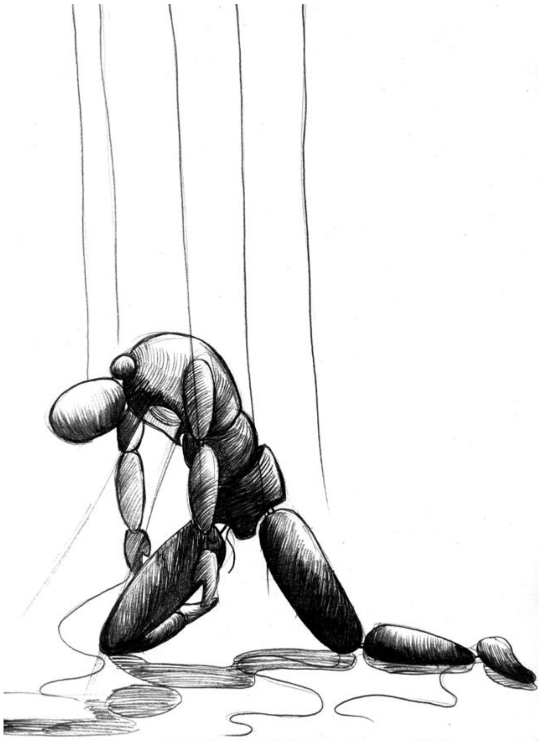


“My puppets are far more liberated than I am. Ventriloquism is a useful way of expressing myself.”

Securing Online Personas

A beginner friendly guide to achieving security for your persona in the hacker's realm
Published on March 27, 2016

Author
Written by deadlock (?)
Puppet Network
www.puppet.zone

Table of Contents

Disclaimer: *I, D/L, am not to be held responsibility for any action or crime committed as a direct or indirect result of what can be learned from this book. I do not condone any form of doxing, hacking, harassment, nor do I condone or encourage any other malicious activity. The information in this document, all of which is available publicly, is legal in this book's country of origin. The legality of this document in all jurisdictions is not guaranteed- it is the responsibility of the reader to check with their local authorities on the matter. . Please do not do anything that results in you breaking any law with what you learn. This book was written without malicious intent. I encourage you, the reader, to be ethical with your learnings, just as I intend to be ethical with my teachings. If a crime is somehow committed in this book, then I lacked any form of mens rea at the time of writing.*

Introduction

Hello, and thank you for taking the time out of your life to read this ebook. My current public aliases are deadlock and Martial as of March 2016. If you wish to contact me, my contact information can be found on the title page or right above this text.

I assume that if you have gotten this far and taken the time to open this file, then you are interested in ensuring that your personal digital security is in-tact, whilst browsing the web, specifically in online hacking communities.

Online hacking communities can be scary, dangerous and hostile places. There are good and bad people in these communities, and as you probably already know, these people often have malicious intentions, even if this isn't always clearly visible to us. You never know who you are talking to online; therefore, people can lie about their identities, intentions and actions. With this in mind, you need to choose what information you share online with great care. It may even be useful to lie about your personal information on occasion or with regularity.

Personal digital security has always been important to me. There have been times where I needed to use the tactics that I will be teaching you about, and there were other times where I had to swear and live by these things in order to continue to enjoy my Internet experience in a safe way. The Internet is a dangerous place, especially if you have an interest in information security or anything that could even possibly relate to the hacking scene. Hackers can be savages, so you will need to learn how to blend into the “scene” without standing out, and be even more secure than the ones who target you.

It is worth mentioning that any content in this book is solely mine unless stated otherwise. I have used many personas over the years, and published many write-ups, so if you begin to suspect plagiarism, you are likely incorrect.

So, let's begin.

The “Just a Man” Philosophy

You are just a man (or woman).

Sometimes we get ahead of ourselves and think that we are high & mighty, powerful, and generally better than others on the Internet as well as real life. It is human nature, we are often arrogant, stubborn, and determined. Who cares, right? Often times such an egoistic outlook will never catch up to us, so a lot of people do not care about many risk factors as a result.

If you are not trying to be anonymous online then this quick read likely will not mean much to you. This is all geared towards hackers, doxers, and whoever else sometimes bites off more than they can chew, or tell a modest fib to seem a bit more 'cool' to their peers.

Hackers - You know that vulnerability you just found in that government website? Remember, if your curiosity gets the best of you, you could very well end up somewhere bad. If you don't believe me, then know that I have actually had a few acquaintances get arrested for things that they did years ago. Law enforcement does not always give up easily, even when you think that enough time has gone by for the case to be forgotten, it sometimes is not. Even though these are things that these lads may have done years ago, it still can catch up to them, just as it can catch up to you.

Doxers - You know that PayPal account you just found? Just think that if you log in to that account, steal some money, and someone were to try to track you down to get you into some trouble for your actions, you could very well be caught and punished. This is especially the case if you do not know how to use a proxy, VPN, or Tor.

Security freak trying to stay anonymous - You know that crazy thing you just did? You know that picture of yourself you just posted on a forum to get responses for a few minutes? You know that one person you don't even know who you just shared a bit of personal information with? None of the people looking at, or reading, this probably care. You are just a man. You are just a woman. You are only human. Nobody really cares, so stop acting like it.

What I'm trying to say is that our emotions and desire to feel powerful can sometimes get in our way and make us do stupid things. We often forget that we're people. So, if you ever think you're taking on more than you can probably handle in the time-being or future just stop and think - I'm only a man.

I will now tell you the short story of the man named Marcus Aurelius who inspired this philosophy of mine.

The Humble Story of Marcus Aurelius

There once was a man named Marcus Aurelius. He was a Roman Emperor from 161 to 180. He ruled with Lucius Verus as co-emperor from 161 until Verus' death in 169. He was the last of the Five Good Emperors, and is also considered one of the most important Stoic philosophers.

Aurelius would regularly walk through the streets with citizens bowing down to him, offering him complimenting words of praise, and even more at times. Despite this, he never wanted have this praise make him lose sight of his goals. So, what did he do? He hired a servant to follow him through the streets and whisper "You're just a man. You're just a man." every time someone bowed, got on their knee, or praised him in some way or another.

Something that you may find interesting is a famous quote of his "Wrestle to be the man philosophy wished to make you." In my opinion, this quote belongs alongside Abraham Lincoln's claim that "the best way to test a man's character is to give him power."

The point that I'm trying to chisel into your brain is that you need to control your urges, and have respect for both yourself and others. Maintain your moral values. Do not submit to temptations without thoroughly thinking about what you are doing first. It is crucial that you always control egoistic habits at any given time.

Introduction to Operational Security

So, what is OPSEC anyway? OPSEC, also known as operational security, is the art of securing information within an operation. OPSEC will play a crucial role in your hacker career. A hacker without OPSEC will never last long since he will be found out, arrested and prosecuted; however, a hacker who utilizes OPSEC to it's fullest potential will prevail. If you are, or are planning to be, a hacker then you absolutely need OPSEC.

Sun Tzu once said that “the opportunity to secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself.” In this guide, you will learn to secure your own persona, so that you do not provide an opening for an enemy to break through your defensive security, and tear your empire down. Secure all information, limit the spread of said information, and live as if you are constantly on the defence in your own battle with the NSA. That is what OPSEC is.

Ultimately, you will want to learn to live, breathe and think OPSEC as a hacker. Let's learn how exactly we will be doing this, just as other hackers already do.

Public & Personal Relations

Relations can be a dangerous thing to dabble in when you are trying to achive operational security. When I speak of relations, I especially speak of real life human-to-human, online user-to-user, and user-to-community relationships. We have probably all heard that operational security phrase “loose lips sink ships”, and if you really think about that saying, you will likely realize how true it is, and maybe even relate to personal experiences that you have had where you or someone you trusted said something, and that special situation all came crashing down either on your or them. Whether you are a hacker, vigilante or even a member of the law enforcement, this type of operational security is especially important to your operations. It sucks not being able to talk about things, but it is often for the better. Let's focus on the two different types of relations that we will be touching base on: *public* and *personal*.

Public Relations

According to the Wikipedia, “public relations is the practice of managing the spread of information between an individual or an organization (such as a business, government agency, or a nonprofit organization) and the public.”

When I speak of anything to do with public relations, I am talking about the interactions that users make with online communities, forums, group chats and social media that people participate in nearly every day of their lives in modern day society. This is an innocent type of relation for the most part, so let's keep it that way.

You will want to limit the information that you provide to websites like Twitter, Facebook or even an online hacking forum. Work on a need-to-know basis; why does another hacker or Twitter follower need to know your date of birth, mother's maiden name, or who your best friends are? Or speaking on a more technical level, why do these people need to know what new rootkit you have been developing, or what guy whose life you just e-destroyed? After all, these are absolute strangers who potentially have malicious intentions, that you are sharing your information with. Why the heck do they need to know any of this? Again, remember that you are just a man.

The other day, I was browsing Twitter and I came across a Tweet from NakedSecurity: “Facebook taunts send another “catch me if you can” crook to jail http://wp.me/p120rT-1jAq”

To sum up the situation, a 40-year-old UK fugitive and convicted drug dealer from Merseyside, Steven Johnson, used alias Facebook profiles to share pictures of his life on the run. The Echo has published photos Johnson posted under the Facebook accounts Simon Woods and Jj Green here and here. In the posts, he graciously shared invitations to Merseyside Police to “catch me if you can”, and he also said things such as “You will never find me! Hahaha.”, as if it were all a game to him.

Unfortunately for this UK fugitive, his game came to a dramatic game over after the police used these Facebook posts to locate him and arrest him. The tactics that police use to track these drug dealers down are the exact same as the ones that they would use on a hacker.

But don't be fooled, that's not the only threat to you either. Hackers and doxers use similar tactics as the police in order to track you down when you post pictures and personally identifiable information anywhere that they can obtain it, such as Twitter or a publicly viewable Facebook profile. A prime example of this is, well, I'll just make a list of people who have fallen victim to these attacks:

http://pastebin.com/raw/sgGpGKJi
http://pastebin.com/raw/3JwCknAm
http://pastebin.com/raw/hvmx1ady
http://pastebin.com/raw/xSX7itce
http://pastebin.com/raw/nPRHSrKq
http://pastebin.com/raw/4H3KPe9H
http://pastebin.com/raw/8tFxtFrd

Note: If these links all go down, you can find more dox examples by using this exact search string on Google: *site:pastebin.com "dox"*

Those should give you a pretty good idea of what type of individuals that you are up against when you're defending yourself online.

My point with this public relations stuff is basically do not post personally identifiable information on the Internet! If you have bad OPSEC (operational security), you will have bad results!

Personal Relations

According to the University of Minnesota, "the concept of [a personal] relationship is very broad and complex. In our model, personal relationships refer to close connections between people, formed by emotional bonds and interactions. These bonds often grow from and are strengthened by mutual experiences."

You will run into like-minded people on the Internet. It is totally okay to make friends, acquire acquintances, and be a part of a public relation like a community-run online hacking forum, but it is not okay to share any personally identifiable information with them. Friends turn to foes. Generosity turns into greed. Partnerships turn into betrayal. You might not fully understand this at the moment, but trust me when I say this next point.

I have been around hackers, I have had friends who were ethical security researchers, and I have conversed with flat-out, straight outta the darknet, drug market, government hacking criminals that you have heard of on the news. Some of them remained loyal, some had "loose lips" which happened to "sink ships", which I won't go into detail about. Others were alright, but in the end, they all left, or I left, and you will too. Everybody leaves in the hacking scene eventually, so don't let them carry your information or secrets with them.

A hacking community is not any place for your personal feelings. Once you join the community, it becomes your second life, not your first. Friends are for real life, not for hacking communities. Quite frankly, if your social life sucks so much that you have no one to talk to about personal stuff in real life, either make change or take it to another non-hacking community... Sharing feelings and life stories is really a daring activity to participate in.

Before we move on, I wanted to include a special excerpt with everyone, outlining one basic rule that should be considered:

> “*Basic rule: Blend in with the crowd, disperse into the stream. Keep a low profile. Don't try to be special. Remember when in Rome, do as Romans do. Don't try to be a smart ass. Feds are many, Anonymous is Legion, but you are onlyone. Heroes only exist in comic books keep that in mind! There are no old heroes; there are only young heroes and deadheroes*”
>
> - The Über Secret Handbook

Degrees of Separation

In this section, we will be making an approach towards the theory of the *six degrees of separation*, and we will be putting a special focus on the first two degrees of this six degree network. For those of you who don't know, the six degrees of separation is the theory that everyone in the world is connected to every other person ever in existence through a chain of acquaintances that has no more than five intermediaries. Let's say that you know five people, and each of them know five people, and each of those five people know five other people, and so forth. At some point, you will be connected with the entire world, each immediate connection of yours being a first degree, then any connection of theirs is the second degree, and so forth, this is the theory of the six degrees of separation.

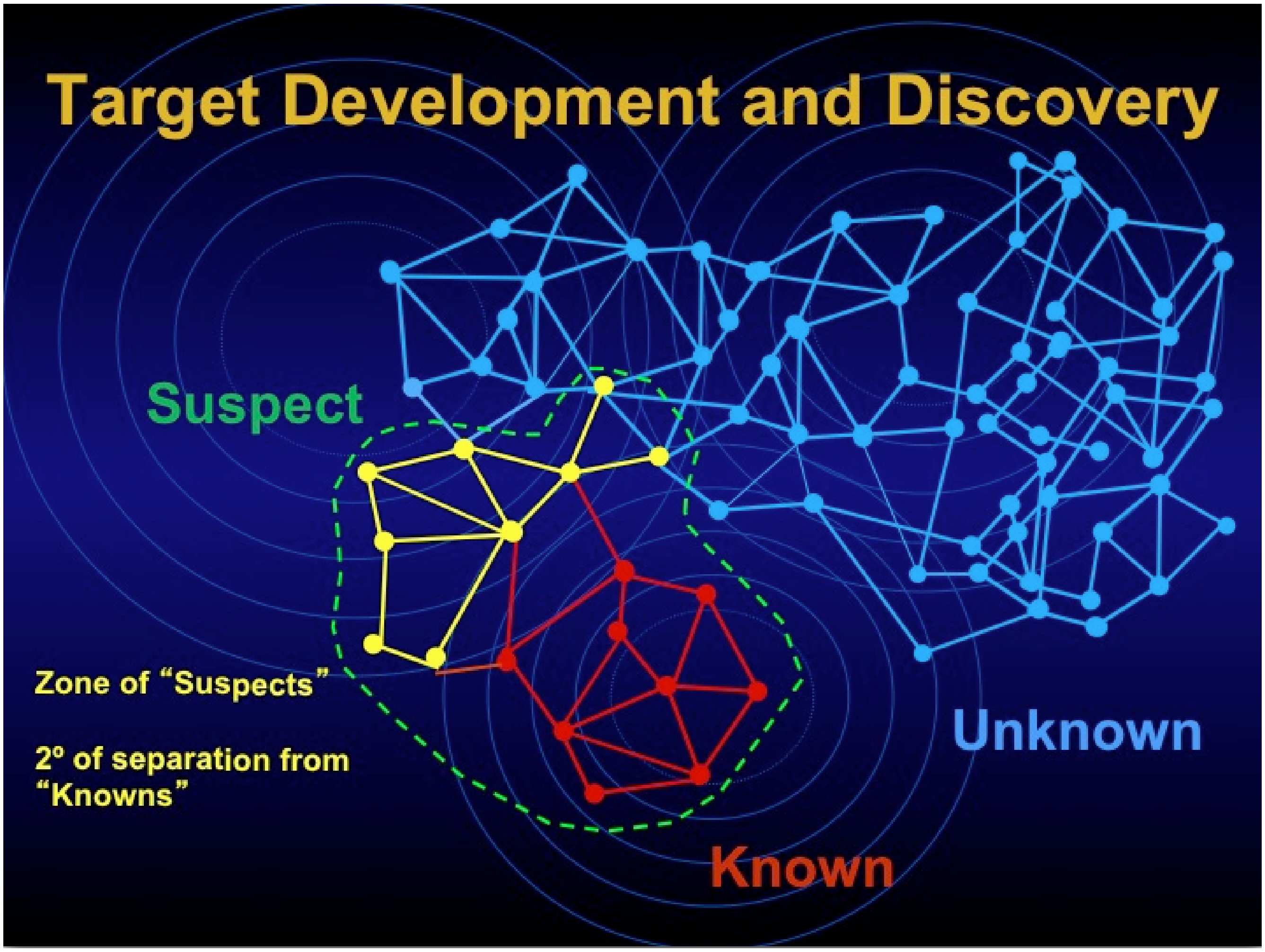
In the 1990's the U.S. National Security Agency developed a project called "ThinThread", ThinThread was discontinued after the attacks that took place on September 11, 2001, and replaced by a new, similar project called the Trailblazer, and Trailblazer has now been replaced with Turbulence. ThinThread had a heavy focus on wiretapping and intelligence analysis. According to zdnet, "the project included legal restrictions and privacy filters that would encrypt and scramble US-related communications to prevent illegal and warrantless domestic snooping."

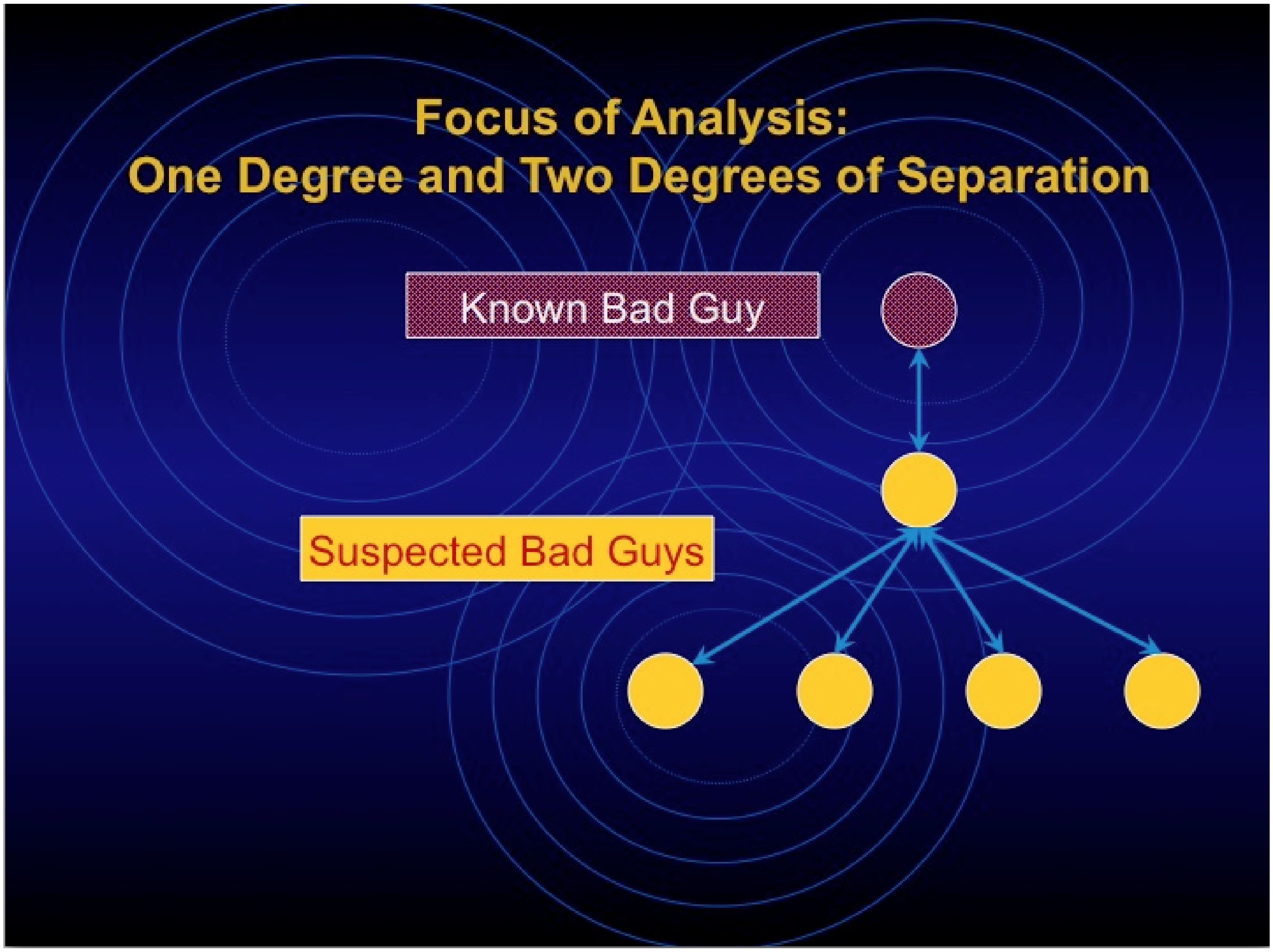
An individual named Tim Shorrock, a writer on US national security and intelligence, said that ThinThread operated in three distinct phases:

1. *First phase:* ThinThread intercepts all call conversation, email and internet traffic on a network and automatically focus analysis on specific targets using specific patterns of information.
2. *Second phase:* ThinThread automatically anonymize the collected data so the identities stayed hidden "until there was sufficient evidence to obtain a warrant".
3. *Third phase:* ThinThread uses the raw data "to create graphs showing relationships and patterns that could tell analysts which targets they should look at and which calls should be heard.

In the third step it is mentioned that ThinThread was used to create graphs to reveal relationships between suspects connected to known "bad guys", and others. When the N.S.A. would surveil these relationships, they would build a network of suspects based on the first two degrees in the six degrees of separation. In other words, by speaking to a known "bad guy", you are automatically listed as a suspect, and so is anyone that you communicate with. Now all of you are on the N.S.A.'s radar.

Just for a review to strengthen your understanding, once ThinThread identifies who is the known criminal, they now look at the first and second degree connections associated with the criminal. In other words, anyone that the known criminal regularly communicates with becomes a suspect in the eyes of the N.S.A., and anyone that those suspects regularly communicate with, become suspects, too; the first and second degree connections are all monitored since they are now suspects. Take a look at two slides from one of N.S.A. whistleblower, William Binney's, presentations for reference.





Focus of Analysis:
One Degree and Two Degrees of Separation

Known Bad Guy

Suspected Bad Guys

Even though the ThinThread project was discontinued, there are still similar, even more sophisticated programs that intelligence agencies all across the world use.

You can prevent yourself from getting caught up in one of these networks by carefully choosing who you communicate with. Avoid communicating with criminals who are open about what they do by mocking the police, attacking the government, and Tweeting their little heart away about the box they just popped. Choose who you connect with carefully. You are just a man; don’t let your ego take over, and become one of those cyber criminals who act like an untouchable king of the world on Twitter or HackForums.

Sharing is Daring

While we’re on the topic of surveillance, I want to ask a question: *have you ever watched a show on Netflix and talked to your friends about said show?* If so, did you know that by sharing what shows you are currently watching puts your personal security at risk? You may be wondering what's so bad about Netflix, but believe it or not, every time you watch a TV show or movie, Netflix actually keep logs on what you watch, for how long, and when you watched it. These logs are a part of the metadata that Netflix keeps attached to your account.

Sometimes we like to share what shows we have been watching with friends on the Internet. Let’s say that you are talking to another person, and you mention that the new season of Breaking Bad just came out on Netflix, and you’re loving it so far. This implies that you are currently, or have been, watching the TV show Breaking Bad on Netflix.

Let’s say that there is an open investigation on you and your activities, and this conversation was had over Skype. Let’s assume that the law enforcement know about the Skype account that belongs to you, so they get a warrant to seize the account, and retrieve all of the logs. Within these logs include chat logs, chat logs that tell the tale of you watching Breaking Bad on Netflix. Now the law enforcement know what show you watch, and that you have an account on Netflix.

The law enforcement now contacts Netflix with a court order, or a warrant, requesting that they share what Netflix accounts have watched certain episodes of Breaking Bad in a set timeframe, and Netflix obeys this court order. Now the law enforcement has a list of Netflix accounts, and they know that one of these accounts belongs to you. This is even easier when it’s an unpopular show that you are watching where only 27 people watched on the day that you said you also did, implying that you are one of 27 people. That’s getting pretty close to home now.

Law enforcement could now progressively use this data to narrow down the list of suspects, and eventually prosecute you if they are successful.

I'm sure that you have noticed a bit of a pattern here by now... Sharing personal information is dangerous! Do not share anything personal, and if you really must then learn to vent it all through disinformation, misinformation, social engineering and just flat-out fibbing on a convincing level. So, let's start by getting a few definitions down:

Disinformation: “False information that is intended to mislead, especially propaganda issued by a government organization to a rival power or the media.” - Oxford Dictionary

Misinformation: “False or inaccurate information, especially that which is deliberately intended to deceive: nuclear matters are often entangled in a web of secrecy and misinformation.” - Oxford Dictionary

Social engineering: “Social Engineering (SE) is a blend of science, psychology and art. While it is amazing and complex, it is also very simple.”, according to social-engineered.net.

The same source continues by defining it as “*Any act that influences a person to take an action that may or may not be in their best interest*.” We have defined it in very broad and general terms because we feel that social engineering is not always negative, but encompasses how we communicate with our parents, therapists, children, spouses and others.”

Let's combine all of these factors into one, and give it the cool name **data poisoning**.

Data Poisoning

For all you know, someone that you regularly chat with could be socially engineering you; compiling information identifiable to you, your friends and your family, just waiting until you are in a state where you are at your most vulnerable. Then eventually, once they are ready, they could exploit that vulnerability (your personally identifiable information). At this point, they could have the potential to tear your life apart bit-by-bit, piece-by-piece. They could make your friends hate you, your family feel uneasy and suspicious of you and they could even make your lover leave you. Hell, they could even plaster your personal information all over the Internet, and all of this could all be done so fast; before you even notice, just because you chose to share that truthful and accurate information about yourself.

How do you prevent this from happening? Data poisoning. As Sun Tzu once said, *"pretend inferiority and encourage [your enemy's] arrogance."* You don't necessarily need to pretend inferiority specifcally, but you really have to lie with the help of disinformation. Put simply, data poisoning is the act of spreading false, misleading information about yourself; hence the poisoning of the data. Your goal when data poisoning is to be so convincing about it that anyone reading any of the disinformation will actually believe it. You want your lies and disinformation to almost work as if they are a part of a big web plotted by you. This web will become your new online identity. Is your name Jack Daniels? Well, it is Captain Morgan to everyone else now. Did you just buy a new car for 5000 USD? Well, you just bought it for 6500 AUD now. Do you enjoy a nice glass of wine on the odd night? Well, you do not anymore – to anyone who is not you, at least... I think you get the point.

Before you are ready to engage in data poisoning, you will need to do a bit of aggravating work and research to determine your new identity. You will need to look into what accounts and information will surround your identity (eg. Facebook, Twitter, ask.fm, GreySec, etc.), and create a unique username, emails, and passwords around that idea. You will also need to determine where this identity is going to be located, what currency they'll be using, their occupation, hobbies, and what there timezone is as well. This identity, like any other, will have an attitude and style, you will need to look into stylometry, create an appearance, and how it will communicate with others too (friendly? stand-offish?). You can create the appearance by finding someone who is unpopular on a social media website and use their pictures (consider stripping any EXIF data before using), but just make sure that you don't actually know the person in the pictures personally. I could go on for a very long time about these things, but again; I think you get the idea that you need to decide on every little bit of information you will be sharing for the sake of consistent disinformation.

Your job is far from done there though. What about when you are chatting in real-time though? When you are on IRC, Skype, Facebook Messenger, XMPP, or something of the like, it can be very easy to slip up. You must ensure that you are always following your schedule and that you do not speak about anything personally identifiable to you. If you have convinced the person you are speaking to that you work a 9-5 job every day then you probably do not want to be talking to them between 9 AM and 5 PM in your persona's time zone. It is also quite common to talk about things that are actually happening in real-time when you are chatting in real-time too. So, what you can do if you are going to complain or talk about something - complain or talk about the complete polar opposite of it. For example, if it is hot outside and you want to complain then complain about how cold it is instead and how the rain or snow will not let off. If you just went through a divorce and are sad, talk about how you just lost your mother and life will not be the same without her but remember that whenever you make up lies like this, you must be consistent with them and add that to an official part of your persona's life -

you must now state that your mother is dead whenever someone asks about her. She is dead now just because you said so, and that is not something that is reversible.

As DIzzIE once said, the aim must always be to present the illusion of transparency, an “I’ve got nothing to hide” hologram. You should want this disinformation and poisoned data to piece together so nicely that they “cannot not believe it”. To do this, you will need to be consistent with your disinformation and make sure that it makes sense. Once you decide on what your persona will be, you can't start changing things and say things that just are insensible. For example you cannot say that you are 18, but born in 1989 on May 2nd and then change your age and data of birth a week later.

Why would you want to lie about all of this? As I said before, attackers could use any of this information to single you out in a crowd even if that crowd contains 7 billion people or billions of indexed pages from Google that your information lies on. I used the example of lying about weather earlier - believe it or not, by talking about your current weather by saying something like "Wow, I just got hit with 16 inches of snow", the said attacker can easily determine your potential locations and continue to keep you under surveillance until they gather enough information regarding your general location to find where in the world you exactly are.

And that, comrades, is the general idea of how data poisoning works. I mentioned in here that you will perhaps need to create a new online persona eventually, but don't worry about any of that just yet, we will get there later. Just relax, go get a glass of water, coffee, or whatever you prefer, and keep on reading, or you can keep reading about this subject by checking out DIzzIE’s paper on “Achieving Anonymity Through Disinformation and Data Poisoning”.

Let Them Find Us (LTFU)

The Let Them Find Us, or LTFU, concept is a concept where you hide in plain sight. The theory here is that people will never find out who you are if you let them think that they already have a pretty good idea of who you are, they will think that there is not much more to actually look for; let them think that they have found us.

In other words, you don't want the one(s) that you are defending yourself from to know that you are trying to hide your real identity from either just them or the Internet as a collective, you want them to believe the fake disinformation that you have intentionally put out there already. They must believe the lies over anything else at all costs. Do not give them any reason to let them think otherwise, stick to your guns, and keep your ego on the down-low. After all, you are just *another* man now. That's all that other people really need to think of you as, a harmless man and not a malicious hacker, even if you are one.

Assuming that you applied the data poisoning techniques that you learned, this should be pretty easy for you. Act with the personality that you gave your persona, stay consistent, and never stop lying.

I think that was a pretty straight-forward concept. But what about when you are discovered by another hacker or the police, then what? Well, hopefully we will have a *plausible deniability* system setup for ourselves.

Plausible Deniability

Plausible deniability is a condition in which a subject can safely and believably deny knowledge of any particular truth that may exist because the subject is deliberately made unaware of said truth so as to benefit or shield the subject from any responsibility associated through the knowledge of such truth. This can apply to protection from both hackers and police, but more so police since there's a difference between the two scenes.

Police and lawyers are required to follow a legal system, so even if the police don't believe you, and they know that you did something, you can continue to deny involvement under certain conditions, and if they fail to provide valid evidence that a judge accepts in the courts, then your case will be dropped, and it cannot be picked up again – you're free to go at this point for that case in particualar; however, criminals and hackers do not have to follow this system. If the criminals targeting you find out who you are, there's typically not much that you can do to convince them that their discovery is false or invalid, they will likely think that you are trying to social engineer your way out of the bad-looking situation at hand, these lies can easily aggravate them too, thus worsening your situation.

We need to remember that plausible deniability can only work if we have a background to support what we are denying. For example, if you are trialed for a hacking incident, and you shared different, unrelated hacking experiences all over public relations or personal relations that have been brought public by a snitch, then things probably won't look too good for you. So, keep your nose clean and you will be fine, or at least keep your activities out of the public eye, news, and especially social media that ties back to any identity of yours; claiming any illicit responsibility is a bad, bad, bad thing for your operational security, just don't do it.

Something worth noting is that plausible deniability doesn't always work, especially when you decide to eliminate any evidence that you already have. Just because it is no longer existent, doesn't mean that the judge can't believe that it was once there before you destroyed it. What I am talking about is called spoliation of evidence in the court room.

According to the Wikipedia, “The spoliation of evidence is the intentional, reckless, or negligent withholding, hiding, altering, fabricating, or destroying of evidence relevant to a legal proceeding. Spoliation has two possible consequences: in jurisdictions where it is the (intentional) act is criminal by statute, it may result in fines and incarceration (if convicted in a separate criminal proceeding) for the parties who engaged in the spoliation; in jurisdictions where relevant case law precedent has been established, proceedings possibly altered by spoliation may be interpreted under a spoliation inference, or by other corrective measures, depending on the jurisdiction.”

So, if you typically don't go about wiping your hard drive with DBAN, and you suddenly wipe it clear of any traces of possibly existing evidence with 5 iterations the night prior to confiscistion of your devices, that may seem a bit off. However, any harsh accusations could easily be plausibly denied if you could prove that you wiped your hard drive on or around the 5th of every month, just as a habit that you have gotten into; this claim has the potential to wipe that evidence straight out of a court room, and maybe even acquit you.

Plausible deniability can also go hand-to-hand with encryption, much like the hard drive hypothesis. It may seem abnormal for you to send encrypted messages to other people on a constant basis, but if you make a habit of it for even chatting about things like your favorite type of pizza, then it shows that it's just a normal thing for you to do in your day-to-day basis.

You could also setup a LUKS killswitch for your encrypted HDD, this is essentially “a patch for cryptsetup which adds the option to nuke all keyslots given a certain passphrase. Once the machine is rebooted and you are prompted for the LVM decryption passphrase. If you provide the nuke password, all password keyslots get deleted, rendering the encrypted LVM volume inaccessible.” You can learn more about this subject here: https://www.kali.org/tutorials/emergency-self-destruction-luks-kali/

To learn more about how to properly destroy evidence and avoiding getting caught doing when doing so, I recommend that you check out this HOPE talk: https://www.youtube.com/watch?v=aRF63yKref.

Building a Persona

NOTE – Please read: I recommend that whenever you use this persona, make sure that you are behind a VPN, especially when you are registering an account or accessing something such as IRC or XMPP. If you don’t know what VPN to go with, look for one that doesn’t log, is offshore, and has a good reputation – I would personally recommend checking out Cryptostorm, they also have a free version of their VPN, but it’s capped at 150 kb/s for upload and download speeds. I also recommend that you don't actually build your persona up until you have finished reading this entire book; both the personal and technical sections, it would be a shame if you built up your awesome social security barriers just to have it all torn down due to a technical error that I might discuss later. Moving on now...

When you are building an online persona, the identity that you come up with will basically be the new you. You no longer will tell stories of your real life, but you will tell stories about your persona's pretend life instead. You must remember what lies you tell, and who you tell them to, and keep on telling them and building off them. You can't say that you are 19 one day, then be 24 the week afterwards. You must take this seriously in order for the entire operation to work out, carelessness is a major violation to any possible rule of secrecy.

Just as the Communist Party of South Africa said in their article *How to Master Secret Work*, “Carelessness leads to arrests. Loose talk and strange behaviour attracts the attention of police and izimpimpi. Secret work needs vigilance and care. Rules of secrecy help to mask our actions and overcome difficulties created by the enemy.”

Maintaning a fake identity can be a very daunting task, but it always pays off in the end. Especially when you login to an account one day to see that someone has tried to dox you, and they actually just doxed your fake identity instead; thus, they actually just improved your anonymity that much more. You used the Let Them Find Us concept alongside your persona, they thought that they found you, published your fake dox everywhere (personal information), and they now think that they won, but you know that they really didn't.

There are actually two ways about using a fake persona: 1. steal somebody's identity, or 2. create a new identity from scratch. If you want to learn more about the first one, contact me via XMPP with OTR, and I will happily teach you about it, just not how to do it as I do not condone malicious, unethical behaviour such as that.

So, how do we go about creating this brilliant fake identity of yours? Well, you are going to need three basic things: persistence, a brain, and common sense. Trust me on the persistence thing because creating personas can get extremely tedious, time-consuming, and boring after awhile. To be clear, there are a million and five different ways of creating a persona. Do it however you please, I will just be going over the concepts of it.

1. Visit http://www.fakenamegenerator.com/ and generate the base of your new identity
2. Let's take a look at some of the results that I got, on the next page. I actually cut out some stuff and reorganized it to fit the size of the page, but just take a look at what basic information I gathered for the base of my new persona

PERSONAL
Name: Jeff H. Garcia
Address: 4847 Carter Street, Belleville, IL 62221
Mother's maiden name: Guzman
SSN: 356-60-XXXX
Geo coordinates: 38.416021, -89.998579
Phone: 618-746-2978
Birthday: November 10, 1994
Age: 21 years old
Zodiac sign: Scorpio
Email Address: JeffHGarcia@jourrapide.com
Username: Satim1994
Password: aeNocho0ah
Website: debrafpawnshop.com
Browser user agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/43.0
FINANCIAL
Visa: 4716 0563 8225 5221
Expires: 1/2021
CVV2: 286
EMPLOYMENT
Company: Joshua Doore
Occupation: Process technician
PHYSICAL CHARACTERISTICS
Height: 5' 10" (178 centimeters)
Weight: 189.9 pounds (86.3 kilograms)
Blood type: O+

Now that we have our basic sheet of information, save it in a text editor. Now you will want to adjust the identity to your liking, you can change whatever you want. For example, I'd personally change that username, and I'd also go as far as to make another Gmail account or something with my persona's name in it to be just that much more convincing. I seriously advise that you make a new email dedicated to this identity that has characteristics of your persona like the real name right in it, and actually sign up for your accounts with it.

Once you have your email setup, some accounts that you may want to make will be things like a Facebook, Twitter, and maybe even share a few things on Google+; you are trying to make it look like you actually have a social life right here. If you just make a Facebook, and change all of the privacy settings to “Friends Only”, including your friendslist, then nobody will even know that it's a friendless dummy Facebook. If they ever go to dox you, they will find your dummy Facebook and likely use that as further support in their dox. If you are by chance curious about what complete strangers see when they visit your Facebook page, you can actually see just that by:

1. Logging into your desired Facebook account
2. Visit your own timeline

3. Direct your eyes to the bottom right of your cover photo, look for the “**...**” panel beside “**View Activity Log**” -- If you can't find it, this is probably outdated information
4. Select the “**...**” panel
5. “**View As**” will show you what your Facebook looks like to somebody with no mutual friends

Besides this, you may want to make the identity even more convincing by plastering the Internet with the username that you will be using, this all just helps make it look as if you've been legitimately using this new alias. You can make up or use a username that is strictly for your alias, the website will tell you where you can create profiles, and it will just make the whole process more automated and easier for you in a sense. The more accounts you create, the better. Make sure that you are using some sort of proxy, a VPN and/or Tor while creating all of these accounts, and that you are using different passwords every time – just in case any of these websites ever have a database breach or something, and your username/email/IP/password are all spread around the Internet, then your data is still fairly 'anonymous' in a sense. Also, you should consider making up a collection of pictures of one certain person to use with your alias, you could search Instagram or Facebook for a random, unpopular person; save all of a random persons pictures, and use them as your own.

When online, you are no longer you at this point; you are your persona. You must never break character, never let your guard down, and pay attention to every message you craft, and to every detail that you choose to share. Stick to your guns, trust no one, and lied to all. Be whoever or whatever you would like to be. Never break character.

From here on out, you are on your own with creating your persona. Go ahead, and be creative with it. I feel that most people should be more than capable of finding creative ways to invent a fake persona, and make it look legit. Just remember to never, ever link that persona to anything outside of the persona's identity, like a personal email – this actually leads me to my next teaching: *persona contamination.*

Persona Contamination

What is persona contimination?

According to The Grugq, the primary danger that you will face when you are using an online persona is contamination. Contamination is when there is contact between any cover identities or your real identity. That contamination will occur when they interact, and it can then be used to trace from one compromised identity through to the other, so it's always important to keep them completely separated and never interact. They need to be in isolation from each other. Even though I will be focusing on the cyber side of things here, keep in mind that you should never be even mentioning any of what you do to your friends, family, or even your life partner. It's just a bad idea should the feds ever move in on you and interrogate your friends. Don't do it.

Maintaining a persona and knowing when to let go

Something else that you need to do is have layers, so simply having an initial cover identity is not sufficient. Once you have one cover identity, you then start creating sub-aliases from that.
It's better to have multiple cover identities so that when you get paranoid and you believe one has been compromised, you can phase it out rapidly and move another one into place.
By definition, a persona is an assumed identity or character or the mechanism that conceals a person's true thoughts and feelings, esp in his adaptation to the outside world.
Though it may hurt to toss away the persona that you have invested so much time, effort, and hardwork into, remember that it still is just a persona created to cover your ass for when you fuck up.

As said before, building up a persona for your secret hacker identity can be time-consuming and tedious, so you don't want to fuck up. You can avoid fucking up in that sense by never contaminating it. How do you do that? For starters, let's look at "The 10 Hack Commandments". I want you to read over this list a few times over and think every single rule listed here through and why you think the rule is on this list.

Seriously. Think about it, and don't continue reading until you have done so.

Rule 1: Never reveal your operational details
Rule 2: Never reveal your plans
Rule 3: Never trust anyone
Rule 4: Never confuse recreation and hacking
Rule 5: Never operate from your own house
Rule 6: Be proactively paranoid, it doesn't work retroactively
Rule 7: Keep personal life and hacking separated
Rule 8: Keep your personal environment contraband free
Rule 9: Don't talk to the police
Rule 10: Dont give anyone power over you

And above all, remember the magic 4 words - Keep your mouth shut!

When you speak to your online hacker friends, remember that they are not your friends, they are cold-hearted criminals who are stupid because they do stupid things like you. If they weren't stupid, then they would be penetration testers, not hackers.When they get caught, they will squeal on you.

When they feel betrayed, they will attack you. When they get bored, they may betray you. Hackers are unpredictable and cannot be trusted.
After all, look at LulzSec; how they were caught, how Sabu betrayed his comrades, and the feds closed in on all of them.

Anarchaos - Told Sabu how he was on probation at some point and received a drug charge. Information was easily used to trace him down. He was later arrested.

Palladium - Told Sabu whenever he changed aliases, and other personal information. Information was also easily used to trace him down. He was later arrested.

Take note that Palladium really contaminated his persona by sharing his new personas with Sabu so carelessly. It is kind of pointless to switch identities and fallback on to a new cover if you already admitted that you are someone who already has a profile being built up. Palladium just allowed "them" (doxer, gov, whoever) to continue profiling his alias as if nothing happened.
This could have been prevented if Palladium had fully "shed" his old persona and started out with a brand new, fresh one -- Kind of how a snake sheds its skin; once it sheds, it never goes back or clings to it.

Several other members were caught in similar ways just because they contiminated their persona by telling Sabu, their trusted "friend", thinks about themselves via instant message.

With all that now drilled into your head, I'll get to it already. When you are discussing anything with anyone online, always abide the following "rules" (bend them as you please).

Let's call these the "*Rules of Anti-Contamination*":

Do not include personal informations in your nick and screen name.
Do not discuss personal informations in the chat, where you are from...
Do not mention your gender, tattoos, piercings or physical capacities.
Do not mention your profession, hobbies or involvement in activist groups
Do not use special characters on your keyboard unique to your language
Do not post informations to the regular internet while you are anonymous in IRC.
Do not use Twitter and Facebook
Do not post links to Facebook images. The image name contains a personal ID.
Do not keep regular hours / habits (this can reveal your timezone, geographic locale)
Do not discuss your environment, e.g. weather, political activities,

And if you do ever speak about these things, try helping yourself through misinfo and data poisoning. For example, if you want to talk about your job, complain about a different job that is not related to yours in any way whatsoever. If you complain in the future, complain about that job as well. This job should actually be one that never leaves your persona. This is your personas career, your persona may complain about his or her job. You may not complain about your job. Another example would be if you're complaining about the weather. If the real you is complaining about the heat, let your persona complain about the cold. Or better yet, make your data poisoning more advanced by looking up their location and complain about whatever the weather is like there.

The more you speak, the more they know;
The more they know about your potential;
The more they know of this, the more they monitor;
The more they monitor, the more they look;
The more they look, the risk of getting caught or blackmailed increases;
Once you get caught, you either get punished by the system,
Or you get attacked by other hackers on the most personal level possible;
When you mess up, you get fucked;
It hurts to get fucked, so don't get fucked by abiding the magic four words:
Shut the fuck up.

Lather, rinse, repeat; stay clean; never contaminate.

Real Identity Safety

Now we have a nice, new persona that we will be using to protect our real identities from being found out. If you by chance read this entire guide, have read other security/anonymity/privacy guides, and plan on learning more later on, just remember that you are only a man. Mankind has a bad habit of making mistakes, so let's take some extra precautions that tie deeper into our real lives.

To be truly secure when it comes to *your online, drug-dealing, cool guy* persona, you must change some of those bad habits, and developing new, potentially foreign habits; habits *must* be changed in order to achieve true security of your new identity.

I believe that if you are going through this much effort to make such a secured persona, then you may have something to hide or you may just be very on-guard when it comes to digital privacy and security. To put you at ease, we will be making an attempt to make the real you non-exist online; the goal here is to make the real you a virtual ghost while maintaining that entirely separate, healthy social balance of personal social media and hacking the planet.

The main subjects that will be addressed will be along the lines of social media, search engines, accounts, passwords, finding save alternative solutions to anything, and even safely answering unknown phone calls. We will even discuss how to remove some of your online footprint following this segment. Let's go over a few things before that though:

Social media – The issue with social media is that your information gets shared constantly. People share a lot of personal information on social media, whether that information be a simple mention of a cellphone number, a professional email on LinkedIn, or a Tweeted picture with your friends and family at a local restaurant on Twitter.

If you are choosing to use social media, regardless of the privacy issues, then that is understandable. So, at least be secure about it by following this checklist on your social media account:

- Are all of my posts and information set to “Friends Only”?
- Is anything on my social media account set to a “Publicly Viewable” setting? Not even your friend list, family relationships or an old profile picture?
- Have I searched through every possible setting and made my profile as private as possible?
- Can strangers see anything personally identifiable to you besides your name?
- Does my publicly viewable profile picture or avatar include anything personally identifiable, such as your eyes, facial structure, or your property?
- Am I aware that my Facebook cover photo is always public, and if friends comment on or like it then potential attackers may look through their Facebook accounts in order to get an approximate idea of who I am, who my friends are, see if they have any pictures of me, my general location, potential workplace and potential schools?
- Am I aware that if any information is found, such as where I work or what school I attend, attackers may attempt to social engineer your employer, school representative or something along those lines, into giving up your personal information?
- Can I do anything to eliminate the possibility of the past two threats, if so, how?
- Am I using real information on social media?

- Your real friends already know who you are, where you work, and where you live, so could I publish some disinformation such as a false last name, hometown, spoken language or work information?
- Am I using a username that cannot be linked to other online accounts?
- Am I using a complex password that is not used anywhere else?
- Is an email address that is linked to any other account attached the social media account? If so, make a new email address and dedicate it to your social media accounts.

Search engines – Google is a great search engine, but according to several sources, specifically TechWorm, "Google has one big flaw. It traces your browsing history and has been in limelight for it user data scraping methods. It saves your search history, scans your Gmail, tracks your location, keeps everything you say to "OK Google," and a lot more. If you are using Google, than, Google probably knows a lot better of your digital habits than yourself."

TechWorm continues explaining that, "Google tracks user data so that it can serve ads that are targeted just for you. Google says, it also saves data to give you better search results which may be quite true. Though Google allows users to opt out of Google's interest based ads and lets you delete your search history, it still saves enough user data to create a digital profile."

The fact of the matter is Google logs and stores your search terms indefinitely. However, Google does claim that they eventually make an effort to "anonymize" the data. Once 18 months have gone by, they further their efforts by "anonymizing" the unique cookie data that gets stored in logs.

So, what are some alternative search engines that you can use, do not log your activity, and respect your privacy? There are actually a couple that I would recommend, but I will only mention three of them: DuckDuckGo, Startpage, and the new default search engine of Tor, the new kid on the block in the search engine realm: Disconnect. All three of those hyperlinks will direct you to each of the search engines' privacy policies. Please read said privacy policies, and make an informed decision to select a search engine accordingly.

Phones – Do not answer the phone with your name, and do not use a personalized answering machine or voicemail message. Typically I would not write about something like this, but I have a huge pet-peeve, which we will get to momentarily.

A personalized voicemail message makes sense if you are using a business phone that is meant to be publicly known; however, it is simply not needed for a personal phone, you do not need to identify yourself, let alone your entire family in your voicemail. This immediately allows any attacker to identify you, and sometimes your family.

As I said before, one big pet-peeve that I have is when people answer their phones with the following words: "*Hello, [name] speaking. How can I help you?*" Why would you answer your phone like this? You are immediately informing a potential malicious caller that this is in fact [name] speaking; your phone number is now verified in the attacker's documentation. Do yourself a favour and ensure that you confidently know who exactly it is that you're speaking to, prior to introducing yourself. This also applies to text messages and email.

Sometimes attackers, scammers and malicious people in general will even go as far as spoofing their phone number to trick you into believing that the call is coming from someone else instead. An example of this would be if somebody was trying to form a dox; a document containing all of your personal information, they may want to verify a phone number, so they call you with their phone number spoofed to look like your bestfriend's landline; the number on your Caller ID may not be the real caller. With that being said, always answer your phone with the possibility of there being a malicious person on the other end of the call.

Real World Discussion – You can have astonishing operations security tactics, online anonymity, privacy, and an unquestionable persona, but this all can be rendered pointless the very moment you tell your friends, family or essentially anyone about what you do and who you are online. Keep your lives completely separate from one another. Never contaminate your persona. *Do not discuss your Internet activity with anyone, ever.*

Real Life Registration – People sign up and subscribe for things unintentionally very often, two scenarios of this could be:

1. You are at Hot Topic, and you are thinking of purchasing some clothing and a few trinkets. You get to the counter with your desired items, and the cashier nicely asks you if you would be interested in registering to be a Hot Topic Club Member to get 30% off all sales, this membership requires you to subscribe to official Hot Topic emails, and for your information to be added to an account in a database identifiable to you specifically.

2. You are signing up for a gym membership, an account must be created in their gym membership database for you. They would like to have a picture of you just to have on file. So, you agree to their unnecessary conditions and allow them to keep a picture of you on file for the rest of your life even though it was not actually mandatory to do so.

There are a lot of ways that you can go about subscribing to mail lists and registering accounts in databases that didn't even realize existed. Just because you are not yet receiving mail or email from somebody does not necessarily mean that you are not on a mail list, or just because you aren't receiving phone calls in regards to your gym membership doesn't mean that they don't still have that information about you on file.

You may be wondering why these even matters, but let me tell you this: there are some bad people on the Internet; malicious hackers, identity thieves, doxers, social engineers who abuse their powers, and so forth. If one of these people, or even a private investigator, has their heart set on tracking you down, they will start calling stores and establishments such as your local Hot Topic and local gyms, attempting to trick them into giving up your information; this information could be anything from an email, phone number, home address to even your social security number.

Attacks such as these are very personal, and if somebody finds out who you are, but they want more information, they will take this avenues in order to track you down and learn every last thing about your real identity.

The best way to defend yourself from attacks focused on social engineering third-parties, whose responses are out of your control, for information is to not associate with yourself with those third parties in the first place. So, the next time that you are at a store and are asked to get a membership with them, just kindly say no unless it is absolutely mandatory. We will discuss how to remove information from these companies and organizations in the *disappearance lab* at the end of this ebook.

Transactions – Credit cards, debit cards and even gift cards leave trails. These trails get intruded on by law enforcement, skip tracers, and private investigators. To prevent this, pay with cash.

Locational Security

Internet users have to connect to the Internet from somewhere, right? Wherever you choose to setup shop, and pursue your Internet activity from, you will want to pay attention to your surroundings. People in the hacking scene typically talk about operating from one of two places:

1. Home
2. A public location such as a store, shopping mall, or fast food joint with an open wifi-network

Without going overboard, I believe that it is okay to work from home. However, you will want to ensure that your home network security is up-to-par, and you will also want to make sure that there is absolutely no possibility of having any information about your home network slip in the process of you connecting to whatever it is that you're wanting to reach. When I say this, I mean you will want to consider using Tor and a reliable VPN together, as securely as possible. Of course, this isn't the perfect setup alone, but it's a start.

But what about if you decide to take your operations one step further, and use an open network? Well, you will want to do a few things:

- Ensure that the open network is legitimate, a hacker may have setup a fake wifi hotspot.
- Consider scouting out what location you'll use, where cameras are, and whatnot prior to the day of the operation
- Look into protocol spoofing, DNS spoofing and MAC spoofing [?]
- Use a customized DNS configuration, I'd recommend OpenDNS.
- Connect to the Internet once you have secured a VPN -> Tor or Tor -> VPN connection
- Continue to act normal, dress normally and out of sight
- Wear a hat or hood to hide your face
- Do not look directly at any camera
- Avoid any cameras
- Sit in a place where there will be no reflections, cameras pointed directly at you, or people looking at your stuff. We want to remain physically hidden.
- Do nothing to stand out
- Leave when you're done, again, without looking at the cameras.

Take any security precautions that you may deem necessary. This is a very basic checklist that is designed just to give you an idea of what you may need to do. I recommend that you do your own research to see what information is visible to a network upon a device connecting to it, and find out how you can hide said infromation. If you have any questions, look it up on a search engine like Startpage. No matter where you are, be sure to guarantee your own safety since no one else will.

Undercover Communication

Note: Always register and access any account only using a VPN and/or Tor; always have at least one layer of security when working with any online account.

The Internet is defined as a global communication network that allows almost all computers worldwide to connect and exchange information. This information is often monitored, just like phone calls are in spy movies. As a result of this, people who desire privacy and anonymity need to communicate as lowkey as possible. How do we do this? Well, there are a few things that we can do.

Email – This isn't the 90's anymore, people have grown away from hosting their own email servers from home. Anyone who isn't planning on hosting their own email server will need to find a reliable email provider that doesn't rob them of their privacy, and preferably offers some type of strong encryption mechanism prior to any encryption that we include ourselves. Never trust any company with your privacy and information, make sure that you encrypt everything.

Some popular clearnet email providers that value your privacy are:

- ProtonMail
- RiseUp
- + Others

Some popular darknet email providers that you may also want to consider looking into:

- SIGAINT
- VFEmail

If you choose to go with a clearnet email provider, I seriously recommend that you use ProtonMail. If you decide that you'd rather go with the darknet, I'd recommend that you use SIGAINT.

You may also want to consider using temporary, disposable email addresses whenever it isn't absolutely mandatory for you to use your main email address(es), I call this burn mail. Burn email addresses are for one-time-use usage. Not to mention that they really help get rid of spam. I would recommend checking out my personal favourite burn mail provider, 10 Minute Mail, if you are interested.

Regardless of what email provider you choose to use, don't assume that is enough to protect your information, messages or identity in general. You should encrypt absolutely every email possible with PGP. Assume that your emails are always being eavesdropped on, and the only way to shoo away those eavesdroppers is by encrypting your messages with that thing I just mentioned, PGP, otherwise known as Pretty Good Privacy.

PGP Encryption – According to TechTarget's article, “Pretty Good Privacy or PGP is a popular program used to encrypt and decrypt email over the Internet, as well as authenticate messages with digital signatures and encrypted stored files.

Pretty Good Privacy uses a variation of the public key system. In this system, each user has an encryption key that is publicly known and a private key that is known only to that user. You encrypt a message you send to someone else using their public key. When they receive it, they decrypt it using their private key. Since encrypting an entire message can be time-consuming, PGP uses a faster encryption algorithm to encrypt the message and then uses the public key to encrypt the shorter key that was used to encrypt the entire message. Both the encrypted message and the short key are sent to the receiver who first uses the receiver's private key to decrypt the short key and then uses that key to decrypt the message.

PGP comes in two public key versions -- Rivest-Shamir-Adleman (RSA) and Diffie-Hellman. The RSA version, for which PGP must pay a license fee to RSA, uses the IDEA algorithm to generate a short key for the entire message and RSA to encrypt the short key. The Diffie-Hellman version uses the CAST algorithm for the short key to encrypt the message and the Diffie-Hellman algorithm to encrypt the short key.

When sending digital signatures, PGP uses an efficient algorithm that generates a hash (a mathematical summary) from the user's name and other signature information. This hash code is then encrypted with the sender's private key. The receiver uses the sender's public key to decrypt the hash code. If it matches the hash code sent as the digital signature for the message, the receiver is sure that the message has arrived securely from the stated sender. PGP's RSA version uses the MD5 algorithm to generate the hash code. PGP's Diffie-Hellman version uses the SHA-1 algorithm to generate the hash code."

An easy guide for using PGP encryption can be found here, courtesy of DeepDotWeb.

Instant Messaging – Instant messaging is just like email messaging, just a lot more instant as the name implies. Although, sending PGP encrypted messages back and forth can be a bit tedious, especially when you are instant messaging. It doesn't help that popular instant messengers like MSN, Skype, and Facebook Messenger monitors all of account activity, including IP addresses, personal information, and worst of all, your plaintext messages. A nice alternative to these services that you can use is called XMPP.

According to the XMPP.org blog, "the Extensible Messaging and Presence Protocol (XMPP) is an open XML technology for real-time communication, which powers a wide range of applications including instant messaging, presence, media negotiation, whiteboarding, collaboration, lightweight middleware, content syndication, and generalized XML routing." In more simplistic terms, XMPP can be used for instant messaging. XMPP is largely popular due to the easy-to-use Off-the-Record (OTR) encryption. XMPP is also known as Jabber. To use XMPP, you will need a chat client that supports it.

Security, encryption, OPSEC, privacy; you name it, and XMPP probably does it better than whatever application you are currently using for instant messaging. With XMPP, you can either find a server that you trust, or you could even host your own and turn logging off yourself to be sure, and perhaps even offer the service to other people to trust and use as well. That alongside OTR is the perfect method of IM for the hacking community as a whole.

I would recommend that you use Pidgin for Windows, Gajim for Linux, and for Mac, you'll have to find a good client on your own.You can learn a little bit more about the clients, and what clients are available here.

You can really pretty much use whatever XMPP server you please. I am personally a big supporter of XMPP.is, and I trust that they do not log and try their best to respect their privacy. The administrators are the same as the ones who run CryptoWorld. I have several reasons as to why I trust them, but I won't bore them unless someone requests further details regarding their server specifically.

But they key thing in picking a server to use is that you need to feel that you can trust them. Look around to see what others in the hacking community use, ask them why they use that server, and what they recommend. Everyone has their preference, just like I prefer to use XMPP.is or RiseUp.net.

It is worth noting that regardless of what server you use for your account(s), it will not matter if they are logging you or you do not trust them for as long as you are always using OTR encryption. They will only be able to log encrypted *jibber-jabber* (hah), that likely nobody will be even attempting. You can research anything further on your own.

It is common for users to have multiple XMPP accounts to separate identities. I have personally probably went through at least 20 accounts in the time that I have used it. I guess it is good for OPSEC to separate your identities to limit what knowledge specific individuals, or anyone, has of you. Most clients such as Pidgin and Gajim support multiple accounts to be used simultaneously.

You can find a list of different XMPP servers here.

OTR Encryption – According to cypherpunks.ca, "Off-the-Record encryption, abbreviated as OTR, is a form of encrypted messaging which allows you to have private conversations over instant messaging by providing:

- *Encryption:* No one else can read your instant messages.
- *Authentication:* You are assured the correspondent is who you think it is.
- *Deniability:* The messages you send do not have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. However, during a conversation, your correspondent is assured the messages he sees are authentic and unmodified.
- *Perfect forward secrecy:* If you lose control of your private keys, no previous conversation is compromised.

It really is not that hard to setup OTR encryption with any popular XMPP client. If you want to learn how to set OTR up alongside one of these clients once you have one downloaded, just do the following:

- Visit your preferred search engine
- Search "How to install OTR plugin on [preferred client]"
- Read
- Learn
- Do

Internet forums – Online message boards are a fantastic way to maintain a community feeling, share knowledge, and seek help for your problems. You can sign up, post threads and messages freely, and have a great time overall. Although, they are also the downfall of many people's personal security, since it is a source of *public relations*, something that we have already discussed.

A big issue with Internet forums is that people get too comfortable within their own community. They often forget that they are in public's sight, including potential hacker's and government agencies such as the NSA, CSIS or the GCHQ; all of which, participate in global surveillance.

Whenever you post on these forums, you will want to take some general security precautions. Usernames should never be unique or the same, different email addresses should be used whenever possible, passwords should always be complex and different, and you should always make sure that you do not post anything that could be considered *persona contamination*. If you insist on posting something personal, *data poison* it; do not post real information about yourself under any circumstances, ever.

And if at all possible, try to keep away from prying eyes by playing with your forum account settings, since government agencies and potential attackers might try to do something like record every time that you appear online on the forum, which can be prevented by doing something as simple as selecting an option in your forum account settings that says *“Do not show when I'm online”*.

How Far Will Law Enforcement Go

“All it takes is a person or persons with enough patience and know-how to pierce anyone’s privacy — and, if they choose, to wreak havoc on your finances and destroy your reputation." – Adam Penenberg

Truth be told, I don't know how far law enforcement can or will go for sure since I'm not a fed, I'm just another security researcher writing about what I know, but I can try to make some sense of it for you from what I do know, so we will be looking at a few precedents.

Legal investigators, skip tracers, and doxers are all something alike; they are willing to spend an excessive amount of time trying to identify you, and bring inconvience to you and your operations. There is one thing that really distinguishes law enforcement agencies when it comes to cyber crime investigations – they are typically more patient than anyone else when attempting to identify you.

Unlike skip tracers who can get away with breaking the law, law enforcement agencies cannot use evidence that they have found in an investigation if it was found in an unconstitutional manner. In other words, they have to follow their own laws whilst investigating you; whereas, you don't necessarily have to do the same when you're taking anti-forensics precautionary measures to combat how the police can go about looking for you.

If law enforcement can find evidence against you, even if they don't know who exactly “you” are, then they will use it in whatever way that is possible to obtain more evidence and information about who you are and what you do.

In an article from *Tested* discussing how *the secret service sold fake I.D.'s to catch identity crooks*, it was stated that *“the US Government’s 'Operation Open Market' resulted in indictments against 55 defendants. More than 125 fake IDs over about five years of activity while going by the username Celtic. Amazingly, the entire scheme started when the government arrested the real Celtic, a Nevada man who got caught shopping at a Whole Foods where he’d previously used a fake credit card.*

Law enforcement discovered counterfeiting equipment among his possessions and learned about his online activities. Adams assumed his online identity and even improved Celtic’s cred, shipping near-flawless IDs and becoming a trusted seller on Carder.ru.”

As you can probably see, in order to maintain your operational security, you are going to want to actively clean up your trails, switch accounts, and constantly cut ties with people and services who pose as a security threat to you and your operations or cause. In this example, a L.E. agency took over a real darknet market alias, and even acted in the real vendor's place. Everybody and everything is a threat to your persona's security.

In another popular precedent, **Silk Road,** an online black market, and the first modern darknet market; operated on a hidden service run by Dread Pirate Roberts, the master mind of the operation. Silk Road users were responsible for a vast amount of illegal drug related transactions in the few past years. One might wonder how a service like this is operated without being shutdown, or people getting caught, and the fact of the matter is that federal agencies don't have a solid hold on hidden services like this, but that's not the point of the matter.

I was reading *The Rise & Fall of Silk Road* today, which I highly suggest that you read, and it tells a tale of US government agencies not being able to find anything out about this drug empire (Silk Road) for over a year. Here is a direct excerpt from the story:

“DPR, as he was often called, was the proprietor of the site and the visionary leader of its growing community. His relatively frictionless drug market was a serious challenge to law enforcement, who still had no idea who he or she was—or even if DPR was a single person at all. For over a year, agents from the DEA, the FBI, Homeland Security, the IRS, the Secret Service, and US Postal Inspection had been trying to infiltrate the organization’s inner circle. This bust of Green and his Chihuahuas in the frozen Utah desert was their first notable success.”

Okay, so we have learned that Dread Pirate Roberts is a mastermind when it comes to his own personal security, but what's this about this Green character being busted, and Green's bust being considered as a success? I said before that everybody and everything should be considered as a direct threat to you, this includes all personal relations because law enforcement will try to make people turn on you and give up information –Green made a claim that he had [personal relations] with DPR, but luckily for DPR, he didn't tell Green much; regardless, the security breach falls within Green's fault, not DPR's, and it was still considered a big first step towards identifying DPR, and infiltrating the Silk Road drug market. The law enforcement will use everything that they can against you, especially your friends.

Eventually DPR was arrested due to a variety of other things, but The Guardian wrote an article discussing *five stupid things that DPR did to get arrested*. I'm going to go ahead and quote these things, but feel free to read The Guardian's article for further information. So, without further ado, five stupid things DPR did that helped law enforcement see to his arrest:

1. He boasted about running his international multi-million dollar drugs marketplace on his LinkedIn profile.
2. He used a real photograph of himself for a fake ID to rent servers to run his international multi-million dollar drugs marketplace.
3. He asked for advice on coding the secret website for his international multi-million dollar drugs marketplace using his real name.
4. He sought contacts in courier firms, presumably to work out how to best ship things from his international multi-million dollar drugs marketplace, on Google+,where his real name, real face and real YouTube profile were visible.
5. He allegedly paid $80,000 to kill a former employee of his international multi-million dollar drugs marketplace to a man who turned out to be an undercover cop. (*Who are you to decide somebody's death? You are just a man, remember that; don't forget the “Just a Man” philosophy.)*

In another precedent, Jeremy Hammond – a political activist and computer hacker – was sentenced to 10 years in federal prison for hacking Stratfor, and stealing private infromation and intelligence. It is claimed that his arrest for the Stratfor case was largely due to him sharing information with Sabu, someone who he thought was his friend, but turned out to be an FBI informant (don't mix this up – an *informant*, not an agent).

According to an article from Alijazeera, “Although [Jeremy Hammond] maintained multiple online screen names to disguise his true identity, Hammond said he became sloppy when he revealed too many personal details about himself to a fellow hacker, which ultimately led to his downfall. He partly blamed his own consumption of weed and acid for allowing his guard to drop."

By Jeremy allowing himself to share personally identifiable information with Sabu, he got arrested; the personal security issue didn't lie within anything technical, but a personal relation instead.

The conclusion of the matter is that the law enforcement's efforts to arrest an individual, no matter who it is, will greatly vary based on the severity of an incident, their online persona's criminal background, and access to evidence. In a hacker's arrest, every case is different, no case is the same. But what remainds the same, is that it only takes one mistake to get caught.

Sun Tzu once said that "the good fighters of old first put themselves beyond the possibility of defeat, and then waited for an opportunity of defeating the enemy.", you are going to want to assume that this is a very similar mentality of everyone who is trying to locate you when carrying out your operations, and even when you are not. Always be on guard with your enemy, never let your defence down. Assume, and act as if, you are always being surveilled.

The 5, 9 & 14 Eyes

While we're still thinking about law enforcement and surveillance, I figured that now would be a good time to introduce you to the *5, 9 & 14 eyes*. Each eye represents another country involved in close intelligence-sharing group.

The original five eyes, the first tier, consist of: *USA, UK, Canada, Australia,* and *New Zealand,* they have a massive network of intelligence-sharing called ECHELON.

The nine eyes, the second tier, just adds *Denmark, France,* the *Netherlands,* and *Norway* to a second network.

The fourteen eyes, the third tier, includes *Belgium, Germany, Italy, Spain,* and *Sweden* in a third network.

To my understanding, the differences between these three intelligence-sharing networks isn't really known at the moment.

So, what's the point of all this? Well, this means that all of these countries are a part of a network that shares your private data with other countries, and let's say that the US needs information from a server in Sweden, they will have to work with the appropriate Swedish authorities, and have them handle the situation on their own, then share what was found afterwards. For example, if you are using a VPN that's setup on a server in France, and you perform a malicious attack, causing an issue in another country like the United States, then the United States can request that France share the information with them, just as the United States would do in return for France.

You are going to want to use services that are not based in those fourteen countries listed. No VPNs, no proxies, nothing in these countries if you plan on doing anything that you probably shouldn't be doing.

This is just a brief summary of what you need to worry about with the fourteen eyes at this point in time. Feel free to research their intelligence-sharing networks more thoroughly if you insist on it.

Leave No Trace

When you are carrying out operations, it is important that you leave no trace in order to protect yourself from being identified, whether it be by removing the activity logs from a server or just by not making a Tweet every day. This is a pretty simple concept, really.

When browsing the Internet, you can reduce the footprint that you have left by changing your user agent, forcing HTTPS, prevent tracking with a browser add-on like Ghostery or Disconnect. You may also want to consider using Tor browser and a VPN. Whenever you view a website, you don’t want to leave any footprint behind, this means making sure that you change your user agent, use some sort of proxy to cover up your IP address from the public eye, and use different passwords, emails and usernames. It’s as simple as that.

When sharing pictures, you will want to scrub them of any metadata first, a type of metadata called EXIF data exists within pictures, remove this by using a tool like exiftool.

When communicating with others delete all logs, and keep none. You don't want to record your conversations on XMPP, Skype or even in email. Delete it all, and make the necessary changes to disable logging on all of these applications.

Do not tell anyone anything that you wouldn't be okay with having publicly viewable on the Internet. If you won't say it on your personal Facebook, then don't say it anywhere. You don't ever know if the person on the other end of the wire is logging your conversation or not, or even planning to dox you in the long run. If they have data about you and chat logs with you in them, and they get arrested or have their computer seized, then the police still have whatever you said even though it was out of your control for the most part.

Limiting Information Exposure

It would be fantastic if we could be content with leaving no traces ever, but that is not always the case. Due to this, we will want to be able to *limit information exposure* to ensure that we have full control of our information and where it is being accessed. To limit information exposure means to control who and what can see which specific information, and when and where they see it too.

Right now, as of this very moment, silence is potentially a vital key to both your modern day and future operational security if you are operating under a particular persona. The information that an individual may leave around helps develop a footprint of data for that persona, it develops a paper trail in a sense. This is what is often referred to as a cyber footprint.

A cyber footprint should be seen as a vulnerability waiting to be exploited to cause harm to your real life directly, as it could act as evidence building up to your real arrest and imprisonment, not only that, but your cyber footprint can be quite revealing as well which dims future opportunity. People will use your past cyber footprint to locate you.

During a hostile reconnaissance operation that is being carried out against you, both law enforcement and malicious users online can gather a lot of knowledge surrounding your persona. The information gathered can, and will, be used against you. Whether this information be maliciously used against you in a dox, or in the court of law, it is all a threat to you. Your cyber footprint is proof of your existence, it is evidence. Without evidence, you are often acquitted of any charges, and without a cyber footprint, there is nothing to dox.

It would be easy to simply just say to never post or share anything with anyone online or offline; do not leave any solid evidence of your online existence; do not use any social media; do not use email or instant messaging services; however, none of these things are realistic. If you can manage to maintain a livable lifestyle by doing so, I am impressed. But if you are anything like me, you are going to want to make it appear as if you have been keeping your nose clean.

In short, you can practice the very basic operational security required for every day communications by not sharing any personally identifiable information in public view, consistently using a VPN as much as possible, avoiding the use of the same emails, usernames, avatars and passwords, and avoiding persona contamination. It really isn’t that hard. Just don’t go posting this and that everywhere and making yourself popular for whatever reason. It really isn’t hard, don’t try to act like anything special.

Everything has a trail. So, try your best to keep anybody in the future from finding the trail of your past. Nobody needs to know that information – your cyber footprint – besides you. Limit the exposure your information can experience, only you can do that right now, as of this very moment.

Controlling Disputes & Manipulating Enemies

Dispute, conflict, and war are all part of human nature. Malicious individuals with the bloodlust required to fuel this desire, and an eye for war are common to find, especially on the dark side of the Internet. Due to this malicious atmosphere, it is crucial to always be prepared for whatever is going to come your way next.

Before you find your way into a dispute, you will want to ensure that you have already won beforehand. More than anything, you will need to be capable of manipulation; however, you will also need to have a solid persona, back-story, and you will want to know exactly what you are doing; although, you will need to discipline yourself at the same time since a solid story and persona alone will not lead you to victory during your dispute.

Sun Tzu once said that “victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win. Thus it is that in war the victorious strategist only seeks battle after the victory has been won, whereas he who is destined to defeat first fights and afterwards looks for victory.” The same concept applies here, a puppet does not control a puppeteer; however, a puppeteer does control puppets. The puppeteers psychological way of being is manipulative, and having full control and capability of manipulation means that you can make your enemy act in desired ways. Thus, allowing you to choose to win almost whenever you please.

In the past, we have discussed limiting information exposure. To limit information exposure means to control who and what can see which specific information, and when and where they see it, too. If your enemy is limited to only this information then you already know every possible point of attack that they have. With an intimate understanding of how your information can be accessed can allow you to even make the next step for your enemy. For example, by limiting the information that your enemy has access to, you could pretend inferiority and encourage their arrogance to make them attack you carelessly, this would ultimately let them think that they have the upper-hand, even if that’s not the case.

Although, this will only efficiently succeed if your enemy does not know that they are a puppet caught in your strings, being manipulated to do your biddings. You are going to want to “appear weak when you are strong, and strong when you are weak.” (Sun Tzu), and you will want to achieve the supreme art of war by subduing the enemy without fighting in the first place. Your enemies are puppets, you are the puppeteer – take control of those puppets, and manipulate them into going in a direction that is most convenient for you, but don’t allow them to know that you are manipulating them.

Allow yourself time to prepare prior to the dispute, and when an Internet dispute happens, you normally will have time. This gives you the upper-hand, the ability to: speak and act with patience and awareness, control your ego, manipulate your enemy carefully. If you apply these three principles, you can win your dispute or battle before it even truly began.

You are a puppeteer, a controller, and manipulator. Information can be controlled, just as puppets are. The opportunity to take control of a dispute, and manipulate your enemy, is always there.

Conclusion

This guide to securing your online persona has been a pleasure to make for the general majority of the Internet, specifically for you "security researchers" out there.

Even though a lot of this content can be seen as overkill in the eyes of the typical Internet user, you must remember that *your persona is only as secure as you make it.* Your own personal security is entirely up to you; your persona's security and pseudonymity is strictly your responsibility to develop and maintain, not mine or anyone else.

If you are still interested in learning more about everything to do with operational security or security, I strongly encourage you to allow yourself to free your mind and do research on your own beyond this guide. I regularly post on my blog, Puppet Zone, if you want to read any more of my content, or if you want to keep up-to-date with my future teachings.

Thank you for reading. It has been a pleasure writing this for people to learn from. This has been the *first edition* of *Securing Online Personas*.