

Forum:[Hack Forums](#)

Thread: [Private Investigation Tutorial: Secure Your ISP Account](#)

Surmise - May 27, 2018, 9:24 pm

Securing your ISP (Internet Service Provider) account is crucial if you want to maintain anonymity online. If an experienced P.I discovers your IP address they can do a lot more harm than just DDos your connection or find your zip code. Through a method known as "social engineering" an attacker can attain the ISP account holder's credentials such as their full name, billing address, phone number, payment information, ssn, mac address, etc. This is why it's important to constantly use a secured virtual private connection when your on your home connection. However if your IP address has already been leaked there is a way to secure you account so that social engineers can not obtain your information.

First, you must call your ISP when their customer service hours are available. If you do not know what your ISP is then go to <http://ip-tracker.org/> and look for "My IP ISP". Make sure you have all of your information ready in case they ask for it such as your account number, street address, etc. Navigate your way through the automated messages to get to the internet troubleshooting department. Once you are connected politely ask the agent to speak to a higher-up or a manager. If they ask why just tell them you are concerned about your account security and you'd prefer to talk to someone in a higher position. Once you're connected to a manager try to explain the following without sounding like a complete fruit basket. "I have people trying to get my information online and I believe they're going to try and hack into my [ISP] account. I'd like to place a flag on my account so that no one can get any information on my account without confirming a pin code." They might ask you additional information to confirm you're the account owner but after that they'll ask you the pin you want and you'll be secure. I've done this with every provider I've had with success. This tutorial is short and simple but not many people know this method and it's great to add further security to your identity.

StackFramed - May 29, 2018, 3:13 pm

You might have a better chance of this working if it were a smaller, local ISP, but generally this isn't going to do much. Employees sit there getting paid next to nothing just to take shit from frustrated customers all day. They will most likely not even notice the note. Even if they do it can be easily overridden with some extra SE. Besides, this isn't even allowed by default. All ISPs have a privacy policy in place disallowing employees from giving out information over the phone, yet ISP doxing is still effective today. A little note will do jack shit.

Tom Cruise - May 29, 2018, 7:05 pm

The issue with this I am sure is that they can still obtain information such as your address/MAC Address/Router name/Name and Last name/Phone number honestly this doesn't change a thing but not to let anyone compromise your ISP account or it makes it harder, I guess I could say it could work but information is gonna come out of somewhere.

I like you thinking :)

Surmise - May 30, 2018, 6:54 am

(May 29, 2018 03:13 PM)StackFramed Wrote: [\[CITE\]](#) You might have a better chance of this working if it were a smaller, local ISP, but generally this isn't going to do much. Employees sit there getting paid next to nothing just to take shit from frustrated customers all day. They will most likely not even notice the note. Even if they do it can be easily overridden with some extra SE. Besides, this isn't even allowed by default. All ISPs have a privacy policy in place disallowing employees from giving out information over the phone, yet ISP doxing is still effective today. A little note will do jack shit. I've done this method personally with two ISP's, both of which were smaller like you mentioned. It worked extremely well both times I had multiple people try and social engineer my information and they weren't able to pull anything. I understand this might not work with larger providers such as Time Warner Cable and Comcast. I've had this method written in my notes for a while now and I just decided to expand upon it and write a tutorial explaining how to do so.

I appreciate your input.

WhiteTiger. - May 30, 2018, 7:49 am

What a useless post.

Almost all IP addresses are dynamic by default.

You have little to no idea what you're talking about.

~WT

Surmise - May 30, 2018, 8:21 am

(May 30, 2018 07:49 AM)WhiteTiger. Wrote: [\[CITE\]](#) What a useless post.

Almost all IP addresses are dynamic by default.

You have little to no idea what you're talking about.

~WTMy IP address has been the same for about a year now. This is still resourceful regardless of whether you have a static or dynamic IP address, don't claim I don't know what I'm talking about when you're ignorant to the entire post. Like another member said ISP doxing is still effective today and so is this method.

?Criminal - May 30, 2018, 6:20 pm

(May 29, 2018 03:13 PM)StackFramed Wrote: [\[CITE\]](#) You might have a better chance of this working if it were a smaller, local ISP, but generally this isn't going to do much. Employees sit there getting paid next to nothing just to take shit from frustrated customers all day. They will most likely not even notice the note. Even if they do it can be easily overridden with some extra SE. Besides, this isn't even allowed by default. All ISPs have a privacy policy in place disallowing employees from giving out information over the phone, yet ISP doxing is still effective today. A little note will do jack shit.

agreed, most tools that are modem provisioning related do NOT store notes on file anyways, only billing tools such as ICOMS allow agents to make notations so anytime you dox by IP the agent will 90 percent of the time never see the note unless they also use a billing tool with the modem provisioning tool. I consider this technique a security by illusion trick, it gives the illusion of security but really doesn't change much however it may impede an attacker that's ISP doxing with anything outside the IP address and even then the note can be overridden with a new notation like stackframed said or flat out ignored if you say the right things. There's many more effective anti ISP doxing methods out there but the most simple one is to just use a 4G LTE modem and the IP will literally change every couple days if not every couple hours, 4G IP pools are expansive because they tend to utilize ipv6 and 4G's are much more complex to dox but not impossible, that's just one example of many.

Condescend - May 30, 2018, 6:32 pm

(May 30, 2018 08:21 AM)Surmise Wrote: [\[CITE\]](#) My IP address has been the same for about a year now. This is still resourceful regardless of whether you have a static or dynamic IP address, don't claim I don't know what I'm talking about when you're ignorant to the entire post. Like another member said ISP doxing is still effective today and so is this method.
VOUCH.

This thread makes complete sense. Regardless of your IP Address' architecture (static or dynamic), ISP DOXing is still a really viable threat, as long as the perpetrator isn't an idiot and knows what they are doing and how to do it.

The amount of static IP Addresses I run into highly outweighs the amount of dynamic ones, at least in my experience. Although the recommendations mentioned in this thread may not be as effective when it comes to larger-based ISP's, it will work for the lower spectrum, and is very helpful to those few.

Great thread, OP. I appreciate it.

Surmise - June 1, 2018, 6:00 am

(May 30, 2018 06:32 PM)Condescend Wrote: [\[CITE\]](#) VOUCH.

This thread makes complete sense. Regardless of your IP Address' architecture (static or dynamic), ISP DOXing is still a really viable threat, as long as the perpetrator isn't an idiot and knows what they are doing and how to do it.

The amount of static IP Addresses I run into highly outweighs the amount of dynamic ones, at least in my experience. Although the recommendations mentioned in this thread may not be as effective when it comes to larger-based ISP's, it will work for the lower spectrum, and is very helpful to those few.

Great thread, OP. I appreciate it.I appreciate your vouch. Like I mentioned before this may not work for everybody, but if it does then it's added security to your identity and that can never hurt.