third party for various reasons; the real reason being that these third parties usually do not exist. At the time that the communication is received, the domain name is usually still available. If it has been registered, the scammers are usually the ones who registered it as part of their operation.

The e-mails usually look very convincing, and many people fall for these scams. The companies appear to be legitimate upon first glance, and the e-mails refer to very official-sounding, but usually non-existent, government departments relating to domain name registration. Often, the registrar that the sender claims to work for is a legitimate company with a legitimate website. A clue that it is a scam is that the sender's e-mail address does not match the company's domain name. The scammers obtain the target's contact information from the WHOIS databases for related domain names.

If you do not do business and do not plan on doing business in the particular country where the inquiry came from, then you can ignore the phone call or e-mail. However, if you do business or plan on doing business in that country, you might consider registering the domain name just not through a scammer. Even though most of these companies can perform legitimate domain name registration services, it is not recommended that you obtain domains through companies that acquire most of their business through scams and charge fees that are at least 2 to 3 times higher than the market average. Instead, registration can be done through the official registrars.

The bottom line is that companies should be suspicious of unsolicited sales calls or e-mails pressuring them to buy domain names.