How to lie to people : Achieving Anonymity Through Disinformation and Data Poisoning.

by **DIzzIE aka x-c0n [antikopyright 2007]**
posted by **Insider**

HOW TO LIE TO PEOPLE ACHIEVING ANONYMITY THROUGH DISINFORMATION AND DATA POISONING

Preamble

When providing information, the worst thing you could possibly do is give accurate, truthful data. This should be common sense. If it's not, close this text and think about why it should be, then come back when you're ready or **** off for good. However, the recourse that many have chosen, the proverbial vow of silence, is no panacea. Actively choosing to refuse to provide information, to give the bloodhounds nothing, will make them uneasy, hungry, suspicious, and, of course, quite vicious. What one must then do is quite simple: give them a false trail to follow. In other words: **Lie** to people. All the time. About everything. Going further, create future lies. Lies that lie in hidden corners just waiting to be stumbled onto by the coming bloodhounds, who will then think they've stumbled onto something genuine. Your goal must then be to pro-actively mold pieces of **** into gold nuggets. Plant your buried scat treasure and watch the ****_ers_ suck it down. The aim must always be to present the illusion of transparency, an *'I've got nothing to hide'* hologram, if you will.

In short: your goal is to go around the web planting poisonous seeds of disinformation, with the intention that others who will try to track you at a later date will stumble onto them and think them to be real. The rest of this brief guide will be about general tips for creating disinformation to preserve your anonymity, it is obviously hardly exhaustive, and is meant to serve as a springboard for inspiring your own acts of data poisoning. However, as this guide is operating under the impression that most people currently do not actively engage in data poisoning, this guide also doubles as a stalker's companion. Pretty convenient, indeed.

Before You Begin

Before you're ready to engage in proactive data poisoning, you first need to do a wee bit of preliminary research. Pick a name for yourself, as well as a unique *user name* (something that when searched for, will only return your name, not 50 million others), email address, as well as a birthday, location, pets, family, hobbies, car, political affiliation, and other basic demographic information. Keep in mind that your intention with this data is that each nugget can and should be used to track you, that is indeed your goal in the creation of this false front (i.e., if your new user name is a reference to a television show which the real you would never watch, start posting on fan message boards and newsgroups for that show, this is discussed further in the section on fabricating your peripheral identity later in this text).

A key ingredient in the successful passing of illusion as reality is consistency. This means that once you pick your initial uninformative characteristics, you'll have to stick with them for all locales you later frequent (e.g., use the same user name on all forums, and tell different people the same lies). After you have the initial information, here are a few more things you might want to take care of (again, these are just a couple examples to prod your own brain into thinking of more **** on its own):

Find a few photos of some unpopular person on social networking sites like MySpace or Facebook, or on public photo storage places akin to Flickr. These will now be your photos. Pick someone of average physical prowess, someone who doesn't have too many friends/contacts listed, doesn't live anywhere near you, doesn't frequent the same web fora that you do, and, most importantly, someone whom you and any of your legitimate contacts are not affiliated with in any way whatsoever.

Try opening the photo file in a text or hex editor. If it is an unmodified file taken with a digital camera, you should see various nuggets of metadata embedded in the file, such as the date the picture was taken, the resolution/camera settings, and, most importantly, the camera model. This will now be your camera. Find a forum for this camera, or failing that, a forum for amateur photography, and make a few posts asking some basic questions about the camera. When someone then searches for you and examines the metadata of your images, your identity will thus further be validated in their bloodthirsty, data hungry eyes.

Any data match serves to validate your illusory identity, any data discrepancy serves to question it. Once you have the photos, open them up and perform a minor modification such as adding an extra pixel. This is to change the MD5 *checksum* of the image file. Each file has a unique number that can be shown by using programs like ChaosMD5 (Elgorithms :: Downloads :: Chaos MD5 the Free MD5 Generator). By modifying the file, you are also modifying the MD5 *checksum*. This is done so that, should anyone later be performing comparisons/searches by MD5, your stolen image will not be presented as a match, therefore improving the chances that your false identity will not be discovered.

If you wish to, create a phone number for yourself, there are plenty of free services such as www.j2.com which give you a free voice-mail box and fax number. Often times the free services do not let you pick your own area code, in which case you will have to make sure that your location matches the area code. If your free number requires a call every X days to be kept active, use a free service akin to phonemyphone.com :: Find your cell phone, escape boring meetings, free telephone reminders, wakeup calls to place the call. Websites such as Area codes locator - Area code lookup by number or city, US and Canada area code listings, area codes directory provide lists of area codes and the states to which they belong, while sites like Telephone Number Location Information allow you to locate the city within a state by using the prefix (the first three digits after the area code). When performing reverse phone *lookups* on site like Free Reverse Phone Number Lookup | WhitePages or Fone Finder query form, be aware that the phone service provider may also be visible. In keeping with our consistency motif, never contradict this data (with natural exceptions, such as if you're stating that you recently moved from X to Y in your fake blog, thus implicitly explaining the geographical discrepancy of the phone number's location and your present residence).

Creating the Core You

Once you have acquired what you feel is a sufficient amount of preliminary disinformation, it is time to start actively engaging in its proliferation; that is, the fun and tedious process of data poisoning. Ten years ago, I would've told you to create a personal homepage for yourself. Today, homepages are obsolete and unnecessary (though if you have the time, additional data poisoning can't hurt; that is, unless you half ass it). Instead, you should set up your core identity on social networking sites like MySpace and Facebook, as well as on blog sites like LiveJournal and Xanga. Create your personal pages using the fake data you generated in the step above: listing your name, email, birth date, hobbies, favorite music, photos, and so on. These are known as the core sites, because they will be the main websites that any bloodhound on your trail will discover first, and which will contain the greatest amount of information about you.

Creating the Periphery You

After you setup the core sites, you will need to extend your data poisoning to various periphery outposts to further entrench the legitimacy of your false identity. Although the periphery you is secondary to the core, it is no less essential; indeed, perhaps more so. The role of the periphery is to dupe the meticulous bloodhound who will spend hours mining through search results, harvesting little **** nuggets here and there, and looking for any inconsistencies that might suggest duplicity. In other words, take the task of creating the periphery as seriously as the core.

Now then, to create the periphery you must cannibalize upon your initial information. If you said you like a certain band, start posting on the message boards for that band, being sure to indicate that you went to any relevant concerts close to your geographic area. If you said you have a certain exotic pet, start posting on newsgroups and message boards asking for advice on taking care of said pet. Rinse and repeat for all other periphery components of your identity: your car, favorite book/author/movie/*pornstar*, favorite hobby, sport team, and so on. Always post on all message boards with the same user name. This will make you easier to track, and make the bloodhound when *ze* thinks that *ze's* just discovered that you not only like Korn, but also have a pet ferret and drive a pimped out Audi.

And lest you're by this point losing faith at the apparently humdrum meaninglessness of it all, keep in mind that there is no such thing as an insignificant detail. Every bit of information can be, and, indeed is, being harvested and subsequently has the potential for being used for tracking you the **** down. To give a (non) trivial example, someone who knows where you live, the car you drive, and the band you like, can then proceed to find you outside of a concert hall on the night that your band's playing. Copacetic?

Real Time Data Poisoning and Time Syncing

Once you have setup the core/periphery *disinfo* centers, your job isn't quite done yet. Indeed, data poisoning is a persistent process around which you must adapt all of your everyday actions, both online and offline. Each time you chat with friends over instant messaging or IRC, you are leaking data. Comments about the weather, current events, even your speech mannerisms, all serve to betray your identity, and therefore must all be modified. You must then engage in real time data poisoning: consistently lying to anyone and everyone you communicate with about everything.

An extension of real time poisoning is time syncing. If you say you have a 9 to 5 job in time zone X, then be sure that you're idle during those times, or explicitly mention that you have Internet access from work/school to present a resolution to the apparent time conflict. Do this proactively, meaning volunteer the information yourself, before the person on the other end becomes suspicious. Saying something like 'I just came back from watching Lesbian Scat Girls VII' when according to your time zone you should be at work/school can be disastrous to your identity (speaking of time zones, don't forget to set the appropriate zone on all of your forums). However, we all slip up and **** up here and there. Such discrepancies can then be explained away with relative ease by stating that you had the day off school or whatnot, as long as they don't accumulate to an excess over prolonged periods of time.

When chatting, it is further advantageous to initiate apparently accidental data slippages. Pretend that you thought you were talking to someone else, and share a seemingly intimate bit of information about yourself, and then follow it up with a *'oh ****, wrong person.'* Similar techniques should be used by accidentally pasting private emails into instant messaging conversations, and then hurriedly explaining that your *fershlugginer* copy and paste keeps jamming, and urging your chat partner to pay the information no heed.

As aforementioned, your very speech patterns betray your identity. In the spirit of practicing what you preach, looking a few lines above you can see that I used a seemingly odd adjective, '*fershlugginer*.' Doing a little bit of research, you'll undoubtedly find that it was a term popularized by MAD Magazine in the 70's, leading you to believe I must be an old school fan of that particular zine, which will in turn lead you to make now intrinsic assumptions about my age, nationality, and so forth. Therefore, you must always strive to saturate your everyday parlance with various cultural (and therefore also potentially geographic) references. If you are communicating via phone or *voip*, which is highly inadvisable as extensive forensic analysis of *voiceprints* can reveal your real identity even when you're attempting to adopt various masking techniques, you should nonetheless use a hardware or software voice modification application, at the very least.

Realtime data can further be poisoned by injecting false descriptions of everyday events. Saying you just got your hair highlighted, a spiffy new tattoo, or even a broken leg, are all as essential as the aforementioned core/periphery identity modifiers. Again, keep in mind the physical location you're supposed to be situated in, and after checking the weather for that day, make appropriate comments about how how/cold it is, and so on it goes...

Finally, keep in mind that if the so-called first rule of forensics is Locard's theory--every contact leaves a trace--then a necessary corollary is that every false contact leaves a false trace. Again: there is no such thing as innocuous data. Every little morsel of information is engorged with salience, and every little morsel can likewise be manipulated to suit your needs; in our case, the poisoning of the unknowing bloodhounds on your illusory trail. Consistently lie your ass off to achieve the much- thought after ambrosia of anonymity.

Cheers.