



# **HANDBUCH ZUR DIGITALEN SICHERHEIT FÜR SEXARBEITENDE**

[projet-evasions.org/chyperguide\\_de](https://projet-evasions.org/chyperguide_de)



**Cypher Sex** ist ein queer-feministisches Kollektiv, das es sich zum Ziel gesetzt hat, LGBTQ\*-Personen, Frauen und Sexarbeiter\*innen bei der Nutzung von Online-Diensten und digitalen Tools durch Workshops, Leitfäden und persönliche Beratung zu unterstützen.

[inventati.org/](https://inventati.org/)



Das **Projet-Evasions** ist eine mehrsprachige anarchistische Initiative, die emanzipatorische Inhalte erstellt und verbreitet. Wenn wir nicht gerade von queeren Sexpartys träume, organisieren wir uns in Netzwerken von glänzende Kompliz\*innen zu Themen die uns inspirieren und betreffen. Tief in uns, unter einer dicken Schicht Glitzer, zittert eine tiefe Feindseligkeit gegenüber jeder Form von Autorität und eine brennende Leidenschaft für die Freiheit... all das verpackt in goldenes und silbernes Schokoladenpapier (natürlich vegan). Papierversionen von diesem Guide können auf unserer Webseite bestellt werden.

[projet-evasions.org/de](https://projet-evasions.org/de)





# INHALTSVERZEICHNIS

## 1. Identity Management

1. Verschiedene Identitäten für verschiedene Vertrauenskreise
2. Einen Pseudonym wählen
3. Takedown-Anträge
4. Ein Handy für jede Identität
5. Avas Tips zu Email-Anbietern
6. Getrennte Email Accounts
7. Sichere Passwörter
8. 2-Faktor-Authentifizierung
9. Avas Online-Konten
10. Konten getrennt halten
11. Gezielte Fotonutzung
12. Nutzungsbedingungen
13. Verschiedene Zahlungsmethoden

## 2. Sichere Verbindungen

1. Öffentlich W-lan Verbindung
2. Anonyme Verbindungen

## 3. Kommunikation mit Kund\*innen

1. Erstkontakt
2. Vorauszahlungen zur Verbesserung der Sicherheit
3. Mit Kund\*innen in Kontakt bleiben

## 4. Online Arbeit

1. Webcam
2. Verkauf von Bildern und Videos
3. Avas Webs
4. Impressumspflicht

## 5. Umgang mit Kund\*innen

## 6. Weitere Ressourcen



# AVA TARNUNG

Ava Tarnung ist eine gender-fluide Person, die u.a. als Escort arbeitet. Ava benutzt verschiedene Pronomen, für diesen Guide hat sie sich für Sie-Pronomen entschieden. Ihre Persönlichkeit und Identität ändern sich aber stark je nach Laune und Situation. Sie hat gelernt, dieses Talent zu nutzen, um sich für ihre Kund\*innen sowie für ihre Online-Aktivitäten als unterschiedliche Personen mit unterschiedlichen Persönlichkeiten auszugeben. Sie ist der Überzeugung, dass die Fähigkeit, sich online und offline als unterschiedliche Personen auszugeben einer der Schlüssel ist, um sich in ihrem Leben vor Stalkern und Anfeindungen zu schützen und ihr facettenreiches Leben zu geniessen.

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

Ava ist ein Nerd. Nach einigen Jahren der Erforschung des Internets hat sie eine Menge darüber gelernt, wie Technologie und Online-Plattformen funktionieren. In Verbindung mit ihrem engen Netzwerk in der lokalen Sexarbeits-Community, hilft ihr das, sich gegen die vielen Unsicherheiten, die Sexarbeitende ausgesetzt sein können, zu schützen.

Um sich zu schützen, verwendet sie bei der Arbeit nicht ihren Passnamen, sondern ein Pseudonym (oder Arbeitspseudonym). Ava hat einen Schweizer Pass und lebt und arbeitet in Zürich als Escort. Sie muss sich demnach nicht registrieren. Je nach Kanton und Form der Sexarbeit sind die Registrierungsprozesse jedoch unterschiedlich. Menschen, die mit einem EU Pass in die Schweiz kommen um im Sexgewerbe zu arbeiten, müssen in allen Kantonen Melde- oder Bewilligungsverfahren durchlaufen. Sexarbeitende können sich [bei den lokalen Beratungsstellen](#) über die in ihrem Kanton geltende Regulierungen und Registrierungsprozesse informieren. Ava empfiehlt Sexarbeitenden, bei der Arbeit nie den Namen zu verwenden, mit dem sie sich registriert haben.



# 1. IDENTITY MANAGEMENT

Um sich vor Stalking oder Outing zu schützen, hat Ava eine völlig andere Arbeitsidentität geschaffen, die weder mit ihrer offiziellen Identität noch mit den Identitäten, die sie mit ihrer Familie und ihren Freund\*innen verwendet, in Verbindung gebracht werden kann.

Hier sind die Dinge, die sie bedacht hat, um ihre Arbeitsidentität und Online-Personen zu verwalten:

## 1. Verschiedene Identitäten für verschiedene Vertrauenskreise

Ava hat sich ihren engsten Freund\*innen gegenüber als Sexarbeiter\*in geoutet, nicht aber gegenüber ihrer Herkunftsfamilie oder ihren Nachbar\*innen. Und sie möchte auch, dass das so bleibt. Es gibt zwar ein paar Menschen, mit denen sie über ihre Arbeit sprechen kann, aber das ist eher die Ausnahme. In der Regel spricht sie nicht mit Menschen darüber, wie sie ihren Lebensunterhalt verdient – ausser sie ist sich sicher, dass sie ihnen voll und ganz vertrauen kann. Sie vermeidet es, mit Menschen, die sie in konventionellen Situationen trifft, über ihre Arbeit zu sprechen.

Aus diesem Grund ordnet Ava ihre Kommunikationskanäle und Social-Media-Konten nach Vertrauensstufen ein, die mit ihren verschiedenen Lebensbereichen zusammenhängen. Für jeden dieser Bereiche hat sie eine eigene Identität:

-  Bürokratie (Steuern, Bank...)
-  Familie
-  Neue Bekanntschaften
-  Arbeit
-  Enge Freund\*innen

Durch die Trennung dieser Bereiche kann sie die Menge an Informationen begrenzen, die sie an Personen weitergibt, denen sie nicht vertraut.

## 2. Einen Pseudonym (Arbeitsnamen) wählen

Wie viele andere Sexarbeiter\*innen auch hat Ava einen Arbeitsnamen gewählt, der cool klingt. Auf kommerziellen sozialen Netzwerken lautet ihr Benutzername Ava "Tarnung" Adam. Sie hat ihrem Arbeitsnamen einen realistischen Nachnamen hinzugefügt. Obwohl er langweilig klingt, gibt es dafür einen wichtigen Grund.



Einige soziale Netzwerke (wie Facebook) haben Richtlinien zu Namensangaben. Diese besagen, dass Nutzer\*innen ihre echten Namen verwenden müssen, anstatt sich so zu identifizieren, wie sie es möchten. Dies dürfen die Plattformen zum Teil auch kontrollieren. Viele Plattformen verlangen für die Registrierung sowohl einen Vor- als auch einen Nachnamen (oder einen Namen, der keine umgangssprachlichen Ausdrücke oder Schimpfwörter enthält). Daher hat Ava ihrem Arbeitsnamen einen gewöhnlichen Nachnamen hinzugefügt. Letztendlich schützt sie das nicht vor einer "Echtnamens"-Kontrolle, aber automatisierte Kontrollen werden ihren Namen nicht sofort als potenziellen Verstoss erkennen. So hofft sie darauf, dass sie ihr Konto für einige Zeit behalten kann.

Nachdem sie sich für einen Namen, einen Nachnamen und einen Benutzernamen für ihre Arbeitspersönlichkeit entschieden hat, recherchierte Ava auch noch gründlich auf verschiedenen Sexarbeitsplattformen um sicherzugehen, dass dieser Name nicht schon von ein\*er anderen Sexarbeiter\*in verwendet wird (oder zumindest nicht von einer Person in ihrer Nähe).



### 3. Takedown-Anträge (Anträge zum Entfernen von Inhalten)

Als Ava einen neuen Namen wählte, beschloss sie auch, alle Spuren zu beseitigen, die ihr Gesicht mit ihrem Passnamen in Verbindung bringen könnten. Sie führt daher eine Suche nach [diesem Leitfaden](#) durch. In ihrem früheren Leben hat sie nicht versucht, ihre Privatsphäre zu schützen und hat nicht besonders darauf geachtet, ob Fotos von ihr online gestellt wurden. Daher war sie etwas nervös, was sie bei ihrer Suche finden könnte. Sie hat auch Angst vor ihrer eigenen Reaktion wenn sie sieht, was es im Internet alles von und über sie gibt. Um Unterstützung zu bekommen, bittet sie eine gute Freundin, ihr bei der Suche nach Spuren ihres alten Ichs Gesellschaft zu leisten.

Was sie fand war nicht besonders überraschend. Dennoch wollte sie alle Ergebnisse verbergen, die ihr Gesicht mit ihrem Passnamen in Verbindung brachten, da sie diesen nicht mehr öffentlich nutzt.

Sie erstellt zunächst eine Liste aller Bilder, Videos und persönlicher Informationen, die sie löschen will. Dann macht sie von all diesen Inhalten Screenshots und befolgt die Anweisungen in [diesem Leitfaden zur Dokumentation von Online-Belästigung](#).

Auf Google gibt es die Möglichkeit, einen Antrag auf Entfernung von Inhalten aus den Suchergebnissen zu stellen. In der EU gibt es das Recht, Ergebnisse mit dem eigenen Namen entfernen zu lassen. In der Schweiz ist der Schutz weniger streng, dennoch lohnt es sich, den Antrag zu stellen. Als ersten Schritt füllte Ava also das [Google-Formular](#) zur Beantragung der Entfernung persönlicher Daten aus.

Dann füllt sie weitere Formulare aus, um Bilder ihres früheren Ichs von [Facebook](#) und [Twitter](#) entfernen zu lassen. Sie befolgt Anweisungen wie die des Takedown-Leitfadens auf der Website „[Without My Consent](#)“, um intime Bilder von anderen Plattformen und Websites löschen zu lassen. Es brauchte ein wenig Geduld, da die Antworten nicht sofort erfolgten, aber die Bilder und andere Informationen wurden schließlich entfernt.





## 4. Ein Handy für jede Identität

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

Ava möchte sicher sein, dass ihre berufliche Identität niemals mit ihrer persönlichen Identität in Verbindung gebracht werden kann - weder von Stalkern, noch von Nachbar\*innen, oder gar von Behörden. Ava weiss, dass Telefone [mehrere Schwachstellen haben](#), die es leichter machen, sie zu verfolgen. Um auf Nummer sicher zu gehen, kauft sie als erstes (nachdem sie sich für einen Arbeitsnamen entschieden hat) für ihre neue Identität ein neues, billiges Telefon mit einer neuen Prepaid-SIM-Karte. Obwohl SIM-Karten in der Schweiz normalerweise auf den Namen des\*der Nutzer\*in registriert werden sollten, versucht Ava, eine vorregistrierte SIM-Karte zu finden. Es gibt auch die Möglichkeit, SIM-Karten im Ausland zu kaufen und in der Schweiz zu nutzen. Ava hat all ihre Online-Arbeitskonten mit der neuen Telefonnummer registriert und greift auf ihre Online-Arbeitskonten nur mit ihrem Arbeitstelefon zu. Wenn sie zu einem\*r Kund\*in geht, nimmt sie nur dieses Gerät mit und lässt ihr privates Telefon zuhause.

## 5. Avas Tips zu Email-Anbietern

Als sie sich auf der Suche nach einem E-Mail-Anbieter machte, der für ihre Arbeit geeignet ist, wusste Ava bereits, dass es keine komplett sicheren E-Mails gibt. E-Mails sind standardmässig nicht verschlüsselt. Wenn eine Person auf den Server zugreifen kann, auf denen die Nachrichten gespeichert sind (oft auf mehreren Rechnern, die sowohl dem E-Mail-Anbieter des\*der Absenders\*in als auch dem des\*der Empfängers\*in gehören), kann sie alles lesen. Das gilt für Ermittler\*innen, aber auch für eine\*n beliebige\*n Systemadministrator\*in, die\*der Zugang zu diesen Rechnern hat.

Ava entschied, dass sie ihre E-Mails nicht für sensible Inhalte verwenden würde. Trotzdem wollte sie sichergehen, dass ihre E-Mails während der Übertragung nicht aufgemacht werden können. Daher wählte sie nur E-Mail-Anbieter aus, die eine HTTPS/TLS-Verschlüsselung verwenden. So ist die Verbindung zwischen ihrem Computer und den Servern verschlüsselt. Sie kontrollierte, ob die TLS-Verschlüsselung tatsächlich funktionierte, indem sie einige Anbieter auf [dieser Webseite testete](#). Hier ist [die Liste der E-Mail-Anbieter](#), die Ava ausgewählt hat.

checktls.com

prxbx.com/email



Um von ihren Kund\*innen kontaktiert zu werden, hat Ava ein Tutanota-Konto. Tutanota verschlüsselt ihre Nachrichten auf dem gesamten Weg mit anderen Tutanota-Nutzer\*innen, sodass die Nachrichten auf den Servern nicht lesbar sind. Allerdings hält Ava diese Verschlüsselung für nicht sicher genug, da E-Mails von und an Personen ohne Tutanota-Account nicht verschlüsselt werden. Alle selbst definierten "sicheren E-Mail-Dienste" wie Tutanota, Protonmail, etc. haben dasselbe System. Sie bieten nur dann eine starke Verschlüsselung, wenn die Emails unter Nutzenden desselben Dienstes verschickt werden (z. B. Tutanota an Tutanota). Ava hält diese Plattformen also für in etwa gleich sicher wie Messenger-Apps, bei denen Ihre Nachrichten nur dann sicher sind, wenn Sie sie mit anderen Personen innerhalb derselben App schreibt.

## 6. Getrennte Email Accounts

Um ihre Identitäten wirklich voneinander getrennt zu halten, hat Ava für jede ihrer Identitäten ein eigenes E-Mail-Konto eingerichtet. Je nach Bedarf nutzt sie dann die entsprechenden E-Mail Adressen für verschiedene Online-Konten. Manchmal braucht Ava nur einmalig eine E-Mail Adresse, beispielsweise um sich bei einem Dienst anzumelden. Dann erstellt sie ein temporäres Konto mit einer Wegwerf-E-Mail-Adresse, wie beispielsweise von [Guerrilla Mail](https://guerrillamail.com) oder [anonbox](https://anonbox.net/index.de.html).

guerrillamail.com

anonbox.net/index.de.html

## 7. Sichere Passwörter

Um sicherzugehen, dass ihre Konten nicht gehackt werden können, verwendet Ava für jedes ihrer Konten sichere sowie unterschiedliche Passwörter. Sie generiert diese Passwörter mit einem Offline-Passwortmanager (z.B. [KeePassXC](https://keepassxc.org)) und stellt sie aus zufälligen Abfolgen von Klein- und Grossbuchstaben, Zahlen und Symbolen zusammen. Weil sie alle Passwörter im Passwortmanager gespeichert hat, muss sie sich nicht alle komplizierten Passwörter merken.

Die einzigen Passwörter- und Sicherheitsfragen, die Ava sich merken muss, sind die, die sie zum Entsperren ihrer Geräte und des Passwortmanagers braucht. Damit sie sich diese leicht merken kann, hat sie diese Passwörter mit der [Diceware-Methode](https://www.diceware.org/) erstellt.

keepassxc.org

eff.org/dice





## 8. 2-Faktor-Authentifizierung

Ava weiss, dass es unterschiedliche Wege gibt, selbst das stärkste Passwort zu stehlen, beispielsweise durch [Phishing-Angriffe](#). Sie möchte auf jeden Fall verhindern, dass jemensch unbefugt auf eines ihrer Konten zugreifen kann. Wenn es möglich ist, richtet sie deshalb immer in den Sicherheitseinstellungen ihrer Konten eine Zwei-Faktor-Authentifizierung ein. Um den zweiten Faktor zu schaffen, hat sie einen Code-Generator (wie [FreeOTP](#)) auf ihrem persönlichen Telefon installiert. Jedes Mal, wenn sie sich bei einem ihrer Online-Konten anmeldet, gibt sie zuerst das Passwort ein und dann den Code, der von der App generiert wurde. Dieser kann nicht auf die gleiche Weise gestohlen werden wie das Passwort. Da jede Online-Plattform die Zwei-Faktor-Authentifizierung anders einrichtet, empfiehlt Ava die Anweisungen zu verschiedenen Plattformen auf dem [Electronic Frontier Foundation](#) zur Zwei-Faktor-Authentifizierung zu lesen.

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-

## 9. Avas Online-Konten (Accounts)

Um ihre Dienstleistungen anzubieten, nutzt Ava sowohl gängige soziale Netzwerke als auch Seiten spezifisch für sexuelle Dienstleistungen. Auf fast all diesen Webseiten hat sie unterschiedliche Konten, je nachdem mit wem sie kommuniziert. Sie verwendet für jede Kontaktgruppe, zum Beispiel Familie, Freund\*innen oder Liebhaber\*innen, unterschiedliche Konten. Sie hat folgende Konten :

| Plattform     | Kontakte               | Echter oder erfundener Name    | Vertrauensniveau in Kontakten | Erotische Inhalte | Wegwerfbares Konto <sup>1</sup> |
|---------------|------------------------|--------------------------------|-------------------------------|-------------------|---------------------------------|
| Facebook      | Freund*innen           | Realisitscher erfundene Name 1 | Hoch                          | Ja                | Ja                              |
| Facebook      | Famillie               | Echter Name                    | Mittel                        | Nein              | Nein                            |
| Instagram     | Freund*innen           | Realisitscher erfundene Name 2 | Hoch                          | Ja                | Ja                              |
| Instagram     | Arbeit                 | Arbeitsname                    | Niedrig                       | Natürlich         | Ja                              |
| Twitter       | Öffentlich             | Arbeitsname                    | Niedrig                       | Ja                | Ja                              |
| Fetlife       | Freund-Liebhaber*innen | Realisitscher erfundene Name 2 | Hoch                          | Natürlich         | Nein                            |
| Callme toplay | Arbeit                 | Arbeitsname                    | Niedrig                       | Natürlich         | Nein                            |
| La Compagnie  | Arbeit                 | Arbeitsname                    | Niedrig                       | Natürlich         | Nein                            |
| And6          | Arbeit                 | Arbeitsname                    | Niedrig                       | Natürlich         | Nein                            |
| Xdate         | Arbeit                 | Arbeitsname                    | Niedrig                       | Natürlich         | Nein                            |
| Tinder        | Arbeit                 | Arbeitsname                    | Niedrig                       | Ja                | Nein                            |
| Tryst.link    | Arbeit                 | Arbeitsname                    | Niedrig                       | Natürlich         | Nein                            |

Alle Konten bei Anbietern, die entweder die Verwendung offizieller Namen vorschreiben, oder das Teilen sexueller Inhalte einschränken (siehe Kapitel „Nutzungsbedingungen“), betrachtet Ava als „wegwerfbar“. Obwohl sie einen realistischen Namen verwendet, um zu vermeiden, dass sie von Facebook Echtnamens-Scans entdeckt wird, weiss sie, dass ihr Konto irgendwann gesperrt werden könnte und sie einen Ausweis vorzeigen müsste, um es wiederherzustellen.

Um ihre Konten getrennt zu halten, vermeidet sie es, sie mit ihrer echten Identität zu verknüpfen. Ausnahmen macht sie nur mit Konten, über die sie mit Menschen kommuniziert, die ihre offizielle Identität eh schon kennen (zum Beispiel mit ihrer Familie oder bei ihrer Bank). Dort hat sie von vorneherein beschlossen, ihre offizielle Identität zu verwenden.

1) Als „wegwerfbar“ Konto bezeichnet Ava Konten, deren Erhalt sie sich nicht sicher sein kann. Das heisst, sie rechnet damit, dass das Konto evtl. gelöscht wird.



Zusätzlich hat sie Konten auf Seiten, die explizit sexarbeitsfreundlich sind (z.B. [Tryst](#)) oder auf kommerziellen Sexarbeitsplattformen. Diese Konten erachtet sie als stabiler als diejenigen auf herkömmlichen sozialen Medien. Dort sind ihre Konten also immer auffindbar. Sie sagt ihren Kontakten, dass sie sie dort finden können, falls ihre anderen Konten plötzlich gelöscht oder gesperrt werden. Doch auch hier hält Ava es nicht für selbstverständlich, dass diese Konten lange bestehen bleiben. Deshalb erstellt sie auf ihrem lokalen Rechner sowie auf einer externen Festplatte eine Kopie von allen Inhalten, die sie behalten möchte.

## 10. Konten getrennt halten

Um ihre Konten getrennt zu halten und sicherzugehen, dass sie nicht miteinander in Verbindung gebracht werden können, hat Ava folgende Methoden entwickelt:

- 🔥 Sie verwaltet ihre Arbeitskonten nur von ihrem Arbeitshandy aus.
- 🔥 Sie folgt nicht denselben Personen von Konten, die mit unterschiedlichen Identitäten verbunden sind.
- 🔥 Sie achtet darauf, dass sie sich nicht selbst mit ihren unterschiedlichen Konten folgt oder „anfreundet“ und, dass sie nicht mit verschiedenen Identitäten die gleichen Inhalte postet.
- 🔥 Ava weiss, dass die meisten Sozialen Medien ihren Standort anzeigen können. Deshalb deaktiviert sie die Geolokalisierung in ihren Apps. Sie aktiviert das GPS in ihren Geräten nur, wenn sie es wirklich braucht.
- 🔥 Ava weiss auch, dass viele Apps und Kameras Metadaten in den Fotos einbetten. Die Fotos können also unter anderem Datum, Uhrzeit und den Standort des Fotos enthalten. Diese Metadaten können auch in den Bildern und Videos enthalten sein, die sie online teilt. Deshalb stellt sie immer sicher, dass die Geolokalisierung deaktiviert ist, wenn sie Fotos und Videos aufnimmt. Auch verwendet Ava [MAT](#), eine gute Software, um Metadaten aus Bildern und Dokumenten zu entfernen.



## 11. Gezielte Fotonutzung

Am wichtigsten ist, dass Ava niemals persönliche Fotos für die Arbeit verwendet. Sie weiss, dass viele Suchmaschinen eine Funktion zur umgekehrten Bildsuche anbieten. Das heisst, dass alle Seiten entdeckt werden können, auf denen das gleiche Bild veröffentlicht wurde. Um zu vermeiden, dass jemand ihre berufliche Identität durch eine umgekehrte Bildersuche mit anderen Identitäten in Verbindung bringen kann, verwendet sie auf ihren beruflichen Profilen oder bei der Kommunikation mit ihren Kund\*innen niemals Bilder, die sie auf anderen Konten veröffentlicht hat.

## 12. Nutzungsbedingungen

Wenn Ava eine neue Plattform oder einen neuen Anbieter verwenden möchte, prüft sie als Erstes die Datenschutzbestimmungen und die Nutzungsbedingungen. Es gibt viele Dienstleister (z.B. soziale Medien, Website-Hosting Dienste, Zahlungstools), die "nicht jugendfreie Inhalte" ausdrücklich verbieten. Das ist extrem breit und vage gehalten und kann alles von Pornografie über Vibratoren bis hin zu erotischen Romanen bedeuten. Ava meidet in der Regel diese Dienstleister oder betrachtet jedes Konto, das sie bei ihnen hat, als „wegwerfbar“. Im Allgemeinen hält Ava nach Plattformen Ausschau, die "nicht jugendfreie" (sprich: sexuelle) Inhalte erlauben, sowie andere Sicherheitsfunktionen wie die Zwei-Faktor-Authentifizierung, Zahlungen in Bitcoin oder andere Methoden zum Schutz der Anonymität bieten.

## 13. Verschiedene Zahlungsmethoden

Für Internet-Einkäufe, die mit ihrer Arbeit zu tun haben (z. B. für den Kauf ihres Website-Domains) vermeidet Ava Online-Zahlungsmethoden, die mit ihrer echten Identität verbunden sind. Um zu vermeiden, dass ihr echter Name mit ihrer Arbeitsidentität in Verbindung gebracht werden kann, verwendet sie Prepaid Geschenk- oder Kreditkarten, die sie in Supermärkten oder an Kiosken kauft (z. B. [Paysafe](#), [Amazon-Geschenkkarten](#) oder [OK.-Kreditkarten](#)). Manchmal bittet sie auch ihre Kund\*innen, solche für sie zu kaufen.

Für ihre Bezahlung nimmt Ava meistens Bargeld entgegen, da dies die sicherste Methode ist und am meisten Anonymität gewährt.

Eine weitere Option, die Ava in Betracht gezogen hat, ist die Einrichtung eines TransferWise-Geschäftskontos, das die Möglichkeit bietet, [Geld über eine E-Mail-Adresse](#) zu senden. Manchmal kaufen ihre Kund\*innen ihr auch Geschenke über eine [Wunschliste](#) (Wishlist).

Zur Zeit wird eine neue App Namens „[Horizontl](#)“ entwickelt, die eine sicherere Lösung für Zahlungen für sexuelle Dienstleistungen bieten soll. Da die App aber noch nicht fertig ist, kann Ava noch nichts darüber sagen, wie nützlich sie sein wird – aber sie behält es im Auge.

kkiosk.ch/de/products/detail/?

paysafecard.co

wishlist.com/

amazon.de/Amazon-De-Geschenkkarten-lm-Stationaeren-Handel/b?currency=EUR&ie=UTF8&language=en\_GB&node=5362203031

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

horizontl.co/get-involved



Um den Kund\*innen nicht zu viel Macht über ihre digitale Präsenz zu geben und um sicherzugehen, dass niemand sie über ihre eigenen Geräte ausspionieren kann, lässt sie ihre Kunden nie für ihre Website oder andere Online-Dienste bezahlen und nimmt keine Geräte als Geschenke an.





# 2. SICHERE VERBINDUNGEN

## 1. öffentliche W-Lan Verbindung

Ava versucht - wenn möglich - unsichere Internetverbindungen wie kostenloses WLAN in Cafés, Bahnhöfen oder Hotels zu vermeiden. Sie weiss, dass die Besitzer\*innen dieser Netzwerke, oder sogar Hacker, sie während des Nutzens dieser Netzwerke ausspionieren können. Daher zieht sie es vor, die mobilen Daten ihres Telefons zu verwenden, beziehungsweise Arbeit mit sensiblen Inhalten zuhause über ihr W-Lan zu erledigen.

Dennoch ist es manchmal einfacher und billiger, öffentliche Verbindungen zu nutzen. Für diese Fälle hat Ava eine Lösung: Sie hat ein VPN auf ihrem Telefon und Computer installiert und aktiviert es immer, bevor sie gratis W-Lan-Verbindungen nutzt.

Hier ist eine [Liste von VPNs](#), die Ava für zuverlässig hält. Sie teilt die Liste mit ihren Freund\*innen, wenn sie nach Empfehlungen gefragt wird. Am Ende hat sie sich für [Riseup VPN](#) entschieden. Sie hält Riseup VPN für besonders zuverlässig, da es von einem autonomen Kollektiv und nicht von einem Unternehmen betrieben wird.

## 2. Anonyme Verbindungen

Avas Freund\*in und Kolleg\*in Anne Onimas ist aus einem EU Land in die Schweiz gekommen, um in der Sexarbeit tätig zu sein. Anne hat sich aber dafür entschieden, keine Arbeitsbewilligung zu beantragen und sich nicht als Sexarbeiter\*in zu registrieren. Das bedeutet, dass sie nach dem schweizerischen Gesetz illegal arbeitet. Deshalb zieht sie es vor, so weit wie möglich unter dem Radar zu bleiben und so wenig Spuren wie möglich zu hinterlassen, wenn sie das Internet für ihre Arbeit nutzt. Sie achtet beispielsweise darauf, die IP-Adresse ihres Heimanschlusses so gut es geht zu verbergen, da die Polizei (sowie Hacker) die IP-Adresse direkt zu ihrem offiziellen Namen und ihrer Adresse zurückführen könnten.

Deshalb hat sie bei der Erstellung ihrer Arbeitskonten (E-Mail, Sexarbeitsplattformen, soziale Medien usw.) den [Tor-Browser](#) verwendet. Sie greift auf ihre Arbeitskonten nur über ihr Arbeitstelefon oder über den Tor-Browser auf ihrem Computer zu.

torproject.org/de

riseup.net/de/vpn

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



# 3. KOMMUNIKATION MIT KUND\*INNEN

## 1. Erstkontakt

Neue Kund\*innen nehmen in der Regel über spezielle Plattformen für das Bewerben sexueller Dienstleistungen mit Ava Kontakt auf. Auf all diesen Plattformen hat Ava sich mit einer E-Mail-Adresse registriert, die sie nur zur Überprüfung der Anfragen potenzieller Neukund\*innen verwendet. So wird ihr normales Postfach nicht von eingehenden Nachrichten und Spam überflutet. Oft fragen potenzielle Neukund\*innen nach weiteren Bildern. Ava hat einen Ordner mit Bildern, die sie genau zu diesem Zweck erstellt hat.

## 2. Vorauszahlungen zur Verbesserung der Sicherheit

Avas Freund\*in Anne Onimas ist nicht als Sexarbeiter\*in registriert und bittet Kund\*innen, die sie zum ersten Mal trifft, immer um eine kleine Vorauszahlung in Form einer Amazon-Geschenkkarte. So kann sie sichergehen, dass es sich um seriöse Kund\*innen und nicht um Polizist\*innen handelt, da Polizist\*innen in der Regel kein Budget für so etwas haben.

## 3. Mit Kund\*innen in Kontakt bleiben

Sobald sie den Erstkontakt mit einem neuen Kunden hergestellt hat, bittet Ava ihn, zu einem anderen Kommunikationstool wie WhatsApp, Telegram, [Signal](#), [Wire](#) oder [Wickr](#) zu wechseln.

Für all diese Instant-Messaging-Apps hat Ava ein spezielles Konto mit ihrer beruflichen Telefonnummer oder (wenn möglich) nur mit ihrer beruflichen E-Mail Adresse eingerichtet. Auf diese greift sie nur über ihr Arbeitstelefon oder über einen speziellen Browser auf ihrem Computer zu.

Wenn sie Bilder oder andere sensible Informationen an einen Kunden sendet, legt sie in der Konversation die Option "verschwindende Nachrichten" fest, damit diese Informationen nicht für immer auf dem Gerät des Kunden gespeichert bleiben. Leider bieten nicht alle Apps die Möglichkeit, einen sehr kurzen Zeitrahmen für Nachrichten einzustellen. Bei WhatsApp gibt es neu die Option, Bilder nach einmaliger Öffnung verschwinden zu lassen (Textnachrichten können erst nach einer Woche verschwinden). Auf Telegram sind verschwindende Bilder nur in den [geheimen „secret“ Chats](#) möglich. Dies ist sehr nützlich um erotische Inhalte zu versenden. Denn Ava möchte nicht, dass die Kund\*innen ihre Bilder und Videos speichern. Ava verwendet deshalb wenn möglich einen geheimen Telegram-Chat,

oder verschwindende Nachrichten auf Whatsapp, Signal, Wire oder Wickr.

Hier sind Anweisungen, die Ava gefunden hat, um das Verschwinden von Nachrichten in den verschiedenen Messenger-Apps einzustellen:

🔥 [WhatsApp](#) (Nachrichten verschwinden nach einer Woche, Bild-Option nach einmaliger Öffnung)

🔥 [Geheime Telegram Chats](#)

🔥 [Signal](#)

🔥 [Wire](#)

🔥 [Wickr](#)

[faq.whatsapp.com/android/chats/how-to-turn-disappearing-messages-on-or-off](https://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](https://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-](https://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-](https://support.wickr.com/hc/en-us/articles/115007397548-Auto-Destruction-Expiration-and-Burn-on-read-BOR-)





# 4. ONLINE ARBEITEN

## 1. Webcam

Als während der Covid-Pandemie die physische Sexarbeit verboten wurde, begannen Ava und ihre Kolleg\*innen nach Möglichkeiten zu suchen, online zu arbeiten. Ava begann mit der Webcam-Arbeit und bot ihren Kund\*innen so Dienstleistungen an.

Was sie anfangs am meisten beunruhigte, war das Risiko, dass ihrer Kund\*innen ihre Sitzungen aufzeichnen und online weiterverkaufen könnten. Bevor sie mit der Webcam-Arbeit begann, stellte sie deshalb einige Nachforschungen an. Sie schloss schnell die meisten Videokonferenz-Tools wie Skype aus, da diese ein [schlechtes Repertoire haben, was Datenschutz angeht](#). Doch auch datenschutzfreundlichere Plattformen wie Jitsi können Nutzer\*innen nicht daran hindern, Screenshots zu machen oder Videoanrufe aufzuzeichnen.

Schliesslich beschloss Ava, Konten auf Plattformen einzurichten, die speziell für die Cam-Arbeit geschaffen wurden. Denn diese Plattformen schützen Sexarbeiter\*innen vor möglichen Risiken, beispielsweise Kund\*innen, die Screenshots machen. Sie führt ihre Online-Sessions jetzt auf Plattformen wie [Manyvids](#) wo dank der Schutzmassnahmen auf diesen Plattformen das Risiko kleiner ist, dass ihre Kund\*innen ihre Inhalte ausnutzen können. Schließlich kann kein Mensch eine Person davon abhalten, mit einem anderen Gerät oder einem mit einer einfachen Kamera ein Bild von ihrem Bildschirm zu machen.

manyvids.com

foundation.mozilla.org/en/privacynotincluded/

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

## 2. Verkauf von Bildern und Videos

Ava verdient auch etwas Geld durch den Verkauf von Videos und Bildern im Internet. Um sicher zu gehen, dass niemand diese Inhalte ohne ihrer Erlaubnis weiterverkauft, überzieht sie alle Dateien mit einem Wasserzeichen.

Um die Erstellung ihrer Inhalte besser zu planen, befolgt Ava die Tipps in diesem Leitfaden für „[Adult Content Creators](#)“.

Ava versucht Plattformen zu verwenden, die ihren Nutzer\*innen möglichst guten Schutz bieten vor Stalking, Belästigung, Doxxing und anderen Risiken.



## 2. Ava Website

Ava hat auch eine eigene Website. Sie möchte einen Ort haben, wo sie ihre Dienstleistungen anbieten kann, der ihr gehört und den sie kontrolliert.

Als sie beschloss, eine Domain für ihre Website zu kaufen, suchte sie nach Anbietern, die Datenschutz im Basispaket enthielten. Aber dann fand sie eine noch bessere Option, auch wenn diese etwas teurer war. Sie registrierte ihre Domain bei dem anonymen Domainnamenanbieter [Njalla](#), wo eine verschlüsselte anonyme Anfrage zur Registrierung einer Domain möglich ist.

Avas Website wird von einem Provider gehostet, der von Sexarbeitenden für Sexarbeitende betrieben wird und den sie in der folgenden Liste von Hosting-Providern gefunden hat. Diese Liste enthält Hosting-Provider, deren Sitz nicht in den USA sind und die deshalb nicht verpflichtet sind, das amerikanische Gesetzespaket [SESTA/FOSTA](#) durchzusetzen, und die keine Praktiken anwenden, die Sexarbeitenden schaden können:



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

Sexarbeitsfreundlich

Isländischer Server

Kostenloses SSL-Zertifikat

Wordpress-Unterstützung



Orange Website: <https://www.orangewebsite.com>

Anonyme Anmeldung (nur per E-Mail)

Keine Protokollierung

2-Faktor-Authentifizierung

100% grüne Energie



Abelohost: <https://abelohost.com>

Offshore"- und niederländische Serveroptionen

Niederländische Gerichtsbarkeit

Umfassende Nutzungsrichtlinien

Kostenlose Website-Migration (mit dem Einjahresplan)

WordPress-Unterstützung

Akzeptiert Bitcoin

Ava weiss, wie wichtig Anonymität für ihre eigene Sicherheit ist. Aber sie möchte auch, dass ihre Kund\*innen anonym bleiben, wenn sie ihre Website besuchen. Daher hat sie ihren Server so eingestellt, dass so wenig Protokolle wie möglich gespeichert werden. Ausserdem hat sie dafür gesorgt, dass ihre Website über das Tor-Netzwerk zugänglich ist.



## 2. Impressumspflicht

In der Schweiz gilt für alle Webseiten, über die Produkte oder Dienstleistungen angeboten werden, eine [Impressumspflicht](#). Das bedeutet: wer «Waren, Werke oder Leistungen im elektronischen Geschäftsverkehr anbietet», muss «klare und vollständige Angaben über Identität und Kontaktadresse einschliesslich derjenigen der elektronischen Post machen». Die Verletzung der Impressumspflicht kann insbesondere als unlauterer Wettbewerb bestraft werden.

Ava weiss, dass sie aus Sicherheitsgründen auf keinen Fall ihre Heim-Adresse in der Impressumspflicht angeben möchte. In der Schweiz erfolgt eine Strafverfolgung jedoch nur auf Antrag – beispielsweise durch ein\*en Konkurrent\*in. Da eine Anzeige also sehr unwahrscheinlich ist, hat Ava beschlossen, lediglich ihren Arbeitsnamen und ihre Arbeits-Email anzugeben. Indem es einen funktionierenden Weg gibt, mit ihr Kontakt aufzunehmen, kann sie das rechtliche Risiko in Grenzen halten.



# 5. UMGANG MIT KUND\*INNEN

Zu guter Letzt hat Ava noch ein paar Regeln im Umgang mit Kund\*innen. Diese nutzt Ava, damit die Kund\*innen keine Chance haben, sie zu kontrollieren, sollten sie sich als Stalker\*in oder Schlimmeres entpuppt.

Wenn sie mit Kund\*innen an öffentliche Orte geht, wo andere Menschen sie sehen können, benutzen sie niemals ihre Kreditkarte. Wenn eine Karte benötigt wird, lässt sie immer ihre Kund\*innen für sie bezahlen.

Ava weiss, dass es billig und einfach ist, ein Smartphone oder ein anderes elektronisches Gerät mit einem [Spionage- oder Trackingprogramm](#) zu infizieren. Deshalb behält Ava ihr Telefon immer bei sich und lässt es nie unbeaufsichtigt rumliegen. Sie nimmt niemals Smartphones oder andere elektronische Geräte als Geschenke von Kund\*innen an - oder sie entsorgt die Geräte so schnell wie möglich. Und da Vorsicht nie genug ist, hat sie all ihre Geräte mit starken Passwörtern geschützt, so dass selbst wenn sie sie verliert oder irgendwo liegen lässt, niemand darauf zugreifen kann.

vice.com/en/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-



# 6. WEITERE RESSOURCEN



ProCoRe, Netzwerk zur  
Interessensvertretung von  
Sexarbeitenden in der Schweiz

[procore-info.ch](http://procore-info.ch)

Überblick und Kontaktangaben  
aller lokalen Beratungsstellen  
für Sexarbeitende in der Schweiz

[procore-info.ch/advice/beratung-fuer-](http://procore-info.ch/advice/beratung-fuer-)

LEXI-APP – App mit Infos für  
Sexarbeitende in der Schweiz  
(Google Play, Apple App Store)

[play.google.com/store/apps/details?  
id=ch.renuo.procore&hl=en&gl=US](https://play.google.com/store/apps/details?id=ch.renuo.procore&hl=en&gl=US)

[apps.apple.com/ch/app/lexi-app/](https://apps.apple.com/ch/app/lexi-app/)

Ratgeber zur digitalen Sicherheit  
der digitalen Gesellschaft  
Schweiz

[digitale-gesellschaft.ch/ratgeber/#e-mails](https://digitale-gesellschaft.ch/ratgeber/#e-mails)

European Sex Worker Rights  
Alliance  
Digital Rights Projekt

[eswalliance.org/digital\\_rights\\_area](https://eswalliance.org/digital_rights_area)

Was tun als Opfer oder Zeug\*in  
von Racial Profiling - Leitfaden

[stop-racial-profiling.ch/de/know-your-rights/](https://stop-racial-profiling.ch/de/know-your-rights/)

Hate Work - Support  
Sexworkers - ein Interview zu  
sexarbeit

[projet-evasions.org/sexwork\\_de](https://projet-evasions.org/sexwork_de)

# FOTOGRAFIE



**KINK\_ANANAS**

Seite 3 / 17 / 18 / 20



**OIL PRODUCTIONS**

@oilproductions  
oilproductions.ch  
Seite 2



**FABIENNE BIERI**

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



**LA FILLE RENNE**

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



**SARAH ZAK**

@sarah\_likesprettygirls  
Sarahzak.com  
Seite 7-8







**2023**

**PROJET EVASIONS**

**PROJET-EVASIONS.ORG**

**EVASIONS@RISEUP.NET**