DIGITAL SELF-DEFENSE

INFOZINE

FOR BERLIN SEX WORKERS



Updated Edition





Ava Tarnung is a genderfluid 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 various 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 within 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 official name on their documents is not Ava so, in order to keep their personal life completely separated from their work life, they do not use their official name as a sex worker. Instead, when registering at the office they requested that their official 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 have just met
- Work
- Close friends

By 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 sex workers, 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 (such as Facebook) tend to base their judgment 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. 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 the guides listed below, so they are sure that nobody else is using that name, at least among sex workers in their city.

[01]

> Access Now - Guide on Self-Doxing [01]
> PEN America - Online Harassment Field Manual - Managing Your Online Footprint and Protecting from Doxing [02]
> The NYT Open Team - How to Dox Yourself on the Internet [03]

[02]

Takedown Requests

When Ava chose a new name they also decided to get rid of any online traces that could connect their face with the name in their official documents for good. Then, Ava also did another name search inspired by the self-doxing guides listed in the section above.

[03]



In their previous life, Ava wasn't trying to protect their privacy so they didn't pay that much attention when people posted their pictures online. Therefore, Ava was a bit afraid of what they might find during their research and of the emotional reactions they might have when seeing the results. To get support, they asked a good friend to keep them company while they were hunting down 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 and screenshots of all the pictures, videos and personal information they wanted to delete, and then followed the instructions in the Digital First Aid Kit guide on how to document online harassment [04].

[04]

Ava knew that, since they live in 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 [05] (this form requires logging into a Google account).

[05]

Ava then filled out more forms to remove images of their past self from Facebook [06] and X (Twitter) [07] and followed instructions such as those offered by the Cyber Civil Rights Initiative (CCRI) [08] and the Without My Consent website's Take Down guide [09] to delete pictures from other platforms and sites.

[06]

[07]

Facebook: Report a Privacy Violation [06]
X (Twitter): Safety and Sensitive Content [07]
Without My Consent: Take Down [09]
Cyber Civil Rights Initiative Safety Center [10]

[08]

As the responses were not immediate, it took a bit of patience but the pictures and other information were eventually removed.

A Phone for Each Identity

[09]

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 [11] so, to be sure, the first thing they did after deciding on their work name was to buy a new phone and a new pre-paid SIM card for their new identity.

[10]

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 phone shop that would sell them a pre-registered card.

[11]



However, buying a pre-registered SIM card in Berlin is becoming harder, so other people Ava knows have decided to get a phone number from online calling services like Hushed [12], Google Voice [13] or Twilio [14].

[12]

In any case, Ava always tops up credit on this alternative phone number to avoid their contract being cancelled and the number being reassigned to someone else.

[13]

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

[14]

Besides the clients, the only other person who has Ava's work phone number 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 at all the times – except for only briefly when they really need to find their position on a map.

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 not only investigators, but also a random system administrator who has access to these machines.


[15]

To learn how to secure their email communications, Ava read the Security in a Box guide on email [15].


[16]

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. Therefore, Ava only chose among privacy-friendly email providers that use HTTPS/TLS encryption [16], 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 the CheckTLS website [17].


[17]

> Ava decided where to create their new mailbox choosing from the list of privacy-friendly email providers on Security in a Box [18].

To be contacted by their clients, Ava uses a Protonmail [19] account which does encrypt their messages with other Protonmail users all along the way so that 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.


[18]

Since all self-defined "secure email services" like Protonmail or Hushmail only offer strong encryption when writing to users of the same service (for example Protonmail to Protonmail), Ava considers these platforms as secure as chat apps, where your messages are secure only if you exchange them with other people who have an account with that same app.


[19]

Separate Email Accounts

To keep things really separated, Ava has a different email account for each of their identities and has created different online accounts according to their different needs using that corresponding email address.


[20]

Sometimes Ava just needs to log in to a service once so they create a temporary account with a disposable email address like the ones offered by Guerrilla Mail [20] or anonbox [21].


[21]

Securing Accounts

Secure Passwords

To be sure their accounts can't be hacked, Ava uses strong and unique passwords for each of their accounts. Ava generates these passwords in a random sequence of lower and uppercase letters, numbers and symbols and uses an offline password manager such as KeePassXC [22]. In this way, Ava doesn't have to remember all the complex passwords because they have stored them in their password manager.


[22]

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 important passphrases with the diceware method [23].


[23]

An Additional Level of Security: 2-Factor Authentication



[24]

Ava knows that even the strongest password can be stolen through various means such as, for example phishing attacks [24]. 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.



[25]

To create the second factor, they have installed a code generator (such as the apps recommended by Security in a Box [25]) in their personal phone so that every time they log in to 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.



[26]

Since each online platform has a different way of setting up 2-factor authentication, when Ava is in doubt they check the 2FA Directory [26] to find the right guide.

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 (social media, website hosting, payment processing companies and so on) 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," reside in jurisdictions known for being more privacy friendly (such as Switzerland or Sweden) or more tolerant

towards sex work (such as the Netherlands), and offer security features like 2-factor authentication and payments in Bitcoin, or other methods that protect their privacy.

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 some of these social media to also communicate with their family, friends and lovers but, of course, they use different accounts for each of these groups of contacts.

Ava has the following accounts:

Platform	Contacts	Real or Fake Name	Trust in Contacts	Not Safe for Work?	Disposable Account
Facebook	Friends	Realistic Fake Name 1	High	Yes *(within the limits of Meta's terms of service)*	Yes
Facebook	Family	Family Name	Medium	No	No
Instagram	Friends *(private profile)*	Realistic Fake Name 1	High	Yes *(within the limits of Meta's terms of service)*	Yes
Instagram	Work	Work Name	Low	Of course! *(within the limits of Meta's terms of service)*	Yes
X (Twitter)	Public	Work Name	Low	Yes	Yes
Fetlife	Friends and lovers	Fake Name 2	High	Of course!	No
Kaufmich	Work	Work Name	Low	Of course!	No
erotik.markt.de	Work	Work Name	Low	Of course!	No
berlinintim.de	Work	Work Name	Low	Of course!	No
Tinder	Work	Work Name	Low	Yes	Yes
tryst.link	Work	Work Name	Low	Of course!	No

Ava considers all accounts on services that require to use official names or restrict adult content or sex work as disposable (see Terms of Use at page 10). For example, they try to use a realistic name on Facebook (to avoid being spotted by Facebook's automated tools that try to identify fake names) but know that at some point their account might be suspended and they would be asked for an ID to recover it. In general, Ava never takes for granted that these disposable accounts will last very long and regularly makes a backup [27] of everything they want to keep, storing it on their computer and in an external hard drive. Their friends who don't own a computer store their backups in secure and privacy-friendly storage platforms [28].

[27]

> Ava has followed the instructions in the Security in a Box guide on backups to create a backup strategy and reduce the risk of losing important pictures, videos and other data [27].

[28]

To keep their accounts really separated, Ava avoids connecting them to their official identity unless they have decided to (or have to) use their official identity in the first place – as they do with their family or their bank, who both know it already anyway. Additionally, they keep more stable accounts so that they can always be found on dedicated platforms – such as on a sex workers-friendly space like Tryst [29] or commercial sex work platforms – and tells their contacts that they can find them on those more stable sites if their other accounts are suddenly deleted or blocked.

[29]



Isolated Accounts

To keep their accounts isolated and to 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 they never 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 and videos which can include the date, time and location of the photo or video 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.
They also know that AI-powered image search engines can be used to find non work-related pictures of their face online. This is why they now share their private pictures just on accounts that only their trusted friends have access to.

Payment Methods

Ava avoids using online payment methods that are connected to their official identity for purchases that can connect them to their work – for example, for buying their website domain name or hosting provider (see page 24).

[30]

To avoid connecting their official identity to their work identity they use prepaid cards they can buy at supermarkets (such as Paysafe [30] or Amazon Gift Cards [31]), or ask clients to buy these for them. Some other options they have considered are listed on Sex Worker Helpfuls [32].

[31]

Sometimes Ava also asks clients to recharge their bank account at a supermarket. For that, they have an N26 account that offers the possibility of sending cash through a bar code [33] – they make 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 barcode scanned at the checkout counter.



[32]

[33]



[34]

Another option Ava has considered is paying for a Wise business account, which gives the possibility of having money wired to an email address [34].

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 can work, it is riskier because the client will see Ava's official name appear in their bank statement.



[35]

Sometimes, instead of requesting money, Ava asks their more regular clients to buy something out of their wishlist on Throne [35] or Amazon [36]. They limit this choice – especially on Amazon – to particular occasions, as getting a lot of gifts may attract the authorities' attention.



[36]

To avoid giving clients too much power over their digital life – and to be sure nobody can spy on them through their own devices – Ava never lets clients pay for their online services (such as website hosting) and never accepts devices as gifts.

Online Gifts as Advance Payments

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 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 police officers generally don't have budget for this.

Securing Connections

Securing Connections When Using Public Wi-Fi Networks

Ava tries whenever possible to not use untrusted internet connections like the free wireless networks (Wi-Fi) they find in cafes, U-Bahn or railway stations and hotels. They know that the owners of these networks (or worse, hackers) might spy on them while they're browsing the Web or using online services. So they prefer to connect through their phone and anyway do most of their sensitive work through their home connection.



[37]

Still, sometimes using Wi-Fi connections is easier and cheaper so Ava's solution for those cases is to use the VPN (virtual private network) they have installed on their phone and computer and always activate it before they use public access points. However, they always keep in mind that VPNs are not a security multi-tool and that for many circumstances connecting through a VPN isn't the most important security step to take [37].



[38]

Ava keeps track of VPNs that are reliable [38], also based on the Electronic Frontier Foundation's recommendations on how to choose a VPN [39], and they share these links with friends who don't know what VPN they should use.



[39]

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 and phone connections, which can lead authorities and hackers directly to her official name and home address.

[40]

Therefore, when she created her work accounts (email, sex work platforms, social media, etc.) she used the Tor Browser [40] and she only accesses these work accounts through her work phone or when using the Tor Browser on her computer.

[41]

Communicating with Clients

First Contact

Ava has several ways they can be reached by new clients. New clients can write to them through a form on their website (see page 24) or on dedicated platforms such as Kaufmich [41] or Tryst [42].

[42]

They also find clients through ads on Erotik Markt [43], 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. In this way, they don't have their main mailbox flooded by incoming messages and spam.

[43]

More Secure Ways of Sending Pictures

Often potential new clients will ask Ava for more pictures, so they have a portfolio of images created precisely for this purpose (see page 14) that they only share via dedicated work accounts.

[44]

Ava knows that some messaging apps like Signal have a feature that will block screenshots in other people's phones. Still, someone could take a picture of their messages with another device or take a screenshot through a desktop app. To make it harder for clients to take screenshots of their pictures, Ava sends them through chat apps that allow for very short automatic deletion time (such as Signal or Telegram secret chat) or sets them to disappear after they have been viewed once (a feature offered for example by Signal and WhatsApp).

[45]

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

WhatsApp (messages will disappear after one week, so Ava tries to avoid sending pictures through WhatsApp) [44]
Telegram secret chats [45]
Signal [46]

[46]

Here are the instructions Ava found on how to set media to disappear after they have been viewed once:

Signal [47]
WhatsApp [48]

[47]

[48]

Removing Invisible Data from Images and Other Files

Ava knows that images, videos, PDFs and many other files may include invisible details they don't want to share with people they don't trust. This information, called metadata, might show, among other things, where Ada was when they took a picture or shot a video.

Usually this information is removed if images or videos are shared through social media or through messaging apps. If they are sent as attachments by email or through chat apps, though, files are not stripped of metadata. To be sure, Ava always removes metadata from images and other files they share with clients or on online platforms they use for work.

> Ava has learned how to remove metadata from files in the Security in a Box guide on how to destroy identifying information [49].

Staying in Touch with Clients

Once they have established first contact with a new client, Ava asks them to switch to a chat app such as WhatsApp, Telegram or Signal [50].

In each case, Ava has created a dedicated account with their work phone number. Ava then only accesses these accounts on their work phone or through a dedicated browser on their computer.

> To secure their communications on WhatsApp they have followed the Security in a Box guide for WhatsApp [51].
>
> To secure their communications on Telegram they have followed the Security in a Box guide for Telegram [52].
>
> To secure their communications on Signal they have followed the Security in a Box guide for Signal [53].



Dealing with Clients

Ava has a few rules on how they deal with clients so that they (or others) have 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, Ava never uses their own credit card. Instead, they ask the client to pay if a credit card is needed.

Ava also knows that infecting a smartphone or another electronic device with spyware is cheap and easy [54], so they always keep their phone with them wherever they go. They never leave it unattended and never accept smartphones or other electronic devices as a gift from clients - or else they get rid of the gift as soon as possible.

[54]

Finally, since caution is never enough, they have locked their own devices with strong passwords so that even if they lose them or leave them somewhere nobody can access them anyway.

Online work

Videochat

Recently, some of Ava's colleagues have started working online. What worried them the most in the beginning was the risk that some of their clients might record their session and resell it online. Before they started camming they did some research and ruled out most video-conferencing tools, including not only commercial platforms but also more privacy-friendly ones, as none of these can stop users from taking screenshots or recording video calls.

Ava and their friends know that the landscape of webcam platforms is constantly evolving. They have an account on several sites and keep updated on discussion forums, such as r/CamGirlProblems on Reddit [55], where they can exchange views on the evolution on the camming industry.

[55]

Selling Pictures and Videos

Ava is also getting a growing 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.

[56]

Some of their friends also hang a sign in the background or wear clothing with their website domain name on it [56] so nobody can remove their watermark and steal their content.

To plan better the creation of their contents, Ava has read DIY guides such as the Dumb Whore's Guide to OnlyFans Success [57] and has been following discussion forums such as r/adultcreatortips [58] and r/onlyfansadvice [59] on Reddit.

[57]



[58]

[59]


[60]

Also, Ava tries to diversify the places they sell content on, and has accounts on most alternative platforms for content creators [60], including Manyvids [61], which puts protections in place to reduce the risk of clients exploiting their content.

Ava's Work Website

Ava also has their own website in order to advertise their services in a format that they control.


[61]

Registering Domains

When Ava decided to buy a domain for their website they looked for providers that included domain privacy protection in their basic package but then they found an even better option. They ultimately registered their domain with the anonymous domain name provider Njalla [62], which accepts encrypted anonymous requests to register a domain and payments made with a variety of platforms including cryptocurrencies.


[62]

Choosing a Hosting Provider

Because Ava understands how important anonymity is for their own safety, in addition to following the general rules on how to choose tools and what to look for (see page 26) they also want their clients to be free to stay anonymous when visiting their site. Therefore, Ava only considers hosting providers that offer ways of securing connections through HTTPS [63] (possibly for free) and record as few logs as possible, and checks that websites hosted on these providers can be accessed through the Tor network.


[63]

Ava's website is hosted by a provider they chose among the options below. This list includes providers that explicitly host adult content, do not implement practices that can harm sex workers and are based in a sex workers-friendly jurisdiction.

Vicetemple [64]
- Based in the Netherlands
- Dedicated to adult content
- Accepts payments in cryptocurrencies

Orangewebsite [65]
- Based in Iceland
- Anonymous sign-up (email only)
- No logging
- 100% green energy
- Accepts payments in cryptocurrencies

Abelohost [66]
- “Offshore” and Netherlands-based server options
- Dutch jurisdiction
- Inclusive terms of use policy
- Accepts bitcoin

Hostinger [67]
- Based in Lithuania
- Accepts adult content


[64]


[65]


[66]

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, phone number or email address and other identifying information depending on the type of company.


[67]

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.

[68]

Fortunately, BesD (Berufsverband erotische und sexuelle Dienstleistungen e.V., the German sex workers union) offers a paid service for impressums [68], as well as a service to comply with the Jugendschutzgesetz (the German law for the protection of youth) [69], so Ava paid for both services and BesD appears in the impressum as the publisher of their website, which is also compliant with the Jugendschutzgesetz.

[69]

How to Choose Tools: What to Look For

Before choosing software or online platforms, Ava always gathers information about the application or service by checking its website and looking at online reviews. Additionally, these are the questions Ava asks themselves when considering a new tool:

•Is the application mature?
Ava knows that security applications and protocols like HTTPS or Signal have usually been around for a long time. New applications are rarely good in regards to security. Before a piece of software can be considered secure, it needs to pass the test of time.

•Is the application based on open-source software?
Some tools (like Telegram for example) have free and open-source user interfaces but their server software is not open-source. Other tools promise security but they are not based on free and open-source software so we cannot really know what they do.

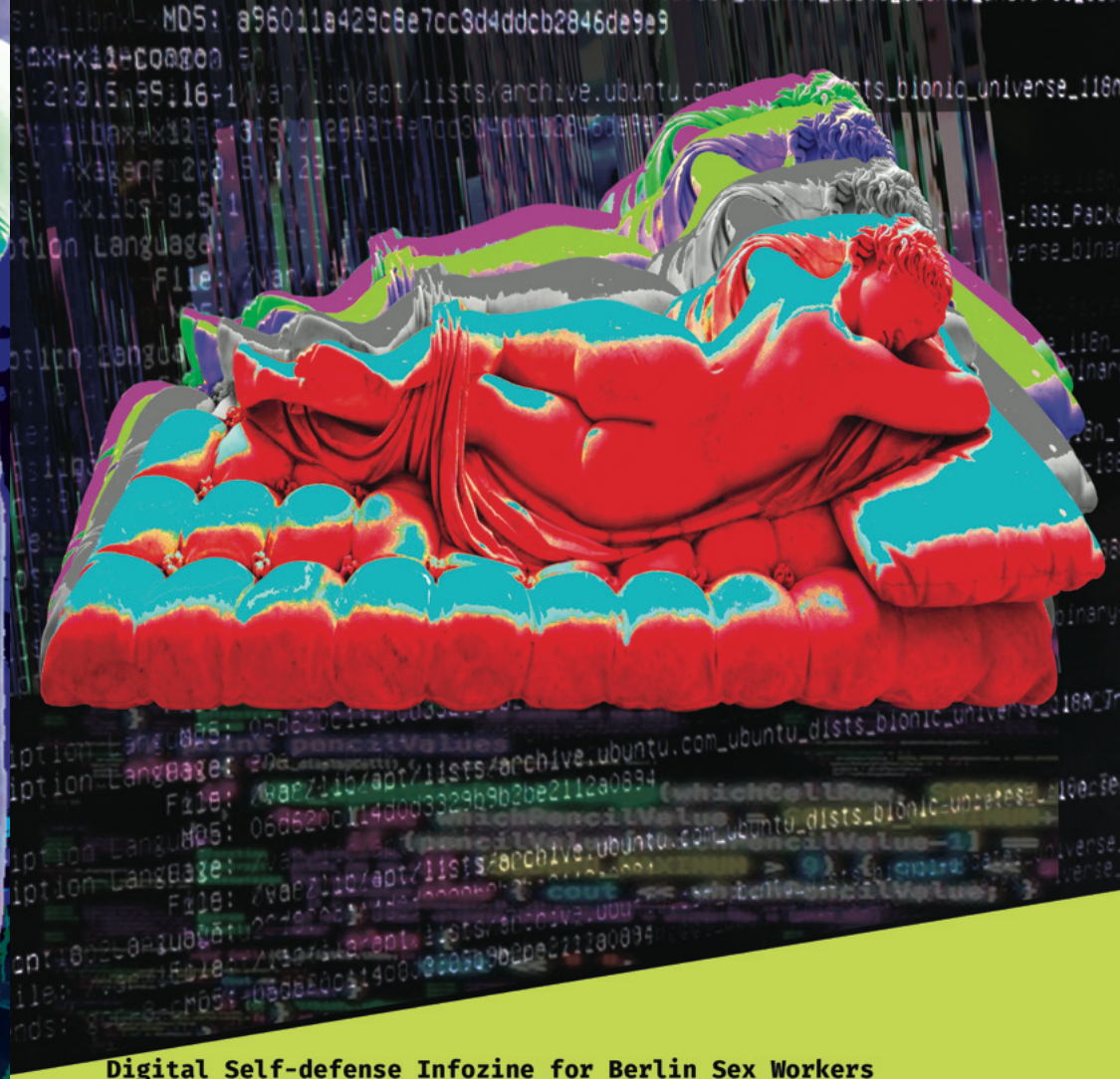
•Does the platform offer a secure HTTPS connection?
Ava knows that they can consider a connection secure when they see a green or closed lock or a shield with a check icon in the address bar of their browser when connecting to a website.

•Is the platform based in a sex workers-friendly jurisdiction or in a country where sex work is cracked down upon?
The laws that regulate a tool depend on the country where that tool or service is based. For example, website hosting based in more sex workers-friendly countries (such as the Netherlands) would make a better choice than choosing a company based in a country where sex work is (mostly) illegal (such as the United States).





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 Fiore 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!



Digital Self-defense Infozine for Berlin Sex Workers
Updated Edition
cyphersex.org

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:
info@cyphersex.org

Bella Merda Publications #0017
Berlin, October 2026
IG @bellamerda.design

HYDRA