Anonymity

<? By cwade12c from HaxMe ?>

cwade12c

Anonymity is an important tool to have at your side when scaping the net.

Rather you are an elite guru or are a general internet abiding user, anonymity

is important to anyone and everyone.

The only thing currently keeping your identity away from sensitive eyes are the current tactics and methods our web has inherited today. What if those tactics and methods change tomorrow?

// Table of Contents

Networks and the User

Scientifically, there are many networks – social networks, data networks, epistemological networks, and more. The one thing that all networks have in common is the boundary of compromisation. If you compromise a network's ability to transmit data securely, you may have access to that data. Data doesn't necessarily have to always be a user driven name or password. It can be many variables; from bytes to infrastructures. The main focus of what we're focusing on however, is THE network, the net, the internet… the home, to hundreds of millions of people, simultaneously transferring data as each nano second passes by. You could be sitting in Kansas right now browsing YouTube, while someone in China is hacking YouTube. Just how safe are your vitals? The internet is a battle field. No where in the net is there a nice, general, safe zone. There is no safe web site, rather the site is protected by SSL and is named Google or not.

Just because I can't hack Google does not mean that Mr. 1337 can not exploit it. There is no such thing as a secure system. There will always be a hole to take advantage of. This is the creed to hackers, and is a law to any savvy programmer. With that in mind, you may be wondering how "alert" you should be. It does not matter if you have a good anti virus and firewall installed, with anti-keylogger protection with a daily root-kit scan preset and ready to go on your terminal. If you have some sort of external network output connected to your system, you, and your information is vulnerable.

Just how vulnerable, you may ask. That, depends on how you define yourself.

- You use your first and last name for a few web applications, like Facebook, email, and YouTube.
- You have a handle which you use for everything.

A handle is a nickname which you go by. In other words, this is equivalent to an X-Box live gamertag. If you have a mixture of both of the above bullets, then place yourself in the 1st bullet's category. If your handle contains your first or last name, then place yourself in the 1st bullet's category. If you are in the 1st bullet's category, you are in trouble. Don't have a panic attack; this does not mean that one has your social security information and you are now screwed. All this means is that you have lost your 100% anonymity out reach.

I myself am far from anonymous online; despite how much I wish I could be anonymous, it is too late to make up for some mistakes I made in the past, and that is why I am writing this guide for you.

There are many ways on how the systems works, and there are many ways to gather information from the system. The system is not intelligent, it is only artificial and is programmed to run certain commands. The net is a system of infinite code to the human mind. While infinite does mean endless, with that noted; means that exploitation is also endless. While exploitation is endless, you can indeed stay on top of the game and avoid exploitation very swiftly. If you are in bullet 1, you need to start over. Delete all traces of anything relating to your name. No Myspace, no facebook – no more of that Runescape with membership, and definitely no emails with your full name in the address!

The internet is cached constantly, so depending on how long you've been in bullet 1, your near 100% anonymity out reach may be out of luck. If it is, we can still get you to about 70%. If you are in bullet 2, or, want to get into bullet 2, read on.

Forms of compromisation

Your identity can be compromised in various ways. There are multiple ways you can do anything in life – this also means there are multiple ways you can leak your information. Take this “logged script” of the life of a regular networking user for example.

- ➔ I connect to the internet for the first time. Yay!
- ➔ I decide to make an email account with my first and last name. Hell, I select my mother’s maiden name for my security recovery question.
- ➔ Now I have my email. Cool, lets go make some friends!
- ➔ I join a bulletin board with my first name and some random numbers.
- ➔ I post at the bulletin board for a while, meet some cool people, and exchange emails.
- ➔ I decide to make a Myspace, upload some photos of myself, and add these cool new friends.
- ➔ My hometown is listed on my profile, and I just posted a bulletin about how awesome Tony’s birthday was. Man, he was so wasted!
- ➔ After using the internet for a few months now, I have decided I want to make a blog to keep my online buddies informed.
- ➔ I change my username from ‘myfirstnamewith289049874’ to something more interesting, finally.
- ➔ I go ahead and purchase a domain name. Yay!
- ➔ I have no money for vBulletin, so I go ahead and download a pirated version and upload the PHP files to my site.
- ➔ My new blog and bulletin board is up and running. Sweet, I now have 20 members!
- ➔ The time has come to make a Paypal. I’ll use the email I first created to link to this Paypal.
- ➔ I have verified my Bank Account to my Paypal, added 2 credit cards, and added my Social Security Number.
- ➔ 2 of my new friends have donated. This is so cool.
- ➔ I have withdrawn $2,000 from my bank and put it into my Paypal so I can make online purchases a lot easier.
- ➔ I love the internet.

How many times do you think this person's information could have been compromised? How much of the information could have been gathered and used against this person? Lets find out.

*Creating an email using First and Last name

*Using mother's maiden name for security recovery question

*Any use of first or last name in a handle

*The exchange of their personal email

**Creating a Myspace with accurate information

**Uploading a photo of you to Myspace

**Posting a bulletin on Myspace, even more so about anything in your real life

*The purchase of a domain name from any public registar

*Any nulled script

*Administrating a website

*Making a Paypal, linking it to a personal account

*Linking your bank to your Paypal

*Adding credit cards/debit cards to your Paypal

*Applying for a Paypal debit card (Social Security No.)

*Receiving money from ANYONE to your PayPal

There are 15 good and easy ways to gather information about the above given person, and that is only from that person creating an email, paypal, myspace, and posting at a bulletin board. Imagine all the other daily activities YOU do on the net! Do you do them safely? Lets analyze.

Creating an email using First and Last name

This is a 100% **no**-**no**. If your email is spidered, if you signup for the wrong thing and they give out your email, if you catch a virus, if your friend tells somebody, IF IF IF IF… then, the enemy already has your first and last name. They snatch your IP address, run a search in your hometown with your first and last name, narrow results down, g-map your location, grab your phone number, the numbers of your jobs and family members… things can get bad if you get on their wrong side. Your first and last name in this world isn't restricted or hidden on the internet all the time. There are only so many "John Smith"'s living in Los Angeles, CA – and it's only a matter of time before the enemy finds the correct one. If you have ever committed a crime or have failed to pay taxes, it becomes 3 times as easy to find you.

Using a mother's maiden name for a security / recovery question

Security questions for emails and other sorts of online applications are used to recover your account if you ever forget your password. How smart do you think it would be to have your email:

Johnsmith123@host.tld

With a security question of your mother's last NAME? They already have your last name, that's 50% of the way there! The best thing to do for security questions is to write your own. Write something which will throw an enemy off. For example:

"What is my favorite song name, backwards?"

Then for your answer, have the answer be the barcode printed on the bottom of your keyboard. Your barcode will always be there, and it will always be in a place where you will have access to. Having a security question of random letters and numbers (alphanumeric) is a GREAT security precaution to add to all of your online accounts. JUST MAKE SURE YOU DON'T FORGET THE ANSWER!

Any first or last name in a handle

This is almost the same scenario as creating an email with your first and last name. Not only does the whole world know your first and last name; but if you use your handle for things like P2P applications, social networks, and websites; your IP Address can easily be obtained, and more information about you can be gathered. It is best to refrain from creating a handle that has anything having to do with any of your real life information. Simply create a "new you".

The exchange of your personal email

IF you ever decide to use a personal email for things like family and business reasons, it is best not to sign up for ANYTHING with your personal email, even if it seems like a legitimate website or service. Never exchange your person email address with anybody; it is best you create a “second” email which you use specifically for things.

I myself, have a whole bunch of emails! One for spam precautions (signing up for websites), one I use for Paypal donations, one personal one, one I use for MSN, one I use for AIM, one that I use for exchanging with people and friends online, and about three other emails I use for other cases. You can never have too many emails, and don’t you forget that.

Creating a Myspace with accurate information

The day you create a Myspace or Facebook is the day your anonymity goes to hell. Even if your profile is set to private, some of your information is public – and then the factor of all your friends’ profiles + unwanted eyes goes into account. You can not control your friends and their profiles, so what happens when the enemy hacks one of your top friend’s profiles and has full access to your profile? Even worse – you don’t know who you are talking to on Myspace all the time. I have hacked plenty of my friends in the past and have social engineered other people through their profiles. Myspace and Facebook are danger zones, so stay away from it if you want your information away from the internet’s archive.

Uploading a photo to Myspace

Rather you know this or not, Myspace and Facebook are opted into a program where even if you delete your photos, they have your photos cached and archived. Your photos go into a database, and the FBI and other agencies can access those photos if they request it via only having your… *drum roll* first and last name. That and, anybody can download your photos and re-upload them ANYWHERE. With facial recognition software advancing everyday, it is best that you keep your real life photos away from the internet.

Posting a bulletin on Myspace

Everytime you post a bulletin on Myspace, it can be read by sensitive eyes; even worse, it could be archived by a bot you have mistaken as a friend. Your best bet is to not post bulletins on Myspace, let alone, even have a Myspace! Myspace is a very dangerous place to be at; and is one of the easiest places to gain intel on any given person if they have a Myspace. If you have posted real life information in bulletins in the past, facepalm yourself now, and do not ever do that again. Leave real life information to real life people, and away from the internet! Call your friends or txt them, just whatever you do, don't do it on Myspace!

Purchasing a domain name

This is not a bad thing, but if you just go ahead and purchase a domain, then you could be in a lot of trouble. There is an information movement that the web archives, called "Who-Is"… and it is a collection of all of the holder's information to each given domain. It is an extremely large database and agency; you go to: http://who.is – type in a domain name, and there you go… you now have the first and last name, address, phone number, and contact email of the owner of the domain. You can avoid this threat by registering with a registar who offers PRIVATE WHO-IS upon domain registration. Some registars try to charge you; simply avoid registars who want to charge you, or, who don't offer the option on the domain registration page itself. Try this site, $8.99 / yr Domain Names with free PRIVATE WHO-IS:

http://arvixe.com

On a side note, just from experience; avoid yourself the trouble and stay away from 1&1 and GoDaddy. Their prices look good, but their ToS and Policies WILL get you into a lot of trouble. 1&1 did not tell me that my domain was ready to be renewed; and they tried to kept charging me without asking me, and they kept getting denied. They sent me NO notice, and I was reported to credit collections agencies, ruining my credit. It's simple: stay awaaaaay from 1&1 + GoDaddy, and… places who charge for Private Who-Is or offer no Private Who-Is.

Using a nulled script

Using a "cracked version" of scripts are dangerous. A nulled script means that a script has been edited of callbacks and whatnot; and anything that has been edited has the potential of containing a backdoor, and out of the 500+ PHP files uploaded and being used on your server, you wouldn't know which file was serving as the backdoor, simply using a one liner *mail()* function to mail the enemy your login information every time you logged into your site. Your best bet is to purchase your scripts, or, use alternate freeware versions. There is no such thing as a reliable, nulled script.

Administrating a website

Anytime you become the admin of a website, many more factors come into play. To protect your information to its full potential, you need to be smart in three areas.

1. Local Side
2. Public Side
3. Third Party Side

Local Side: Locally, your website needs to meet secure standards. You need to be running the latest version of PHP, you need to be running the latest server kernel, and you need to make sure that you used the best security precaution methods when customly coding your own files. Disable dangerous PHP functions, turn safe_mode on, store sensitive files outside of your public_html directory, don't allow ' % and other dangerous characters in any sort of fields which are processed. Use good coding habits and always be aware. Raw Access logs are your best friend.

Public Side: Publicly, you need to be careful on what you display. We're not talking about the art of exploitation anymore, we're now talking about how you display yourself as a person, and how any ties could play a factor of finding out your credentials and real life information. Leave no trace backs. If you can live with it, be somebody you aren't – but that doesn't mean you need to give up your personality and good habits!

Third Party Side: Any http:// aspect aside from your own domain and files we will consider third party. Rather you use an API, an iframe, or some sort of include; you need to be sure that anything third party does not link to your main aspects of personal information whatsoever. If you have a Paypal and receive donations on your website; make another Paypal with a fake name. Accept donations on the fake Paypal, and every month send your collections from your fake Paypal to your real Paypal.

Administrating a website is important. Never leave your website unattended for more than three days, even if you have other staff helping hold down the fort. If you can not attend your website for more than three days, ask for an administrator you trust to report to you everyday somehow any new intel.

The main keys to administrating a website are:

- ✓ Having a private WHO-IS
- ✓ Having a good reputation
- ✓ Having no trace-backs + a disguise
- ✓ An A+ Local Side
- ✓ An A++ Public Side
- ✓ An A+++ Third Party Side

Paypal Hazards (Linking your bank, adding cards, applying for a PayPal card, receiving money)

Paypal is probably the biggest online source for securely sending money, receiving money, and using Paypal to purchase items and subscriptions. While Paypal is extremely secure, extremely secure things require a lot of information from you. In order to have a verified Paypal account, you need to enter in your First and Last name, an email address, a phone number, and an address. Now these can't just be random letters and numbers like we can enter on some sites; because if you start handling a lot of money and have false information, you can get charged with fraud. Paypal is an important part of the internet; if you use it responsibly, you can get around multiple roadblocks.

Linking your bank: A user links their bank account to Paypal to verify their Paypal account. This is a great feature because you can send money in between your bank account and your paypal account. This is also risky as most of the time this almost always confirms your identity. There are indeed ways around this, but there aren't legal ways around this.

Adding cards: A user can add credit and debit cards to their Paypal account to make payments for specific items easier and more doable. This is risky because of the name on the card(s) and for VARIOUS traceback issues.

Applying for a Paypal card: A user can apply for a Paypal debit card by entering in their social security number. I would never enter my Social Security number on the internet, despite how secure Paypal actually is. You can come up with your own reason of why you shouldn't do this right now.

Receiving Money: Everytime you receive money from somebody, they gain your contact information. So, our enemy could send us $0.01 as a donation, and then they would have a lot of your intel. Seems like a bargain to some.

The bottom line is that PayPal is a very dangerous place to be at. I'm not going to say you shouldn't use it, because PayPal is a very powerful tool for making payments and receiving money online! I'm saying, if you don't know how to use it appropriately, then you shouldn't use it. PayPal is, and will probably always will be, a one-go-show. I have used a fake name on PayPal before and wanted to withdraw money from my PayPal into my bank. Obviously, a fake name + my real name on my bank account sparked some problems. Long story short, I lost $200, and was fined $50 by my bank. Use PayPal effectively, and don't be stupid with it.

Secure Tips

While we've been talking about all of the ways you can be compromised, lets start talking about ways you can protect yourself. Afterall, this read wasn't written to scare the reader. Anonymity is something special; and if you have it good, you should be very happy. Anonymity is sort of like money, however…

Certain people get a certain amount of money for their jobs.

Users get a certain amount of anonymity for their group.

A good hacker is probably going to have more anonymity because they don't want to be public with their information. A regular internet user who just uses the internet for Myspace, YouTube and emailing is going to have horrible anonymity because they are more public with their information. HOWEVER; if you work harder at your job, you can get a bonus. If you are a regular internet user, you can work harder to remain the same regular internet user, but have the anonymity of a hacker.

The first step you're going to want to take is creating yourself a handle. If you do not have a handle (nickname), here is an idea on how you can get started. Think of something you really enjoy. Thing of your favorite number, and think of your favorite color.

Bluballer34

You can get more technical and creative with your handle if you wish, and replace some letters with numbers which look like the letters.

BLuba113R34

These however, are just examples that were written off of the top of my head. Take five minutes, and come up with a name you want to go by for the rest of your internet days.

So after you've gotten yourself a handle, you're going to want to abide to that handle. Never go by your first name on the internet! If you decide to make a Myspace or Facebook for some reason, do not upload a photo of you – and use your handle for the fields of First and Last name for social network based sites. Have minimal information about yourself and add people who you only trust 100%.

Create a few email addresses. One for spam, two for casual, and then, +1 additional one for any MAJOR service you will be subscribing to. Make sure the email accounts do not link to each other whatsoever; never have an “additional email address” selected, unless it is locked down and is secure!

Never use the same password for everything. I know so many people who do; and I’ve been able to gain so much information on a person just because I had gotten their one password they so happened to use for everything – emails, paypal, youtube, and work. Use an alphanumeric (aZ09) password. For example:

xD3AlfM49dAeFjaN

If you can’t remember your passwords, keep a master log somewhere safe, or, use LastPass. LastPass is a secure service which manages all your website logins and information for you. If you decide to go this route, have an extremely secure password for it. My password for LastPass happens to be about 64 characters long.

Take additional precautions. Anti-virus software and firewalls are great, but I myself, have a kernel level software installed which encrypts my keystrokes at kernel level before they are actually interpreted.

Kernel -> Encryption -> Encrypted text wherever you type it -> Software, instantly decrypted

Additional precautions are always good to have. If you have a master password log, make sure it is encrypted and it is only accessible through a special code or password.

Hide your IP Address. Enroll yourself in a Virtual Private Network. Forward internet activity via SSH to mask your IP address. Do whatever you can to hide your IP Address. When downloading files from the internet, make sure you have PeerBlock installed. Never use CGI/HTTP proxies unless you are desperate. Some free, good proxies are:

*Hotspot Shield

*TOR

*HideMyAss Premium

Encrypt your connection. Encrypt both your incoming and outgoing packets, to guard yourself from a monitoring ISP or a government agency. I myself always have UltraVPN running.

Link accounts. Use a fake account for your main source, and transfer variables to your real account through multiple fake accounts.

Get off of Internet Explorer. Get something faster and more secure, like Firefox or Chrome.

Get friendly. Start to get away from GUI and get familiar with CLI. You will have a lot more freedom out of Windows. When kids grow up, they move out. When you become familiar with computers, guess what – time to move out. *NIX yourself.

Delete online data when you are done using it. If you are pasting information via a pastie based website, make sure you have the option to delete your paste. Delete uploaded files when you are done sharing them – so make sure you have a registered account.

Use a voice distorter when using VOIP. If you are serious about what you do, then you could see why this is a big plus.

And last but not least, always be ready to disappear. If you ever become compromised, end your handle, delete your accounts, and start fresh. ALWAYS be ready.

Entering the net from scratch

The following is going to be a dramatic and fictitious log about what I would do if I were to start the net from scratch and were extremely paranoid about my anonymity. You can take some of these habits and vary them to best suit you.

When first connecting to the internet, I would go and get myself Mozilla Firefox and Google Chrome. I would install them both and say "goodbye" to Internet Explorer. From there, I would download Kaspersky Antivirus and Commodo Firewall. I would install them and set their settings to best suit my needs of protection. After this, I would install KeyScrambler to eliminate threats of keyloggers. I would then download UltraVPN to encrypt my inbound and outbound connection, and to assign me a private IP Address. Through this, I would go ahead and download PeerBlock, and would download all of the anti-government and anti-piracy IP lists. I would have PeerBlock run on startup, along with my other downloaded and installed softwares. Now I would pick myself a handle I would go by. I will give myself a fake name, age, and location as well – just in case anybody asks for my story along the way. Time to create my first email – I will create myhandle@host.tld at gmail, aol, yahoo, and live. Then I will create a spam email address at gmail, to handle potential spam in the future. For each of the emails I have created, I have used a different 16 character alphanumeric password. I am keeping my passwords stored in an AES encrypted .txt document which I have masked as a .jpg file, and hidden in my C:\Windows directory. Now I am going to create myself a YouTube account. I know YouTube sends A LOT of email notifications, so I'm going to assign my own specific email address to YouTube. I think I'll use my Yahoo one for YouTube, and that email will never again be touched. Now I think I'll go make a Myspace. I'm still using UltraVPN and Peerblock, and Myspace tends to be tricky and annoying with their emailing system… I'm going to assign Myspace specifically to my aol account. Now that I am registered at Myspace, I'll use my fake credentials, and in the About Me… I'll give them my fake story. I'll add my real life friends, and will disable comments on my profile. If they ask about why I am hiding, I will tell them why; and I will only use MySpace to message them about general internet topics – nothing too real "lifeish". I will use an animated avatar for my Myspace photo; and I'll use a picture of some chubby dude as my backup. ☺ Now, I'm going to go register at multiple forum boards. For these forum boards, I'll use the same spam email address I have made. I'm starting to meet some cool new people; they want my story, so I give them my fake one. It's time to create my website. I start off at x10hosting and have some loyal members. I decide that I want to receive donations via Paypal. I make three paypal accounts. One main one, one middle one, and one fake one. I use the fake one to receive the

donations. I transfer the donations from the fake one with the fake name to the middle one, which also has fake credentials. From the middle one, I transfer the donations to my real Paypal which has my real life credentials. I have linked my real Paypal to a personal email address which nobody but myself will ever know of; and it is NOT RELATED TO MY HANDLE WHATSOEVER.

I now have money to purchase a vBulletin skin, but not vBulletin itself. I proceed to download a pirated version of vBulletin, with PeerBlock ON. The pirated version of vBulletin is the retail, meaning, not nullified or modified. I check the md5 checksum of the files compared to vBulletin's stated checksum just to make sure there is no possible backdoor. There isn't. Now, I proceed to nullify the script myself, by removing all callbacks. Now that I have successfully nullified the vBulletin script by myself, and am assured that there are no backdoors; I have it running on my site. I make a $15 donation to vBulletin through my middle man account, and I buy a vBulletin skin from some other site through my fake account. My fake Paypal accounts were verified from Pre-Paid Debit Mastercards I purchased at the super market. Now I get my site going. A month later I decide to get myself a domain name. I do so, with private WHO-IS ticked even before I purchase the domain. I'm now moving from x10hosting to some offshore hosting in another country who aren't liable to give my information out; though, I am paying them through my middleman PayPal account, and that won't matter. I earn enough money to donate the rest of what is needed to pay for a legal vBulletin to the vBulletin organization. My site is going good, and is growing. I'm starting to get a little too much attention on my handle. Should I change it?

I somewhat used to be like the person described above. I was known as Devin Cummings, age 28 from Los Angeles, CA, 90001 working for X1 Security Corporations. I had a Myspace, a fake picture, and a few different handles throughout my time.

I finally decided I wanted to give it up when I knew that helping people wasn't going to be easy being so "anonymous". I'm no longer Devin.

Paypal, email, & ISP worries

These are the big three which can cost somebody their anonymity. These three things are powers of the web, if you will. Paypal, because they are like “The Bank” of the internet… email, because it is used for almost all means of personal information transferred through the web, and our ISP’s… because our ISP provides us the ability to connect to the internet; which also gives them the ability to monitor what we visit and download.

PayPal: PayPal is one of those services that requires your accurate information for it to be useful to you. PayPal is one of those things where if you want to work with money, you can not hide your identity. First and foremost; PayPal is the last thing you would ever want to get hacked. Your phone number, address, and other contact information could easily be stolen; as well as your money, and your routing number to your bank. If you want to have a legitimate PayPal, but yet; what to remain anonymous, create a chain of PayPal accounts, as mentioned earlier. One should be created with a one-time PayPal only email address, with full accurate contact and bank information. The second should be created with one of your “spam” email addresses, with fake information and activated via a Pre-Paid Debit Card ($5 at any super market). The third PayPal account should be made with another spam email and with a fake information; you should activate it through someone else. There are many forums online that have communities where they will help you activate your account. You can even BUY an activated PayPal account online for no more than $10.

Email: Email is a service which is frequently used on many levels. It is used on personal levels, management levels, and corporate levels.

Personal Levels

Personal levels are emails sent back and fourth between friends and family.

Management Levels

Management levels are email notifications / activations, subscriptions, and reminders from important services and whatnot.

Corporate Levels

Corporate Levels are emails for businesses and work; administrative purposes, and other such related tasks. These emails are all usually sensitive.

If you are a regular internet user; the odds are you have an email address. Most internet users have one big, clustered email address they use for everything. Third party services, games, subscriptions, PayPal, and work. If this is the case, your chances of staying anonymous just became a lot lower. Having multiple email accounts is a core priority to anonymity; and is good practice to avoid tracebacks.

ISP: ISP stands for Internet Service Provider. There are many different ISP's around the globe, and they provide internet for yourself and I. Each ISP has their own policies and terms of service. Some monitor downloads, some don't. Some have bandwith caps, some don't. Some block certain websites, some don't. The internet is meant to be a place of freedom of speech. Your first priority is to find a ISP who will not monitor you, and who will not bandwith cap you. After you have found one, you should dig in on their terms of service, and abide to their terms as best you can. Almost any law agency can contact an ISP and gain contact information of a person if they have probably cause via an IP Address. Imagine if the enemy can social engineer! See **Security Tips**, and how to go about hiding your real IP Address from others.

While there are solutions to best anonymize yourself while using PayPal and email, you can't fully hide from your own ISP! It is best to start encrypting the traffic which passes through your router/modem. If you have a dynamic IP address, you should try to renew your IP address every week or so. If you have a static IP address, you're going to want to use a chain of proxies more often than a dynamic user would. Using a third party DNS which doesn't monitor you is also recommended; try out OpenDNS, for example. They're fast and also help protect your anonymity! How about that?

Conclusions

To be anonymous is to be nameless. If you are sly, and wish to work in the shadows, then some of the tips found in this guide is strongly advised. The tips found in this read are not advanced, professional tips. They are freeware, opensource and logical tips collected from experience; and are bound to work if you apply them to suit your own style. I myself do not follow half of these tips, though I did write this guide. I am less anonymous than you think; I'm just enough anonymous to keep certain information away from those who don't need to see it.

We are all apart of this growing network; and while we just sit on two different sides, we are virtually connected. There are no bounds to perfect security; so while there isn't, it is best that you start making your own security. Why not invest in a gun safe instead of just having the safety turned on your weapon?

The internet is filled with many wonderful and marvelous souls. The internet is also filled with lots of scumbags and trolls. The internet is a place where anybody can be who they want to be; you get to live the Peter Pan life the second you choose to. While we can't remain fictitious throughout our entire life; and in fact, would probably like to be credited on discoveries and major contributions we do make TO the internet, you SHOULD do all you can do to protect yourself and your family, because you never know who you might just piss off.

-EOF

== cwade12c @ haxme.org ==

== 8:34 PM Pacific Standard 28 Feb 2010 ==