**Hacking eMail by Hacking DNS MX Records**

The president of Fastmail sent me a link this week which highlights a weak point in security, which are DNS registrars.

The link pointed to an article on the web about the guy who was the proud owner of the Twitter handle N. [He says](https://medium.com/@N/how-i-lost-my-50-000-twitter-username-24eb09e026dd) people frequently offered him money for it as a short name like that is difficult to obtain.

But he stubbornly hung on even when someone offered him $50,000. Now he wishes he had sold it, as someone stole N from him by hacking his DNS registrar thus taking away his email which let the hacker obtain the Twitter password.

**GoDaddy and PayPal, supposed Conduits to Crime**

I am not sure how much of what the victim says is true, but it was enough to convince the editor of that website to publish his article. Some of this sounds fishy.

The victim says the hacker contacted PayPal who gave him the last 4 credit numbers of the credit card account of the account holder over the phone. Then he used that to convince GoDaddy to let him change the recovery email on the account.

There is something missing here as GoDaddy requires a customer number and a pin. But let's assume this guy is telling the truth and analyze what went wrong and what you could do to protect your system.

**DNS Registrars and Email**

If someone cannot hack your email account by stealing your credentials, they can hijack your email by taking over your account with your DNS registrar.

In this case, this is what happened. The hacker used social engineering to convince GoDaddy to give him access to the victim's DNS account. Having gained access to login to the domain, the hacker then changed the MX records on the account. Then he was able to point the victim's email to whatever system he wanted where he could create that same email address.

Losing your email is much worse than losing any other password, because email is how people recover passwords from most sites. So the hacker went to the Twitter account of N and requested a password change. That mail was sent to the hacker's newly acquired email address. The hacker had now taken over the victim's Twitter account.

But things would get worse.

The hacker had access to the victim's DNS account. So he changed all the contact and administrative information on the domain. So when the victim called GoDaddy to protest, they said they could not help him, since he was not associated with the account.

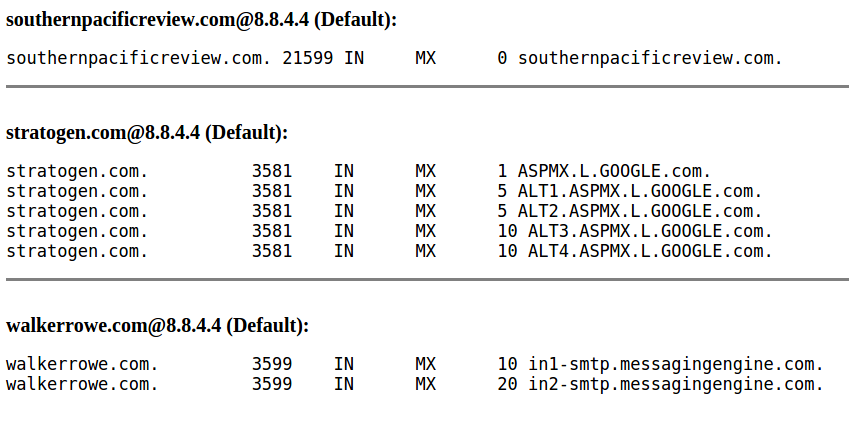
**TTL**

After he had been robbed, the victim presented a good idea how someone could protect themselves against this way. That would be to set the TTL (time-to-live) value to a high value in the MX record.

TTL is the time-to-live of a DNS record. When a DNS server has a DNS record in its cache, it will not consult the authorative source (i.e. the registrar) until the record has expired. If the DNS server does not have the record, it will ask DNS servers in its area for that. If they do not have it, the DNS server will look up the chain until it reaches the authoritative source.

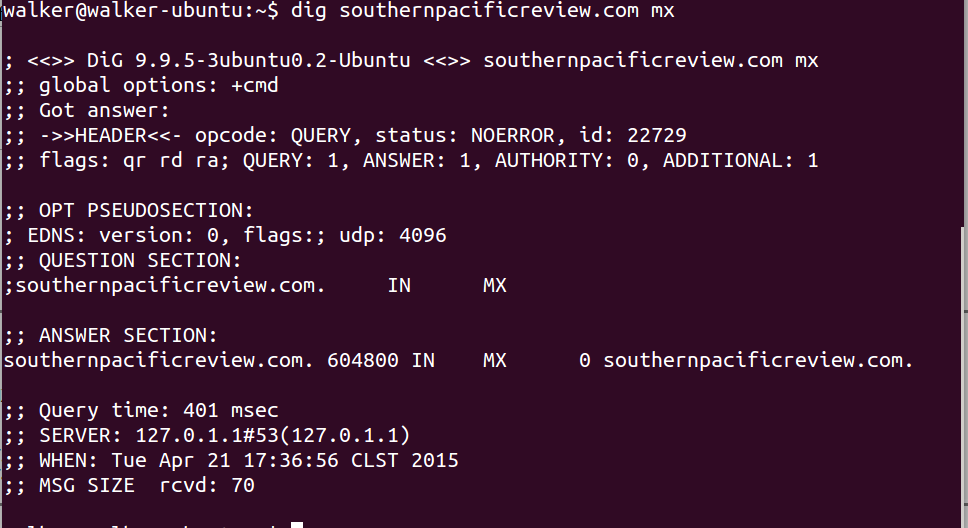
Your strategy would be to set the time-to-live to a high value and hope that the DNS server the hacker is using with his new email account does not consult the authoritative source, which would have been changed right away.

Let's illustrate. Here I run the dig command online and then run it from the command line. Dig is the command to query a DNS server. You can see three different domains below and their MX records. On the first one, the TTL value is 21599 seconds, which is 6 hours. As you can see this is querying the DNS servers at Google, whose IP addresses 8.8.8.8 and 8.8.4.4 are widely known.



We changed this DNS record a few hours earlier to set the DNS record to 604800 seconds, which 168 hours or 7 days. This should give you time to contact the registrar and get your DNS record back.

That is shown below in the dig command issued against another DNS server. This is the situation that you want. Because if a hacker changes you account they might have to wait up to 7 days to snatch your email meaning have it sent to the new address.



How would you know that your DNS record has been hacked? The provider should send you an email notifying you of any changes made at ther instant is was changed. If you they do not tell you then you could be in the impossible situation of this poor fellow if you registrar will not give you back your account over the phone.

If everything is as this guy says then PayPal and GoDaddy and other registrars need to improve their employee training so they do not give away any information, especially the last 4 digits of a credit card, over the phone.

This is worth a phone call to your register to ask them what are their policies and what additional steps you can take to protect your domain.

All seems to have ended well, as you can see now that the author of that article has [his Twitter account N](https://twitter.com/N) back. He must have finally been able to get someone on the phone.