

It won't happen to me, right?

It won't happen to me, right?

That's what I thought! As many of you have probably already read in DNJournal or elsewhere, last week was a rough week for me.

I awoke Monday morning to discover that I had been hacked. Someone had stolen my domain name, CFJ.com, from my Godaddy account. At the time, we didn't know if it was isolated to that name or...

even just to Godaddy. So of course, wide spread panic ensued.

To clarify, the thief did not hack into Godaddy. It appears that they installed a keylogger on my computer, most likely by sending me an email which I in turn opened (although not necessarily with an attachment).

The keylogger then tracked my keystrokes for an uncertain period of time and relayed the information back to the thief until he/she had all the information they need (i.e.- my Godaddy Username and Password).

The whole thing was well planned and carefully orchestrated. The thief never even took possession of the domain name him/herself. The domain was sold on NamePros.com through private messaging on the forum prior to them logging in to my Godaddy account and pushing the domain to the account of the unsuspecting (perhaps naïve) buyer. The whole thing only took a couple of minutes.

The transaction, as I said, took place on NamePros.com. The thief sold/traded CFJ.com for a sum of cash plus 15 other domain names, mostly 3 Character .NET, .ORG and .COM domains. What boggles my mind is how someone could think they could buy a 3 Letter .COM for a bag full of mediocre domains and a small amount of cash? The buyer didn't even take the time to check the WHOIS first and see if they were actually negotiating with the owner of the domain or an authorized representative! Please, do us all a favor (as well as yourselves) and when you see a 3 Letter .COM domain name being advertised for sale on DNForum or NamePros at \$3,000 or less, use your better judgment and take a pass. At least do your due diligence to make sure you aren't buying stolen goods. If we all took some precaution it would make it a lot harder for these criminals to resell the stolen domains in the short window that they have to offload them and we could start making some progress towards stopping them.

I have to give a big applause to Godaddy, and specifically to my Executive Account Manager Tess Diaz, for the way that this situation was handled. They acted fast, were able to lock down the domain so as to prevent it from being transferred out of Godaddy, and everything was surprisingly non-bureaucratic, contrary to what people often

believe Godaddy can be. I actually find it hard to believe that any other registrar could have, or would have, acted in such an effective manner. In the end, we were able to recover CFJ.com safely back in to my account in just about 12 hours! Record time for a domain theft recovery. However, I can tell you that those were a rough 12 hours. Although they don't advertise it, Executive Account customers are eligible for a free security service at Godaddy called "Domain Transfer Validation Service". This service does not allow any domains to be transferred away from your Godaddy account without verbal authorization and a separate, secure authorization PIN from the account holder and can only take place at a pre arranged phone number which is not stored in your account (necessarily). Further, the only person authorized to transact these transfers at Godaddy is your account manager. Of course, I have now entrusted my portfolio of domains to this service and will begin migrating many of my domains not registered at Godaddy over to my Godaddy account. To my knowledge, no other registrar offers such a service.

I must also give a special thanks to Warren Weitzman whose advice on this matter was crucial in my timely recovery. Warren, unfortunately, was recently victim of an even larger hijacking when 12 of his most valuable domain names were stolen from his Enom account. It took 2 weeks to recover all of his domains, but luckily they were recoverable. Warren's advice to publicize the theft as broadly as possible was critical in the recovery process. Informing other domain investors, who are in general the only on demand buyers for these stolen names, is very important in order to prevent further reselling of the domain and complicating of the recovery process. It is also important to broadcast the theft because these are rarely isolated incidents and often, as was the case this time, there are other stolen domains also being marketed and often the owners haven't even discovered the theft yet. Awareness is a key element in prevention.

Domain Hijacking is on the rise, whether it's due to the depressed economy, ever increasing domain values or simply that these cyber criminals see the security weakness in the domain registration and registrar model and are exploiting it while they can, I'm not certain, but it is likely a culmination of all of these factors. These guys are clever, and unfortunately by definition, they are always one step ahead of the security software such as Anti-Virus and Firewall protection. Updates are created in response to new types of attacks.

I'd like to make one last note. Although I don't often like to speak badly about anyone as it doesn't reflect well, in this case something needs to be said and I can only hope it gets a reaction. NamePros.com was entirely uncooperative and unresponsive in this incident. Despite multiple phone calls and emails, I received no response and no assistance in this matter from them. The thief used NamePros to transact the stolen domain name(s) and the whole thing is well documented through private messaging and a forum string which I do not have access to without the help of NamePros. This information is critical to law enforcement in finding the identity of the thief, yet NamePros refuses to cooperate in any way whatsoever. As one of the leading forums in the domain industry, NamePros has a responsibility to help protect the community from these criminals. NamePros.com has often been the platform of choice for these criminals to offload their stolen goods and yet NamePros does nothing about it and takes no action in assisting the victim's (who represent their community) or law enforcement. I am sad to say that this time around, NamePros.com has failed me...shame on you!

Protect yourself the best you can with good antivirus software and firewall, but remember that awareness of your domain activity and having good contacts at your registrars is essential for protecting

your domain investments. Happy Domaining!