



Created By: mothered

<https://www.socialengineers.net>



How To Effectively Anonymize Your SEing Activities

Everything you do In life has an element of risk. Be It travelling to work on the highway at maximum speed, thereby Increasing the chance of an accident due to losing control of your car, or simply crossing the road on a busy street and neglecting to look at both directions to see oncoming traffic heading straight for you, **there will always be some degree of danger or threat** - no matter how minimal It may be at the time. **When you're the one who's In charge of your very own actions,** It's pretty simple to take precautionary measures by analyzing the risk factors and making conscious decisions that will reduce your exposure to potential threats, however **the same cannot be said for social engineering as a whole.**

Sure, you're well aware of what you're doing on your end when formulating your method against the nature of both the company & Item you'll be SEing, but the moment your attack vector Is executed, It's a totally different story - **you never know for sure what happens on the other end of the spectrum** - namely when representatives are assessing your claim. For example, **due to an excessive amount of refunds, your account may be flagged at any given time** which will trigger an Internal and external [Investigation](#), and If the company **conclusively deems your behavior Is fraudulent, there's nothing stopping them from notifying the police** or other law enforcement agencies.

Now It's not my Intention to put you In a state of panic, but more so to point out that (although rare), the probability of being handcuffed based on the above scenario Is realistic and **"can" (not "will")** come your way when you least expect It. **Here's where the problem comes In.** As an advanced SE'er yourself who's been consistently hitting companies of all shapes & sizes for many years to date, **"you'd tend to overlook the consequences of your behavior"** and because SEing has become a common routine In your life, **you don't realize just how serious It Is.** After all, **you're obtaining goods via Illegal means** and the ramifications If caught, pretty much speaks for Itself.

As a result, It's paramount to not only take extra special care with each and every entity you're SEing, but to also **"anonymize your social engineering activities"** where applicable. What this means, Is to disassociate Identifiable details that're linked to your personal profile, devices, online accounts, payment systems and so forth, **all of which could potentially reveal the user behind the keyboard** - evidently **"yourself"**. And depending on the events of your SE, things like **account closures and transactions declined & reversed**, are well and truly likely to take place. So how do you prevent all this from happening?

Well, you cannot prevent It In Its entirety (nothing Is "100%" secure!), but rather Implement safety and privacy measures, that will **significantly minimize being exposed and help keep**

your personal information and credentials where they belong - within the confines of your local environment. That's where I come in, by introducing a few very effective methodologies on how to maintain the highest level of anonymity in all facets of **"company manipulation and exploitation"**.

Now I'm not suggesting that you should take everything (of what you're about to read) on board - I have no idea of how you operate, nor is it any of my business to ask - even if I had the power to do it. So pick and choose those that are relevant to your SEing circumstances, and **be sure to use your selection with every subsequent SE thereafter**. Okay, so without further delay, let's make a start with **"online account anonymity"**.

Online Account Anonymity:

It's all well and good if you're social engineering a given company every few months or so, but when you're hitting the same one many times in succession, **particularly in close timing and with high value items**, the likelihood of your online account being flagged and deemed suspicious, is almost a certainty. This can lead to your account being permanently locked, or in the **"absolute worst-case scenario"**, a **cease and desist notice** will be issued to you by the company's legal representatives. Although the probability of C&D notice is quite slim, there's still a chance that it may come your way - **if you keep SEing with "greed"**, as opposed to using common sense and good judgement.

On the other hand, you may be taking the utmost care by covering every angle to ensure your SEs don't set off alarm bells, but irrespective of that, **you're the type of SE'er who prefers to remain anonymous with every SE performed**. Whatever the case may be and the reasons behind your decisions, I will show you **how to protect your real online account** (that contains your personal info) by changing **"every identifiable detail"**.

Yes, you've read that right - in order to detach yourself from your real identity, inclusive of all the tools used during your SEing activities, **it's imperative to "create a completely different account profile"** - for the fact that many companies such as **Amazon**, can actually detect multi-accounting **only by "the device you're using!"** even when everything else has been altered. Do I need to elaborate on it further? I didn't think so. Now that you have a clear understanding of that, here's my list of recommendations.

- Change of full name (family & given name)
- Change of date of birth (where applicable)
- Change of full residential address. If need be, use a drop (refer to the next topic)
- Change of email address (no need to explain this!)
- Change of phone number (new SIM on a fake account or a [Burner service](#))
- Navigate via a VPN (NordVPN, IPVanish, ExpressVPN will suffice)
- Use a different device (one that was NEVER used with previous accounts)
- Change your MAC address ([this free tool](#) does an excellent job).
- Use a VCC- Virtual Credit Card (as discussed In the topic after the next)
- Use a GC- Gift Card (an alternative to a virtual credit card)
- Use a different password (nothing similar to the old account)
- Navigate via a private search engine (prevent your online behavior being tracked)

Anonymous Delivery Point:

The location used to accept your deliveries from the carrier who will be dropping off your packages, **can reveal a lot about who you are on a personal level**. Whether It's your very own home or one that belongs to your parents, all It takes to Identify Its occupants, Is to **perform a reverse address lookup** and depending on the service used, the full name, phone number and email address will be returned In the search results. And If that's not concerning enough, **real estate lookups are available to anyone who wants to know more about the property Itself, as well as Its current owners** - at the very least, the **first name** will be available which can be used with other bits of Information to build an entire profile about the person In question.

All the above, Is purely an example of just how easy It Is to grab (at the minimum) the name of a given person **with only an address on hand** and when social engineering here and there, companies have Internal tools & resources that make the job a lot easier. So how do you hide the fact that you live at your residential address? Moreover, how and where do you physically accept your goods by not disclosing your place of residence? The answer Is simple - **use a "drop house", that's also known as a "drop address" or "drop" on Its own** and as such, the company and their carrier partner will never know where you live, thus It adds another layer of anonymity to your personal ID.

If you're reading this as a beginner SE'er, I'd say you're at a loss as to what a **drop house/address** relates to, so allow me to briefly define It for you. **It's a physical location In the form of a residential home, that does not belong to the SE'er and Is solely used to receive**

packages when ordered from an online retailer/store. That is, Instead of using your real address for deliveries, you'd opt for a "**vacant**" remote home that has no association to you whatsoever and when your package is due to arrive at the drop, **you meet the driver there and accept it** - as though you're living at the house.

As simple as it may sound, **you cannot choose any property that comes to mind**. Why? Well, what if it's occupied at the time the carrier delivers your package? I don't need to explain what happens next! So to help you locate a suitable drop house, I've listed a few topics below that have proven to work well, particularly when using the [DNA method](#) and also for [advanced replacements](#). Obviously, you will not be using the lot, so **select the one(s) that you're comfortable and most importantly, confident in utilizing with your SEs**.

Properties Advertised For Sale

In order to collect packages at another person's property, **it's crucial that it must be vacated at all times**, however when SE'ers look for a home that's "**listed for sale**", they instantly assume that it's unoccupied and while this may predominantly be true, it's not always the case. Think about it logically for a minute. If you're selling your house, "**would you immediately leave the moment the for sale sign is erected, or wait until it's sold and then move out?**" I, for one, would prefer the latter (sold and move out) and I'm quite sure you share the same viewpoint, hence a "**for sale sign**" **doesn't necessarily mean the house is empty**. Why would the seller leave way before the settlement date, when there's no reason to do so?

Sure, **prior to packing his bags and moving out**, the home owner (and the spouse) may be employed on a full time basis and spends his/her time at work 5 days a week from 9:00 am-6:00 pm which is perfect to schedule your delivery to suit those times, but **many carriers deliver outside business hours - either very early in the morning, or late at night**. As such, **you must be absolutely certain there's no one living there** and one way to find out, is to do a little surveillance work by visiting the premises "**in the evening and late at night**" throughout an entire week. If you don't see any lights switching on and off, then it's not occupied. Also, **have a look if the letterbox is overflowing with brochures, advertisements etc**. If it is, it's clear that there's no one there to collect them.

Properties Advertised For Rent/Lease

This is my favorite to use as a drop address, for the fact that it's almost guaranteed that the owner of a place that's **"listed for rent"** is awaiting tenants ready to move in, therefore **he/she (or anyone else) will not be occupying it**. For instance, when you were legitimately house-hunting for a property advertised for lease/rent and spoke with the agent and arranged a physical inspection, **how many times did you find its owners hanging around watching TV?** I'd say your answer is never, or perhaps less than a handful of occasions. In my experience, over 90% of landlords prepare the property by cleaning the carpet, repainting the walls, carrying out some maintenance work and then vacate the premises.

That being said, the last thing you need is for the carrier driver to pull into the driveway and someone answers the door to accept your consignment, thus **you must be completely sure that it's unattended**. To do that, you can apply the scenario as per the example in the topic above, or (where available) **"call the landline number to see if anyone answers the phone"** by doing it during the evening, and especially late at night - everyone is home at that time either relaxing, or asleep. **If nobody picks up the phone, then there's your answer.**

Now you're probably thinking of how you're supposed to get the number when you only have a residential address to work with, but you'll find that it's a lot easier than you think. Stating the obvious, **hitting a Google search for homes that're advertised for rent**, will return pages of results and if you look hard enough, there's bound to be a phone number listed somewhere in the article. Alternatively and as already discussed, **reverse address lookups such as Spokeo or Intelius**, are very beneficial when looking for publicly available information. If you happen to know the **first & last name** of the person, enter that - it will return the same results as the reverse address.

A Foreclosed Home

Without a shadow of a doubt, this is one of the best and most effective methods that you can confidently use as a drop house - and that's because **it's conclusive that no one is occupying it 24/7**. You will not find a **"foreclosed home"** with **"its owners"** actively living there, so rest assured, **it will always be vacated**. The question you're likely to ask is **"I've never heard of a 'foreclosed home', so what exactly is it?"**. I'll be more than happy to answer your concerns as follows. When home owners cannot pay their weekly/monthly repayments on the mortgage for an extended period of time, **the bank seizes their property and puts it up for sale.**

In other words, the bank wants to reclaim any financial loss they can, hence they'll advertise the home on the market for a quick sale and **given the house has been taken over by the**

bank, **"It's empty awaiting to be sold"**. The only drawback of a foreclosed home, is that it's not very common that you'll locate one in the vicinity of where you're currently living, but they do exist and **the way you find one, is by sifting through real estate websites**. If it's a foreclosed home, it will be listed as such - the agent cannot withhold any details, **they are obligated by law to advertise the property for what it is**.

The same applies when you're physically looking for it - along with a huge **"For Sale"** sign stuck on a board at the front of the premises, there will be a **"Foreclosure"** (or some variation) notice next to it. This is a mandatory requirement, **so there's no chance that it'll be mistaken for a house that's purely up for sale**. Now there's one thing that you must be aware of - because it's unoccupied, **"squatters" may decide to move in**, so be sure to make a note of this prior to selecting the one you plan to use with your SE.

Payment System Protection:

What you've done so far, is implemented privacy and anonymity measures with your **online account** and **residential address**, by disassociating your personal credentials and replacing them with material and information that has no relation to you whatsoever. However, **it serves very little purpose if you can be identified in other ways** - namely **"the payment system you use for each purchase when SEing"**. Although some details such as your credit card PIN number remain private, companies do have the capacity to view (at the minimum) **the card holder's name and account number, which can pinpoint who you are**. Consequently, if you neglect to anonymize your payment system altogether, there is not much point in applying everything that you've just read in this article.

For example, have you **created a multi-account with Amazon** using a fake name, address, phone number, different password and another computer to log in, **only to find that your account was closed shortly afterwards**? If your answer is **"Yes"**, then there's a high possibility that your **"payment system"** was responsible for the identification and termination of your Amazon account. So how are you supposed to use a fictitious bank account (and the like), when transactions are actively being debited and credited? Well, you don't touch your real account, but instead **use a "VCC" (Virtual Credit Card) to hide and protect it**, but before I discuss how it's done, I'll explain what defines a virtual credit card.

Unlike your normal plastic credit card that can be used to buy stuff at your local mall by swiping or inserting it in the machine, a virtual credit card is quite the opposite - **"It's not a**

physical card, but rather some random number that's generated by the VCC provider", and is associated to your real credit card. Put simply, **It's a temporary 16-digit number** that comes with an expiry date and a CVV (Card Verification Value) number, much the same as what you see on your physical plastic card. Generally speaking, here's how it works. When you purchase something on the Internet, **the online merchant will "only see your virtual credit card number"** and not your real one, therefore the details of your actual real card will not be exposed.

There is no difference in how the transaction is performed and the best part about it, is that no one can tell that you're using a VCC. **Everything is done against your "virtual credit card", but in reality, the money is taken out of your "real credit card",** hence the merchant will never know who you are, and you can cancel the VCC anytime you like and get a new one thereafter. But what about the **card holder's name**, you ask? Evidently, you cannot use your own, so you'd need to **opt for a provider that allows you to add any name you like** - one of which is a service named [Abine](#). Of course, there are many others, but I'm not going to spoon-feed you - as an SE'er yourself, it's your job to research, not mine.

Anonymously Selling SEd Items:

This article has exceeded its reading time by a lot more than what I anticipated, so I'll try to keep this topic as brief as possible. In terms of SEing non-technological items such as footwear, makeup, fragrances, hair care etc, **the item itself is not manufactured with any type of identifiable markings** (more on this shortly), thus it can be sold without worrying about the buyer coming back to bite you at a later date - even if you didn't mask your personal details during the SE. For instance, if you SEd a **bottle of Chanel Coco Perfume Spray**, and received a replacement instead of the refund you were hoping for, there's no dramas when selling it - **"you cannot be traced purely by the item"**.

However, the same cannot be said when **selling tech-based products** to the likes of AirPods, cell phones, smart watches and tablets - **they all have unique identifiers attached, namely "serial numbers and/or IMEI numbers"** and if you didn't anonymize your online account at the time of your SE, the **IMEI and/or serial can be used to link the item back to yourself**. For example, if you've sold an iPhone that you SEd by using the [DNA method](#), **you're not supposed to have received it**, therefore its IMEI may well be placed in a pool of blacklisted numbers. Now when the buyer attempts to activate it with a particular carrier service, they'll

decline It and If he decides to take matters further, **you'll be held responsible for selling an Item obtained via fraudulent means.**

As you can see, **when selling goods with serials/IMEI numbers**, It's not only vital to anonymize your purchase by creating a fake online account, and protect your payment system and doing the same with your delivery address by using a drop house, but **you also need to plan on how to distribute your Item to the buyer through the Internet**. If you haven't worked It out already, of equal Importance Is to **"advertise online using a similar approach"** - fake account, a virtual credit card to accept the transaction, a **burner service** as a point of contact and so on and so forth. In short and simply stated, **"use the same/similar anonymity measures when buying and selling"**. Pertaining to **where** to sell, there's no shortage of websites - eBay, Facebook Market Place, Craigslist and obviously Amazon will suffice.

In Conclusion:

Given that every company believes an SE Is a legit claim, If you treat It as such by manipulating It accordingly without raising suspicion, there's no doubt that It's perfectly fine to use your real credentials. But **many SE'ers (such as refunders) prefer to completely hide their activities**, and rightly so - Items are not refunded and replaced on legitimate grounds and as a result, **concealing every Identifiable detail related to your personal profile Is first and foremost**. If you're reading this article from an anonymous standpoint, you're now well Informed on how to social engineer without leaving a digital footprint behind, nor any chance of being tracked and Identified from one SE to the next.

You may reference my work, only If you credit Its source namely

<https://www.socialengineers.net>

Downloaded From:

<https://www.seing.org>