

DIGITAL SELF-DEFENSE INFOZINE FOR BERLIN SEXWORKERS



Digital Self-defense Infozine for Berlin Sexworkers
by Cypher Sex
inventati.org/cyphersex/

Cypher Sex is a queer feminist collective aimed at empowering LGBTQ* people, women, and sex workers in their use of online services and digital tools through workshops, guides, and personalized consultancies.

Got questions? Need personal advice on how to protect yourself online?
Write to:
cyphersex@lists.riseup.net

Bella Merda Publications #0017
Berlin, March 2021
IG @bellamerda.design

HYDRA



This zine is the result of a collaboration between Cypher Sex, the Hydra Café and the Berlin Sex Worker Community. The recommendations included here were gathered during many conversations of all kinds, both one-on-one and focus groups. Thanks to the valuable input of all people involved, we can now present you this great zine. A big thank you to Flo from Cypher Sex for their know-how, for gathering all these recommendations, and for the loving preparation of this zine. A huge thank you also to Bella Merda Design for the beautiful art work! Many thanks to Lara M., who helped keep the connection to the community alive. And of course thank you to all the awesome and smart sex workers who participated in the discussions and so willingly shared their knowledge and secret tricks with us.
Enjoy reading and implementing these helpful tips! Stay safe!

An Impressum Without an Official Name

In Germany, The Telemediengesetz ("Telemedia Act" in English) requires that websites published by individuals or organizations based in Germany disclose information about the publisher, including their name and address, telephone number or e-mail address, and other identifying information depending on the type of company.
Since Ava is registered in Germany, they would also need to put their official name in the impressum of their website, but this would expose them to stalking or outing, so following this rule isn't an option for them.
Fortunately, BesD (Berufsverband erotische und sexuelle Dienstleistungen e.V., the German sex workers union) offers a paid service for impressums, as well as a service to comply with the Jugendschutzgesetz (the German law for the protection of youth), so Ava paid for both services and BesD appears in the impressum as the publisher of their website, which is also compliant to the Jugendschutzgesetz.

is.gd/nryqxj

is.gd/3Z3BwJ

Dealing with Clients

Finally, Ava has a few rules on how they deal with clients, to give them (or others) zero chance of controlling them in case one of them turns out to be a stalker, or worse.
When going out with clients to public places, where other people might recognize their face, they never use their credit card and have clients pay for them if a card is needed.
They know that infecting a smartphone or another electronic device with spyware is cheap and easy, so Ava always keeps their phone with them. They never leave it unattended and never accept smartphones or other electronic devices as a gift from clients - or else get rid of the gift as soon as possible.
And since caution is never enough, they have locked their devices with strong passwords, so even if they lose them or leave them somewhere, nobody can access them anyway.

is.gd/J9MAV1



Ava Tarnung is a gender-fluid person who works as an escort among other things. Their personality and identity change a lot depending on the mood and the situation, and they have learned to use this natural gift also to impersonate different characters for their clients and for their different online activities. They think that knowing how to perform different personas both off and online is one of the keys to secure their life from stalkers and haters as well as to enjoy their multifaceted life.
Ava is a nerd. After some years of explorations on the Web, they've learned quite a lot about technology and how online platforms operate. This knowledge, together with the close-knit contacts they have with the local sex workers community, helps keep them secure against the many threats sex workers can face.
Ava lives in Berlin and has officially registered as a sex worker. The name in their documents isn't Ava, and to keep their life completely separated from their work, they would like to not use that official name as a sex worker. So when registering at the office, they requested that their name be replaced by their alias (or work pseudonym) in their registration certificate (the so-called Whore ID).

Identity Management

To protect themselves against stalking or outing, Ava has created a completely different work identity that cannot be connected to their official one, or to the identities they use with their family and friends.
Here's all the things they have considered to manage their work identity and other online personas:

An Identity for Each Level of Trust

Ava has come out as a sex worker to their closest friends, but not to their family of origin or neighbours – and they prefer to keep it that way. While there are some people they can immediately talk to about their work, in general they don't talk about how they make a living to people who haven't gained their full trust, and they avoid talking about their job with people they meet in more conventional situations.
Therefore, Ava has organized their communication channels and social media accounts by levels of trust - which are also connected to their different life spheres. They have one identity for each of these spheres:

- Bureaucracy (taxes, bank…)
- Family
- People they has just met
- Work
- Close friends
- separating all these spheres, they can limit the amount of information they give to people they don't have any reason to trust.

Choosing a Name

Like many pro dommes, Ava has chosen a work name that sounds cool, but on commercial social networking platforms their username is Ava "Tarnung" Adam. They have added a real-sounding surname to their work name and, although this sounds boring, there is an important reason.
On the internet, platforms that have "real name" policies (like Facebook) tend to base this judgement on an individual's legal name, rather than allowing them to identify as they choose. Many companies require both a first name and surname for registration (or a name that doesn't contain any slang terms or profanities), so Ava has added a common surname to their work name.

Ava's Work Website

Ava also has their own website to advertise their services in a place they own and control.
When they decided to buy a domain for their website, they looked for providers that included privacy protection in their basic package, but then they found an even better option, even if a bit more expensive. They registered their domain with the anonymous domain name provider Njalla, which accepts an encrypted anonymous request to register a domain.
Ava's website is hosted by a provider run by sex workers for sex workers that they found in this list of hosting providers. This list includes hosting providers that are not based in the U.S. and are not bound to enforce the American law package SESTA/FOSTA, and that don't implement practices that can harm sex workers:

njal.la

- **Red Umbrella**: https://redumbrella.ch/
  - Sex worker friendly
  - Icelandic servers
  - Free SSL certificate
  - WordPress support
- **Orange Website**: https://www.orangewebsite.com/
  - Anonymous sign-up (email only)
  - No logging
  - 2-factor authentication
  - 100% green energy
- **Abelohost**: https://abelohost.com/
  - “Offshore” and Netherland-based server options
  - Dutch jurisdiction
  - Inclusive terms of use policy
  - Free site migration (with one-year plan)
  - WordPress support
  - Accepts bitcoin

Because Ava understands how important anonymity is for their own safety, they also want their clients to be anonymous when visiting their site – so they have set their web server to record as few logs as possible and have made sure that their website can be accessed through the Tor network.

Online work

Videochat

Most recently in 2020, when the Covid-19 pandemic hit hard and sex work was banned in Berlin for some time, Ava and their colleagues started exploring ways of earning money through online work. This is when Ava started using their cam to have sessions with some of their clients.
What worried them most in the beginning was the risk that some of their clients may record their session and re-sell it online, so before they started camming they did some research and ruled out most video-conferencing tools like Skype, which has a history of not protecting its users' privacy or even more privacy-friendly platforms like Jitsi, which can't stop users from taking screenshots or recording video calls.
In the end, Ava decided to create an account on two platforms that have been created on purpose for cam work and protect sex workers from many possible threats, including clients taking screenshots. They now do their online sessions on Rare Bird Calls and on Manyvids, and can be sure that new clients can't exploit their contents thanks to the protections in place on these platforms.

foundation.mozilla.org/en/privacynotincluded/skype/

manyvids.com

rarebirdcalls.com

Selling Pictures and Videos

Ava is also getting a small income from selling videos and pictures online. To be sure nobody can re-sell these contents without their permission, they always add a watermark to all of them.
To plan better the creation of their contents, Ava followed the tips in this Guide for Adult Content Creators.
Eventually, Ava decided to sell their videos and pictures on AVN Stars, which does a good job with protecting adult content creators from stalking, harassment, doxxing and other such threats.

is.gd/fR1gPk

stars.avn.com/explore/trends

Ultimately, this won't protect them if they fall under the radar of the "real name" policy enforcers, but automated controls won't spot their name as a potential violation and they can hope to keep their account for some time.
Once they chose on a name, a surname, and a username for their work persona, Ava also did thorough research on various sex work platforms, as well as following this guide, so they are sure that nobody else is using that name, at least among sex workers in their city.

guides.accessnow.org/self-doxing.html

Takedown Requests

When Ava chose a new name, they also decided to get rid for good of traces that could connect their face with the name in their documents, so they also did another search inspired by this guide.
In their previous life, they weren't trying to protect their privacy so didn't pay much attention when people posted their pictures online. So they were a bit afraid of what they could find during their research and of the emotional reactions they could have seeing the results. To get support, they asked a good friend to keep them company while they were hunting traces of their old self.
What they found wasn't particularly unexpected, but they wanted to hide the results connecting their face to a name they weren't using publicly any longer.



They first made a list of all the pictures, videos, and personal information they wanted to delete, and made screenshots of all of them, following instructions in this guide on how to document online harassment.

Ava knew that, being a citizen of the European Union, they could request Google to remove results with their name from search results. So, as a first step, Ava filled out Google's Personal Information Removal Request Form.

Then they filled out more forms to remove images of their past self from Facebook and Twitter, and followed instructions such as those offered by the Cyber Civil Rights Initiative and the takedown guide in the "Without My Consent" website to delete intimate pictures from other platforms and sites. It took a bit of patience, as the responses weren't immediate, but the pictures and other information were eventually removed.

A Phone for Each Identity

Ava wants to be sure that their work identity can never be connected to their official one - not by stalkers, or neighbours, or even by state authorities.

Ava knows that phones have several weak spots that can make them easier to track.

So, to be sure, the first thing they did after deciding on their work name was to buy a new cheap phone with a new pre-paid SIM card for their new identity.

Although in Germany SIM cards should be immediately registered under the user's name, in Berlin it wasn't hard for Ava to find a friendly Späti that would sell them a pre-registered card.

Ava has registered all of their online work accounts with the new phone number, accesses their online work accounts only with their work phone, and when they go to their work appointments they only bring this device with them and leave their other personal phone at home.

Besides the clients, the only other person who has Ava's work phone is their most trusted friend, as this is the only person who always knows about their work appointments and will check on their phone to be sure everything is fine with them.

Ava is also aware that a common stalker might find out where they are by looking at geolocation metadata in the pictures and posts they publish online, so they have disabled GPS access for the apps in their phone and keep their GPS off all the time – except for only briefly when they really need to find their position on a map.

is.gd/JBbLYv

techsafety.org/documentationtips/

cybercivilrights.org/online-removal/

withoutmyconsent.org/resources/something-can-be-done-guide/take-down/

ssd.eff.org/en/module/problem-mobile-phones

facebook.com/help/contact/1440596240892 2

help.twitter.com/en/forms/safety-and-sensitive-content/private-information

Here are the instructions Ava found on how to set disappearing messages in the different IM apps they use:

- WhatsApp (messages will disappear after one week)
- Telegram secret chats
- Signal
- Wire
- Wickr

faq.whatsapp.com/android/chats/how-to-turn-disappearing-messages-on-or-off/?lang=en

telegram.org/faq#q-how-do-self-destructing-messages-work

support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages

support.wire.com/hc/en-us/articles/213216845-How-do-Timed-Messages-work-

support.wickr.com/hc/en-us/articles/115007397548-Auto-Destruction-Expiration-and-Burn-on-read-BOR-



Communicating with Clients

First Contact

The way new clients usually get in touch with Ava for the first time is through dedicated platforms like Kaufmich or Tryst.
They also find clients through ads on Erotik Markt, where people can publish ads to look for specific erotic services.
On all these platforms, Ava has registered with an email address that they only use to review potential new clients' requests, so they don't have their usual mailbox flooded by incoming messages and spam.
Often potential new clients will ask them for more pictures and Ava has a portfolio of pictures they created precisely for this purpose.

kaufmich.com
tryst.link
erotik.markt.de

Advance Payments to Improve Security

Ava's friend Anne Onimas isn't registered as a sex worker and (to be sure she doesn't get involved in a police raid) always asks clients whom she meets for the first time to send her a small advance payment through an Amazon Gift Card. In this way she can be sure the client is legit, as generally police officers don't have budget for this.

Staying in Touch with Clients

Once they have established a first contact with a new client, Ava asks them to switch to some other communications tool like WhatsApp, Telegram, Signal, Wire, or Wickr.
For all these instant messaging apps, Ava has created a dedicated account with their work phone number, or (when possible) only their work email, and they access them only through their work phone or through a dedicated browser in their computer.
When sending pictures or other sensitive information to a client, they set disappearing messages in the conversation so this information won't stay forever in the client's device. Unfortunately, not all apps offer the possibility of setting a very short time frame for this, so for example WhatsApp or common Telegram chats don't let users have a message disappear after some seconds, which is a very useful functionality when sending erotic pictures that Ava wouldn't like clients to store or take a screenshot of. This is why whenever possible Ava opts for a Telegram secret chat, Signal, Wire or Wickr, and prefers not to use WhatsApp.

signal.org
wickr.com
app.wire.com
is.gd/k3Vj1e

Ava's Tips on Email

When they started looking for an email provider that would be good to use for work, Ava already knew that there is no such thing as a secure email. By default, emails are not encrypted and if someone can access the servers where messages are stored (often over several machines belonging to both the sender's and receiver's email provider), they can read everything. This includes investigators, but also a random system administrator who has access to these machines.
Ava knew that they would not use their email for any sensitive content, but they still wanted to make sure that their email could not be tapped while in transit. So they only chose among email providers that use HTTPS/TLS encryption, which encrypts connections from their computer to the servers, and they made sure the TLS encryption was actually working by testing the provider they'd chosen on this webpage.
This is the list of email providers Ava chose from.
To be contacted by their clients, Ava has a Protonmail account which does encrypt their messages with other Protonmail users all along the way, so messages are not readable in the servers. However, they don't consider this encryption reliable enough because emails with people who do not have a mailbox on Protonmail are not encrypted.
Since all self-defined "secure email services" like Protonmail, Tutanota, etc., only offer strong encryption when writing to users of the same service (for example Protonmail to Protonmail), Ava considers these platforms as secure as IM apps, where your messages are secure only if you exchange them with other people who have an account with that same app.

checktls.com
prxbx.com/email/



Separate Email Accounts

To keep things really separated, Ava has a different email account for each of their separate identities and has created different online accounts, according to their different needs, with that corresponding email address.
Sometimes Ava just needs to log into a service once so they create a temporary account with a disposable email address like the ones offered by Guerrilla Mail or anonbox.

guerrillamail.com

anonbox.net

Secure Passwords

To be sure their accounts can't be hacked into, Ava uses strong and unique passwords for each of their accounts. They generate these passwords, consisting in random sequences of lower and uppercase letters, numbers, and symbols with an offline password manager (like KeePassXC). Then, they don't have to remember all the complex passwords because they have stored them in the password manager.
The only passphrases Ava needs to remember are the ones they need to unblock their devices and password manager. To memorize these easily, they have created these passphrases with the diceware method.

keepassxc.org

eff.org/dice

An Additional Level of Security: 2-Factor Authentication

Ava knows that even the strongest password can be stolen through various means, like for example phishing attacks.
They want to by all means prevent someone from accessing any of their accounts without authorization, so whenever possible they set up 2-factor authentication in the security settings of their accounts. To create the second factor, they have installed a code generator (like FreeOTP) in their personal phone so that every time they log into one of their online accounts they first enter the password and then a code generated by the app, which cannot be stolen in the same way as a password could.
Since each online platform has a different way of setting up 2-factor authentication, when they're in doubt they check the Electronic Frontier Foundation's instructions on 2-factor authentication to find the right guide.

ssd.eff.org/en/module/how-avoid-phishing-attacks#1

freeotp.github.io

is.gd/X9GSg5

Secure connections

Securing Connections When Using a Public Wi-Fi

Ava tries whenever possible to not use untrusted internet connections like the free Wi-Fi they find in coffee shops, railway stations, or hotels. They know that the owners of these networks, or worse hackers, might spy on them while they're connecting to the internet, so they prefer to use data in their phone and do most of their sensitive work through their home connection.
Still, sometimes using these connections is easier and cheaper so Ava has a solution for those cases: they have installed a VPN in their phone and computer and always activate it before they use free Wi-Fi access points.
This is a list of VPNs Ava considers reliable and shares with their friends when they don't know what VPN they should use. But in the end, they decided to use Riseup VPN, which they consider even more reliable as it is run by an autonomous collective rather than by a company.

nytimes.com/wirecutter/reviews/best-vpn-service/

riseup.net/en/vpn

Anonymous Connections

Ava's friend and colleague Anne Onimas has chosen not to register as a sex worker, so according to the German law she is working illegally. Since she doesn't have a European passport and needs to regularly renew her visa, she prefers to keep as much under the radar as possible and to reduce the amount of traces she leaves when she uses the internet for her work. So she makes sure, for example, to hide as much as possible the IP address of her home connection, which for the authorities (and for hackers) could lead directly to her official name and home address.
Therefore, when she created her work accounts (email, sex work platforms, social media, etc.) she used Tor Browser, and she only accesses these work accounts through her work phone, or when using the Tor Browser on her computer.

torproject.org

Terms of Use

Whenever Ava considers using a new service, the first thing they check is the service provider's Privacy Policy and Terms of Service or Acceptable Use Policies. There are many service providers (i.e. social media, website hosting, payment processing) that explicitly prohibit "adult content" - which may be defined broadly to include anything from pornography and vibrators to erotic fiction.
Ava generally avoids these service providers, or considers whatever account they may have with them as disposable.
In general, Ava keeps their eye out for platforms that do not prohibit "adult content" and offer other security features like two-factor authentication or payments in Bitcoin or through other methods that protect their anonymity.

Different Payment Methods

Ava avoids using online payment methods that are connected to their real identity for purchases that can connect them to their work (e.g. for buying their website domain name or hosting).
To avoid connecting their real identity to their work identity they use pre-paid cards they can buy at supermarkets (like Paysafe or Amazon Gift Cards), or ask clients to buy these for them.
Sometimes they also ask clients to recharge their bank account at a supermarket. They have an N26 account that offers the possibility of sending cash through a bar code - so they do a screenshot of the bar code in their N26 phone app and send it to the client, who can then go to a supermarket and pay the money by having the bar code scanned at the checkout counter.
Another option Ava has considered is paying for a TransferWise business account which gives the possibility of having money wired to an email address.
Some of Ava's colleagues also have their clients send money through a standard wire transfer to their bank account by giving them their IBAN without their name. Even if this works, this is riskier, as the client will see their official name appear in their bank statement.
To avoid giving clients too much power over their digital life, and to be sure nobody can spy on them through their own devices, they never let clients pay for their website or other online services and never accept devices as gifts.

paysafecard.com

is.gd/fhWB8o

n26.com/en-de/cash26

wise.com/help/articles/2932105/can-i-send-money-to-someone-with-only-their-email-address

Ava's Online Accounts

To advertise their services, Ava uses both mainstream social networking platforms and specialized platforms for sex work ads. At the same time, they use different accounts on almost all these websites to also communicate with their family, friends, and lovers, but, of course, they use different accounts for each of these groups of contacts.
They have the following accounts:

Platform	Contacts	Real or Fake Name	Trust in Contacts	NSFW?	Disposable Account
Facebook	Friends	Realistic Fake Name 1	High	Yes	Yes
Facebook	Family	Family Name	Medium	No	No
Instagram	Friends	Realistic Fake Name 1	High	Yes	Yes
Instagram	Work	Work Name	Low	OFC!	Yes
Twitter	Public	Work Name	Low	Yes	Yes
Fetlife	Friends and lovers	Fake Name 2	High	OFC!	No
Kaufmich	Work	Work Name	Low	OFC!	No
erotik.markt.de	Work	Work Name	Low	OFC!	No
berlinintim.de	Work	Work Name	Low	OFC!	No
Tinder	Work	Work Name	Low	Yes	Yes
tryst.link	Work	Work Name	Low	OFC!	No
Switter.at	Public	Work Name	High	Yes	No

Ava considers all accounts on services that require to use official names, or restrict adult content or sex work (see "Terms of Use" below), as disposable. They try to use a realistic name on Facebook, to avoid being spotted by Facebook's bots that try to identify fake names, but knows that at some point their account might be suspended and they would be asked for an ID to recover it.
To keep their accounts really separated, they avoid connecting them to their real identity unless they have decided to use their official identity in the first place (as they do with their family, or their bank - who both know it anyway). Additionally, they keep more stable accounts where one can always find them such as on dedicated platforms like Tryst or Switter (two sex-worker friendly spaces) or commercial sex work platforms, and tells their contacts that they can find them there if their other accounts are suddenly deleted or blocked. However, Ava never gives for granted that these accounts will last very long and makes a backup of everything they want to keep in their local machine and an external hard drive.

tryst.link

switter.at/about



Isolated Accounts

To keep their accounts isolated, and be sure that they cannot be connected to each other, Ava follows these additional rules:

- They only manage their work accounts from their work device.
- They don't follow the same people from different accounts connected to different identities.
- They are careful never to befriend one of their identities with another separate identity, and never to post the same content with different identities.
- Ava knows that most social networking platforms will display their location whenever they can so they disable geolocation in their phone apps and only activate the GPS in their devices when they really need it.
- Ava also knows that many apps and cameras will embed metadata into their photos which can include the date, time and location of the photo among other things. This metadata may be included in the pictures and videos they share online, so they always check that geolocation is disabled when they take pictures and shoot videos.

Dedicated Pictures

Most importantly, Ava never re-uses personal photos for work. They know that many search engines offer reverse image search functionalities that can identify all the places where a picture was published. To avoid someone connecting their work identity with other identities through a reverse image search, they never use pictures they have published in other accounts on their work profiles or when communicating with their clients.

