



DIGITAL SECURITY GUIDE FOR SEXWORKERS

projet-evasions.org/cypherguide_eng



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..

inventati.org/cyphersex



Projet-Evasions is a multilingual anarchist initiative that creates and diffuses emancipatory content. When we're not daydreaming about sexpositive evenings, we're organizing ourselves into networks of sparkling accomplices on subjects that inspire and concern us. Deep inside us, under a thick layer of glitter, simmers a deep hostility to all forms of authority and a burning passion for freedom... all wrapped up in golden and silver chocolate paper (vegan, of course). Paper versions of this guide can be ordered on our website.

projet-evasions.org/en



SUMMARY

1. Identity Management

1. An Identity for Each Level of Trust
2. Choosing a Name
3. Takedown Requests
4. A Phone for Each Identity
5. Ava's Tips on Email
6. Separate Email Accounts
7. Secure Passwords
8. 2-Factor Authentication
9. Ava's Online Accounts
10. Isolated Accounts
11. Dedicated Pictures
12. Terms of Use
13. Different Payment Methods

2. Secure connections

1. Securing Connections When Using a Public Wi-Fi
2. Anonymous Connections

3. Communicating with Clients

1. First Contact
2. Advance Payments to Improve Security
3. Staying in Touch with Clients

4. Online work

1. Videochat
2. Selling Pictures and Videos
3. Ava's Work Website
4. An Impressum Without an Official Name

5. Dealing with Clients

6. Further Resources



AVA CAMOUFLAGE

Ava Camouflage is a gender-fluid person who works as an escort, among other things. Their personality and identity change a lot depending on their mood and the situation, and they have learned to use this natural gift 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 securing 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.

procore-info.ch/en/our-members

To protect themselves, Ava does not use their legal name at work, but a pseudonym (or work pseudonym). Ava has a Swiss passport and lives and works as an escort in Zurich, so they do not have to register. However, the registration process varies depending on the canton, residency status and type of sex work. People who come to Switzerland with an EU passport to work as full service sex workers must register in all cantons. Sex workers can find out about the regulations and registration processes that apply in their canton from the [local counseling centers](#). Ava recommends that sex workers never use the name they have registered with when working.



1. 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 are all the things they have considered to manage their work identity and other online personas:

1. 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.

2. 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 "Camouflage" 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. 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.



3. Takedown Requests

When Ava chose a new name, they also decided to get rid of traces that could connect their face with the name in their documents for good, so they also did another search inspired by [this guide](#).

In their previous life, they weren't trying to protect their privacy so they 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](#).

Google offers the option of requesting the removal of content with your name from search results. In the EU, you have the right to have results with your own name removed. In Switzerland, there are fewer legal rights, but you can still try making the request. So, as a first step, Ava filled out the [Google form to request the removal of personal data](#).

Then, they filled out more forms to remove images of their past self from [Facebook](#) and [X \(Formerly Twitter\)](#), and followed instructions such as those offered by the [Cyber Civil Rights Initiative](#) and [the takedown guide from 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.

guides.accessnow.org/self-doxing.html

techsafety.org/documentation/tips

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

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

cybercivilrights.org/online-removal/

facebook.com/help/contact/144059062408922

google.com/webmasters/tools/legal-removal-request?complaint_type=rbbf&visit_id=637202230061146146-20083139&rd=1





4. A Phone for Each Identity

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

Ava wants to be sure that their work identity can never be connected to their official one - not by stalkers, 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 it is a legal requirement in Switzerland for SIM cards to be registered in the user's name when purchased, Ava tries to find a pre-registered SIM card. It is also possible to buy SIM cards abroad and use them in Switzerland. 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.

5. 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 had chosen on [this webpage](#). This is the [list of email providers](#) Ava chose from.

To be contacted by their clients, Ava has a Tuta Email account, which encrypts their messages with other Tuta 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 Tuta are not encrypted.

Since all self-defined "secure email services" like Tuta, Protonmail, etc., only offer strong encryption when writing to users of the same service (for example Tuta to Tuta), 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.

6. 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](#).

7. 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 passwords 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](#).





8. 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](#).

freeotp.github.io

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

eff.org/deeplinks/2016/12/12-days-2fa-how-enable-two-factor-authentication-your-online-accounts

9. 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	Erotic Content?	Disposable Account ¹
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	Yes	Yes
X (twitter)	Public	Work Name	Low	Yes	No
Fetlife	Friends and lovers	Fake Name 2	High	OFC!	No
Callme toplay	Work	Work Name	Low	OFC!	No
La Compagnie	Work	Work Name	Low	OFC!	No
And6	Work	Work Name	Low	OFC!	No
Xdate	Work	Work Name	Low	OFC!	No
Tinder	Work	Work Name	Low	Yes	No
Tryst.link	Work	Work Name	Low	OFC!	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](#) (a sex-worker friendly space) or commercial sex work platforms, and tells their contacts that they can find them there if their other accounts are suddenly deleted or blocked.

1) Ava defines an account as "disposable" if they aren't sure that they will be able to protect the account from being deleted. This means that she expects that the account may be deleted..

However, Ava never takes 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.

10. 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 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. Ava also uses [MAT](#), a good software to remove metadata from images and documents.



11. 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.

12. 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.

13. 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](#), [Amazon Gift Cards](#) or [OK.-Credit cards](#)). Sometimes they ask clients to buy these for them.

For their payment, Ava usually accepts cash, as this is the safest and most anonymous method of payment. They always asks for the cash upfront so they don't risk the client refusing to pay afterwards.

Another option Ava has considered is setting up a TransferWise business account, which offers the ability to [send money via an email address](#). Sometimes their customers also buy them gifts via a [wishlist](#).

Currently, a new app called "[Horizontl](#)" is being developed to provide a more secure solution for payments for sex workers. As the app isn't ready yet, Ava can't say anything about how useful it will be nor whether it will be available in Switzerland - but they are keeping an eye on it.

kkiosk.ch/de/products/detail/?id=299

paysafecard.com

horizontl.co/get-involved

wishlist.com/
amazon.de/Amazon-De-Geschenkkarten-lm-Stationaeren-Handel/?
currency=EUR&ie=UTF8&language=en_GB&node=5362203031

wishlist.com/

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.



2. SECURE CONNECTIONS

1. Securing Connections When Using a Public Wi-Fi

Whenever possible, Ava tries not to 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.

riseup.net/de/vpn
nytimes.com/wirecutter/reviews/best-vpn-service/

2. Anonymous Connections

Ava's friend and colleague Anne Onimas came to Switzerland from an EU country to work in sex work. However, Anne decided not to apply for a work permit and not to register as a sex worker. This means that she is working illegally under Swiss law, so she prefers to stay under the radar as much as possible and to reduce the amount of traces she leaves when she uses the internet for her work. For example, she makes sure to hide her home IP address whenever possible, as this could lead authorities (and hackers) directly to her official name and home address.

That's why, when she created her work accounts (email, sex work platforms, social media, etc.) she used [Tor Browser](#), and she only accesses her work accounts through her work phone, or when using the Tor Browser on her computer.

torproject.org



3. COMMUNICATING WITH CLIENTS

1. First Contact

The way new clients usually get in touch with Ava for the first time is through dedicated platforms specifically for advertising sexual 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.

2. 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.

3. 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 in the client's device forever. Unfortunately, not all apps offer the possibility of setting a very short time frame for this. However, if something goes wrong during the meeting, they keep a backup of the messages as proof in case they need to take legal measures.

WhatsApp now has the option to make pictures disappear after they have been opened once (text messages can only disappear after a week). On Telegram, disappearing pictures are only possible in the [secret chats](#). This is very useful for sending erotic content. Ava does not want customers to save their pictures and videos. Ava therefore uses a secret Telegram chat if possible, otherwise disappearing messages on WhatsApp, Signal, Wire or Wickr.

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, images after opening once)

🔥 [Telegram secret chats](#)

🔥 [Signal](#)

🔥 [Wire](#)

🔥 [Wickr](#)

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

support.signal.org/hc/de/articles/360007320771-Verschwindende-Nachrichten-festlegen-und-verwalten

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-



4. ONLINE WORK

1. Videochat

In 2020, when the Covid-19 pandemic hit hard and sex work was banned 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](#). Even more privacy-friendly platforms like Jitsi 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 platforms like [Manyvids](#), where it's more difficult for clients to exploit their content thanks to the protections in place on these platforms. Unfortunately, there is no such thing as absolute protection. After all, nobody can stop a person from taking a picture of their screen with a different device or an old school camera.

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

letagparfait.com/en/wp-content/uploads/2020/12/adult_content_creators.pdf

2. 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 better plan the creation of their contents, Ava followed the tips in this [Guide for Adult Content Creators](#).

Ava tries to use platforms that offer its users the best possible protection against stalking, harassment, [doxing](#) and other threats.

en.wikipedia.org/wiki/Doxing

manyvids.com



2. 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:



Red Umbrella: <https://redumbrella.ch>

- Sex worker friendly
- Icelandic servers
- Free SSL certificate
- WordPress supportg



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 Netherlands-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.





2. An Impressum Without an Official Name

cyon.ch/blog/impressum-Websites

In Switzerland, all websites offering products or services are theoretically subject to a [legal notice requirement](#) (« Impressumspflicht »). This means that anyone who "offers goods, work or services in electronic commerce" must "provide clear and complete information about their identity and contact address, including electronic mail". Violation of the obligation to provide a legal notice can be punished in particular as unfair competition. Ava knows that, for security reasons, they do not want to include their home address in the legal notice. In Switzerland, however, prosecution only takes place upon request - for example by a competitor. As it is very unlikely that they will be reported to the police, Ava has decided to only provide their work name and work email. By having a functioning way to contact them, they can limit the legal risk.

5. 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 debit/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.

[vice.com/en/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x](https://www.vice.com/en/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x)



6. FURTHER RESOURCES



ProCoRe, Network Organization of Counseling Centers for Sex Workers in Switzerland

procore-info.ch/en

Overview and contacts for all local counseling centers for sex workers in Switzerland

procore-info.ch/advice/beratung-fuer-sexarbeitende

LEXI-APP – App with information for sex workers in Switzerland (Google Play, Apple App Store)

play.google.com/store/apps/details?id=ch.renuo.procore&hl=en&gl=US
apps.apple.com/ch/app/lexi-app/id1347841110

A short guide on digital self-defense

digitale-gesellschaft.ch/ratgeber/en/

European Sex Worker Rights Alliance

Digital Rights Projekt

eswalliance.org/digital_rights_area

How to act as a victim or witness of racial profiling

stop-racial-profiling.ch/en/know-your-rights/

Hate Work - Support Sexworkers - ein Interview zu sexarbeit

projet-evasions.org/sexwork_eng

PICTURES



KINK_ANANAS

Pages 3 / 17 / 18 / 20



OIL PRODUCTIONS

@oilproductions
oilproductions.ch
Page 2



FABIENNE BIERI

@lafabphotography
fabiennebieri.com
Pages 9, 12, 21, 22
Pages 4, 14
@thekalisudhra



LA FILLE RENNE

@lafillerenne
lafillerenne.fr
Pages 1, 6, 9, 10, 11, 15, 23



SARAH ZAK

@sarah_likesprettygirls
Sarahzak.com
Pages 7-8





2023

PROJET EVASIONS

PROJET-EVASIONS.ORG

EVASIONS@RISEUP.NET