



McCord Web Design

2254 Ravenna Court • Waldorf • MD 20603-4966
Office: 301.705.7303 • Fax: 301.705.7618
Visit us on the Web at www.McCordWeb.com

Spoofing of Your Domain Name and What to Do About It

What is Spoofing?

Spoofing is an illegal practice of using someone else's domain name or email address as the sender or reply to address on an email note. This is a common practice used by spammers and it is illegal as detailed in the Federal Can Spam Act of January 2004.

We have been a victim of spoofing for 5 weeks and have worked successfully to identify the businesses that profited from the spammers, exerted pressure on those businesses to stop trading with the resources that were using the spammers, and significantly diminished the amount of spoofing of our own domain name. In this White Paper, we will tell you how we curtailed the spoofing and some of the actions you may want to take if this ever happens to you.

There is nothing more precious to your business than your good name and reputation! When someone else on the Web uses your business name to sell mortgages, male enlargement pills, Rolex watches, health insurance, pharmaceuticals, or various other sundry items, you can certainly feel overwhelmed that millions of people are thinking that you are actually participating in promoting this stuff. For us it was particularly difficult as we design and manage newsletter campaigns and we consider the spoofing detrimental to the growth of our business and damaging to our credibility of being a national resource for newsletter design and email campaign management. Our nationwide search engine positioning for newsletters is also the reason that we feel our domain was targeted by the spammers.

If this happens to you, don't be discouraged, get mad! You **can** do something to stop the spoofing and to protect your good name.

How Do You Know If You Are a Victim of Spoofing?

If you start getting a large amount of returned mail in your inbox, and we mean large, you may be a victim. Our mail spiked to over 1200 returned emails per day. Another signal is email from people you do not know asking you to remove them from your list. At first we were confused by this, but these notes must be taken seriously. Take a moment and look closely at some of the returned mail that you receive. Is your domain name listed as a sender?

Out of the thousands of returned mail that we received, we saw sender's names like Brenda.Fair@McCordWeb.com, Judy_Jones@McCordWeb.com, Carlo.Ferar@McCordWeb.com. There were permutations of every name possible, but what was most disturbing was that our domain name was used with every name and was listed as the sender and reply to address.

What Should You Do If Your Domain Name is being Spoofed?

The very first thing that you should do is to contact your web hosting agent and let them know what has happened. They may have specific tips and actions for you to take. At the very minimum you should confirm that your mail server has not been hijacked and is not involved in the actual sending of the spam that is using your domain name. Usually the agent will ask for several complete messages to review the header information to confirm this.

Our hosting agent confirmed for us that we were not the sender, and also offered to help us with Internet Service Providers in case we were banned or blacklisted because of the spoofing. Although

McCord Web Design is your nationwide resource for web design and internet marketing.
Visit us on the Web at: www.McCordWeb.com.

McCord Web Design

spoofing to the normal person is very disconcerting, be aware that you are not alone in having this happen to you. Unfortunately this is a common practice used by spammers in an effort to get readers to open their advertisement. Your web hosting agent knows this and understands that you are a victim.

The next thing you should do is to set up a folder in Outlook or Outlook Express and use a rule to send the returned mail to the folder. Save them, as you may need access to some of the messages as evidence. At the beginning we deleted everything as our hosting agent said that the spammers would move on to another victim in a week or so. When it persisted into the second week, we started to be concerned that it would not stop.

Report This Illegal Activity to the Federal Trade Commission (FTC)

If the activity continues past the first week, don't think that it will go away on its own. We didn't really get serious about finding the spammers until week 3. In the meantime, visit the FTC's website at <http://www.ftc.gov/spam/>. You may want to bookmark the page, as once you find a domain name, business, or individual that you have tracked the spam to, you can file a formal complaint against them. In about week 2 or 3 of your spoofing attack, start forwarding the returned mail to the FTC at their special database address spam@uce.gov. The mail that you send is entered into a database to look for overall patterns. We routinely sent 10 to 20 per day to the FTC.

One important note on the FTC: you would think that once you find the spammers that the FTC would step in, but because there is no money that is lost or invested because of the spam, do not expect any action to happen on the FTC's part. We were discouraged by this, but it is understandable that the FTC is investing their time in going after the really bad guys who are stealing money or identities. It is still important to file a complaint as you can use this a leverage to have legitimate businesses who are dealing with the spammer to take notice of you and to force them to stop the spoofing. Spoofing is illegal and any legitimate American business does not want to be involved in it!

Respond to People Who Send You Notes

It is awful to get notes from individuals who really think that you are involved with the spam. We received obscene cursing notes, demanding "stop this spam" notes, and "who are you?" notes. It is important to respond to these people to protect your business name and to let them know that your domain name is being spoofed, that you have nothing to do with the spam, and that you have reported the action to the FTC.

We always apologized to each individual that had received the spam even though we didn't send it. When they fired off their email, they didn't know that we weren't involved. Also, we had many people ask us to unsubscribe them. We sent them a note and explained that we could not unsubscribe them as we were not involved in the scheme. With a situation like this, we feel that we had to make an effort to put a human face on the problem and that we were real people who were being victimized.

You **will** get unsubscribe notes, be ready for them. We went to many of the actual websites that were referenced in the spam mail links. Nearly all had an unsubscribe page. Every single one we saw had what looked like a way to unsubscribe, but none had code in the page to process the unsubscribe request. You entered your name, clicked submit, and your request went nowhere.

When the Spoofing Doesn't Stop

If the spoofing continues into the third week, then you really have to take action as your domain may end up being used indefinitely. At this point we called the State Attorneys Office and were referred to the County Sheriffs Office. A Sheriff came out to our office to process our complaint. We found out that this is a hot topic with law enforcement right now. Many spammers are actually involved in identity theft. As ours was simply a spoofing situation, even though it is damaging, we had not been bilked out of money. As it was a Can Spam violation, spoofing fell under Federal jurisdiction. Even though not much happens by getting the Sheriff involved, you can tell your spammers and businesses using the spammers

that you have reported the matter, or that you will be reporting the matter by a certain date. If you can file a report with law enforcement, do so and record the case numbers.

What is Your Domain Selling Today?

We finally got so sick of the spoofing, that we decided that we would become a "customer" in order to catch the people who were using the leads generated by the spam and exert pressure on businesses to not fund the spammer. Our domain name was being used that day to sell mortgages so we clicked a link in one of the returned emails and completed an online loan application. We used our real name, phone number and address. This is really important: you need to save the spam in a special folder that has the link you clicked, as the people you catch will want to see the proof that they have been caught via spam and also you need to use your name and address on the application as this will identify you for tracing your lead back to the source.

The next morning; we got a phone call from Doreen at Quality Database wanting to confirm our interest in getting a new mortgage. We asked her to supply her business name and address, neither of which was legitimate upon research. We explained the situation and demanded that the spoofing stop and that their IT Manager call us. Then we started to get phone calls from mortgage brokers. We explained the situation. We decided that if we couldn't find the spammer, we would try to discourage these seemingly legitimate businesses from dealing with whomever they had bought their leads. Wherever we could get a business name, phone number, address, or web address, we researched it. For each address or contact we could identify and verify, we sent a formal cease and desist letter complete with the section of the Can Spam Act that was being violated and a synopsis of our problem. We let them know that we considered them part of the problem and that they were engaged in an illegal activity; even as an unwitting accomplice. In each note, we asked for them to turn over to us the lead generation company name who had supplied our lead to them.

As the IT staff from these resources called us, we had to send the spam that we had used to click the link to them showing the proof of our claim. After 3 days, we applied for another loan to see who we would catch this time. Again we repeated the same actions, emailing the cease and desist note, speaking with the President or CEO of the firm and following through by sending the proof of the original message and link.

Fortunately we found several CEO's who really helped to unravel our mess. Several were able to trace our lead back to one lead generation company called 4EveryMarket also know as LeadNation. We had 2 separate businesses supply us this company's name. If you are working on solving your own spoofing problem, know that a Can Spam violation means something to the businesses that you are approaching to report the violation. Don't waste time with tech support, go to the top, to the President or CEO of the firm and let them know your situation, that you consider it damaging to your business, and that it is a violation of Federal law.

Finding Your Spammers

In our research, we have found some great tools for tracking down spammers and try to getting their web hosting pulled or their domain name cancelled. The reality is that most of our spammers are working out of Costa Rica or China, so you may never really be able to find them, but knowledge is power and the more knowledgeable you are of the situation, the more seriously your correspondence to businesses who use the spammer will be taken.

Find domain names and IP numbers by looking at the headers of the emails that are returned to you. Some IPs will even make that easy for you by including the complete headers in the note that says why they are returning the message to you. In Microsoft Outlook, view the header by opening the message. Click View then Options.

McCord Web Design

Here are several great online research tools for researching domain names and IP addresses once you have them from the headers:

<http://centralops.net/co/DomainDossier.aspx> Research domain names and IP numbers

<http://www.dnsreport.com/> DNS Report identify mail servers

http://www.networksolutions.com/en_US/whois/index.jhtml Whois database by Network Solutions

<http://www.internic.com/whois.html> InterNIC Whois Database

<http://pgl.yoyo.org/odp/whois.php> Whois server information for out of country lookups

<http://www.yellowbook.com/> Look up business addresses and phone numbers

Approaching Domain Name Registrars, DNS Servers, and Hosting Agents

If you can identify a registrar where the domain name was originally registered, a DNS server, or hosting agent from the domain name registration, phone the registrar to complain, send an email to the abuse department (usually abuse@domainname.com) to complain about the spoofing activity to the hosting agent or DNS agent. Make sure to mention that this is illegal based on the US Federal Can Spam Law of January 2004. If you can identify that the registration credentials for the domain registration are fictitious, then phone the registrar and talk to a real person. Our spammer used the city as Baabba, in Ba state in country LB. He used this in several registrations with Tucows. We called the Tucows staff and they were able to turn these domains over to the abuse department for closure.

Web hosting firms will close an account that is used for spamming and ICANN will shut down a domain where the registration information is not legitimate and holds registrars accountable for the legitimacy of these records.

What Made Our Spoofing Come Nearly To A Stop?

What actually made our spoofing nearly stop was putting the squeeze on the lead generation company that was named by 2 mortgage companies as the supplier of our lead from the online application. We sent a formal cease and desist letter and followed-up with a phone call. We have been told by their IT person that if they can identify which "rogue affiliate" has done the spoofing, they will turn them over to us for prosecution. The same day, we went from over 1200 returned emails to our typical 150 to 200 spams per day most which gets filtered out by our anti-spam software.

We consider our experience a mixed success. No, we actually didn't completely stop the spoofing of our domain name, but lowered it to a marginal amount. What we found out is that these spammers are very slippery and that they are funded by legitimate businesses. If you are buying leads or email addresses for newsletter campaigns be very careful. Make sure that you see samples of the form that will actually generate the lead. Is the form in compliance with the law? How will the lead resource drive leads to the form? Ask for specifics and examples to be emailed to you. Check out the firm on the Internet for complaints that may be posted in Blogs (such as ours) or reports from other people who have identified that firm as the source of their own victimization. Make sure that you are not feeding the supply and demand market that is driving this black market cottage industry as your own domain may be selling Rolexes and mortgages next!