

DNM VENDOR BIBLE

Table of contents

1. About
2. General Tips
3. What Not To Do
4. Setup
5. Packaging
 - General
 - How to package
 - Return addresses
 - Stealth
6. Shipping
7. Cashing Out
 - General
 - Buying with btc
 - Getting the btc to the exchange
 - Selling your btc
 - Keeping your assets safe
8. Various Resources

About

Hello and welcome to the Darknetmarkets bible for vendors. While the DNM bible for buyers aims to be a complete guide and walk-through for buyers, this is not the case for this bible. The following information will just be a **help** for already operating vendors or people who want to become one.

Being a successful DNM vendor is an extremely complex topic and is an ongoing job. There is much more information you need to gather before becoming a vendor than just reading the DNM vendor bible. If you do not want your vending career to end with your conviction, here are just a few points you have to consider:

- you have to know the ins and outs of the DNM buyer bible.
- you have to be aware of news in the DNM scene by following market forums and other discussion places. If someone posts valuable information about vending for example, you better take notes.
- you have to stay up to date on law enforcement actions, especially the ones that happen in your country. Know when your competitors get busted and why, know what method the customs use to check packages, know if there is an ongoing LE operation in your area that focuses on DNM vendors, . . . and many more factors. A tiny mistake can be enough for LE to throw your ass in jail. This is not an exaggeration, just one tiny mistake is enough for LE to catch you. Be it a partial fingerprint that you left when packaging, or an accidentally unencrypted message, LE will do everything to exploit every single mistake you make.

Moreover is vending a real job, not just a hobby. If you fuck up, you flush your life down the drain. You will most likely get jail time, spend thousands of dollars on a lawyer, get disowned by your family, get news articles about you being a drug dealer published, get a permanent record which will prevent you from getting jobs left and right in your entire future life. **If you can not deal with the consequences of getting caught, do not become a DNM vendor.**

So as you see, vending is not just something you start when getting bored or thinking it would be "cool". If you do not want to get caught,

you do not even get to brag about what you are doing. Every person that knows about your operation and is not working for you, is one too many. Do **not** expect any real life fame from being a DNM vendor. And if you get some, you are doing it wrong.

There is also the common misconception that a DNM vendor makes fast and much money. This is utterly wrong. A DNM vendor will have to wait **much** longer till he actually gets to hold cash in his hands for the product he sells. A normal, offline dealer for example just meets up with the buyer, sells the gram of coke and gets the money in cash.

The DNM vendor however, has to check the buyer history and validate the address, then accept the order, package it without leaving any fingerprints or DNA traces, then use suitable transportation methods to drop the package off at strategic locations, then wait days till the buyer receives his order. If you are in luck, the buyer will not try to scam you and the package will go through without getting seized, so the buyer releases the bitcoins to you. Now you still have to exchange the bitcoins into actual dollars, and that is a whole topic itself because you need to break the link between the bitcoins you got through drug dealing and the ones you sell on the bitcoin exchange, you need to use cash-out methods that leave no or very little paper-trail (you will see later why this is crucial), . . .

All this is a pain in the ass and madly time consuming. So if you are not willing to go these many extra miles or not willing to deal with the technical side of being a DNM vendor (if you for example want to skip using Tails you can fuck right off), then stick to offline dealing. It is not a shame to admit that being a DNM vendor is too complicated or elaborate for you, because only a part of people reading this is actually ready to become a proper DNM vendor. If you want to make quick and easy money, go the traditional way of drug dealing.

Now that the "easy" part of being a DNM vendor is debunked, let's get to the "much money" part. You probably know a handful of kingpins that made a small fortune by selling on DNMs and some of them are still not caught. This gives some wanna-be vendors the false implications it will be the case for them too, which is wrong.

In fact many DNM vendors are just small time ones that make a couple of hundreds or a couple of thousands dollars profit and then stop vending. It is the silent majority you rarely hear about. And there is nothing wrong about that since you should expect to fall into that category too. While you are vending you will **always** have to keep in mind that it is better to leave the game as a free man and with some money you made, than getting busted with large amounts of drugs and money.

Many people do not know when to stop because they get blinded by the online fame and reputation they have. You will sooner or later read about them in news articles and court documents. Do not become one of them.

Please note that the DNM bible is only possible because a lot of awesome people dedicated countless hours of their free time to writing the tools you will use when following the guide. So please show your appreciation to them by making a donation to the torproject, Tails and/or GnuPG once in a while. If you have money to buy drugs, you also have money to reward the people who make it possible for you to order drugs safely to your front door.

Happy reading and stay safe.

General Tips

When getting asked if you provide alternative payment methods (e.g. paypal) or other OpSec compromising things, do not accuse the buyer of being law enforcement and go on a long rant about the government and drug laws. Instead give the user a short refusal and do not waste much time on it. No insults or accusations, keep it brief and professional.

There is a limit for how long you should vend. If you start vending it is only a matter of time till law enforcement puts you under investigation. How long that takes depends on several factors such as the product(s) you sell, your ability to fly under the radar (if you are a very extroverted vendor or keep it to yourself), your profile (if you indicate that your OpSec is shit, e.g. listing a phone number will attract law enforcement like flies to shit).

But sooner or later law enforcement is going to investigate you. You do not know when this is, so you have to stay cautious all the time, not just step up your OpSec after vending for some time. When this phase begins, it will solely depend on your OpSec, cleverness and creativeness how long it will take, as well how much resources law enforcement invests into getting your ass into jail. As you will read later on that page, there are great differences in how long the investigations take.

However, your goal is not to vend until you get busted. You need to quit while being ahead. If you want to vend for several years, you **need** to terminate your vendor accounts and start all over again several times. In general, no vendor should vend over 1,5 to 2 years. This is a good time period to ensure that the investigation that law enforcement runs is not too much in progress (i.e. already observing your home) but you destroy the one that is already in progress and flush their month long work down the toilet. Then, if you still want to vendor, start all over with a new vendor identity and with following the tips below.

This is what you should aim for. Yes, it is god damn time-consuming and shitty to start all over again and giving up your valuable reputation. Nobody likes to do it, but if you value your freedom you need to do it. All busted vendors have one thing in common: law enforcement had simply enough time to investigate them. If you are smart you do not do the same mistake, but switch vendor identities after 1,5 to 2 years.

If you do it right, you can vend for years and make insane money. Sounds better than decades in jail because you could not say goodbye to your vendor reputation, doesn't it?

So since you now know why it is crucial to switch vendor accounts, here is what you need to keep in mind when doing so. Starting under a new vendor alias is much more than just creating a new account and start vending there. It would actually be counter-productive if you would do that since you would only loose your reputation and customers and law enforcement would still be able to easily connect the two vendor accounts.

You have to change many aspects in your vendor operation and your behaviour in order to avoid law enforcement being able to draw the connection and therefore destroying all the effort you put into appearing as a new vendor. These aspects you have to change include for example:

- Your writing style. If you wrote like a 5th grader with your old account, you have to make the switch and for example behave and write like a professional businessman.
- The key size if your PGP key. If for example you used 2048 bit before, create a new 4096 bit one.
- The sort of your vendor name. That means if your old vendor name was "goodVendor", you should not call yourself "greatVendor" but rather something completely different, like "JohnSmith Inc".
- Your online times. If you logged into your vendor accounts every evening, it is now time to change these times.

- Your mail drops. Instead of going in the same area to drop off your packages, move in a completely different direction and drop them off there.
- The vendor persona. That means if you played a tight-lipped one-man vendor before, try acting like a vendor collective which for example mentions on their profile page how their operation is run by several people and has dedicated shippers.
- How you package the orders. That not only means using different package material but also changing your stealth and package layout.
- The time when you stop using your old account and start using your new one. That means, do not immediately start using the new account after you gave up the old one. Make a several month long break for example or operate both at the same time for a month or so (only recommended if you already have some experience and can strictly separate the two vendor identities).

There are many more aspects that you have to consider. The above are just to give you a general idea of what you have to remember. Keep in mind: if you only forget changing one, or fuck up changing one of those aspects, all your effort can be worthless. You definitely do not want that, so be systematic when changing your vendor identity.

It will not be easy to switch vendor identities, but it will be worth it.

Do not accept orders where the customer did not encrypt sensitive data (like his address) with PGP. This will not only improve the DNM scene as a whole by promoting better OpSec but also protect the buyer and yourself. For example if the market gets seized LE will have his address and if you accept orders from such users they usually make other OpSec mistakes too and would be more than willing to tell LE everything when they get caught (buyers who confessed everything and even told LE from which vendor they ordered are not rare).

Keep as little bitcoins on the market as possible. This is important for buyers but even more for vendors who deal with much larger sums. The past showed that vendors (other users of course too) often get scammed and lose their money, do not be one of them. Or at least make sure you lose as little money as possible by withdrawing your earned bitcoins immediately after the purchase was finalized.

Do **not** include any additional and unnecessary information in the packages that you sent. That means for example do not print your vendor name on the product you packaged, even if it is inside. It is useless (the buyer already knows that he made an order with you) and is a great help for law enforcement when they seize the package.

Manage your online times. That means do not log in right after you get home and do not go into vacation mode at the exact same dates as when you actually go into vacation in real life. It would not only be extremely incriminating when law enforcement is already observing you, but also when they compare the vacation data and login data (which are all public and get collected by law enforcement) with the suspects lives' they have. So add some delays and padding, for example only log in during specific parts of the day although you could access the markets more often. Go into vacation for some days although you just continue your life as usual and if you actually go into vacation in real life, do not match these dates with your break on the DNMs.

Create an identity. Create a character for yourself, build it and maintain it. It also helps writing the characteristics of the identity down in a text file (of course stored on your persistence volume in Tails) so you do not accidentally leak your real persona.

A good relation with your customers is crucial, but don't turn into a vendor who can be scammed easily. Be fair and honest, but don't go around giving free reships or refunds after every complaint. You **WILL** get a ton of customers who are out there to score free drugs from you. Don't be afraid to take a negative feedback once in a while.

Source as **many** items offline as possible. That means do not order all your vending equipment from amazon, this already got a t least one vendor in jail as you should know from the General Tips chapter. Instead purchase as much of your needed equipment offline in stores and pay with cash. You really do not want your past mistakes and sloppiness to haunt you later in your vending career.

Keep your operation as small as possible. That means only add new workers if **absolutely** necessary. Every person that knows something about your operation is a risk. You can never erase or take back what you told someone (let's not talk about murder), so a confidant is a permanent risk to your freedom. Needless to say that nobody that is involved in your operation should know anything about it. The ones that are should be kept in the dark as much as possible.

Use the need-to-know principle: if they do not need to know something for doing their tasks, do not tell them it. Need a reason? "*Sadly, the fed's #1 informant was XanaxKing's friend of 15 years.*" (source). And this is by far not the only case where vendors got betrayed by confidants: "*The primary suspect's girlfriend, reported in many articles the suspect's "cohabitor," texted her boss information about the operation. She said her boyfriend "operated a vast drug trafficking ring."*" (source). Because of such retards, it is necessary to be **extremely** careful when adding new workers. It is best to do it all yourself, in the end you get more profit that way too.

Do not taunt law enforcement. They are just doing their job and you do yours. There is no reason for you to insult them or make fun of them by making reddit posts that provoke them by telling nobody will every catch you. This is childish behaviour. Be mature and keep it professional.

Not sure what to sell?

Only three things matter. Firstly, the quality. And after that, the only two factors are how much you pay for it and how much you charge for it.

The most profitable substance is the substance that you can get for the best quality for the best price, as long as you can pass those savings on to your customers. If you plan on being a vendor, the dark net enables sellers of even some pretty obscure drugs to find a huge market.

My point is that no matter what drug you sell, if you have the highest quality and the best price your product sells itself and you will make more money than you ever dreamed you would, as long as you have a steady supply. again.... doesn't matter what drug it is.

(source)

Read up the laws that you are breaking. Seriously. By just investing a few hours into this, you can easily reduce your future sentence up to several years! There are common pitfalls which you should be aware of that can easily increase your sentence, even if you do not find it fair of would think of it as a factor that would increase your sentence.

There were countless people before you, that are in the same or similar situation as you are now so it is not unknown legal territory. The tips are there. Read them.

As you will learn in the What not to do chapter, there are great differences how long the law enforcement investigations take. They can take only one month (for the vendor BTH-Overdose) but can also go over 20 months (for the vendor Hedon). So your goal is not to hope that law enforcement will not invest much into your investigation, but to make it the job of the investigating agents as hard as possible. Do not give them as less information as possible and keep your OpSec tight at all times. If you then also try your best to fly under the radar (by not being overly active on forums and not taunting law enforcement), you can greatly increase the length of an investigation. Remember: your goal is **not** to vend as long as possible, but to quit while you are ahead.

Find a good place, or several ones, where to store the majority of your product. It is **absolutely deadly** to store it all in your house or other properties associated with your name, because this is the first place law enforcement will look. And trust me, if there is something hidden, they will find it. Here [some discussion](#) about stashes, make sure you read it.

You will have leftovers from your packaging or other stuff that is vending related. **Do not put that in the garbage.** It already costed several vendor their freedom. Just one example:

In August 2016, DEA agents recovered pieces of evidence from Heady Warez's trash, including "26 pieces of paper with various handwritten acronyms, colors and numbers, such as '10 yellow Benz,' '85 Xan,' '10 OC 40 orange,' '6 D&G,'" which closely resembled online drug listings posted by "USTOUS" for benzodiazepine and alprazolam, both psychoactive drugs, and oxycodone, Infante wrote.

[\(source\)](#)

It is **crucial** that you destroy all that potential evidence. It is best to burn it, throwing it away in other trashcans that are not linked to you may work too but then the trash should not be usable for law enforcement (i.e. shred paper for example).

Make sure your product is tested. A popular vendor a few years ago sent out pounds of sugar without realizing. Some people send out analogues without realizing. Some people press/lay their own product and send out bunks without realizing. For the sake of customers and reship/refund costs, **test your product.**

Use 2-Factor Authentication. There are no excuses fro not doing so.

Do not scam. You already have law enforcement hunting you so that last thing you need is angry customers who know details about your packaging, stealth, . . .

Some vendors have made a practice of overwriting comments on a periodic or as-needed basis (for example on reddit). This seems to be driven by an intent to complicate retrospective information gathering, but is largely ineffectual. There are trivially simple-to-use tools that can circumvent this practice, and it should not be part of any vendors' or buyers' OpSec strategy.

You should always assume that as soon as you submit a comment or post, it will be stored forever. The same goes for any other information that you transmit to websites.

For a tangible example, try this link:

[http://apiv2.pushshift.io/reddit/comment/fetch/?author=\[RedditUsernameWithoutBrackets\]&limit=500&sort=dsc](http://apiv2.pushshift.io/reddit/comment/fetch/?author=[RedditUsernameWithoutBrackets]&limit=500&sort=dsc)

Delete one of your recent comments, and see if the full text is still available.

Nothing said reddit or on any other forum can be scrubbed. If a past statement compromises OpSec, the appropriate response is to burn the account and start fresh, not attempt a half-assed redaction. As a vendor, you do not always have the luxury of being able to mitigate past mistakes by starting over with a new account, so **think before you write**.

What not to do

There are many DNM vendors who got busted and there will be many more. To avoid being one of them, you will have to read about them, analyze what they did wrong and then take counter measures to avoid doing the same mistakes. A bad vendor does not learn from his mistakes, a normal vendor learns from his mistakes but a good vendor learns from the mistakes of other vendors.

In the following there are three summaries of several vendor busts, make sure you read them completely as well as the discussion in the comments.

Summary #1

Summary of 6 vendor busts: what they did wrong

submitted 8 months ago by [wombat2combat](#)

There are many reports and articles on dnm vendors getting busted, but it is not always easy to find valueable information about the bust and what led to it. In order to provide a safer dnm experience for everyone I will post a summary of 6 busts which contain things that the vendors did wrong and gave law enforcement and advantage and things that they did right which disrupted the investigations.

To vendors reading this: please take 5 minutes of your time to read the summaries and make sure that you are not doing the same mistakes that your competition did. Also I know some of you have already collected information about vendor busts and I am asking you to share it with the community here to make the dnms a bit safer.

Bust #1: Alexandrus

sources:

<http://fokus.dn.se/alexandrus/> [english: <https://translate.google.com/translate?hl=en&sl=sv&tl=en&u=http%3A%2F%2Ffokus.dn.se%2Falexandrus%2F>]

<http://norrnan.se/nyheter/blaljus-nyheter/harifran-skotte-han-storsta-narkotikaligan-408757> [english: <https://translate.google.com/translate?sl=auto&tl=en&js=y&prev=t&hl=en&ie=UTF-8&u=http%3A%2F%2Fnorrnan.se%2Fnyheter%2Fblaljus-nyheter%2Fharifran-skotte-han-storsta-narkotikaligan-408757&edit-text=>]

notes:

- continued to vend under the same alias after SR got seized, his data was handed to Swedish LE by the FBI
- selling unique products in his country [no other vendors who sold cannabis edibles in Sweden]
- no job, might be suspicious although he had no criminal record
- didn't pulled the Tails USB stick out when the raid took place → be always in the same room when you have booted Tails
- use many different mailboxes [he used 60]
- keep the packaging area clean [no DNA]
- use a printer for the destination and return addresses, use real return addresses but they shouldn't report the letter to LE if it is mailed back to the return address [i.e. drug house instead of a company address]
- LE monitored only the most strategic mailboxes, not all 60
- when he delivered the letters to a monitored mailbox, LE got his name because he drove there with his car
- LE opened the mailbox right after he left and took out the letters he sent, but let the letters go through [329 letters in total] → no warning signs for the vendor that he was being monitored
- LE made test purchases from the vendor and found that he sent drugs to the test purchase address after they opened the mailbox again → maybe only accept buyers with a history after some time

- Vendor was watched by LE out of cars parked near the mailboxes
- Vendor had the latest issue of the Narcotics Officers Association's magazine → stay informed about LEs tricks

Bust #2: Area51 a.k.a Darkapollo

sources:

discussion

link:https://www.reddit.com/r/DarkNetMarkets/comments/4y34cp/step_by_step_dissection_of_a_darknet_vendor_bust/

timeline: <https://www.deepdotweb.com/2016/08/26/timeline-arrests-alphabay-vendors-area51-darkapollo/>

notes:

- both vendors had their PGP keys registered to same email address
- they used this email address on social media accounts linked to their real name
- LEOs made two orders and a drug and fingerprint analysis showed the fingerprints of one suspect on both packages (on the Mylar and USPS envelope)
- LEOs did a comparative analysis with the already gained information to identify who purchased the postage:
 - a) they were able to identify the time, date, and location the postage was purchased via the Postage Validation Imprinter (PVI) label
 - b) postage for parcel #1 was purchased via an SSK (Self Service Kiosk) located near the residences of both suspects
 - c) PVI labels were bought with the same credit card -> LEOs were able to identify additional postage being purchased utilizing the same card number
 - d) photos are taken during each SSK transaction -> LEOs identified one of the suspects
- vendor(s) used the same return address for both undercover purchases and one intercepted parcel, probably for many other ones too

- the intercepted parcel was probably detected because LEOs searched the mailcover database for the return address used for the two undercover purchases -> switch return addresses regularly
- vendors were already part of an investigation because they also sold their products near their residences in real life

Bust #3: CaliConnect

sources:

<http://arstechnica.com/tech-policy/2016/08/if-youre-an-alleged-drug-dealer-dont-use-asshole209-as-a-password/>

notes:

- used the same account on several markets over a long period of time → strong case for LE
- weak PGP password (“asshole209” with 209 being his area code)
- LE installed a GPS tracking device on his car with a search warrant
- trademarked his own vendor name using his real name
- used post offices near his home to ship his packages
- he accepted non-bitcoin payments in the past which had his identity tied to them
- kept incriminating things at his home: numerous items associated with the distribution of narcotics, including anti-static bags, a digital scale, food saver vacuum sealing bags; Amazon boxes with plastic storage bags; a trash bag containing marijuana, a box containing a sealed bag of marijuana, also pieces of clothing apparel with the label 'caliconnect'
- allowed law enforcement to search his nearby storage units → do not consent to searches or seizures
- told agents who questioned him that he traded bitcoins
- he and his SO had no job for 6 years but could still pay all the bills
- found unencrypted things associated to the CaliConnect profile: the black and gold 'Caliconnect' logo in use on AlphaBay, an installation of

Tor, and a decrypted message that matched, identically, the controlled Buffalo, New York, transaction

Bust #4: Owlcity

sources:

https://www.reddit.com/r/DarkNetMarkets/comments/4vw1f7/alpha_bay_seller_owlcity_arrested_due_to_checking/

notes:

- used no protection for looking up tracking numbers -> use a VPN [not Tor because it is too suspicious] or a third party tracking website
- LE began in-person surveillance of Leslie [owner of the wifi from which the tracking number was checked] -> watched him drive to the post office with additional orders and intercepted the packages
- ISP monitoring of Tor activity, correlation of Owlcity inactivity with computer repair

Bust #5: Pfandleiher

sources:

<https://web.archive.org/web/20160317052841/http://www.zeit.de/2014/12/drogenhandel-silk-road-pfandleiher> and <https://web.archive.org/web/20160317052819/http://www.zeit.de/2014/12/drogenhandel-silk-road-pfandleiher/seite-2> [no direct translation link available, please copy the text from the article and manually enter it into a translator]

notes:

- was jobless and drug addicted but also lived a lavish lifestyle
- investigation started after one wrong delivered package and a tip
- LE monitored the suspect over months

Bust #6: Shiny Flakes

sources:

[https://web.archive.org/web/20160310112332/http://motherboard.vic
e.com/read/the-rise-and-fall-of-shiny-flakes-germanys-online-drug-
market](https://web.archive.org/web/20160310112332/http://motherboard.vic
e.com/read/the-rise-and-fall-of-shiny-flakes-germanys-online-drug-
market)

[http://www.nbcnews.com/news/world/germany-drug-bust-finds-4m-
haul-destined-online-sale-cops-n322146](http://www.nbcnews.com/news/world/germany-drug-bust-finds-4m-
haul-destined-online-sale-cops-n322146)

<https://www.guern.net/Black-market%20arrests>

notes:

- investigation was sparked by an undelivered package which was opened for insufficient postage bouncing to the fake return addresses
- lead to profiling of his packages, tracing them back through the postal system, surveillance of package stations and him mailing them, and finally undercover buys & seizures of additional packages
- had not purged his customers' data, and in conjunction with the profiling and intercepting of sent packages, this led to a reported total of "38 locations were searched and five other individuals were arrested" on 2015-03-10
- had a clearnet site
- operated from his home

stay safe.

Summary #2

Summary of 4 more vendor busts: what they did wrong

* by [wombat2combat](#)

Since my previous post

[\[https://www.reddit.com/r/DarkNetMarkets/comments/5ephb0/summary_of_6_vendor_busts_what_they_did_wrong/\]](https://www.reddit.com/r/DarkNetMarkets/comments/5ephb0/summary_of_6_vendor_busts_what_they_did_wrong/) was well received by the community here I decided to do a second part. Unfortunately this post is not as elaborate as the first one because I already summarized the most interesting and most documented ones in the first part.

Nevertheless it is worth reading if you are a vendor or just a curious buyer.

Before I start with the summaries I want to mention three points that came up during my research:

- **Never** use business addresses as return addresses. After reading through many cases I noticed that law enforcement only got involved into them because businesses received mail containing drugs [that they obviously did not send] and alerted them. Vendors that got investigated and eventually busted because of that are: Italian Mafia Brussels, Dr. Xanax, Evilution [just to name a few]. Although the business return address might make the packages less suspicious and more likely to get through customs it will backfire much harder when it gets returned to the alleged sender. Since the business is legit and does not want to get into trouble, the employees will **always** report the returned packages.
- **Never** trust anyone. The sentence gets thrown around a lot but it is worth repeating because if you are committing a crime with someone else, this person will always be a security risk and if law enforcement puts him under enough pressure he will sooner or later snitch on you. A dnm related example: XanaxKing's friend of 15 years became the most valuable informant in his case. Therefore your goal should be to involve as little people as possible in your operation and do not give them more information than you have to [the less they know the less they can tell law enforcement].
- Quantik posted some information about the Dr. Xanax case some time ago and included a link to an audio recording where law enforcement explained in court how they busted Dr. Xanax. Although I have the link [<https://infotomb.com/i2iba>], infotomb is offline since quite some time now. Therefore I want to ask the community here if anyone downloaded it or summarized the content of it.

Now as promised the summaries:

In order to provide a safer dnm experience for everyone I will post a summary of 4 busts which contain things that the vendors did wrong and gave law enforcement an advantage and things that they did right which disrupted the investigations.

Bust #1: Dr. Xanax

sources:

<https://www.deepdotweb.com/2015/10/23/quantikxanax-releases-intel-from-drxanax-bust/>

<https://www.deepdotweb.com/2015/10/13/dnm-vendor-dr-xanax-busted/>

notes:

- used a supplement shop which contacted local law enforcement because of the returned packages they received
- with the tracking of the packages that got returned law enforcement got a video of the guy who posted it
- postal workers were asked to look out for this guy -> when someone recognized him he asked another postal employee to check the car ID
- law enforcement then seized all the packages over the next 9 days, followed him, bugged his car, and found the remaining infrastructure
- he only used 17 different post offices to drop off the packages [thanks to [/u/CoXan](#) for the tip]

Bust #2: ErKran

discussion link:

https://www.reddit.com/r/DarkNetMarkets/comments/4t47d2/swedens_biggest_vendor_busted/

sources:

<https://www.deepdotweb.com/2016/07/21/swedens-largest-darknet-vendor-busted-authorities/>

<https://translate.google.com/translate?sl=auto&tl=en&js=y&prev=t&hl=en&ie=UTF->

[8&u=http%3A%2F%2Fwww.sydsvenskan.se%2F2016-07-15%2Ffatal-for-storskalig-narkotikahandel&edit-text=&act=url](http%3A%2F%2Fwww.sydsvenskan.se%2F2016-07-15%2Ffatal-for-storskalig-narkotikahandel&edit-text=&act=url)

notes:

- sourced his products in bulk and internationally -> customs seized one of the packages and investigation started because of the large amount
- investigation revealed many other packages addressed to non-existent companies in his town, he picked them up there
- most used addresses were put under surveillance -> quick arrest

- he carried a handgun, cash and some drugs while picking up the package
- he probably talked and revealed another member of his group who gave away the warehouse that served as the vendor headquarter
- computers revealed that the group was vending on dnms and how many transactions they made; would not be the case if they used tails
- one of the guys had a stash [apparently a small pump house] in the forest which was found by school kids -> teacher informed police but they could not find a suspect at the time -> police now has a suspect in that case because of the ErKran bust

Bust #3: Evilution

sources:

<https://www.deepdotweb.com/2016/11/04/belgian-amphetamine-vendor-arrested-due-to-insufficient-postage-on-his-packages/>

<https://web.archive.org/web/20161027134259/http://kw.knack.be/west-vlaanderen/nieuws/criminaliteit/twintiger-uit-torhout-dealde-wereldwijd-synthetische-drugs-via-de-onderwereld-van-het-internet/article-normal-239819.html> [google translator not working for the URL, copy the text manually and paste it into the google translator]

notes:

- at least six packages got returned to sender because of insufficient postage
- he always used the same return address [a local computer shop], owner of the shop naturally contacted the police -> investigation started
- police analyzed the returned packages -> discovered fingerprints -> vendor was already arrested previously -> law enforcement got a name to the prints
- vendor had 4000 bitcoins at the time of the bust, he received most of them through legal programming jobs but now it is difficult to determine which bitcoins originated from drug dealing -> do not mix legal bitcoins with illegal obtained ones

Bust #4: HollandOnline

discussion link:

https://www.reddit.com/r/AgMarketplace/comments/2ywpkv/vendor_busted/

archived version with some of the deleted comments:https://web.archive.org/web/20150314112159/http://www.reddit.com/r/AgMarketplace/comments/2ywpkv/vendor_busted

sources:

<https://www.deepdotweb.com/2015/03/12/dutch-vendor-bust-hollandonline/>

<https://web.archive.org/web/20160325231658/https://www.om.nl/actueel/nieuwsberichten/@88570/aanhoudingen/> [google translator not working for the URL, copy the text manually and paste it into the google translator]

notes:

- random police officer witnessed a suspicious transaction where someone moved transported goods from the trunk of one car to another -> got arrested
- the arrested man was already on law enforcement's radar because he was suspected to operate, amongst others, the vendor account HollandOnline
- sold on Silk Road 1, 2 and Agora under the same alias -> vendor already was heavily on law enforcement's radar
- bitcoins seized -> bad opsec setup
- another group member was only 20 years old at the time of the bust -> missing life experience and online fame led to operating under the same alias and ultimately his arrest

That is it for now, if you know other busts that could provide useful information or additions to the summarized ones please leave a comment here.

One last shameless self-promotion: I developed an Addon for Firefox [also compatible with the Tor browser] which lets you view selfposts of NSFW subs [like this one] without having to enable JavaScript. The source code is of course publicly available, so check it out if you want to boost your

opsec:https://www.reddit.com/r/DarkNetMarkets/comments/5ek0lm/a_present_for_the_lurkers_on_here/

Summary #3

2 more juicy vendor busts and what they did wrong

submitted 19 hours ago * by [wombat2combat](#)

Over the holidays I found time to go through more than 100 pages of criminal complaints, indictments and other resources that described how the vendors Blime-Sub (a.k.a. BTH-Overdose) and CaliGirl got busted. Now what is different compared to the first two parts [[#1](#) and [#2](#)] is that these two cases are described in great detail and walk the reader through the entire investigation step-by-step.

Since they are quite lengthy I outlined the important parts of the investigation and wrote down the mistakes that the vendors did which eventually led to their bust. While the Blime-Sub bust is quite fresh [just 2 months ago], the CaliGirl case dates back to the good old SR days. However it is one of the best documented ones and many of the investigation techniques are still used today. In this edition we have some classic pitfalls like getting identified while buying the postage or leaving a detailed money trail but also some new ones, that have not been mentioned in the previous two parts.

I strongly encourage every vendor to read through these notes and analyse their own operation so they do not make the same mistakes that their colleagues/competition did. In the end it is not only your own future that is at risk but also the one of your customers. Please read the **whole** post because it not only includes stupid vendor mistakes that you probably would never make, but also some tricky pitfalls which you would miss out if you just skim the post.

Before I come to the busts themselves I want to briefly talk about some aspects that are so important that I think they deserve a specific mention:

- If there is one thing the government does not fuck around with, it is money. For example the CaliGirl complaint contained over a dozen sites that went over every single cent the vendor ever received or

deposited into his bank accounts. Every single company, from Wells Fargo to Western Union and MoneyGram, had extremely detailed records about where every cent came from and where it went, as well as IP addresses, log-in times, locations of used ATMs, . . . This shows that vendors should avoid banks and wire transfer services whenever possible, because they all keep records and once they hand these over to law enforcement you are absolutely fucked.

- Know your limit. Many vendors just keep vending under the same name for years as if law enforcement is not interested in them. However what all these busts have in common is that law enforcement simply had enough time to investigate the vendors. So vendors remember to take a break once in a while and enjoy the reward of your hard work instead of ruining everything you have worked for in the past years by vending until you get busted. Better quit with some nice extra cash and your freedom than ending up in one of these summaries below.
- Law enforcement not only analyzes the content of seized packages but also the package itself. That means they look for any traces you may have left, for example fingerprints. This has proven to be useful and already led to arrests, just take a look at the Area51/Darkapollo or Blime-Sub/BTH-Overdose busts. So vendors should avoid leaving any fingerprints or DNA traces on and in the package because it not only allows to check if a suspect is the wanted vendor but can also reveal for example the eye and hair color of the person that left the DNA [<http://www.medicaldaily.com/DNA-test-can-reveal-hair-eye-color-humans-living-800-years-ago-244266>]. That would give law enforcement a big advantage when they stake out mail boxes. Here a really simple guide on how to remove these traces: <http://biononymous.me/wp-content/uploads/2016/09/Tabloid-BiononymousGuide.jpg>

Bust #1: CaliGirl [Matthew Jones]

sources:

https://www.justice.gov/sites/default/files/usao-mdfl/legacy/2014/05/30/20140530_Jones_Complaint.pdf

https://www.reddit.com/r/DarkNetMarkets/comments/2c2i3f/caligirl_criminal_complaint_excerpts/

notes:

- one involved Task Force Agent [TF agent in the following] even has "additional advanced training and experience in Computer Networking and Unix Systems Administration" -> that was 3 years ago, imagine how many resources they put into dnm vendor investigations nowadays
- vendor used an alias similar to his real name [Matthew Jones]: Mateo Jones
- CaliGirl was among the top 5% of all vendors operating on SR -> high profile
- law enforcement made 2 undercover purchases on SR and 6 off-site [all between July 2013 and March 2014]
- law enforcement was able to identify what products he sold how often and his total sales volume because SR provided a detailed public record of it -> do not use markets that do not obfuscate this information
- although CaliGirl used many different return addresses some of them were handwritten and some were business addresses [not a smart idea, see part 2], plus the tracking number revealed where the packages were shipped from
- for his fifth purchase the TF agent placed the order on January 3, 2014 but requested that it should not be shipped until January 23 [this could be a potential red flag for other vendors] -> the TF agent then had time to go to the mail processing plant that handled most of the previous undercover packages and attempted to profile additional packages that matched packages sent by CaliGirl
- they found and seized 4 matching packages which originated from one mail collection box half a mile from Jones's residence away, all 4 packages had the same return address and one of it was the undercover order
- on January 13, 2014, the TF agent opened a suspicious package [taped excessively] that was sent to one of Jones's drops [where he received the products that he resold under the CaliGirl account], it contained almost 700 Hydrocodone tablets and was addressed to "Tyler Zedai"
- CaliGirl offered the TF agent a special deal for Hydrocodone tablets and also sent him information about them [a link to a pill identification website] -> the branding and picture supplied by CaliGirl matched the seized tablets on January 13 -> the TF agent made the purchase

- for his next undercover order [undercover purchase #8] the TF agent claimed to be short on bitcoins and CaliGirl provided him with a contact [name, telephone number and local bitcoins username] that could sell him bitcoins for cash -> that contact [Jones] was CaliGirl himself
- apparently the TF agent told Jones [when they talked about purchasing bitcoins] that he wanted to provide him with \$1k to convert into bitcoins and then transfer the coins to CaliGirl [Jones should transfer the coins to CaliGirl not the TF agent] -> indication that Jones at least knew CaliGirl [because Jones knew CaliGirl well enough to send him the coins]
- after the bitcoin purchase from Jones [\$952, because Jones took a commission] the TF agent contacted CaliGirl about the order -> CaliGirl said that it had already been shipped and the \$1k were credited towards the purchase -> further indication that Jones and CaliGirl are somehow connected
- the phone number that CaliGirl gave to the TF agent to contact Jones in order to buy bitcoins was purchased on Jones name one minute before CaliGirl mentioned it in his message -> further indication that CaliGirl was probably Jones
- the features of the packages that CaliGirl sent which remained consistent included: the manner in which the sender and recipient addresses were printed and affixed, the placement and method of postage, and the type of envelope utilized -> made package profiling easier
- the postage used for the purchase mentioned above was an Automated Postal Center [APC] computer generated postage stamp -> the TF agent was able to get the purchase date and location of the machine that was used to buy the postage
- since the machine stored images of the persons that used it, he was also able to get an image of the person who bought the postage in question -> compared this image to known images of Jones [including publically available images on facebook] -> matched
- postage was paid for by the utilization of \$5.00+ face-value stamps and the tracking numbers were affixed prior to mailing for every package -> he did not have to pass the packages over a post office counter where he could get identified by postal staff or video surveillance systems ->

however he fucked up with the package sent on March 18, 2014 which had APC printed postage

- he used the same return address for every package but switched it once every week -> this and other mistakes allowed detailed package profiling which made it possible for law enforcement to identify a total of 135 packages sent by Jones -> **package profiling is a great threat so take counter measures**
- some return addresses that CaliGirl used were connected to his real identity [Matthew Jones]: e.g. a Hotel address where he stayed or a company which he owned -> do not do that
- Jones' P.O. box [where he received his products which he resold] was opened under his name and "Tyler Zeddai" -> all incoming mail was addressed to Tyler Zeddai but always picked up by Jones or his spouse -> manager found that suspicious [he did not contact law enforcement but when the TF agent interviewed him he was *very* talkative -> maybe avoid P.O. boxes from "EZ Mail Services"]
- **vendors: if you have to use P.O. boxes switch them once in a while [and use different companies] so it is more difficult for law enforcement to uncover the whole scope of your operation. also do not use these addresses for other purposes like opening bank accounts, which Jones did.**
- the TF agent also reviewed records obtained from Amazon about Jones' purchases which included purchase, shipping, billing, and IP address information -> he bought zip lock baggies and bubble mailer manila envelopes which were also used for shipping the undercover purchases -> **do not order your shipping equipment online or at least not with your identity**
- he also travelled to Colombia frequently -> the TF agent compared these dates with the times when CaliGirl was on vacation -> matched -> **vendors should go to fake vacations [vacation mode on the market but continuing their everyday life] and extended vacations [do not go into/come back from vacation on the exact days when you actually go away/come back]**
- *Note:* Jones bought Oxycodone and Hydrocodone in Colombia and shipped them to the P.O. box mentioned above: it is easier and cheaper to get these products in Colombia and they are marked like many other

tablets -> careful inspection or laboratory analysis needed to identify them -> preferred by drug traffickers

- Xoom [an online wire transfer service where he had an account with his real data] revealed that he transferred over \$58k from January 2012 to August 2013 to Colombia
- some of these transfers were sent to "Mateo Jones" which is an alias utilized by Matthew Jones on facebook -> **please learn to separate identities properly**
- transactions have been structured in a manner to intentionally avoid triggering money laundering and reporting requirements [e.g. multiple transaction on the same day to the same person] -> say hello to another charge
- he should have taken the money in cash with him on the plane or mail it to Colombia instead of producing all the detailed evidence by using Xoom
- "The Wells Fargo counter and ATM deposits [to one of Jones' accounts] were in inconsistent amounts, occurred on a variety of dates, and were made at a variety of geographical areas. Based on my training and experience, this activity is consistent with Bitcoin sales where a Bitcoin customer makes a pre-arranged counter-deposit into a Bitcoin dealer's bank account. The deposit slips contain only the minimum amount of information required to make a cash deposit. Based on my training, experience, and this investigation, this is common behavior utilized by Bitcoin exchangers and drug traffickers a when utilizing counter deposits to transmit currency." **this was written 3 years ago, vendors should finally start using methods that do not create extensive and suspicious paper trails to cash out their bitcoins**
- he used small variations in telephone numbers, addresses and other identifying information for receiving funds in his Western Union account -> this is a common method drug traffickers and money launderers utilize to avoid detection by law enforcement -> do not do this
- Jones used only one account on the exchanges [local bitcoins and and bitcoin-otc] to cash out his bitcoins for his entire vending time and also publicly linked the accounts on both sites

- 'fun' fact: a screen shot [exhibit 1] shows that law enforcement does not even disable javascript globally and seems to be using windows -> they really need to step up their opsec :)

Bust #2: Blime-Sub a.k.a. BTH-Overdose

sources:

<https://www.justice.gov/usao-edca/pr/fentanyl-and-heroin-sold-dark-web-marketplace>

<https://www.justice.gov/usao-edca/press-release/file/918811/download>

discussion link:

<https://www.reddit.com/r/DarkNetMarkets/comments/5imn2j/blime-sub-arrested-according-to-press-release/>

I also wrote an article on deepdotweb about this bust using these notes, so if you read it you can skip the following

notes. [/u/deepdotdeepdotweb.com](https://u/deepdotdeepdotweb.com) can you please post a short 'confirmed' comment so that people know that I am not bullshitting?

notes:

- after getting training on how to use dnms a DEA agent began analyzing and investigating top heroin vendors on alphabay in january 2016
- he initiated a full investigation into the vendors Blime-Sub and BTH-Overdose in september 2016
- he knew they were shipping from the west coast (possibly somewhere in california) because customers mentioned it in forums
- BTH-Overdose (Emil Babadjov) used the same email address for his pgp key as he used for his facebook account with his real name (but written backwards)
- Babadjov made a public facebook post in september 2015 that people could contact him through the email address he also used for his pgp keys
- on November 14th, 2016, the agent sent a subpoena to coinbase to get any information they have about the email address
- he received replies from Coinbase on the very same day and one day after:

- the email address was used to create an account in November 2015 for "Emil Babadjov"
- on March 18, 2016, he attempted to create another account with the name "Emil Babadjov" and the email address "blimesub@***.com" -> do not mix vendor identities with exchange accounts and do not use vendor email addresses for any other purpose than talking to customers
- on November 14th, 2016, the agent got Babadjov's address (through his drivers license) and found out that he was arrested in 2013 for possession of controlled substances (but the charge was dismissed)
- on October 19, 2016, the agent bought \$800 worth of bitcoins to buy 3g heroin on the next day from Blime-Sub on alphabay
- the parcel (UC parcel #1) arrived on October 25 at the undercover address and he got the return address and tracking number of it
- the product in the package was submitted to the DEA western regional lab for fingerprint and drug analysis after it got tested positive for heroin
- the agent got a response from the lab on November 10, 2016, which stated that it was a mix of heroin and fentanyl
- the US postal inspector was able to conduct comparative analysis of these parcels to identify who purchased the postage for UC parcel #1
- due to the Postage Validation Imprinter (PVI) the US postal inspector was able to see that the postage was bought on september 18 2016 at 4:03 PM via a Self-Service Kiosk (SSK) 0.7 miles away from Babadjov's known address
- the US postal inspector gave the photo that was taken by the SSK system during the transaction to the agent
- he identified the person in the photo as Emil Babadjov according to the drivers license and social media photos of Babadjov
- on November 16, 2016, the agent received another response from the DEA western regional lab that stated that two fingerprints belonging to Babadjov were found on the exterior of UC parcel #1

That is it for now, if you know other busts that could provide useful information or additions to the summarized ones please leave a comment here.

One last shameless self-promotion: I developed an Addon for Firefox [also compatible with the Tor browser] which lets you view selfposts of NSFW subs [like this one] without having to enable JavaScript. The source code is of course publicly available, so check it out if you want to boost your opsec:https://www.reddit.com/r/DarkNetMarkets/comments/5ek0lm/a_present_for_the_lurkers_on_here/

Summary #4

Here a (list) of many DNM arrest, pay especially close attention to the busts that involved vendors that sold the same product as you or were located in your country.

But this is by far not enough, you will have to constantly watch out for new vendor busts and check what they did wrong.

Setup

General

This chapter is about the technical side of your vendor operation. Luckily you just have to follow the instructions in the DNM Buyer Bible to set up Tails, learn how to use it. how to chose a market, . . . Make sure you actually read every chapter since you have to know how a buyer will behave and what will set off red flags for him.

This is **crucial** and if you for example do not set up Tails you already fucked up. There is not excuse for a vendor to not use Tails.

Important: when choosing a printer, you have to make sure it works with Tails. If it does not you are compromising your own OpSec and risk getting yourself in jail just because of that one part of your setup. Handling customer's addresses is not something you should take lightly, always make sure that the information does not leave Tails

(obviously other than on a paper printed by the printer). For more information about specific printers check [this thread](#).

Before you start, make sure you also [read this discussion](#) so you know what you can expect when you are starting to vend.

BACK-UP YOUR DATA. You must must must have at least **2** copies of your persistence data. It is extremely [easy to do](#) and only takes a few minutes. You're fucked if your PGP keys, passwords and Bitcoin wallets disappear.

Tip: when setting up your electrum wallet on Tails, you can start the wallet creation process several times till you get a seed that you can remember better (e.g. because the word order makes more sense and is easier to remember).

Please also keep in mind that in some countries, law enforcement can force you to reveal your password and therefore incriminate yourself. You need to do your own research about the situation in your country regarding this topic.

To avoid loosing your bitcoins because of that, you could have a wallet which you rarely use but holds the majority of your funds. The only trace of it is the seed that you remember in your head. That way nobody can prove that you own more than the bitcoins in your usual vendor wallet (the one that you frequently use). That means you could be forced to give out your Tails password but they would only see your frequent wallet in electrum. If you want to access that big wallet just restore it from seed and delete it again when you are done. If you do that, make damn sure you do not forget that seed.

Alternatively you can create that wallet on an offline, non-persistent Tails, then save the seed on a flash drive and dig a hole for it in the desert. To store the seed you can somehow sneak it into your wedding vows, write a song where beats correlate to 1s and 0s that spell out your seed in binary. Whatever it is, come up with some definitive way to remember it.

When uploading your product pictures, follow the chapter [Uploading images securely](#) from the DNM buyer bible.

How safe is it to use an internet connection at home for vending?

There several complaints where law enforcement analyzed the timing of the Tor usage coming from the suspected vendor's home connection along with his times when he was home and the vendor account being active on DNMs. However if that is the case, law enforcement usually already has a pretty strong case against the vendor they monitor that way. Therefore it is usually better to spend your time, energy and resources on other factors that can get you busted more easily (e.g. packaging).

If you want to hide your Tor usage though, you should go with the Whonix setup described in the [DNM Buyer Bible](#) since it is hard to chain a VPN with Tails. With Whonix you just need to follow the setup steps from the DNM buyer bible and then install the VPN software on the host OS. So your future login process would look like this: boot host OS -> start VPN software (recommended to set it to start automatically) -> starting Whonix (according to the instructions in the DNM buyer bible).

Using a public WiFi also introduces additional risks: you would need to travel to that access point every time you want to log in (which allows law enforcement to still monitor your behaviour and correlate it with the login times of the vendor on DNMs) and you for example need to protect yourself against other people that may look at your screen.

It would come in handy in case of an IP address leak though as it would just show that the vendor used a specific public WiFi and not lead right back to your home address. However these are very unlikely when you are using Tails or Whonix with the security slider set to high, plus such attacks usually do not get wasted on (normal) vendors.

If you have the chance to use a WiFi that is not yours without leaving your own house (e.g. an unsecured network belonging to your neighbour), then you should use it. Otherwise stick to your own WiFi and use Whonix with a VPN if you are seriously concerned about hiding your Tor usage.

Packaging

General

This chapter is about how to package the orders you get properly.

Before you start packaging right away or listing your products, you need to work out a packaging process first. To get ideas for stealth and decoys you can order from other vendors who sell the same product or a similar one and are known for their good stealth. That will point you in a general direction and give you some ideas how to properly conceal the package content. Do **not** copy their packaging methods.

While you can also use services like [Bitcoin Postage](#) to buy postage with bitcoins, it is highly discouraged since such companies are known to give out their customers information to law enforcement.

Furthermore make sure you also read [this post](#) (as well as the comments) about packaging and customs.

Here more information about what to avoid when packaging from various sources:

- [USPS](#)
- [FBI](#)
- [A Canadian source](#)
- [SoBran Inc. - a company which provides mail screening service](#)

How to package

Depending on what you are going to sell, you should vacuum seal it at least once and package it in Mylar too, to avoid getting the package seized because of the smell it leaks. If you ship internationally, a decoy is necessary because the package will pass through two customs (in the origin country and the destination country), unlike a domestic package which will go through far fewer checks.

The location for packaging it the first time (like vac sealing weed) and the second one (putting it into a MBB) have to be different because

you do not want to get the outside of the packaging material to get in touch with the product itself. Different rooms for that are also alright. If the outside is contaminated because you did all the packaging in the same room where the product lays around, dogs will far more likely hit on the package. This not only means a dissatisfied customer and a potential loss for you (e.g. if you reship), but also increased attention from law enforcement on your operation.

Note: know how much to frank your packages with. If you make mistakes there, the packages may not get delivered to their destination but opened by post office workers. That is a recipe for getting an investigation started.

When packaging the product, you need to be careful to not leave any fingerprints or DNA traces inside or outside the package. To prevent that wear **at least** long sleeve shirts, two layers of gloves (e.g. first cotton ones and then rubber ones over that because some gloves are too thin and can still leave partial fingerprints), a hairnet or ski mask and other clothing that covers your bare skin to avoid leaving traces during the packaging. Ideal would be a full body suit (example) because it not only looks and feels cool but also is way better than the workaround with the clothing described previously.

When you have a rough idea of how you are going to package your product, it is very helpful to write down the steps that you are going to make. That means write out the whole process in full, e.g. in steps like "roll out paper on the table" and "put gloves on". After you are finished with that read through it and correct things while imagining the whole packaging process.

When that step-by-step guide is ready, make a test run and package something that is legal and similar to the product you are going to sell. While doing that you will notice thing you have forgotten in the guide or things you should do better. Alter the guide after you did the test run accordingly. Then send the test package to your address or one that you control to see if everything works fine.

After it arrived successfully you can repeat the test packaging process again to see if the changed details work and if you can improve the process even more.

Note: you have to treat every package carefully and make sure that you do not make mistakes when packaging it. Law enforcement does not care if you leave a fingerprint or DNA traces on a 1 gram order or a bulk one, they fuck you either way. Here one example for a thread about vending (specifically about leaving traces on the packages), which you constantly look out for when browsing DNM related forums.

You should also wipe the packaging material (e.g. vac sealed bag, MBB, . . . not the outside of the package itself) with alcohol to reduce the smell and remove potential traces. So the first wipe after you vac sealed the product and the second time after you put it into the MBB.

Return addresses

You could use real addresses of individuals living in a rather poor part of a town. So if law enforcement starts to investigate they think it is just one of the drug dealers living there who sends the packages, and if the packages gets returned the individual is less likely to report it to the police. Maybe using a fake address once in a while is not bad either, since the worst case would be that the few packages you sent with a fake return address get opened by postal workers but the content is not enough to start an investigation. It also puts a bit less heat on the real return addresses (the ones from the poor parts of the town) the vendor primarily uses.

But keep in mind that you can also cause a lot of trouble for the people living under your return addresses. So avoid picking ones that for example have a single mother with kids living there.

However return addresses **always** should be within reasonable range of the used mailbox. It is suspicious if the return address is in a complete other town than from where it was sent.

Also these techniques are only a way to delay and disrupt investigations to a certain extent. You will have to switch your accounts sooner or later as described in the General Tips chapter, if you do not want to get busted.

Other concepts:

Use a real return address of a business or a shopping center. But use a fake second line something like office 58 but there is no office 58 at a gym and the post office knows not to return it but will still put it on the truck. Another good one is use a fake apartment number like apartment 7 when there are only 6 apartments. Same things USPS will direct the mail the mail man will see no box. This method is going to get burned soon since USPS is cracking down on those fake/semi real return addresses.

Another concept is using the the return address of a P.O. box and using different names on them as USPS does not cross check the name of the box and where it is coming from. So you could say John Smith P.O. box 2284 and well it will never go return to sender since that does not exist.

Stealth

Every few months a journalist will get the bright idea to make an easy story by buying some drugs from a DNM and talking about how terrible it is that it was so easy. They often give detailed photographs and descriptions of the packaging. Since the journalists usually end the article by saying everything was handed over to the police, these are certainly not stealth methods that are covered by security by obscurity. In the following a few concrete examples.

NOTE: detailed talking about stealth on [/r/DarkNetMarkets](#) and [/r/DarkNetMarketsNoobs](#) is not allowed! Please read the rules for details.

Weak stealth example:

A fucking DVD case

<https://archive.li/o/sVVd4/https://www.bitnik.org/r/2015-01-15-statement/>

<https://archive.li/o/sVVd4/https://www.bitnik.org/r/2015-03-04-xtc-is-xtc/>

<https://archive.li/o/sVVd4/https://www.bitnik.org/r/2015-04-15-random-darknet-shopper-free/>

!MEDIENGRUPPE BITNIK

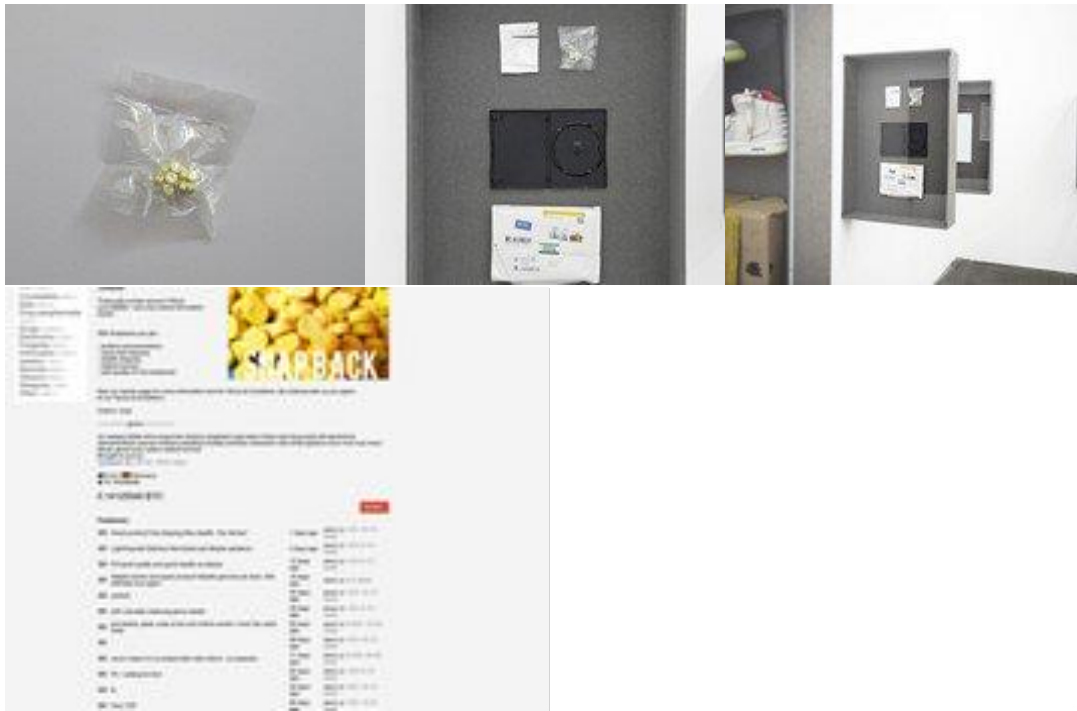
RANDOM DARKNET SHOPPER (2014 - ONGOING)

29.10.14 | No. 6

ECSTASY 10X YELLOW TWITTER 120MG MDMA

**RANDOM DARKNET SHOPPER JUST BOUGHT 10 ECSTASY
PILLS OF FROM GERMANY FOR 48\$**





Ecstasy 10 yellow Twitter Pills 120mg Mdma
Ordered by Random Darknet Shopper (29 Oct 14)
for 0.1412554 Bitcoins
Status: Arrived (4 Nov 14)
Shipped from Germany
Item No. 6

The pills were vacuum-sealed in aluminium foil and placed inside a dvd case, so they would look like a dvd in a x-ray scan. The vendor promised very fast shipping and stealth packaging. Both seem true. The parcel was sent from Germany and crossed the border and customs to Switzerland without any problems.

Original description:

«Beautiful yellow round pills with twitter logo, beveled edges and breaking line on the back...»

Medium stealth example:

Ecstasy pill hidden in candy packet

Is your postman delivering drugs?

By Jim Connolly and Anna Doble Newsbeat reporters

5 Jan 2017

Large amounts of illegal drugs are being delivered unknowingly by UK postal workers with few checks, Radio 1 Newsbeat has found.

For several months we have been investigating drugs in the post bought on the dark web.

We heard that "millions of pounds of drugs are bought online every day" via the hidden layer of the internet where dealers can sell drugs anonymously.

Royal Mail said it does not knowingly carry any illegal items in its network.

Newsbeat spoke to delivery staff who said they had "definitely handled suspect packages" but there was "nothing they could do".

You can also explore this story in a different way. Newsbeat Explains is a new way of experiencing news piece by piece - [click here to try it with this story.](#)



Image caption Packages sent from dark web drug suppliers to our reporter

There are fears that users buying drugs this way are more likely to widen their substance choices, with dangerous consequences. And users we spoke to believe there's a "99% certainty" that drugs ordered via the dark web will get to them.

The Home Office says it is spending £1.9m trying to "increase understanding" in how organised crime networks "adapt and diversify" using technology.



Image caption Yvette Cooper visited Newsbeat to see our findings for herself

Chair of the Home Affairs Select Committee, and Labour MP, Yvette Cooper is looking at how the police can "keep up with new and changing forms of crime".

"We need to know there's a proper approach to enforcement taking place," she tells Newsbeat.

"One of the things we want to know is how the police are able to co-operate with different organisations.

"What is happening to link up [the police] with postal services or with customs or with other organisations? What's the government doing to lead this?"



Image caption Newsbeat reporter Jim Connolly logs onto the dark web with Chris Monteiro, an independent cyber-security expert

How we tested the system

Newsbeat obtained MDMA, cannabis and former legal high, Spice using Bitcoin on the "dark web", a collection of thousands of websites that use anonymity tools to hide their IP address.

This part of the internet also contains a marketplace for drugs like heroin and steroids - as well as weapons and fraudulent documents.

We accessed the dark web via the Tor browser, free software which conceals users' identities and their online activity from surveillance.

Deliveries to a PO Box took around a week to arrive.

When they did, we gave them to a government-approved lab for testing and destruction.



Image caption An ecstasy pill we bought on the dark web arrived wrapped inside a packet of Haribo sweets

"Unless there are massive raids on markets any time soon" causing "a loss of consumer confidence", this "hidden" drug market will keep growing, says Chris Monteiro, an independent cybersecurity expert and researcher.



Image caption The pill was packed inside cling film to make it feel soft

"Talk of better prices and improved purity will continue to spread and eat away at the offline market," he explains.

And he adds: "Government and police are more interested in data breaches and weapons [than drugs]."



Image caption But there is no guarantee of what you are really buying on the dark web

Waiting for a special delivery

Former user "Steve" tells Newsbeat he bought marijuana, cocaine, ecstasy, and psychedelic stimulants on the dark web.

He describes a time he and a friend ordered drugs to take to a festival.

"We were waiting for a package, for an ounce of MDMA to be delivered.

"We see the postie drive down and we get very excited. She gives me the package, I sign for it... happy doo-dah.

She had no idea she was a part of the drugs trade

"Steve"

Former dark web drug user

"Me and my friend found it incredibly funny how she gave us the post - and had no idea.

"She handed it over and said 'thank you very much' and I said thank *you* very much.

"She had no idea she was a part of the drugs trade."

What "Steve" did was illegal and could have resulted in a jail term for possession of drugs with intent to supply.

What post workers told us



We went out with a postman who wanted to remain anonymous.

"Patrick" told us that it's illegal for him to open suspect parcels and there's "nothing he can do about it".

"You tell the managers and all they say is you need to deliver it."

He added: "If it's got a stamp on it, you post it. We don't have drug dogs to smell every parcel. We don't have the resources to X-ray every parcel. We just have to deliver it and take the risk."

I've spent 14 years as a postman in uniform and I have never seen a drug dog

Postal worker

"Our job is to deliver it safely to the customer."

Newsbeat has been told that some random spot-checks do occur but most staff we spoke to had never seen a sniffer dog.

"I've spent 14 years as a postman in uniform and I have never seen a drug dog," one worker at a London depot said.

Another said: "You hear rattling of things like pills and assume they're legitimate, but how would we know?"

"I've definitely handled suspect post, but once we have it in our mail bag we have to deliver it," said another.

On a forum used by postal workers we heard from a number of people who all noted that they had handled packages which had smelled of cannabis.

Many described there being more checks in the past when the depot had a customs office on site. Mail being sent within the UK does not seem to undergo the same scrutiny.



Are people trying new drugs because of the dark web?

Yes, according to data from the **Global Drug Survey [GDS]**.

"About a third of people said they'd broaden their drug-using repertoire," says Dr Adam Winstock, from Kings College and GDS, who also says "millions of pounds of drugs are bought online every day".

"So it's like 'we've noticed you like LSD and magic mushrooms, perhaps you'd be interested in 2CB or DMT'..."

"I think there is absolutely that effect," he tells Newsbeat.

"You're always worried that an increase in repertoire increases the likelihood that someone comes across something that might be harmful."

One in five people who responded to the 2016 Global Drug Survey said they had bought drugs on the dark web - or had friends buy them for them.

Are any countries tackling drugs in the post?

In New Zealand more has been done to stop drugs in the post.

"New Zealand is an anomaly in that only 2% of those who took our survey said they'd bought drugs on the dark net," says Dr Winstock.

"The reason people don't go shopping on the dark net in New Zealand is because there's really good co-operation between the police and the postal services and their borders are unbelievably good."

This more joined up approach has led to New Zealand's customs service seizing three times as many suspect packages over the past two years.

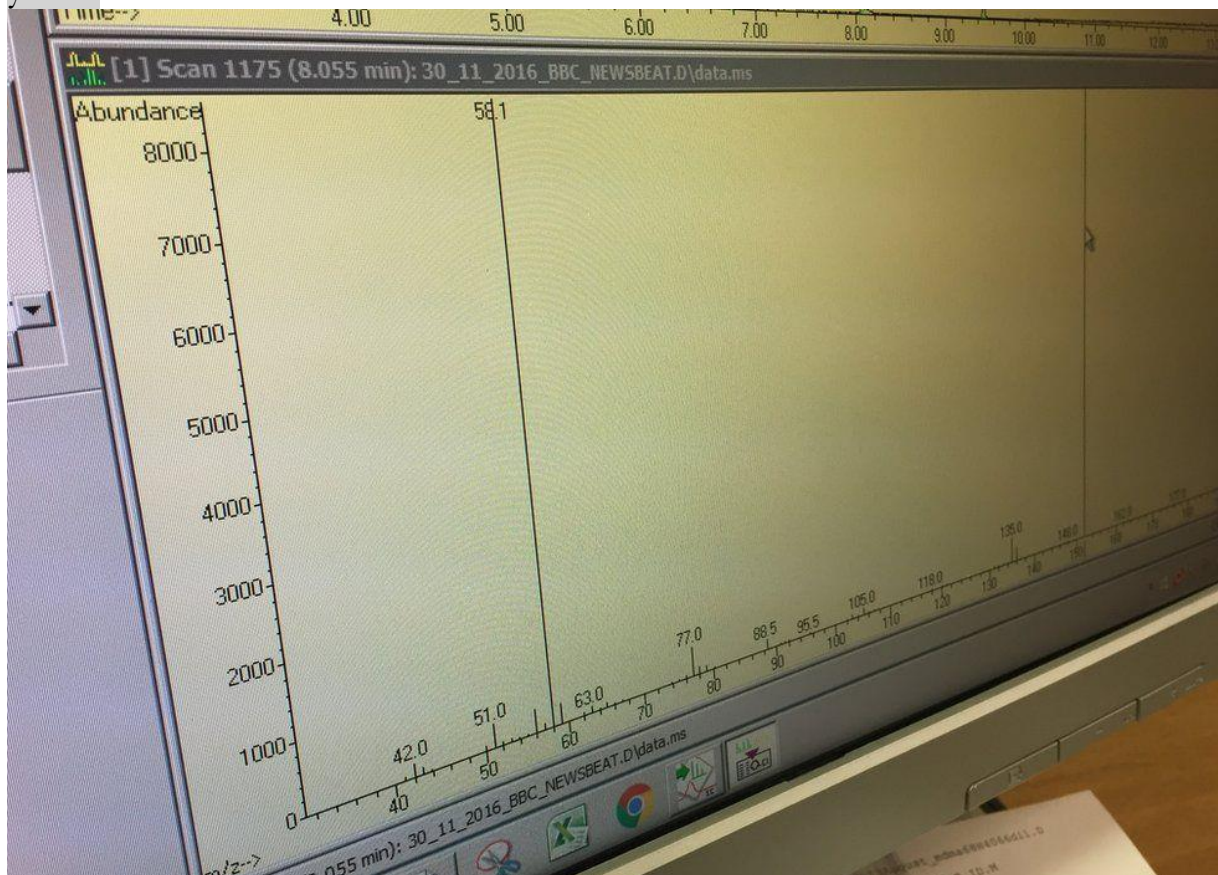


Image caption We bought an ecstasy pill on the dark web for £5 plus £3 postage. Tests found the pill's only active ingredient was MDMA

What British authorities say they are doing

In a statement, the Home Office told Newsbeat: "We have committed to spending £1.9bn on cybersecurity over the next five years, including boosting the capabilities of the National Crime Agency's National Cyber Crime Unit, increasing their ability to investigate the most serious cyber crime."

A Royal Mail spokesman said: "Where Royal Mail has any suspicion that illegal items are being sent through our system, we work closely with the police and other authorities including the Medicines and Healthcare products Regulatory Agency to assist their investigations and to prevent such activities from happening."

Strong stealth examples:

Sealed into a booster pack

"I was so amazed on the stealth. It was a letter that said some bs about thank you for entering our Pokemon contest but sadly you didn't win. Here is a complimentary gift. Inside was a sealed pack of pokemon cards and the k [ketamine] was in a bag taped to the back of one of the cards. I've never since received anything even close to that stealth."

An Online Drug Dealer's Best Friend: the U.S. Postal Service Vendors on the dark net are more than happy to share their step-by-step guide to stealthy drug trafficking, including hiding pills in Pokémon cards

Author: Eric Markowitz

Posted: 10/09/14 07:52 EDT

This page has been shared 18 times. View these Tweets.

You might think dark net drug dealers use some super secret delivery method to get their products point A to point B. Maybe, you thought,

it's some sort of stealth drone that dispatches from some clandestine warehouse and drops off the packages in the dead of night. Not exactly.

They use the post office—and the government isn't happy about it.

“The postal service—the mails are—being used to facilitate drug dealing,” former Attorney General Eric Holder said at a Senate committee hearing earlier this year. “It is shocking to see the amount of drugs that get pumped into communities all around this country through our mail system, and we have to deal with that.”



Former U.S. Attorney General Eric Holder

REUTERS

In some sense, it's a bit embarrassing (for the government) that drug dealers are using one of its own agencies as the go-to service for shipping product. But you really can't fault the USPS—they're just not equipped to scan and investigate each package. They've also been losing money pretty much every year for the last decade due to the lower volume of "snail mail" being sent. So their budget probably doesn't allow them to hire an army of investigators. In July, the USPS announced it would shed some 3,000 employees by the end of 2015.

Now, it seems, the USPS is getting a new line of business—but it's not the business they want.

Just like an eBay vendor shipping a vintage Casio calculator watch, dark net vendors use the USPS to move their product. Unlike with eBay vendors, though, the main topic of discussion is "stealth." (Check out Vocativ's investigation of where dark net drugs come from.)

Staying anonymous while shipping has become the fixation on online forums like Reddit's r/DarkNetMarkets. As dark net marketplaces grow, more people are purchasing drugs online. And more sellers are jumping in to meet that demand. Naturally, there's an appetite for this sort of information.

It makes sense: If a package is ever seized, vendors want to make sure inspectors can never trace the package back to them. This doesn't just mean using a fake return address. It's a more intricate process—and vendors are happy to share their knowledge online.

It starts with the postage. Naturally, a vendor doesn't want to buy specific stamps online with a personal credit card. Notes one vendor on Reddit:

"You can purchase postage online anonymously with a prepaid card. There's several companies you can purchase the postage from, and all you have to supply is a weight, and addressing info."

Then, which shipping service? Pretty much all dark net vendors stick with the USPS first-class shipments. Why? It's simple. Compared with private shipping services like FedEx, the USPS (theoretically) has more protections against warrantless searches.

According to the USPS, “first class letters and parcels are protected against search and seizure under the Fourth Amendment to the Constitution, and, as such, cannot be opened without a search warrant.”

Vendors are surprisingly helpful to first-time dark net dealers on forums like these. In another recent thread, one commenter notes:

“In addition to what these two said, ship something 13 oz or smaller and you can do it with first class stamps, otherwise you can use other ways of concealing your identity.”

Then comes the packaging. The idea is straightforward: Even if the package does get opened by authorities, it shouldn't be readily apparent that there are drugs inside. There are entire discussions online about the definition of “good stealth.” Writes one:

“Honestly all sellers need is a single high quality MBB [moisture barrier bag] and it will do the job. ...It provides a high quality seal and visual.”



Disguised as a SIM card

My first impressions were that the LSD was packaged to look like a SIM card, right down to the piece of paper with detailed instructions.

<https://archive.li/o/vYFph/https://thehustle.co/microdosing-buying-lsd-online>

<https://thehustle.co/microdosing-buying-lsd-online>

30 Days of LSD Microdosing Part 1: Buying LSD Online

My microdosing experiment begins with an adventure into the "dark web" to score some... stuff.

BY STEVE GARCIA

FEBRUARY 3, 2016



In my last post, I wrote about why I have decided to experiment with taking microdoses of LSD for 30 days. Here I'm going to start off by showing how you might get some LSD.

If you live in San Francisco, then getting LSD might be as easy as just paying a visit to the infamous Haight Street. But if you want a better idea of what exactly you're buying, or aren't living in San Francisco, then here is the process you might take:

The darknet

You may have heard of the 'Darknet' or 'Dark Web' already; the shadowy place where hackers sell Uber accounts and people buy child porn. The first definitely exists, the second is well hidden, and it's overall just a giant database of websites that aren't trackable or traceable by normal means. But there is accountability, which means that when you're buying drugs from one of the dark marketplaces, people will leave reviews and ratings, very much like eBay. So when buying LSD here, it's highly likely that it will live up to its reviews.

Here's how you start:



The screenshot shows the Tor Project website. At the top left is the Tor logo, which consists of the letters 'T' and 'r' in a purple font with a white onion bulb in the center. To the right of the logo are three navigation links: 'Home' (highlighted in a light yellow box), 'About Tor', and 'Documentation'. Below the navigation is a large green banner with the text 'Anonymity Online' in white. Underneath this, it says 'Protect your privacy. Defend yourself against network surveillance and traffic analysis.' There is a purple button with a white onion icon and the text 'Download Tor' with a small downward arrow. To the right of the button is a list of three bullet points, each starting with a white arrowhead: 'Tor prevents anyone from learning your location or browsing habits.', 'Tor is for web browsers, instant messaging clients, remote logins, and more.', and 'Tor is free and open source for Windows, Mac, Linux/Unix, and Android'. Below the banner are two sections: 'What is Tor?' and 'Why Anonymity Matters'. 'What is Tor?' has a sub-header and a paragraph: 'Tor is free software and an open network that helps you defend against a form of network...'. 'Why Anonymity Matters' has a sub-header and a paragraph: 'Tor protects you by bouncing your communications around a distributed network of...'

Step One: Download Tor

To get started browsing the darknet, you need to install a separate browser called Tor (normal browsers can't visit darknet websites). The logo is an onion because darknet websites end in .onion (instead of .com).

Once you've downloaded and installed Tor, open the app and you'll see loading bars as it starts to configure the service (it takes a while to load each time that you use it). I want to mention here that this is a very high-level explanation of these services; it gets a lot more complex and you

can do a bunch more things to stop tracking with nodes, etc. But for the basic user, this guide should suffice – click here if you want to enter the rabbit hole.

Step Two: Find the right marketplace

As I mentioned already, what you can buy on the dark web tends to be illegal. Sure, people will sometimes sell handmade soaps and cookies, but generally we're talking guns, drugs, and forgeries. Which is why a number of websites get taken down pretty regularly, so what I recommend today might not be available in a year.

A good place to start your search is with Grams, a Google-style engine for .onion websites. The URL for Grams is: <http://grams7enufi7jmdl.onion/> (again, this won't work in your normal browser, so you'll need to copy and paste this URL into Tor).

I'd suggest searching Grams for 'acid' (as LSD is sometimes too short a phrase to search for). You'll get a large number of results with links to different storefronts. Now, I need to explain dark marketplaces a bit more. They range from open – anybody with the URL can use them – to closed, which is where you need a personal referral code. Most will make you create an account, and you register with a made up username and password. Make sure to remember them, there's no *forget password* email box here!

DeepDotWeb aggregates marketplace data and warns you about which are doing well, and which have become shady.

Currently popular marketplaces include:

- [AlphaBay](#)
- [Outlaw Market](#)
(these are .onion links for Tor)

Note these two terms: FE and Active Vendor. They're good to understand.

FE (Finalize Early): This means that funds get released before the transaction is confirmed. This is good for sellers as it reduces risk, but

can scam buyers as there's no recourse if you don't get purchases. Avoid if you can.

Escrow / Full Escrow: This is ideal as it means your Bitcoins are held by a third party till your transaction is complete. You get the most security this way.

Awesome. But now you need to make sure you can pay for those lovely mind-altering drugs. For this, you'll need a Bitcoin wallet.

Step 3: Set up a Bitcoin wallet

Bitcoin, is, at its most basic, a digital currency; a service that lets you make untraceable online payments. I've used a number over the last couple of years, and have lost around \$5,000 on one, the Mt. Gox scam. Because of this I'm now a lot more careful of where I choose to put my money, and my current favorite is Coinbase.

It's free to create an account and you'll have one in under five minutes. You use your cell phone and email address to register. Now you link this to the account you've already created on one of the dark marketplaces. On the darkmarket, go to "add funds" to your account and it will give you a Bitcoin address. Use this to send money through your Coinbase account, and your account on the dark marketplace will be updated. Alternatively, some ask for your Bitcoin address, so you can update your account that way.

Now you can buy items!

Browse by category

- » Digital Goods 7333
- » Drugs 14098
- » Drugs Paraphernalia 388
- » Services 407
- » Other 788

Onion mirrors

[Ichudifyeqm4ldj.onion](#)
[jd6yhuwcoivehvd4.onion](#)
[t3e6ly3uoif4zcw2.onion](#)
[7ep7acrkunzdcw3l.onion](#)

Wallet

Your bitcoin address

17yYR1zWGutjxsrZZAewU72whb6MLmapXc

! Send bitcoins to the address from above to deposit bitcoins into your account. After you have sent bitcoins to this address the deposit will show up instantly as pending balance. After an average of 20 minutes (2 confirmations) the deposit is confirmed. Addresses are valid for one month.

Balance ₿ 0.00

Withdraw

Amount

BTC-Address

Withdraw PIN

Transaction Fee: ₿0.0001

Links

- » Forum
- » Help
- » Vendor application
- » Earn money

₿ Exchange

\$ 391.2
€ 363.6
£ 278.3
元 2605.4

News

- » Earn money by finding bugs
14/01/2016
- » Forum Relunched
20/03/2015
- » Invite friends and earn money
07/03/2015
- » Have a Black Market Reloaded account?
11/12/2013
- » Dream Market Beta went online
15/11/2013

Hint: Javascript enabled

Adding Bitcoins so you can buy things

Click to purchase, and you'll get an invoice and an estimated delivery date. AlphaBay gives you an option when you're checking out to 'encrypt your message using the seller's public key'. You should definitely check this box, as you don't want to be giving out your address in plain-text on these kinds of places.

Step 4: Prepare with a microdosing toolkit

While I waited for my LSD to arrive, I started getting my space prepared. There are differing opinions online, but the common factor seems to be testing the drugs to check they're what they promised.

I bought the LSD test plus kit (\$17.99) and a glass dropper (\$3.99) for taking it.

The goal is to dilute the LSD into distilled water or vodka and then drop it on your tongue. I have lots of vodka, so that part was easy.

Microdosing prep and arrival

I was a little concerned about having the drugs sent to my address, so I used a P.O. Box to get them delivered. Then they arrived at my place in a nondescript envelope.

My first impressions were that the LSD was packaged to look like a SIM card, right down to the piece of paper with detailed instructions. I paid around \$16.30 including shipping; the tests and prep tools actually cost more than the drugs! I cut a tiny piece off with a sharp knife and dipped it in the drug solution test (you're supposed to use plastic gloves, as you shouldn't handle LSD with your bare hands, but I forgot to buy them, so just used cutlery). The tiny square turned the drug test from clear to red, which confirmed that it was LSD.

I was glad to know it wasn't a dud. I purchased 120mcg, so I figured that this remaining ~100mcg would last me a couple of days since I'd be starting low and upping my dosage as I got acclimatized.

I'll update you with my progress as I go on, and let you know if I've found this to improve my productivity and creativity.

Ready, steady, dose

Wanna follow along? Over the next month I'll write a post each week about my energy, productivity levels, and overall mood right here on The Hustle.

At the end of my 30-day experiment I'll write a recap, which hopefully will become a resource for anyone interested in doing the same.

Shipping

This chapter is about actually dropping off your packages and sending them.

Since you have already read the vendor bust summaries you know that dropping off your packages is a weak link between your online identity and the receiver of the order. In the past law enforcement used that weakness to trace back where the packages come from and then stake out the places where you drop the off.

Therefore it is necessary to take a lot of precautions when dropping off your packages, some of them are listed in the following:

- Read [this article](#).

Point For Safe Shipping

POSTED BY: [DEEPPDOTWEB](#) NOVEMBER 26, 2013 IN [ARTICLES](#), [FEATURED](#) [LEAVE A COMMENT](#)

An interesting thread that was posted on reddit today:

http://www.reddit.com/r/SilkRoad/comments/1rhq7z/safe_shipping_what_is_it/

Following a great AMA thread with a postal worker:

<http://www.reddit.com/r/reloaded/comments/1rdgb0?sort=hot>

I would take these advices with a grain of Salt but its a great sum up of the information thats been floating around this topic on the forums:

=====

This is based off extensive research of FBI, DEA and Customs manuals.

Safe shipping

What it is

Safe shipping means packaging and mailing products in ways that minimize risk for all involved. Safe shipping is more than packaging a

product to reduce risk of interception, it is also using techniques to avoid liability for the shipper and recipient for any seized products.

List of things customs looks for

The following is a list of things customs uses to screen for suspicious parcels. A suspicious attribute of a parcel is called a flag. A single flag is often not much of a problem, but the more flags a package has the higher the chances it will be intercepted.

1. No return address
2. Restrictive markings (such as writing "Personal!" on the envelope)
3. Misspelled words
4. Poorly typed or written text
5. Excessive postage
6. Addressed to an incorrect title
7. Sent from a foreign country
8. Sealed with tape
9. Emits a strange odor (Including masking agents such as coffee, perfume and fabric softener sheets)
10. Lopsided, uneven, rigid, bulky or otherwise uneven weight distribution
11. Oily stains, discolorations and crystallizations on packaging
12. Packaging appears to be re-used
13. Package looks generally poorly prepared for shipping
14. addresses are hand written
15. addresses contain misspelled information (such as names, streets or cities)
16. Originate from a drug source state
17. Are addressed as being sent from an individual to an individual

18. Return address ZIP code does not match ZIP code of the post office the package is being sent from
19. A fictitious return address is used
20. List a sender or receiver name of a common type (Such as John Smith)
21. Make use of names that are not connected to either address
22. Package makes noise when shaken
23. Redistribution of weight is felt when package is moved or tilted

List of Ways customs uses technology to detect packages

1. Terahertz ray scanning

“illuminating a target envelope with tunable terahertz radiation and analyzing the absorption spectra of the resulting image. The results are cross referenced with a database of spectra to check for the chemicals of interest.”

Currently it takes ten minutes to fully scan and analyze a single letter, although increasing this speed to one minute per letter is in the grasp of current technology. Even with this potential decrease in the amount of time it takes to scan individual letters, this system could not be implemented en masse without slowing the mail system down to a screeching halt. It is much more likely that this technology will be used to scan mail that has already been flagged by customs personnel using other methods.

1. infrared and X-ray scanning

Infrared scanners and Xrays work fundamentally in the same way. They are used to detect irregularities in envelopes or packages, which is possible cause for further investigation by other more precise means.

1. Drug dogs

Drug dogs are trained to detect even trace amounts of controlled substances in the mail and are used by virtually all customs agencies world wide. Despite their excellent ability to detect certain

substances, the overwhelming amount of mail in the system means that they will not be able to sniff all mail. In addition to this, drug dogs are not trained to smell the vast majority of existing psychoactive substances, and due to the staggering number of said substances it is virtually impossible that they ever will be.

1. Drug residue detectors

“traces of controlled substances are collected on a small filter held in the end of a vacuum sweeper hose which has been previously tested to insure no contamination. The instrument uses an analytical technique in which the traces of controlled substances on the filter are heated to vapors and ionized. The time required for the ions to drift through an electric field is measured and the substances are identified by the “drift” time through the electric field. ”

list of ways customs trace intercepted mail and gather evidence

1. Fingerprinting the outside and inside of a package
2. Handwriting analysis
3. Analyzing paper and ink
4. Analyzing type impressions
5. Forensic analysis of trace evidence (Adhesives, fibers, hair, paint, paper, plastic, rubber, tape and insulation from safes).
6. Post office surveillance of individuals suspected of sending or receiving drug mail
7. To bust recipients of intercepted drug mail, customs officials will often dress as postmen and make an arrest after the suspect accepts the package. Often times they will allow a few minutes to pass in hopes that the suspect will have opened the package.
8. There are reports of tracking devices being hidden inside intercepted packages when they are being sent to a safe location such as fraudulently obtained PO boxes. The tracking devices then follow the recipient back to their base location where an arrest is later made.

Packaging tips for senders

Labeling

1. Use a real return address but make sure it has no connection to you. Ensure the ZIP code used is the same one of the drop box you plan to send the package from. A generally sound practice is to use the legitimate address of an apartment complex but do NOT specify an actual number.
2. Change return addresses, especially the name sent from, on a semi frequent basis. The name used should be generic but not overly common.
3. Keep the front of the package as clean as possible. It should have no markings other than a shipping and return address.
4. Double check to make sure all information is correct. Also ensure that all words are spelled correctly.
5. Both addresses should be typed and printed, not handwritten. Ensure the printer used has minimal connection to you (paid for in cash, from a friend, not used for other things)
6. Exact postage should be applied neatly to the package.
7. Do not seal the package with tape
8. Use self adhesive envelopes and stamps.

Packaging

1. Do not attempt to use masking scents
2. Double vacuum seal the substance, attempting to spread substance out as thinly and evenly as possible
3. Using heavy duty tape, secure the vacuum sealed bag to a piece of construction paper. Make sure it is secured tightly and that product does not make noises when shaken.
4. Fold the construction paper over on itself to make it take up as little area as possibly yet still be accommodating for the vacuum sealed bag.

5. If the thicker cardboard priority envelopes are available, the first envelope should be inserted into one of these. Both envelopes should be addressed.

Security tips for senders

1. At all stages of packaging gloves should be worn. Latex gloves should NOT be used by themselves. Tight fitting gloves made out of cloth or some other material should be utilized. During the stage of packaging where you come in contact with the substance, latex gloves should be worn over the regular gloves. After the substance is vacuum sealed, the latex over gloves should be removed and disposed of before coming into contact with the outer parts of the packaging, to avoid contaminating it with trace amounts of the substance.
2. Hairnets and long sleeved clothing should be worn during all stages of packaging to prevent hairs from entering the package.
3. Packages should not be sent from inside post offices but from random drop boxes away from cameras and buildings with cameras. Some care should none the less be taken to disguise facial features and identifying marks.
4. keep in mind that the total weight of a package sent via one of the drop off boxes, at least in the United States, is 13 ounces or less.

Security tips for recipients

1. The best option for recipients it to use PO boxes or PMBs obtained with fake identification. Mom and Pop box companies often have poor security compared to franchises, for example they are less likely to require photocopies of the ID and also are less likely to have a camera system, or if they do have a camera system it is probably very poor as compared to a big franchise company. Recipients using PO boxes should wait for a lengthy yet random period of time after the package arrives to attempt retrieval. This waiting period dramatically decreases the chances of being apprehended as prolonged surveillance is very expensive. Disguising efforts should be utilized when retrieving packages, and test runs should also be attempted.

2. Another excellent option is to have packages sent to abandoned buildings or houses. The same security methods should be applied as when using a fraudulently obtained mail box.
3. If a recipient must have a package delivered to a place connected with them, they should ensure said place is clean between shipments. Clean houses of friends can also be used. Upon receiving a package to a place with connections to the recipient, they should not open it and write return to sender on it. After several days, then the package is safe to be opened. Recipient should NEVER select to have shipping methods which require a package to be signed for.
4. Regardless of the place the package is delivered, the recipient should opt the quickest shipping method possible so long as a signature is not required. This way if there are delays in shipping, it can alert the recipient, and it will require any interceptor to rush getting warrants prepared before a suspicious delay in package delivery is noticed. Tracked mail with out delivery confirmation is an excellent option, as the recipient can follow the status of the package online (using Tor!) and can be alerted if the package is held by customs for a prolonged period of time. Edit/Delete Message

- Do not drop the packages near your home or other locations that you visit frequently. It basically means do not shit where you eat. If you do not follow this step LE will have it much easier to narrow your location down, and your case will look much worse in court if the locations where the vendor (who you allegedly are) dropped all his packages in your area. For a few examples of vendor who did this mistake just go back to the vendor bust summaries.
- When going to your drop off your packages avoid using any transport measures that can be linked to your identity. One vendor for example (Alexandrus) used his car to drop off his packages which was how he got identified. You need to find ways which do not give away your identity, so avoid using cars, train/bus/tram/subway if they have

cameras, . . . Instead use more anonymous transportation measures like a bike, go by foot or public transport without cameras.

- Carry as little electronic devices with you as possible. Smartphones, smartwatches or any other similar devices constantly transmit all kinds of data to third parties which will bite you in your ass in an investigation.
- Do **not** leave any fingerprints on the outside of the package when dropping it off. This is crucial since several vendors already got caught because LE found their fingerprints on the outside of the package and then was able to search for them in databases and/or compare them with the ones that their suspect has. So make sure you wear gloves take other precautions. If it would be too suspicious to wear gloves (like if it is very hot and good weather) you can use see-through gloves and/or drop the off when it is dark. Finger condoms (the ones used in kitchens) can also be used as gloves in public to prevent leaving fingerprints on the outside of your packs. They are less obvious than other gloves, especially in the summer or in the daylight.
- You can also use folders or large boxes to drop off packages. Looking normal while not getting fingerprints on packages can be difficult. For this you can use folders (the \$0.50 paper ones you find at any drug store) for envelopes, or a larger box for packages. Simply place all envelopes/boxes on the larger receptacle without getting fingerprints on them, go to the blue box, then tilt them all into there so they simply slide in.
- Wear some proper clothes when you go out to ship and avoid looking like the typical neighborhood dealer (sweatpants, a weed themed hat, . . .). If you look in the mirror and think "Wow that guy would never sell drugs", then you have the right outfit. Bonus points if it also makes it harder to identify you, e.g. a pair of sunglasses or a hat can make it difficult for LE to get your real name just by making pictures of you. But make sure that it also does not make you look suspicious (like wearing a hoodie and sunglasses at night).
- Find proper locations to drop off your packages. The locations and methods you can use vary from each country but an important thing

you need to pay attention to, is that you do not get video taped while doing it.

- About shipping tracked orders: This is dangerous. Consider paying someone to do the shipping for you, for example, shipping costs about 19 euro's and you pay a guy 10 euro's per package he ships for you. You charge the customer 20-25 euro's and the rest comes out of your own pocket. Paying the difference is not the end of the world because it might keep you out of jail. The only thing you need to do is ship the packages that need to be shipped with track and trace to your drop off guy, but you can ship those in a bigger envelope - un traced. So you stay completely anonymous.
- Keep in mind that sometimes customers can see online when the label was created and where it was accepted using the informed delivery feature for packages coming to their address. Even without you giving them any tracking number.
- Get a label printer. Costs about 100 euro's but its totally worth it.

Cashing out

General

Cashing out your hard earned bitcoins is the last step you have to make in order to finally get your earnings into cash. But just because you are close to the finish line, it does not mean you can be sloppy now.

Also, read up about the KYC (Know Your Customers) laws and regulations. You can cash out small amounts of bitcoins with (anonymous) debit cards this way.

Buying with btc

Try to purchase as much of your product with bitcoins. Are you able to get 1000 xtc pills for 900 euro's cash? Offer your connect 1k in bitcoins. The 10% mark-up may seem high, but in the end your profits are still more than enough to account for this. Cashing out bitcoin can be a pain in the ass, so unless you have a stable and secure way to do it; take every opportunity you can get to turn bitcoins into cash or product.

Getting the btc to the exchange

To get your bitcoins to the exchange you can not directly send them from your DNM wallet or personal electrum wallet on Tails to the exchange, because this would make it way too easy for law enforcement to look at some of your transactions on the blockchain and then maybe being able to determine your exchange account(s).

So at the very least you have to go the sending bitcoins path for buyers backwards but ideally you should also take some additional security measures. One would be tumbling the bitcoins, there are many different ways how to do it (from centralized third party services to open source software or a do-it-yourself solution by exchanging the btc into a different cryptocurrency and then back), you have to choose what measures you will take and if you also combine them.

Selling your btc

There are many ways to buy and sell bitcoins anonymously. Getting money dropped in your bank account from different people around the world is only going to work if you are small-time. But if/when you start clearing a few hundred thousand a year from random strangers around the globe depositing cash into your account, then your ass will be under a microscope for having so much money dropped in your bank account. Probably even much less will still get you unwanted attention from the feds.

The What Not To Do chapter already showed it pretty nicely that once law enforcement is on you, all the bank records will backfire tremendously. Since all the non-illegal institutions (like Wells Fargo or PayPal) are required to keep extensive logs, they will of course be released to law enforcement when they are working on getting your ass in jail.

So it is **strongly** recommended that you choose a method that does not produce a paper trail or at least a very small one (such as selling the btc in-person for cash). It would be shame if you get caught because you were sloppy in the very last steps of your vending cycle.

Whatever path you go: stay away from fraud/identity theft. It's tempting because it completely removes you from the money, but it complicates things and just adds another possible angle of attack for law enforcement to come after you or for you to fuck up and get caught.

Keeping your assets safe

If you already cashed them out, please read this discussion about storing and hiding money. If you still have some parts of your profit in btc, make sure they are not seize-able by law enforcement. That means do not keep them in online wallets (does not matter if DNM or exchange), only your own, personal software wallet it secure (e.g. electrum on Tails) that is on a protected OS.

OPSEC Discussion Burying cash money.

submitted 12 months ago by **AlpraKingRetired Kingpin**

How safe is it from sniffing dogs? Can dogs find it if its vacuum-sealed into individual bags and hidden under at least 6 feet of dirt in a large forested land? We talking about 1-1.5 cubic meter of cash.

-
- [119 comments](#)

- share
- all 119 comments
- sorted by:
- [best](#)

[–] [Tawse](#) 189 points 12 months ago
Put it in a 55 gallon drum. Bury it in the desert. Buy a lottery ticket with numbers that correspond to the GPS coordinates of the drum. Hang it on your refrigerator with a magnet for safe keeping.

- [permalink](#)

[–] [AlpraKingRetired Kingpin](#) [S] 92 points 12 months ago
then wait till a bunch of nazi supremacists find the ticket and kill your brother in law?

- [permalink](#)
- [parent](#)

[–] [LordDongler](#) 17 points 12 months ago
Then a guy with a suped-up hole puncher retrieves it for a cut and kills a small town cop

- [permalink](#)
- [parent](#)

[–] [Korberos](#) 1 point 11 months ago
Just in case you forgot: The nazis don't find the ticket. Walt calls them and gives them the coordinates so they can kill Jesse because he thinks Jesse is coming there to kill him and steal the money.

- [permalink](#)
- [parent](#)

[–] [DerkNatMerkats](#) 2 points 12 months ago
Damn nigga

- [permalink](#)
- [parent](#)

[–] [Sanhua](#) 1 point 11 months ago

Then the ticket wins

- [permalink](#)

- [parent](#)

[–][mirrorlucy](#) 1 point 8 months ago
breaking bad dude

- [permalink](#)

- [parent](#)

[–][Tawse](#) 1 point 8 months ago
Did you figure that out all by yourself?

- [permalink](#)

- [parent](#)

[–][Wingman417](#) -31 points 12 months ago
Is this from some kind of bad movie?

Also, protip -- thermal-printed ink tends to fade.

- [permalink](#)

- [parent](#)

[–][mrfenegri](#) 22 points 12 months ago
It's from Breaking Bad

- [permalink](#)

- [parent](#)

[–][deleted] 12 months ago
[deleted]

[–][g0 west](#) 10 points 12 months ago
It was what the show was almost entirely about

- [permalink](#)

[–][VicDamone Jr](#) 2 points 11 months ago* (', attr(title), ')
This comment has been overwritten by an open source script to protect this user's privacy. It was created to help protect users from doxing, stalking, and harassment.

If you would also like to protect yourself, add the Chrome extension [TamperMonkey](#), or the Firefox extension [GreaseMonkey](#) and add [this open source script](#).

Then simply click on your username on Reddit, go to the comments tab, scroll down as far as possible (hint:use [RES](#)), and hit the new **OVERWRITE** button at the top.

Also, please consider using an alternative to Reddit - political censorship is unacceptable.

- [permalink](#)

[–][deleted] -27 points 12 months ago
so, some bad movie then ;)

who am i kidding, its the BBMC documentary

- [permalink](#)

- [parent](#)

[–][deleted] 12 months ago
[deleted]

[–][Harry Fraud](#) 5 points 12 months ago
I am officially confused

- [permalink](#)

[–][deleted] 3 points 11 months ago

I'm confused as to why i got downvoted, I wanna keep my worthless internet points

- [permalink](#)

- [parent](#)

[–][Harry Fraud](#) 3 points 11 months ago

Same lol check my history I think some comments will do very well but like then ur suddenly at -27 karma questioning all those prior life decisions hahaha

- [permalink](#)

- [parent](#)

[–][deleted] 1 point 11 months ago

people can suck man, like you get a couple initial downvotes or upvotes and everyone follows the trend.

- [permalink](#)

- [parent](#)

[–][deleted] 12 months ago
[deleted]

[–][deleted] -1 points 11 months ago

im somewhat proud of how much i got downvoted for such a stupid comment.

- [permalink](#)

That way you could get prosecuted and sentenced, but you would still have (some) of your profits when being free again. Do not underestimate that part: it is a lot better to have some money after everything went wrong, than being broke as fuck and not being able to find a job because of your criminal record.

Various Resources

There are many resources about vending who got published over the time, some of them will be listed in the following because they do not fall in a specific category (like packaging or shipping). Make sure to read **every single one** of them as well as the discussion in the comments. Learning how to become a successful DNM vendor is not something where you can take shortcuts.

AlpraKing's OpSec guide

Chapter 1

- Lots of Advice Alpraking's OPSEC guide to being a successful kingpin.
- submitted 1 year ago * (', attr(title), ') by AlpraKingRetired Kingpin
- [For sale only \\$1999.97 unti.....](#)
- pls UPVOTE cuz FREE.
- So you want to ship hundred of thousand of pills a week for years and stay safe?
- Here's a couple of tips to keep you safe. I've been here since SR 1.0 under various aliases and have, over the course of my-3 years online career , shipped over 10 million pills. I used to press pills myself. Now last time i've seen a press was a year ago. I'm basically just smoking bowls and trolling on reddit now.
- **1. Outsource**
- Outsourcing simply refers to the noble art of hiring other people, "pawns of the checker", to do the dirty work. You want to hire clean people that dont arise suspicions. They will be doing the

dirty work so you want to hire someone who isn't already involved in drug trade or has priors. Don't get me wrong, you'll do everything in your power to protect them. Remember, if your guys catch heat, it can propagate to deeper layers fairly quickly and ultimately, to you.

- **2. Separate Administration & Execution**

- Have a layer of people who are doing the "boss" work and another one who is doing the "executive" work. Boss work is mainly paperwork and verifications to ensure everyone is doing his job properly and numbers balance and quality control is in check. Administrators don't get their hand dirty as that they will not handle the drugs themselves, but they will make sure packs are being shipped, tracking codes are being handled, productions are being made correctly and such. Administration is a promotion for executives who have shown a great degree of skill and loyalty. You can't put just anyone to overlook someone else's work. You have to get someone who has done it before and will be able to train new personnel or solve irregular issues. I normally promote my executors to administrators once they have shown that they can handle any issue from their business. I have them hire one of their friend and pay both from my own pocket. Employees kind of like hearing "hey, how about you keep your salary, train your friend to do your job, and you both will earn the same thing, paid from the big boss' pocket." More than money, people want power. Give power to people who want power and keep the money for yourself.

- **3. Treat your employees well but do NOT overpay them.**

- Treat your employees well by giving them insurances, paid vacations & trips, surprises bonuses, gifts and such. Do NOT give them a large payout even if they're pressing or shipping hundreds of thousands of pills. If someone becomes too comfortable with his pay, his quality of work will lower. you have to keep your employees dependant on you. Overpaying employees = Bad work. Double loss. For example in my own company all employees have a health insurance. they are allowed up to 1500/month in private medical, psychological bills paid by my expense) If not used, it will be given as a bonus

vacation trip every couple months. Any lawyer time they might need for questions is also paid by the company.

- **4. Don't hire people under 30 years old**
- Both in the administrative and executive field. People under 30 years old are reckless, like to hang out in bars and brag to friends. People over 30 years old (get 40,50+ if you can) tend to be more straight with their shit. Much less likely to steal or botch the work and normally know the value of money. If you can get someone 40 yo+ that doesn't have a record, its most likely someone who already had a full-time job and knows how to work decently and not do dirty shit. Im 20 btw.
- **5. Inform your people**
- Tell them the truth. what they're risking, what to expect, have them meet your own loyal people who already been arrested for you and have them testify about the backup they had for not snitching. People will be much less likely to switch on you if you've told them exactly the truth. Don't go around with "There's no risk!" bullshit. Not only will your guys not believe you but they'll totally go nuts when they get arrested if you do.
- **6. Back your own people**
- Make sure all of your people are properly lawyered up. have them know by heart the name and phone number of their designated lawyer (under your control) and have them meet regularly, all expenses paid by you, in order to strengthen this trust between the lawyer and the employee.
- **7. Don't hire people yourself**
- People close to you, that you love and value, should not be getting their hands dirty on the long run. have them quit, or promote them quickly, if you have them on the field. As soon as they've mastered their work, have them hire their own friend to do your work, and pay both.
- **8. Rotate your employees between jobs**
- By rotating your employees between various work in your company you not only prevent heat from accumulating on one particular place or person, confusing investigations, but you're also contributing to their general training. this has various positive consequences; You are able to better target the quality

and flaws of your various employees by having them try numerous different things. Also, if a branch of the operation is arrested, you can quickly reach out to your other personnel who has done similar work in the past to fill the voids.

- **9. Have separate different secret workspots, and different labs.**

- In order to confuse investigations, its mandatory to have different personnel, workspots, and labs. If i feel that heat is growing on one lab, I can quickly clean it up, have the worker stop and lay low for a while, and i simply transfer the workload over another less-heated up lab and production-guy. Its very difficult to see all the connections amongst various people especially when dealing with over 30 employees, but its needed. These connections are what will carry heat. I tend to think of it a bit like a computer would:

- **10. Get it down to numbers. (TLDRs; skip this part)**

- its hard to explain this part with words so I'll give an example with numbers.
- You suspect your packs are being profiled. If there is profiling going on, your courier is going to be considered the starting point of the heat. We will give it a 80% heat rating for this very event. Considering the courier access 3 times a week a stash, you will give the stash a 50% heat rating, just from this very link. the stash himself is linked to the lab, but only access it onces every 2 weeks. you will give your lab a 15% heat rating from this very event. Your treshold of risk is 70% (meaning you will shut down someone/somewhere that has over 70% heat rating), at this point you will shut down the courier and have him lay low, but the heat is not yet sufficient to close the stash and the lab, at 50% and 15% respectively
- Now a few days later you see a cop car parked on the street of your lab. This very event is worth 50% heat on your lab, and will also drip a 20% heat on your stash and 5% on your courier due to the links.
- Now shit got hot. Everything is above 70%. closing the entire branch.

- You'll admit it doesn't take math to notice that if your packs are being profiled AND a cop car is seen near your lab, you must be pretty hot as a whole and you SHOULD shut down. All I did was add numbers to follow the flow of heat and decide wisely what is hot and what is not. My objective is to keep all places around 30-40% heat which i consider a stable zone. If 60-70% is reached im going to start investigating very closely, but I will not close it down. If it busts 80% then its being closed down and laid low for a few weeks. Its not accurate because you have to estimate everything with little to no information, but it definitely helps seeing things and calculate your moves. If an event bust 150%, i will completely dismantle the place and move it to another spot.
- **11. Trust buffers.**
- Always have a layer of administration between you and your executives. You don't hire any executives, have your administrators do it. By doing so, NO ONE at risk of being busted knows who you are, let alone that you exist. If employees get caught and want to snitch, all they'll snitch is your administrator, who you should have sufficient trust in to believe he wont snitch you also.
- **12. Family links between employees are powerful.**
- If you testify in court, you don't get to choose who you snitch and who you don't (In Canada at least). You snitch everything or nothing. So it helps if employees get caught with members of their families, because they are much less likely to snitch as it would involve having them snitch on their own family. You can also use the trust between members of a single family to your advantage. You can normally trust your employee's brother or sister pretty much the same as you can trust your employee. assuming both work for you.
- **13. Control the money**
- Do not reveal how much you're making or how much people are making relative to one another. Its none of their business. I normally fund in cash one of my administrators with a lot of cash and he pays everyone by sending them cash in the mail, or bitcoins. He makes comptability records and bring them to me

so i can see where the money went, before I handle more cash/btc to him.

- **14. Encrypt everything**

- Have your employees familiar with tails & tor+pgp communications. Anyone minimally professional will take some notes. Make sure all your employees from the top to the bottom is familiar with TAILS and has a secure passphrase. Have them place all their documentation and notes there. Any paper hanging around must be burned.

- **15. Avoid keeping illegal shit around the "dangerous hours".**

- I refer to "Dangerous hours" as week-days 5AM to 8AM. My experience has shown me 90% of large drug raids occur during this time period.

- **16. Not everyone has to know everyone.**

- Its everyone's dream to think its like the movies where we gangsta organise "cartel parties" where everyone is invited. It doesn't work that way. If someone doesn't have to meet someone, don't make them meet. Don't take the risk of adding up more "heat rating" by creating un-necessary links between individuals who are not directly connected.

- **17. Keep "jokers"**

- Jokers are last-resort cards that allow you to solve dangerous issues or take-over control of your business in the event of catastrophic problems. Pictures of your employees naked, hacked passwords to their facebook, knowing their addresses, etc. Anything you can use against them if shit goes wrong helps.

- **18. Be diplomat when kicking people out**

- Always be very diplomat when kicking people out. Give them a nice fat good-bye paycheck and specify you're giving them this paycheck to "forget everything". Keep good terms and explain your decisions with opsec and that you're doing this for their own protection.

- **19. If your company screw up, pickup the pieces, dont flee.**

- Believe me, its worth more in the long run if you admit to being busted/admit to problems, refund everyone, close shop for a few months, and come back, than it is to exit scam and start under a new name. It builds confidence in the long run. Its easy to be

honest when your business goes well. But its in the bad moments that you show your true face. If you've been fucked in the past, been honest with everyone then came back, it gives an assurance that the same will happen if there's a fuckup in the future. How many vendors look so perfect until they start having issues? and when they do, most will run with customers money. If you are honest with customers despite problems, it will reward you later. It also helps looking at yourself in the mirror in the morning knowing you haven't fucked over a ton of people with less wealth than you.

- **20. Always change**

- Always change lab locations, stealth, rotate employees, open and closes front or laundering shops. Have several at the same time so you can switch work between places. Its like playing whack a mole with LE. If you stay too long in one single place, you'll get caught. I do not believe in "megalabs" with super OPSEC that are stable for years. A decentralised network of several small labs & dispatch places, constantly changing places, is the best. Its even better when you can afford to change places AND employee at the same time. Literally drops heat rating to 0%

- **21. Make sure your team's opsec is always on point.**

- Meet regularly with your administrators and have them tell you all the problems. Never get angry and don't judge them. They'll be much more open if they do not fear your reaction. Everyone can make mistakes. Your administrators should have the same attitude toward their employees. A transparent company allows you to see more problems and react accordingly.

- **22. Don't flash**

- Don't. Just don't. Fuck nice cars & nice houses as long as you are on the field or know directly people who work on the field. That will get you heated up more than anything else. Pile your money, hide it and work on laundering it with as much care and opsec as you do with your drugs. Fuel it in a legitimate business, with customers, then start laundering it slowly. Remember, as long as your money isn't properly laundered, its virtual. Anything you buy with it is a cursed gift that will increase your

own heat and can also potentially be seized by LE. You can start flashing when all your work has been securely outsourced or when you retire.

- **23. Dont get high on your own supply**

- You should actually never even have your own supply in your house or somewhere that could be linked to you. It also impairs your judgement and can worsen paranoia, narcissism and other personality problems you tend to develop being in the drug business. Especially Xanax. Dont take Xanax and take important decisions; you will regret it.

- **24. Prepare for an arrest**

- Prepare yourself, psychologically and with your lawyer, your family, your administrators, in the event of a bust. Make sure you have cash readily accessible by your trusted people and have a plan. You won't be able to interact much with the outside world starting the very moment your door is rammed. And you won't be told when it would happen. Run "simulations" of a scenario where you and several of your administrators are arrested. Make sure someone can take your place or at least handle your personal stuff, and get yourself a lawyer early on the payroll. Everytime you go to sleep in your bed, it might be the last night you get to pass there for a couple years. And everytime you peacefully wake up in the morning, congrats yourself that you have survived yet another day.

- **The end**

- Well not really, I wrote that nonstop just spewing out ideas. I think I could continue until 100. but my coke binge is over and i'm growing tired of writing. Good luck with your high-volume ambition, plebs. >:)


- **TL;DR:** <https://anony.ws/image/JYCI>

- **P.S.** Whoever is pressing fentanyl in xanax bars; Stop. Please. You're attracting LE attention on my game and making me lose sales due to everyone freaking the fuck out in the streets. And you're killing people. It's wrong.

- [Chapter 2](#) (dead link)

- Chapter 3

Question / Discussion Alpraking's The Kingpin Handbook - Chapter 1.3

submitted 1 year ago * (', attr(title), ') by AlpraKingRetired
Kingpin [ Retired Kingpin]

This one is aimed at vendors at large, and less on high-volume vendors.

30. Never answer online blackmail attempts

No matter how truthful the dox info might be, never pay for it "not to be released". By doing so you are confirming that the information has value. If you pay a dox ransom, you're confirming it has value and nothing will stop your ransommer from creating a new account a few months later and extort you again. Don't say yes, don't say no, don't flame the extorter, just ignore the message and refresh the page to make it disappear from your "unread" list. And most likely nothing will happen. In the worse case scenario, you will be doxxed (publicly, or to LE, who cares). This can help LE by orienting correctly its investigative efforts, but it doesn't count as evidence, even if your real name show up everywhere, it only counts as "hearsay". You would probably pay such a ransom to "preserve your opsec", but now imagine if the ransommer was actually a LE deep into an investigation trying to confirm if its really you? If you pay the ransom, you're pretty much confirming this is you. Who would pay a ransom if the dox info was wrong? Also, people attempting to dox you are most likely criminals as well and are bluffing, as I doubt any of them really wants to call LE and tell them shit; the first thing the cop they're talking to on the other end of the phone might wonder is "how do you know this? are you involved?". I've seen SO MANY times people go nuts over "OMG HE'S GONNA DOX ME he will send drugs to my house with no opsec!!!111" that i still shake my head over the memories of conversations I had with some of my resellers, a while back.

31. Clean up!

Clean up regularly. This means that routinely, and prior to any illegal stuff, clean everything. This includes regularly cleaning your entire house of illegal stuff. If you use recreational drugs, keep them all in one place,

along with any other incriminating shit. You don't want a long-forgotten unencrypted USB key full of customer info being found under your desk in the event of a raid. By cleaning your house regularly, you ensure that you know what is where, and what might be possibly found if your house was raided. If you're transporting drugs, clean your car BEFORE and AFTER. You don't want a single pill on your backseator some joint left-overs to serve as a "probable cause" for your car to be searched, especially if you're transporting bulk drugs.

32. Stay cool and have the "I'm not doing anything wrong" attitude when talking to LE

Convince yourself that what you're doing is routine work, and prepare a plausible excuse to justify your movements if you're transporting something illegal. This will be of use if the cops stop you on the road. Remember, unless they have a warrant or probable cause, they can't search your car. This winter, I had a shipment of 700k xanax pills that was moving from our lab to a transit place in a vehicle, and because of the weight of the pills in the trunk, the driver miscalculated the time necessary to break and crashed off-roads into the snow. Cops came and started asking questions. We gave a plausible story (wont go into details), It was late during night, the car was clean (in appearance) and the driver had a real job and didn't look like a druggo. Eventually we got the car towed and went on our way without any issues. If you look nervous as fuck in front of the cops because you have drugs in your car, you're going to make them suspicious. It is the nature of cops to see criminals everywhere and they are always on their guards. If you look suspicious, they're gonna dig.

33. Know your rights

Have you seen the "Am I being detained" videos on youtube? these are a pretty good example of what you should know. Hire a lawyer and get yourself very familiar with your rights, so that you know when you are really forced to comply or not. Most LE don't even know your rights (or their powers) and will start doubting themselves if you look very confident and say "No, you are not allowed to do that without a warrant" and insist on it. A bright cop might use some sort of good worded phrase to raid you, such as "I'm gonna have to ask you to get

out of the vehicle" <-- see what I did there? **to ask you** . He's asking you permission, say no.

34. Launder your bitcoins

Bitcoins are very easy to launder. First, tumble them out from the markets to a tumbler. Then, create a front-company, registered, with a real service/product that accept bitcoins. create invoices, and pay them directly from the tumbler. Each transaction will look like its coming from a unique btc address. Once laundered, just send your btc to any exchange and cash them out. Once the papertrail is created, there is no need to hide them anymore. You're gonna have to pay your taxes on anything you launder. High volume of laundering will attract heat on you, especially if your company looks too obviously like a laundering company, so keep it to a minimum. Pay everything you can with cash and keep your laundered money to pay things that the government can find easily as owned by you (property, cars, etc). to look even more legit, you should also pay some of your life expenses that everyone has with your clean money, such as your groceries or gas. When I go to the grocery, I tend to ask the cashier If I can pay 50\$ with debit and the rest (450\$+) with cash. This way, im creating a credible bank statement. It looks like im paying my gas, grocery, etc even tough the amounts are low. Having paper bills that prove you are paying 50\$ a week in groceries and 20\$ in gas look alot less suspicious than not paying for groceries or gas ever at all, especially if you have an expensive car. You should not need to launder more than 50-100k a year with this method. 100k a year is more than enough to pay your mortgage on a big house and a nice car. Just make your bank statement look like you eat ramen noodles every week, and thats why you can afford a high mortgage despite having only 100k a year in declared income.

35. Update!!

Update regularly Tails, Tor and keep up to date with recent LE busts. You want to keep TOR up to date to avoid using an obsolete version with known vulnerabilities. Its easy to get used to it and be lazy and not change your software version. This is bad opsec both with software and in real life; you want to be made aware as soon as a particular opsec procedure or software version is obsolete. If you look at most kingpins throughout history, most of them made millions of dollars during 5, 10,

15 years and eventually got busted and were sentenced to life. More often than not because they kept using the same methods over the years, and LE investigative methods eventually caught up. Now, with the Internet, we can keep up with what LE is doing on a large scale, and keep up with what is still safe and what is not. There is also no excuse not to update tor, tails or any other software you might be using for your business, regularly

The End

Feel free to post your questions, I will answer to the best of my knowledge.

- Vendor Setup Example #1

For Vendors: My Setup [vending since SR1]
submitted 2 years ago by **VendorSetUpThrowaway**
Hey /r/DNMs!

I've been operating since SR1 in 2011. I've been operating freely since then, and I feel I have a somewhat secure setup for vending. This post is specifically for vendors, buyers will not need this level of security or planning.

Your handle

The longest I have kept a single handle is 6 months. The long-standing, large players are always the first targets of LE. The benefit of Tor is you CAN create a new identity! If you were able to delete or disown yourself from your past mistakes, wouldn't you? This is firstly about minimizing impact of being caught. Why get sentenced for 4 years worth of breaking the law, when it could just be a couple of months?

I have actually discussed the above with other vendors, and some have admitted to pulling their BTC out and burning the handle in the past. I personally have not scammed my customers. You don't bite the hand that feeds, and I make plenty enough money as it is. However greed is something we'll never get rid of in this market, and is present in any aspect of life.

The less people, the better

Next, I operate entirely on my own. In terms of sourcing, I have only had to contact my suppliers twice in the past year (to increase shipment sizes). We have a system which includes a "warrant canary"-type scenario, where if they do not act on something within a time-frame, I know something has gone wrong on their end.

I implemented this system with my suppliers more than 2 years ago and have not had a false positive since. Plan ahead. There's millions of dollars invested in catching you each year.

Your office

I have a semi-legitimate business in IT. I have my own office and warehouse. This not only allows me to separate vending from personal at even a physical level, but also allows for me to have shipping/packaging equipment and all of the large-scale vending necessities without raising suspicion.

My office environment includes 24-hour live surveillance and alarms which I've installed myself. There are motion sensors on the inside that notify me when there is movement in the office when I am not present. The majority of the camera's and sensor's aren't visible from outside, just enough to detract burglars.

Your computers and network

My network and computer setup includes:

- A router which routes all traffic through a VPN which I have setup myself in a separate physical location. This address has no link to me aside from sending me video of the server room, and notifying me if any movement occurs around my server. If someone touches my server, I know I need to burn everything.
- A mini computer (like an ODROID) which has Whonix installed. This is so my IP/personal location can never be gathered from my main work station via exploitation or of my own accord.
- My main work station of course has all the bells and whistles of modern OpSec encryption, there are plenty of guides for that. However an additional level I have on top of that, is a dead man's switch. I have a small RFID device attached to my wristwatch. If I walk away from my terminal, the work station closes all applications, nulls the memory and shuts down. You will find with Ulbricht being arrested they had to catch

him logged into the DNM. Now if I am pulled away from my desk, or even step back - everything is covered. (Be sure to go to the toilet before you start.)

Other thoughts

There are many pro's and con's of having a separate place for packing and shipping your products, and conducting your DNM business on the computer (taking orders, responding to queries, etc).

My entire IT setup is pretty water-tight. However having product on-premises can be somewhat risky. It's always a good idea to have the minimum amount of product at your regular place of packaging.

Separate the bulk of your product from your day-to-day requirements. You may want to even go to a level of splitting month, with week, with day product-requirements in separate locations.

Why share this?

I've been extremely lucky. I started off with a decent amount of capital and happened to already have a reliable supplier who I've continued to do business with since starting. I started vending for the money and it has been more lucrative than I thought possible.

However I am now at a point in my life where I can retire, raise a family and do what I like. So I plan to close-up shop and cash out my remaining BTC in the next few months and work on my own projects. Vending isn't an enjoyable life, I work a monotonous 9-5 40-hour week like everyone else. My advice to vendors is to set your limit and quit once you reach it.

Finally, tell no one what you do. Have a good cover for your business. I do occasionally do legitimate work which is obtained by word-of-mouth. You can't avoid that without raising suspicion. I have been in a relationship for 3 years and I wouldn't dare put the responsibility of knowing what I do on my SO, or my family, or my friends.

Good luck, be safe.

Vendor Setup Example #2

- **OPSEC Shipping Procedure (remain completely stealthy)**
(self.AgMarketplace)
- submitted 2 years ago by **The Drug Store** Verified Vendor
- Alright this is going to be a pretty complete "How-To" for Vendors, and buyers alike that wish to remain completely ANONYMOUS when shipping drugs through the mail - USPS. Please upvote this if you find this information useful/informative. You will notice I say to get certain things off of ebay, the reasoning behind this is the bubble mailers are generic and they are bulk, so they will not be at all traceable. Same thing applies to the other materials. As far as shipping company, you will want to stick with USPS for the simple fact that they do more volume daily than FedEx and UPS combined. As well they are constrained by federal law to get a search warrant if they want to open your package, FedEx and UPS can open them at will without one, so this is very important.
- Pre-packaging: - Stamps or postage, now this is tricky because if you are using stamps you want to buy them either online, or if you do get them from your local post office you will want to pick them up by the edges, touching the stamp book, or stamp bare handed will leave your prints on them, so DON'T TOUCH THEM unless it is by the edges. If you decide to get tracking on it, make sure you use erroneous information that way it can't be tied back to you. Say you use USPS.com or stamps.com etc, use false info as your info, and do not schedule a pickup at your house. Drop your packages off in a mailbox, or at a business address.
- Preparation Area: - Make sure your work area is sterile, meaning you keep all areas that you will be working on free of fibers, hair, saliva, blood, matter other than the drugs being packaged, etc. You want to keep it as clean as possible at all times to ensure that you continue to stay in business. Being even a little bit lax can mean the difference between prison and freedom, so keep that in mind. Best practice would be to keep all your materials in this area and

make sure to be mindful of keeping it clean, wipe it down before you do anything work-wise.

- **Materials Needed:** - Rubber Nitrile Gloves (purchase on ebay, or a local store in cash) - Face mask (optional, but recommended) - Hair net (optional, but recommended) - Bubble Mailers (purchase off ebay) - Small boxes (for those that are ballsy, can be found online) - Packing Tape (purchase off ebay, cheapest kind is fine) - Printer Paper (any local store will work, wal-mart) - Printer (MAKE SURE YOU PAY IN CASH AT A BUSY STORE FOR THIS) - Scissors (doesn't really matter where you get these) - Zip Lock baggies assorted sizes (to put your drugs in, can be found on ebay) - Food Saver for vaccuum sealing bags (can be bought online) - Aluminum Foil Zip Lock Mylar bags - whatever size you think you will need (can be found on ebay, you can get 200 for about \$19.00) - Drugs or other illegal stuff (obviously)
- **Packaging:**
- Prior to handling any of the above mentioned Materials, you will want to ensure you do not come in to direct contact with pretty much everything, with the exception of the printer, gloves, face mask, scissors. Remember, paper, mailers, mylar bags, zip lock bags, tape, and boxes can hold prints so make sure you WEAR YOUR GLOVES - even some pills can hold on to prints, so that is something to keep in mind!
- When you do start packaging, if you do not have a face mask, breathe through your nose only - that way no saliva dna ends up on, or in your package. You might also want to hold the package away from your body while packing to ensure no fibers end up on or in the package as well. I recommend the following to ensure safe practice: Take a shower before packing to wash any loose hairs, fibers, or any other matter off your body that might otherwise end up falling in to your package, you may also want to consider in buying hair clippers to shave your head (not bicked, but say the next setting up) for good hair maintenance, or wear a hair net. It would be wise to either shave your arms, or wear a long sleeve shirt while packing as well to keep stray hairs at bay. While all of this may sound very paranoid it is in fact the only way to stay off the radar, because all it takes is 1 stray hair, or 1 partial fingerprint to sink your business, while it seems like nothing, it in

fact means everything regarding keeping you in business and from being caught!

- So now that you have all that in mind, you also will want to print both your customer addresses, as well as you fake info for return info. Now return information is a must to keep all red flags off your packages, there are several factors that cause red flags to USPS. So keep all of this in mind:
- Red Flags that USPS looks for: - Buldging or odd shaped packages - Packages with ANY aromatic odor - No return address - Fake return address - Zip code different from the city package is shipped from - Extra tape on bubble mailers (boxes are fine with tape obviously) - Extra postage paid on a package - Shipping via express mail - Hand writing on package - Incorrect shipping address
- So while putting your package together, you want to avoid writing on your package, which is why you print out your addresses, now, you don't want to use fake info for the return address because it is a red flag, so just go in the phone book and find someone across town and use their info for the return address. One to three flags on a package is pretty normal, but one flag that is something that they will raise eyebrows over is odor of your package. You do not want ANY SMELL coming from your package. Which is why you use multiple layers of baggies, combined with vaccuum sealing.
- Shipping: - When you are all done packaging your customer orders, and before taking off your gloves, apply firmly postage/stamps on them, and then put all your mailers in a plastic grocery bag so you don't make direct contact with them when walking/driving to a nearby mailbox. As such, make sure that the mailbox you mail from has infrequent passer-byers, and no cameras. Usually cameras are around the middle of town, or at high profile buildings. So finding a mailbox around a side street is ideal for shipping off the radar. When you arrive at the mailbox, make sure that you are not being followed, easiest way would be to just check your rear view mirror when leaving your house, etc. If you see someone following you, then find another place, or time to mail them. If it ever gets to that point then someone is suspicious of your activity, which is just something to always be mindful of, borderline paranoia and patience keeps you in the

game. When you grab your bag of bubble mailers, keep them in the bag when approaching the mailbox to keep your fingerprints off them, I would say wear gloves but this would raise suspicion of people walking by "like why the fuck is this guy wearing gloves", so keeping it less obvious is key. Grab the bag from the bottom, and move the handle of the bag out of the way of the mailers, then open the mailbox, and drop them in. Save the bag for next time :)

- If you liked this or found it informative then please vote it up! I appreciate it!