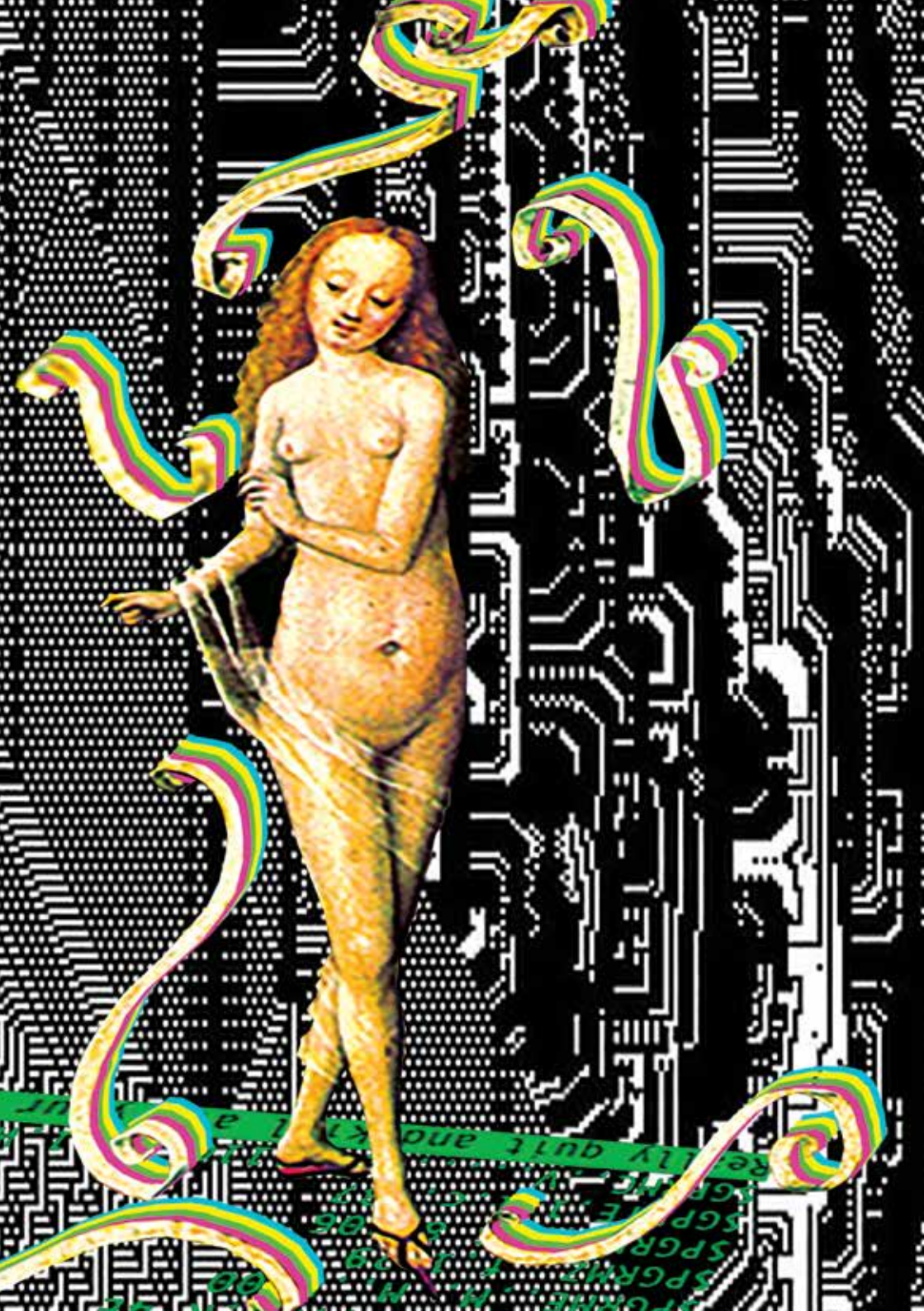
HOW TO CYPHER SEX: A MANUAL FOR COLLECTIVE DIGITAL SELF-DEFENSE GUIDES



HOW TO CYPHER SEX:

A Manual for Collective Digital Self-Defense Guides

How To Cypher Sex:
A Manual for Collective Digital Self-Defense Guides

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

This manual is available online as a shareable PDF with hyperlinks at cyphersex.org.

Cover design and illustrations by Bella Merda Design

Printed by books factory

December 2023

This publication has been made possible with support from Constant, a non-profit, artist-run organization based in Brussels since 1997. constantvzw.org

Cypher Sex would like to thank

Noah, Lara, Gergana, Hydra Cafe and workshop participants,
Liad, Lucy, Æris, Lenke, Constant, Elodie, and Peter

for their contributions in developing this manual.

TABLE OF CONTENTS


QUEER
HOOKERS

Preface

Why make a manual for collective self-defense guides? In this preface, we discuss the founding of Cypher Sex in response to the 2018 US-based bill FOSTA/SESTA and describe the processes we adopted to create the first two digital self-defense guides for sex workers in the United States and Germany. Additionally, we discuss the importance of creating new localized guides that take into account local sex workers' specific needs and self-defense strategies for the particular legal and social context where they operate.

FOSTA/SESTA: Censorship in Disguise

On April 11, 2018, the United States passed a combination of two bills, "Allow States and Victims to Fight Online Sex Trafficking Act" (FOSTA) and "Stop Enabling Sex Traffickers Act" (SESTA), into Public Law No: 115-164, more commonly referred to as FOSTA/SESTA.[1] While this law was passed under the guise of fighting sex trafficking (and politically justified the Department of Justice's seizure of Backpage.com, despite the fact that had already happened five days earlier[2]), FOSTA/SESTA actually made an exception to Section 230, a law (originally part of the Communications Decency Act of 1996 which was a codified form of the Communications Act of 1934) that generally provides immunity for website platforms with respect to third-party content.[3] FOSTA/SESTA's stated aim is "to amend the Communications Act of 1934 to clarify that section 230 of such Act does not prohibit the enforcement against providers and users of interactive computer services of Federal and State criminal and civil law relating to sexual exploitation of children or sex trafficking, and for other purposes."[4] As the international non-profit digital rights group Electronic Frontier Foundation explains, while Section 230 does provide legal protection for providers from their user's actions and statements it does

1 Public Law No: 115-164 is available at https://www.congress.gov/115/plaws/publ164/PLAW-115publ164.pdf.

2 For more information, see: US Department of Justice: Office of Public Affairs, "Justice Department Leads Effort to Seize Backpage.Com, the Internet's Leading Forum for Prostitution Ads, and Obtains 93-Count Federal Indictment," last modified April 9, 2018, https://www.justice.gov/opa/pr/justice-department-leads-effort-seize-backpagecom-internet-s-leading-forum-prostitution-ads; and Laura Jarrett and Sara Ashley O'Brien, "Justice Department seizes classified ads website Backpage.com," *CNN*, cnn.com, last modified April 6, 2018, https://edition.cnn.com/2018/04/06/politics/backpage-doj-seizure/index.html.

3 Section 230 states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." (47 U.S.C. § 230(c)(1)). For more information on Section 230, see: Electronic Frontier Foundation, "Infographic: Why Section 230 Is So Important," https://www.eff.org/issues/cda230/infographic.

4 For more information on FOSTA/SESTA, see: Norman Shamas, "A Brief Introduction To FOSTA-SESTA," *GenderIT*, genderit.org, November 2, 2018, https://www.genderit.org/resources/brief-introduction-fosta-sesta.

not provide protection for an individual user's actions and statements online and does not protect companies that violate federal criminal law, such as is the case with the "sexual exploitation of children or sex trafficking."[5]

Under this legal ambiguity, online service providers were forced to calculate their own risks and the results silenced online speech by forcing internet platforms to censor their users. In preemptive fear of US lawsuits, most internet providers used globally (Instagram, Paypal, Mailchimp, Craigslist, etc.) have updated their Terms of Use and other policies to prohibit (or greatly restrict) any "adult content" including not only pornography and erotica but also sex toys and sex-positive education. By March, Craigslist had already shut down their personal ads sections.[6] As of May 2018, Facebook and Instagram (later called Meta) created an entire Community Standards section dedicated to "Adult Nudity and Sexual Activity" and, as of October 2018, to "Sexual Solicitation," both of which have been continually updated.[7] Perhaps most famously, after being removed from the iOS App Store, Tumblr banned all "adult content" in December 2018.[8]

While most of these platforms now explicitly prohibit escort and similar services, Paypal's "Acceptable Use Policy," for example, additionally prohibits "certain sexually oriented materials" and "items that are considered obscene."[9] As Subha Wijesiriwardena wrote for *GenderIT* in 2019: "The language around 'obscenity' forms one of the key legal bases for censorship in many countries; the idea seems to originate from colonial-era laws around obscenity which aimed to criminalize sexual expression and sexuality-related material (which could include sexuality-related educational information) as it was considered 'harmful' to society," not to mention criminalizing forms of sexual behavior.[10] This, in turn, not only directly affected sex workers' safety and ability to work online but, through the sexualization of queer content and more, has had long-term ripple effects on the online representation of sex-positive and queer cultural activities more broadly.

5 Electronic Frontier Foundation, "Section 230," https://www.eff.org/issues/cda230.

6 Nitasha Tiku, "Craigslist Shuts Personal Ads for Fear of New Internet Law," *Wired*, wired.com, last updated March 23, 2018, https://www.wired.com/story/craigslist-shuts-personal-ads-for-fear-of-new-internet-law.

7 Facebook Community Standards, "Adult Nudity and Sexual Activity," https://transparency.fb.com/policies/community-standards/adult-nudity-sexual-activity; and "Sexual Solicitation," https://transparency.fb.com/policies/community-standards/sexual-solicitation.

8 Shannon Liao, "Tumblr will ban all adult content on December 17th," *The Verge*, theverge.com, December 3, 2018, https://www.theverge.com/2018/12/3/18123752/tumblr-adult-content-porn-ban-date-explicit-changes-why-safe-mode; and "Tumblr's adult content ban means the death of unique blogs that explore sexuality," *The Verge*, theverge.com, December 6, 2018, https://www.theverge.com/2018/12/6/18124260/tumblr-porn-ban-sexuality-blogs-unique.

9 Paypal's "Acceptable Use Policy" additionally has limitations on "Mature Audience Content" including "adult DVD's, magazines and other adult themed products or services" as well as any online dating services, available at https://www.paypal.com/us/legalhub/acceptableuse-full. In another example, Mailchimp's "Acceptable Use Policy" additionally prohibits not only pornography and sexually explicit content but also "hookup, swinger, or sexual encounter sites or services" as well as "adult entertainment" and "novelty items," available at https://mailchimp.com/en/legal/acceptable_use.

10 Subha Wijesiriwardena, "Private Parts: Obscenity and Censorship in the Digital Age," *GenderIT*, genderit.org, June 24, 2019, https://www.genderit.org/feminist-talk/private-parts-obscenity-and-censorship-digital-age.

Anti-Prohibition and Harm Reduction

In the fall of 2018, queer feminist hacktivists and net artists from squats and collectives all over Europe gathered at XM24, an established squatted and self-managed social center in Bologna, Italy, that would be evicted just one year later.[11] During this edition of the Eclectic Tech Carnival (/ETC), an attempt was made at creating a network of sex workers, ex-sex workers and allies "in order to create a permanent working group looking at sex work and online security."[12] While many participants in this session already had a good approach to online self-defense, some of the solutions suggested in the workshop could not be applied everywhere. For example, acquiring anonymous phone numbers was possible in some countries but not in Italy, where an ID card is required to buy a SIM card. In the UK, some forms of sex work are legal but users need to submit a passport to use many online platforms. In another example, someone had thought of a solution to avoid being outed as a sex worker online that actually increased the risk of stalking by clients. While a working group on sex work and online security was not born immediately after, the complexity of localized contexts became clear.

This made us reflect on our overlapping professional experiences developing websites for sex workers and digital security training for human rights groups and organizations, alongside our personal experiences as kinky, queer, polyamorous psychonauts. While starting to get involved with queer techno parties in Berlin, we got a deeper sense of the principles of harm reduction that are indispensable for the sex and drug-positive scenes those parties are fostering.[13] Anti-prohibition becomes a much more multifaceted and important concept when organizing events full of people cultivating an awareness of what risky activities could entail for themselves and others with the aim of minimizing possible issues that could arise. Harm reduction is based on empathy, complicity and solidarity: we try to create safer spaces where we can enact our desires—however risky—while limiting possible damages through informed consent, collaboration and watching out for each other.

The point where a harm reduction approach enters the online world is where digital tools are used by or with marginalized folks practicing activities such as sex work, networking with other kinky people, or simply using a dating app. When our bodies or desires are exposed, the border between the digital sphere and our physical safety is so porous that our only protection is trust in our community; for example, trust that a removable

11 For more information on XM24, see: "Self-managed social centres in Italy: Bologna," Wikipedia, last updated September 10, 2023, https://en.wikipedia.org/wiki/Self-managed_social_centres_in_Italy#Bologna.

12 Eclectic Tech Carnival program, "Sex Work Online," https://eclectictechcarnival.org/ETC2018/program/#-sex-work-online.

13 While popularized in relation to drug use, many harm reduction advocacy groups also recognize overlaps with sex work and other "risky" activities. See, for example, Harm Reduction International, "Fact Sheet: Sex Work & Harm Reduction," https://harmreduction.org/issues/sex-work/harm-reduction-facts. In the BDSM community, this typically takes the form of detailed discussions around consent models. For example, see: OH Yes Please, "Acronyms Models for Consent," https://ohyesplease.org/lessons/acronyms-models-for-consent.

sticker covering a phone camera is going to protect us from being filmed in a dark room and outed on social media. By organizing queer parties, we try to promote community building and this sense of trust. But for some less privileged people, trust cannot be sufficient and self-defense strategies become necessary against prevalent stigmas, queerphobia, transphobia and misogynistic patriarchal threats. In cybersecurity terms, these threats take the form of outing, doxing, stalking, defamation, non-consensual publication of intimate media and hate speech, among others.

Cypher Sex for Digital Self-Defense

When the consequences of FOSTA/SESTA became clear for sex workers in the United States, they began organizing and circulating tips on safer tools that they could use to protect themselves and their online accounts and media. Besides being hosted on Google Drive (where content was already being censored[14]) or spread in PDF form (which was impossible to edit and update) these first lists of recommendations offered no explanations on why and how each tool should be used. In this form, "digital security" became a package of rules that people felt they needed to apply regardless of their particular circumstances. Many times these lists offered a promise of anonymity where no anonymity was really necessary (or possible) and did not include any threat model or details on what each tool could be used for.

Finding no comparable existing resource, in 2019 we founded Cypher Sex (a play on "cypher" as a nod to encryption and "safer sex") to develop a digital self-defense guide for sex workers in response to the challenges facing our marginalized communities post-FOSTA/SESTA. We wrote the first guide featuring the digital dominatrix "Eve Pentest" and her digital self-defense strategies based on multiple interviews and discussions with sex workers in the United States. After answering urgent requests by our contacts, we asked them questions to obtain a clear picture of what risks they were mainly worried about and what they needed to protect. This helped us define a persona, "an archetypical description of a user that embodies their goals" that "can also be useful for identifying threats, vulnerabilities and likely areas of risk in their given environment."[15] Thus Eve Pentest was born, the user persona of a professional dominatrix who works in the United States post-FOSTA/SESTA.

14 For an example of Google censoring queer content, see https://support.google.com/docs/thread/200185949/google-is-now-monitors-our-drives-for-sexually-explicit-material-excuse-me.

15 Duncan Ki-Aries and Shamal Faily, "Persona-centred information security awareness," *Computers & Security*, Vol. 70, September 2017, 663-674, https://doi.org/10.1016/j.cose.2017.08.001.

Shortly after, we got in touch with Hydra e.V., a sex worker advocacy non-profit association in Berlin, Germany, and began offering workshops in collaboration with tech-savvy sex workers who wanted to acquire more digital security skills.[16] For these workshops, we applied a participatory threat modeling approach where an introductory round also served as a brainstorming session on what participants perceived as digital threats in their work and life.[17] We then analyzed those threats together to find protection strategies that could work for the people in the room.

While the COVID-19 pandemic lockdowns halted techno parties, kink events, and most legal sex work, the need for digital self-defense information only increased. Despite strict social distancing and compulsory face masks, the workshops at Hydra Cafe attracted even more participants as they wanted to find ways of earning money through online sex work and to learn about new threats they might face with this shift. After seven workshops at Hydra, as well as a dedicated session at the 22nd International WomenLesbianTrans*-Inter* BDSM Easter Conference in Berlin (held online due to COVID-19), a second guide for Berlin-based sex workers was developed and released in December 2021 featuring "Ava Tarnung," a genderfluid escort.[18]

Using specific personas helped us create a compelling narrative and convincing scenario for our self-defense guides. Having identified what our contacts most needed to protect, we described protection strategies that could be applied to each scenario based on an overarching principle of multiple identity management.[19] Through this persona-centered approach, we could convey the reasons for using certain tools, rather than offering techno-optimistic instructions that focused on ultimate solutions for security and "anonymity." In this way, we hope the reader can figure out for themselves what strategies they actually need for their own activities. In other words, we have tried to empower our audience so they have the information they need to decide whether they want to use the tools listed in the examples of our guides or choose something else. Thanks to this approach the Cypher Sex guides could be used virtually by anyone who has a similar threat model and needs.[20]

16 For more information on Hydra Cafe, see: https://www.hydra-berlin.de/en/cafe.

17 For more information on participatory threat modeling, see: Julia Slupska, Scarlet Dawson Duckworth, Linda Ma, and Gina Neff, "Participatory threat modeling: Exploring paths to reconfigure cybersecurity," Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems, Article: 329, May 2021, 1-6, https://doi.org/10.1145/3411763.3451731.

18 Both Cypher Sex guides were magnificently illustrated by the queer duo Bella Merda Design, who also has illustrated this manual. More information on Bella Merda Design can be found on Instagram at https://www.instagram.com/bellamerda.design.

19 For more information, see the *Gendersec Guide to Multiple Identity Management* available at: https://gendersec.tacticaltech.org/wiki/index.php/Step_1.

20 The guide for Berlin sex workers has been recently localized into German (https://projet-evasions.org/chyper-guide_de/) and French (https://projet-evasions.org/projet-evasions-org-cyberguide_fr/) for the Swiss context by Projet Évasions (https://projet-evasions.org) in collaboration with ProCoRe (Prostitution Collective Reflection), a national network advocating for the interests of sex workers in Switzerland (http://procore-info.ch).

Lost in Translation

Following the guide for Berlin-based sex workers and a presentation at the TransHackFeminist Convening at Calafou in August 2022, Cypher Sex received many requests for translating these first two guides into other languages for other contexts. Despite our open-ended approach which leads from goals and motivations to protection strategies based on a specific threat model, a digital self-defense guide for sex workers cannot be easily translated or used by any sex worker in any other country or context. Although there are four main approaches to sex work in national laws (criminalization, full decriminalization, partial decriminalization, and legalization)[21], the condition of sex workers can vary depending on many factors including the way national regulations are applied locally as well as the kind of sex work they practice (and hence their social class), religious beliefs, the general perception of sexuality and sex work, the role of women in society, accountability of law enforcement agencies, and so forth.

All these variables also affect the threat model of sex workers, whether in the digital or physical sphere. For example, they will likely wish to hide their online activities from authorities in a state that criminalizes sex work, while this need may be less urgent in a country where sex work is usually tolerated. And while some sex work activities like camming are practiced only online, some sex workers hardly ever use online services and only need a phone and a messaging app to stay in touch with their clients. Therefore, a simple translation of these context-specific guides would not prove particularly useful in a different social and legal context. Given the multiplicity of possible scenarios, guides for sex workers need to be shaped together with the community who needs it while identifying the specific threats they face to create a persona that matches their context, activities and goals. This is why, after creating the first guide for the US context focused on professional dominatrixes, we then wrote a second guide addressed at sex workers in Berlin.

While some of the recommendations provided in both guides can be applied to most situations (e.g. how to create strong passwords), most of the strategies suggested in the Cypher Sex guides vary based on differences of the workers' economic condition and the solutions that the local community applies to protect themselves from risks connected to their psycho-social security (stalking, outing and harassment—both physical and digital), as well as to their legal situation (e.g. prohibition in the US, legalization in Germany). This is why Cypher Sex decided to work on a manual for writing localized guides with basic outlines, resources, links, suggested approaches and interview questions relevant for different

21 For more information, see: Yale Global Health Justice Partnership, "The Law and Sex Work: Four Legal Approaches to the Sex Sector," April 2020, https://law.yale.edu/sites/default/files/area/center/ghjp/documents/the_law_and_sex_work.pdf.

international locations that advocates self-empowerment through the use of online identity management and other digital self-defense strategies.[22]

Not Done Yet

More than five years after its enactment, FOSTA/SESTA has largely been deemed a "miserable failure." As Melissa Gira Grant explained in 2021, "In the first in-depth legal analysis of SESTA/FOSTA and its impact, published in the *Columbia Human Rights Law Review*, Kendra Albert, Elizabeth Brundige, and Lorelei Lee concluded, in part, that 'though the exact legal applicability of FOSTA is speculative, it has already had a wide-reaching practical impact; it is clear that even the threat of an expansive reading of these amendments has had a chilling effect on free speech, has created dangerous working conditions for sex-workers, and has made it more difficult for police to find trafficked individuals.'"[23] Despite this, anti-porn lobbyists recently began pressuring Reddit to shut down all of its NSFW communities.[24] And while last autumn the stopsesta.org coalition "filed their opening brief in a case that seeks to strike down the law for its many constitutional violations,"[25] the EU Commission (again, under the guise of fighting child exploitation) is currently considering a law, commonly referred to as chat control, that would enable law enforcement access to encrypted chat messages.[26] In other words, these forms of censorship in disguise, implemented with the excuse of "protecting women and children," are not going away any time soon but are, in fact, expanding. Whether you are part of a marginalized community that has been directly affected or not, what you are able to access, share and pay for online has already been heavily censored.

22 This work has being supported by Constant, a non-profit, artist-run organization based in Brussels since 1997, through a Techno-disobedience commission. More information is available at https://constantvzw.org/site/-Techno-desobeissance,246-.html.

23 Melissa Gira Grant, "The Real Story of the Bipartisan Anti–Sex Trafficking Bill That Failed Miserably on Its Own Terms," *The New Republic*, newrepublic.com, June 23, 2021, https://newrepublic.com/article/162823/sex-trafficking-sex-work-sesta-fosta; and Kendra Albert, Elizabeth Brundige, and Lorelei Lee, "FOSTA in Legal Context," *Columbia Human Rights Law Review*, Issue 52.3, https://hrlr.law.columbia.edu/hrlr/fosta-in-legal-context/.

24 Samantha Cole and Emanuel Maiberg, "Anti-Porn Lobbyists Pressure Reddit to Shut Down Its NSFW Communities," *Motherboard*, vice.com, May 1, 2023, https://www.vice.com/en/article/m7bvbv/anti-porn-lobbyists-pressure-reddit-to-shut-down-its-nsfw-communities.

25 The Woodhull v. United States - Appellants' Opening Brief is available at https://www.eff.org/document/woodhull-v-united-states-appellants-opening-brief.

26 Netzpolitik, "Why chat control is so dangerous," EDRi20, edri.org, November 17, 2021, https://edri.org/our-work/why-chat-control-is-so-dangerous.

1

Why Self-Defense?

In most resources, guides and trainings, the tips and strategies used to protect ourselves from harm when using online tools and digital devices are usually presented using the terms "digital security" or "cybersecurity." In this manual (and our previous guides), we prefer to focus on "self-defense" from a more self-empowered position rather than on the term "security." For example, when we think about security we tend to think about something monolithic like a nuclear fallout bunker. While these shelters are certainly considered relatively safe in one of the worst scenarios imaginable, finding security in such a place means there is very little else you can do apart from passively hiding underground until the end of time. Additionally, from the surveillance of citizens in the name of "State security" and the violation of refugees rights in the name of "national security" to "maximum security prisons" and "security measures" used to restrict basic human rights for women and children, the word "security" has often been used to support policies that actually limit the freedom of migrants, minorities and even entire populations of totalitarian states.

When used in the digital sphere, the term "security" additionally usually refers to a top-down vision of protection from digital threats that are often based on mainstream perceptions rather than on facts. For example, consider how the 1983 movie *WarGames* led then-US President Ronald Reagan to sign The Computer Fraud and Abuse Act of 1984 whose interpretation would become so broad and vague that it would eventually turn online activism into a serious felony comparable to an armed attack.[1] As already discussed in the preface, we have more recently seen fighting the "sexual exploitation of children or sex trafficking" used to undermine net neutrality with FOSTA/SESTA, as well as a law package that the EU Commission is currently preparing, referred to as "chat control," that would enable law enforcement access to all encrypted chat messages under the guise of fighting the "sexual abuse of children."[2] However, these are just a few examples of how the internet has been demonized and "cybersecurity" has been used as an excuse to keep society under surveillance and control while undermining the usage of digital tools for social justice, individual liberation and free culture.

1 Declan McCullagh, "From 'WarGames' to Aaron Swartz: How U.S. anti-hacking law went astray," *CNET*, cnet.com, March 13, 2013, https://www.cnet.com/tech/tech-industry/from-wargames-to-aaron-swartz-how-u-s-anti-hacking-law-went-astray.
2 Netzpolitik, "Why chat control is so dangerous," EDRi20, edri.org, November 17, 2021, https://edri.org/our-work/why-chat-control-is-so-dangerous.

Without a deep reflection on these trends, often even technologists tend to apply the same top-down cybersecurity approach when using their skills to support grassroots movements and civil society. In the past few years, we have seen attempts at "teaching digital security" to activists and human rights defenders by training them on the use of "secure tools" without making sure that those tools actually matched their threat model with their needs and goals. In the end, this so-called "digital security" approach is counterproductive because tools that are secure but make life more difficult tend to be discarded in favor of less safe approaches that have proved to be good enough to reach a specific outcome. In other words, in emergency cases or when our stress level peaks, we tend to accept some risks as long as we can achieve what we need to overcome an acute crisis.

A Holistic Approach to Digital Self-Defense

Digital self-defense can only be effective if it has a holistic approach. Even when a threat is based exclusively in the physical or in the digital sphere, its ramifications always encompass all the contexts of our life; physical, psychosocial, digital and political. For example, intimate partner violence can extend from the physical to the digital level through spying apps or through surveillance over social media accounts while attacks started by mobs at the digital level can expand to the physical level through doxing and physical threats. Of course, violence of any kind always exposes survivors to trauma which can lead to further harm at the social and physical level; for example, due to bias against psychological issues or because of psychosomatic disorders.

A more empowering approach to protection starts with participatory threat modeling; a collective reflection of our fears including what is more or less likely to happen to us, who our adversaries and allies are, as well as how we can improve our practices to better protect ourselves, our activities and our peers. Fundamentally, we consider how to reach our practical goals and even to make some dreams come true. In this manual, we call this overall participatory approach "digital self-defense" and we use this term to talk about the practices of digital protection with the hope to encourage those interested in writing a digital self-defense guide to take control of their own digital safety. Through techniques aimed at assessing risks in online practices, the users of this manual will be able to reflect on their own needs and goals and thus be empowered to choose specific solutions for their own guides that can help them secure their current practices—instead of adapting their existing practices to new tools for the sake of a higher "security."

We also see the word "self-defense" as fundamentally linked to feminist collective organizing; particularly in regards to sharing knowledge, skills and best practices. Feminists have historically used this term to talk about women's right to protect themselves and to assert their

rights and boundaries. However, in order to consider all the possible levels where harm can happen, self-defense also needs to adopt an intersectional approach that includes queer people, sex workers and other marginalized groups. In order to correctly assess and address the threats for a specific group or individual, we need to consider their social and political context and take into account the multiple systems of oppression and domination they are exposed to. Let's not forget that online violence is just an extension of physical violence and can sadly amplify it even more. In short, we believe knowledge on how to protect ourselves from digital threats should be shared among the most vulnerable groups.

Finally, we look at self-defense from a harm reduction perspective. Especially when considering queer communities and sex workers, an approach to risk management should be non-judgmental. Some, many times less privileged, communities engage in activities that are considered "high risk" by mainstream society and a harm reduction approach focuses on limiting potential ensuing damages instead of denigrating those activities. In other words, we should respect an individual's capacity to take a conscious risk when deciding to face less safe scenarios.

While we recognize the holistic dimension of self-defense, in this manual we focus on digital self-defense for sex workers. This is both because we have already been working with sex workers post-FOSTA/SESTA and because sex workers already turn to their own community networks to find efficient self-defense strategies on the physical and psychosocial levels.

2

Sex Work Networks and Community Building

This chapter is written by Snezhinka and discusses various formal and informal community networks used by sex workers.

All sex workers share a unique position in our society. On the one hand, we are highly visible and often fetishized. Yet, on the other hand, we remain completely invisible and voiceless. Paired with the influence of our society's moral politics, this presents a challenging situation to navigate. We become the most visible when there is a problem, particularly when people think we need to be saved. That's when discussions about us occur on television, in political debates and special regulatory laws. The only place where we can openly share our experiences and be ourselves without fear is among fellow sex workers. There, we can relax and let our guard down. It is incredibly difficult to trust those who claim they want to help. While their intentions may be good, our experiences often reveal underlying motives. It could be a client harboring romantic hopes, a friend making us their "edgy" token sex worker pal or a well-meaning feminist secretly viewing us as victims of the patriarchy.

When reaching out to us, it's essential to understand that "the sex work community" consists of distinct communities with varying degrees of connection among them and with differing access to state benefits and privileges. We attempt to describe this complex landscape with the term "whorearchy," reflecting the power dynamics within the sex work scene. These power structures mirror broader societal inequalities and manifest in sex work through language barriers, legal status, physical abilities, gender identity, migration status, racism and more. You cannot simply rely on the testimony of one sex worker to represent the entire community. Understanding these complexities requires significant effort and it's crucial to listen to us rather than pursuing your own agenda.

Our countries' legal definitions of sex work have a substantial impact on our livelihoods. It ranges from criminalization (where sex work is prohibited by law) to legalization (where sex work is legal but with special regulations). The "Swedish model," which criminalizes clients, poses the same problems as full criminalization under the guise of protection. Only with decriminalization and the same rights as other professions do we have the best working conditions. Not many countries see the benefits of supporting us and giving us the tools to empower our situation. All too

often are we forced to work illegally. The question is: Where do we turn to when we experience injustice?

In light of these challenges, including social stigma and the threat of violence, we created a wide array of networks hidden from the public view. Some are improvised, while others are well-established, and may be in-person or online. These networks are closely guarded and are the backbone of safety and knowledge-sharing for us. The topics discussed in these networks are diverse and include problem-solving related to various aspects of the field. We are the experts—having troubleshooted and found creative solutions to the numerous obstacles we face every day. If you wish to support us, it's essential to acknowledge and respect these networks and collaborate with them.

Working online has become increasingly unstable in recent years. Since SESTA/FOSTA (see the preface for more information), the platforms we have relied on for years are disappearing overnight. Valuable profiles with a significant following are getting blocked in moral raids across all social media. This is just one example among many of laws that control sex workers under the disguise of protection (in this case "fighting sex trafficking") while actually putting us in more precarious situations. In addition, we are exposed to assaults from individuals who leak our data to our friends, family, and co-workers. It's nearly impossible to figure out how to deal with this alone. In our networks, we find empathy and a judgment-free zone. Regardless of our needs and goals in these situations, they are taken into account when we seek solutions.

Creating a safe and welcoming environment for us is no easy task. I was recently involved with the Hydra Café, a community space for sex workers in Berlin, where we employed various strategies. The Hydra Café opened in 2019 as a second location and community center of Hydra e.V. Hydra is an organization advocating for the rights of sex workers in Berlin and provides counseling and meeting opportunities. From the early conceptualization days of the Hydra Café, we emphasized that sex workers are on the forefront and adopted a peer-based approach. We wanted a close exchange with the communities and encouraged participation by shaping the Hydra Café according to the needs of the visitors; peers provided support to their peers, organized events and conducted workshops.

From the moment we heard about Cypher Sex's digital self-defense zine, we were eager to implement this topic more deeply at Hydra Café. We initiated a workshop series called "Digital Self-Defense," as well as a clinic called "Cypher Sex," where people could seek help and support if they encountered problems online. The efforts to organize these initiatives were equally distributed between allies and sex workers. Some sex workers possessed significant technical knowledge while some allies were well-versed on sex work topics and, if knowledge was missing, it was shared between each other. This was not a top-down knowledge exchange but a col-

laborative one. In this way, it was possible to provide support tailored to different communities in Berlin. Equally important was letting the participants guide the process by making each workshop an opportunity to adjust the learning material based on group feedback.

It’s beautiful to witness how a single zine has evolved into a community movement—and this manual stands as proof that more positive changes are on the horizon!

3

Methods

Digital Self-Defense Aims and Limitations

Before getting too deeply into digital self-defense, it is first worth stating what we mean by "digital" when we talk about digital self-defense, as well as defining the limits of digital self-defense—especially in contexts where physical risk for sex workers is so overarching that digital self-defense strategies can only have a restricted impact.

Digital self-defense is about protecting activities that use digital tools or platforms as well as information that is stored or transmitted through digital tools or platforms. In the context of sex work, this includes:

1. Safeguarding the possibility of carrying out online activities including both sex work directly (such as camming and selling videos) and the usage of online platforms (whether specialized or mainstream) for advertising sex work services. This includes the use of social networking platforms and other online tools (such as a personal website) while preserving one's privacy and safety.

2. Protecting data that is stored online or on physical devices (such as computers, phones and hard drives) from being accessed or used by third parties without consent; for example, in police seizures or through non-consensual publication.

3. Protecting personal devices from unauthorized access to private information including surveillance through spyware and inbuilt features such as GPS and synchronization with other devices, and similar kinds of abuse.

4. Protecting one's identity in online communications; when using social networking platforms or messaging apps but also when establishing a first contact with a client or when receiving online payments.

These protections need to apply to all sex workers—from those working on the streets and those hired by brothels to escorts, cammers and those who work in the porn movie industry. But in some contexts, the kinds of threats sex workers face are such that none of these digital self-defense strategies can offer complete protection from the physical and psychosocial risk they are exposed to. In places where sex work is illegal or has an ambiguous legal status and crackdowns are frequent, sex workers are often exposed to abuse by the authorities. In case of police raids, in some countries any digital evidence of having engaged in sex work can be incriminating and lead to imprisonment and worse for the people arrested. This is one of the main reasons why we consider it crucial to base any digital self-defense strategy on a participatory threat modeling exercise conducted with a wide community of local sex workers.

The digital self-defense guides we have developed for Cypher Sex are based on two tools developed in the fields of human-computer interaction (HCI) and user experience (UX) design, participatory threat modeling and personas, as well as online identity management that aims at creating a separate digital identity for each life domain.[1]

Participatory Threat Modeling

Participatory threat modeling is "a feminist cybersecurity practice" where "participants define their own cybersecurity threats, implement changes to defend themselves, and reflect on the role cybersecurity plays in their lives."[2] As already discussed in Chapter 1, the term "cybersecurity" is connected to hierarchical approaches that dictate what people should worry about based on assumptions by a restricted group of (mostly white, cisgendered and frequently male) specialists rather than eliciting and listening to people's actual concerns and questions in a non-judgmental way. This top-down approach is based on the widespread assumption that the problem with security is human behavior; or, in few words, "the user is the problem."

Instead, a horizontal approach to digital self-defense goes through a process of participatory threat modeling that identifies needs, requirements and solutions, while also taking into account psychological and sociocultural factors. By inviting actual users in specific social contexts to define their own digital threats, it is easier for them to find ways that are most suitable to protect themselves from those threats. Especially

1 For participatory threat modeling see: Julia Slupska, Scarlet Dawson Duckworth, Linda Ma, and Gina Neff, "Participatory threat modeling: Exploring paths to reconfigure cybersecurity," Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems, Article: 329, May 2021, 1-6, https://doi.org/10.1145/3411763.3451731. For more on personas see: Alan Cooper, Robert Reimann, David Cronin, Christopher Noessel, Jason Csizmadi, Doug LeMoine, *About Face: The Essentials of Interaction Design*, 4th ed. (Indianapolis, IN: John Wiley & Sons, 2014).

2 Slupska, et al., "Participatory threat modeling," 1.

in the case of marginalized groups who are used to feeling excluded by technical language and may consider some digital technologies hard to use, it is crucial to create a safer space where people can feel included and encouraged to contribute to a reflection on their actual concerns; for example, if their use is connected to socially stigmatized activities like sex work or queer dating. This is why our guides have been developed based on preliminary discussions directly with sex workers using an open set of questions for one-on-one online interviews (with multiple professional dominatrixes in the U.S.) and through in-person focus groups and digital self-defense workshops (at Hydra Cafe in Berlin, Germany[3]). Questionnaires used for online interviews and focus groups as well as a workshop agenda may be found in the following chapter.

Persona-based Design

Personas are "composite archetypes based on behavior patterns" that help develop an understanding of a user's goals in a given context.[4] Originally developed for user interface design, they have been also applied to the design of security awareness tools and resources.[5]

Personas are user models that are represented as specific, individual human beings. They are personifications of specific motivations, goals and behavior that define the usage of a certain tool and through this personification they elicit empathy in designers as well as in users themselves.

Personas do not represent all possible users of a tool but, by designing a tool with a persona in mind, it can be possible to satisfy the needs of a wide group of users. Further, it is also likely that people who do not belong to that group are still also able to find the tools that are useful to achieve their own goals.

In the case of Cypher Sex, we have developed three personas based on the preliminary research, interviews, surveys, focus groups and workshops we facilitated; first, with professional dominatrixes based in the United States in the wake of FOSTA/SESTA and then with sex workers living in Berlin.

3 For more information on Hydra Cafe, see: https://www.hydra-berlin.de/en/cafe.
4 Cooper, et al., *About Face*, 62.
5 See, for example, Duncan Ki-Aries and Shamal Faily, "Persona-centred information security awareness," *Computers & Security*, Vol. 70, September 2017, 663-674, https://doi.org/10.1016/j.cose.2017.08.001.

Based on the results of our initial research and interviews with U.S.-based sex workers, we learned our constituency was a specific segment of providers mainly focused on BDSM services, highly literate and connected to a strong network of peers. Thus, we developed the persona called Eve Pentest whose main goals were:

- Protecting information she sold to clients, stored using online services or used for advertising.
- Keeping her private life separate from her work life.
- Avoiding being caught by the authorities in a place where sex work is illegal and sanctioned.
- Keeping her current clients and finding new clients.
- Having a safer space for work both offline and online.

In addition to identifying her end goals, we also added some fictional details that would make our persona more compelling so that readers could find her credible and identify or empathize with her. Adding illustrations around this persona made our guide convey even more emotional force and connected our character with a sex-positive and sex workers-friendly imaginary.

We applied a similar method to the Berlin guide except we created two personas in light of the difference in status between registered and non-registered sex workers in Germany. We created a primary persona called Ava Tarnung, "a genderfluid person who works as an escort," and a secondary persona called Anne Onimas, whose name suggests a migrant background and who is not registered as a sex worker and has therefore a less privileged status. This means that Anne Onimas needs additional self-defense measures that are similar to those recommended for those in the United States, where sex work is mostly illegal.

Finally, for this manual on how to create digital self-defense guides we have created a placeholder persona called Plaise Filler. This persona does not have a back story as it is supposed to be replaced with the new personas that will be created for new guides.

The new personas' back stories, needs, goals, motivations and scenarios will depend on the situation and the results of participatory threat modeling with other groups of sex workers and/or in different countries.

The main steps for building a persona are:

- Interview different groups of people.
- Identify behaviors: include significant behaviors but don't include behaviors you haven't observed in your research and interviews.
- Create persona types connected to the needs and goals of the people you have interviewed.
- Describe their behaviors and activities, issues and possible solutions you have seen applied in your research and interviews.
- List three to five end goals for this persona.
- Choose a first and last name.
- Add some demographic information such as age, geographic location, kind of work, etc.
- Add some further descriptions in order to bring the persona to life but not so much detail it becomes distracting.
- Add an image of the persona or create photographic collages to convey their emotions and experiences.

Separating Life Domains

Cypher Sex's approach to digital self-defense is fundamentally based on a strategy of identity partitioning. In all our knowledge-sharing efforts we suggest that readers and workshop participants reflect on how their activities vary according to the social domain (friend, family, work and advocacy networks, etc.) where they happen. For example, there are things that you only do with friends or family and other things that you only do for work or for your activism. By mapping these social domains, it is possible to create multiple identities and keep them separated to protect the most sensitive information from the risk of leaks in social domains that are less secure. In the case of sex workers, for example, separating their work identity from the identity they use to keep in touch with their family can protect them from being unwillingly outed to their relatives.

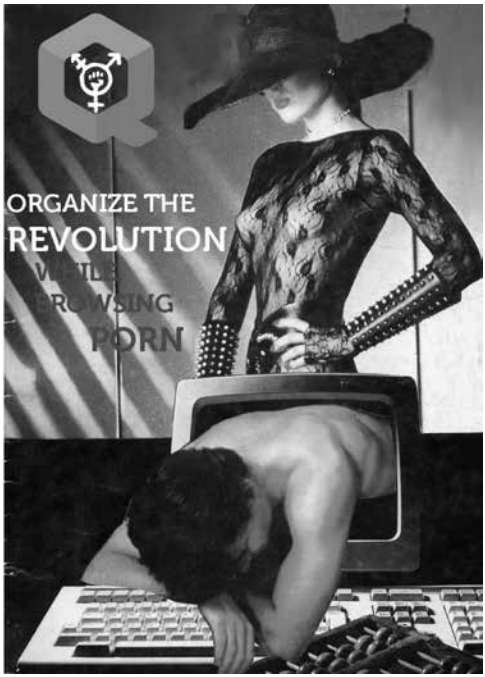
++

Gendersec Guide to Multiple Identity Management

https://gendersec.tacticaltech.org/wiki/index.php/Step_1

++

In our guides, we additionally suggest the creation of fictional personas to give an identity more depth and credibility. In this way, Cypher Sex guides are based on creating fictional identities both for personas who are used to embody the needs and goals of our constituency and as a tool for others to use to improve the protection of each of their lives' domains.



++

Organize the Revolution While Browsing Porn

a zine on queer online identity management

https://archive.org/details/queer-online-zine-2017

++

This methodology has also been used for the development of security tools such as Qubes OS, an operating system that increases protection by creating separated environments for each digital activity or virtual identity. A description of Qubes OS and other tools for identity management is included in Chapter 6 on context-specific modules.

4

Interview and Workshop Templates

This chapter includes an open set of questions for one-on-one online interviews, questionnaires used for online surveys and focus groups, as well as a sample workshop agenda that may be adapted for the needs of each community.

Interview Questions

These questions may be a helpful reference when conducting one-on-one interviews.

• Do you work and live in the same place?
  Is your official address the same as your home address?
  How do you connect to the internet? From where?

• Where do you store your files and information (offline and online)?
  Where do you store your data? How does it work?
  Do you use a password-protected website?
  What happens if these files become public?
  What happens if these files disappear?
  What happens if the authorities access these files?
  Do you think it could happen?
  Has it already happened to somebody you know?

• Do you publish texts and media on the internet that can be visible to everybody? Where?
  On your own website? What hosting platform?
  On a social media platform? Somewhere else?

• What would happen if the published materials or your work identity was connected to your real identity, home address, etc.?
  Who might want to use this information?
  The authorities? Others? For what reasons?

• What would happen if your readers' or clients' identities were disclosed?
  Is your platform protected through HTTPS?
  Does your platform allow for anonymized connections?
  Does your platform keep logs of visitors?
  Does your platform/website have ads or commercial statistics?

- What tools do you use to communicate?
  - What email providers?
  - Which tools do you use to communicate with whom?
  - On which devices?
  - What would happen if someone (the authorities or others) intercepted your communications?
  - What would happen if someone (the authorities or others) accessed these communications after they have happened?

- Do you use social media for your work?
  - What do you use the social media for?
  - Communication, publishing, advertising, networking?
  - Which platforms do you use?
  - Do you have one or more accounts on these platforms?
  - Do you use the same nickname on different social media?
  - Do you publish the same photos on different accounts?
  - Do you share contacts among accounts?

- Do you access your account(s) with one or more devices?
  - Which devices?
  - Do you use a computer? What operating system?
  - Do you run antivirus software?
  - Do you regularly update your operating system and software?
  - Do you have a screen lock?
  - Is your hard disk encrypted?

- Do you have one or more phones? What kind of phone?
  - What do you use your phone(s) for?
  - Publishing? Networking? Camera? Other?
  - Do you use it for communications? With which tools?
  - Do you keep your GPS active all the time?
  - Do you keep your Wi-Fi active all the time?
  - Do you keep your data active all the time?
  - Do you have a screen lock? What kind?

- Are you ready to learn how to use new tools?
  - How much time can you spend for learning?
  - Can you persuade your contacts to use different tools?
  - Can you spend money for securing your digital life?

Questionnaire for Workshop Participants

This questionnaire may be shared before a workshop as an email or in the form of an online survey conducted on a trusted platform. For this second option, we suggest using Nextcloud Forms on a trusted Nextcloud instance. For example, you can create a Nextcloud account on the cloud service offered by disroot.org or in the systemli.org cloud, two projects that offer secure online services to activists. For more information on secure online survey tools, check out Access Now Digital Security Helpline's community documentation.

++

Access Now Digital Security Helpline: Secure Survey Tools

https://communitydocs.accessnow.org/284-Secure_survey_tools.html

++

- What do you mainly use the internet for in your work?
- Do you use a computer for your work?
- What operating system (Windows, macOS, Linux)?
- Do you use your work computer for other activities?
- Do other people have access to your work computer?
- What phone do you use for your work? Android or iPhone? Something else?
- Do you use your work phone for other activities?
- Do you lock your computer and your phone? How?
- Do you use an email account for your work? What do you use it for?
- Is it a dedicated work account or do you use this email also for other stuff?
- Do you use the same password for more than one account?

Focus Group Questions

These focus group question may be used during a breakout session at the beginning of a workshop. Start by asking the participants to share their names and their main kind of sex work activity. After forming breakout groups based on shared sex work activity, consider the following questions:

- What is a worst-case scenario that you want to avoid?
- Is this something that you know has happened to other local/regional sex workers?
- In the same country?
- What consequences would there be if this was to happen to you in the future?
- What are you and/or others doing to avoid this threat?

After some discussion, the participants report back to the group about the threats they have identified from the breakout session. The discussion then turns to addressing protection against those threats. The following questions then may be asked based on the topics addressed:

- What platforms do you use for work?
- What platforms do you put your ads on?
- How do clients get in touch with you for the first time?
- How do you communicate with clients after your first contact?
- What social networks do you use for work?
- What other social networks do you use?
- Do you have one or more phone numbers?
- Are they all registered under your legal name?
- Do you have your own website?
- Where do you store your work pictures, videos, etc.?
- Do you connect to the internet from home or from public spaces? Are you aware of the risks in connecting from public spaces?
- Do you or other people you know use platforms that are more friendly towards sex workers? Which platforms are these? Why do you consider them sex worker friendly?

Digital Self-Defense Workshops

You can learn a lot about the needs and goals of your community by running digital self-defense workshops with a holistic and inclusive approach that start from the participants' needs.

We suggest mapping the needs and goals of your workshop attendees by first sending them a preliminary survey if possible (see "Questionnaire for Workshop Participants" on page 31) and then by asking them to brainstorm their questions on digital threats and their use of digital tools in the initial part of your workshop. We suggest organizing the rest of the workshop around the topics highlighted in this initial brainstorming exercise. While it is always a good idea to include the topics in the necessary modules listed in Chapter 5, it is important to always dedicate enough time to the main topics that reflect the needs of your group.

Learn more on how to organize a digital self-defense workshop in these resources:

Security Education Companion, a free resource for digital security educators

https://www.securityeducationcompanion.org

Cyberwomen, a digital security curriculum with a holistic and gender perspective

https://cyber-women.com

Safe Sisters: Digital Safety Trainer's Assistant, guidance and suggestions for new and experienced trainers

https://safesisters.org/wp-content/uploads/2022/06/Digital-Safety-Trainers-Assistant-smaller.pdf

LevelUP, resources for the global digital safety training community

https://www.level-up.cc

Digital Security Training Resources for Security Trainers

by Cooper Quintin (last updated Fall 2019)

https://medium.com/cryptofriends/digital-security-training-resources-for-security-trainers-spring-2017-edition-e95d9e50065e

Holistic Security: Trainers' Manual, a project of Tactical Tech

https://holistic-security.tacticaltech.org

Sample Digital Self-Defense Workshop Agenda

What follows is a sample digital self-defense workshop agenda that may be used for in-person or online workshops lasting 1.5 to 2 hours.

1. Introductions (15-20 minutes)

- Ask the participants:
  What's your name and what is your main kind of sex work activity?
- Introduce yourself. Describe the workshop agenda and the Cypher Sex manual as needed.
- Most importantly, discuss the approach of this workshop:
  We learn together.

2. Breakout groups based on sex work activity. Ask each group to consider the following questions. (10-15 minutes)

- What is a worst-case scenario that you want to avoid?
- Is this something that you know has happened to other local/regional sex workers?
- In the same country?
- What consequences would there be if this was to happen to you in the future?
- What are you or others doing to avoid this threat?

3. Participants report back to the group about the threats they have identified from the breakout session. (10-15 minutes)

4. Discuss how to manage identities online. Consider the following points. (10-15 minutes)

- We have to think of each of our online identities as a persona/ social mask. On the internet, each one of our identities, even the one connected to our official name, is a “virtual” identity.
- What is in a name? Discuss real name policies.
- A story for your persona...
- Add details: linguistic fingerprint, work, skills and interests, psychological attitude...

5. Discuss how to separate identities online. Consider the following points. (10-15 minutes)

- Pseudonymity vs. anonymity
- Introduction to metadata, in particular with regards to images
- Self-doxing
- Basic security measures to avoid account hacking: passwords, password managers, 2-factor authentication, regular software and system updates, possibly different devices or at least different browsers
- Secure connections and anonymous connections: VPN and Tor Browser
- Related questions:

  Do you connect to the internet from home or from public spaces?
  Are you aware of the specific risks in connecting from public spaces?

6. Discuss the management of identities. Consider the following points. (10-15 minutes)

- Devices
- Email
- Telephone number
- Payments
- Related questions:

  What platforms do you use for work?
  What platforms do you put your ads on?
  Do you have one or more phone numbers?
  Are they all registered under your legal name?

7. Discuss social networks and other online platforms including work-related websites. Consider the following points. (10-15 minutes)

- Social networks and online platforms
- Separate profiles including contacts and pictures (geolocation)
- How to choose/What to look for
- Websites
- Buying a domain and whois privacy
- Local laws on the registration of websites
- Choosing a hosting provider
- Related questions:

  What social networks do you use for work?
  What other social networks do you use?
  Where do you store your work pictures, videos, etc.?
  Do you have your own website?

8. Discuss work-related communications. Consider the following points. (10-15 minutes)

- Email
- IM apps: Signal, Telegram, Wire
- Wickr (wickr.com) and Confide (getconfide.com)
- Related questions:

  How do clients get in touch with you for the first time?
  How do you communicate with clients after your first contact?
  Do you or other people you know use platforms that are more friendly towards sex workers?
  Which platforms are these? Why do you consider them sex worker-friendly?

5

Digital Self-Defense Guide: Necessary Modules

This chapter includes modules that we think should feature in any digital self-defense guide for sex workers and queer groups. In terms of localization, these modules can mostly be translated as they are, but consider replacing links to resources in the target language when possible.

As discussed in Chapter 3, for this manual on how to create new digital self-defense guides we have created a placeholder persona called Plaise Filler. This persona does not have a back story as it is supposed to be replaced with the new personas that will be created for new guides.

How to Choose Tools: What to Look For

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

- **Is the application mature?** Plaise knows that security applications and protocols like HTTPS or Signal have usually been around for a long time. New applications/software 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?** Plaise knows that they can consider a connection secure when they see a green or closed lock 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).

Terms of Use

Depending on the platforms used by your community, in this module you may want to add (or change) some of the recommendations on what to look out for.

Whenever Plaise 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 (such as social media, website hosting and payment processors) that explicitly prohibit "adult content," which may be defined broadly to include anything from pornography and vibrators to erotic fiction. Plaise generally avoids these service providers or considers whatever account they may have with them as disposable.

In general, Plaise keeps their eye out for platforms that do not prohibit "adult content," reside in jurisdictions outside of the "Five Eyes" (an anglophone intelligence alliance including Australia, Canada, New Zealand, the United Kingdom and the United States), and offer security features like two-factor authentication and payments in Bitcoin, or other methods that protect their privacy.

Identity Management

To protect themselves against stalking or outing, Plaise 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 Plaise has considered to manage their work identity and other online personas:

An Identity for Each Level of Trust

Plaise 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, Plaise 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

In this module, we have used the persona Ava Tarnung from the guide for Berlin-based sex workers as this example applies better to their name than to our default persona Plaise Filler.

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 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 followed the self-doxing guide below, so they are sure that nobody else is using that name, at least among sex workers in their city.

++

Access Now Digital Security Helpline: Self-Doxing Guide

https://guides.accessnow.org/self-doxing.html

++

Tips on Email

When they started looking for an email provider that would be good to use for work, Plaise 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.

Plaise 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, Plaise only chose among email providers that use HTTPS/TLS encryption, which encrypts connections from their computer to the servers, and they made sure the TLS encryption was actually working by testing the provider they'd chosen on https://www.checktls.com.

++

Privacy-Conscious Email Services

https://prxbx.com/email

++

To be contacted by their clients, Plaise uses a Protonmail 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 do not consider this encryption reliable enough because emails with people who do not have a mailbox on Protonmail are not encrypted.

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

Separate Email Accounts

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

Sometimes Plaise 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 (guerrillamail.com) or anonbox (anonbox.net).

Secure Passwords

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

++

KeePassXC: Cross-platform Password Manager

https://keepassxc.org

++

The only passphrases Plaise 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.

++

EFF Dice-Generated Passphrases

https://www.eff.org/dice

++

An Additional Level of Security: 2-Factor Authentication

Plaise knows that even the strongest password can be stolen through various means such as, 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.

++

EFF Surveillance Self-Defense: How to Avoid Phishing Attacks

https://ssd.eff.org/module/how-avoid-phishing-attacks

++

To create the second factor they have installed a code generator (such as 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.

++

FreeOTP: Two-Factor Authentication

https://freeotp.github.io

++

Since each online platform has a different way of setting up 2-factor authentication, when Plaise is in doubt they check the Electronic Frontier Foundation's instructions on 2-factor authentication to find the right guide.

++

EFF: How to Enable Two-Factor Authentication For Your Online Accounts

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

++

Isolated Accounts

To keep their accounts isolated and to be sure that they cannot be connected to each other, Plaise 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.

- Plaise 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.

- Plaise 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, Plaise 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.

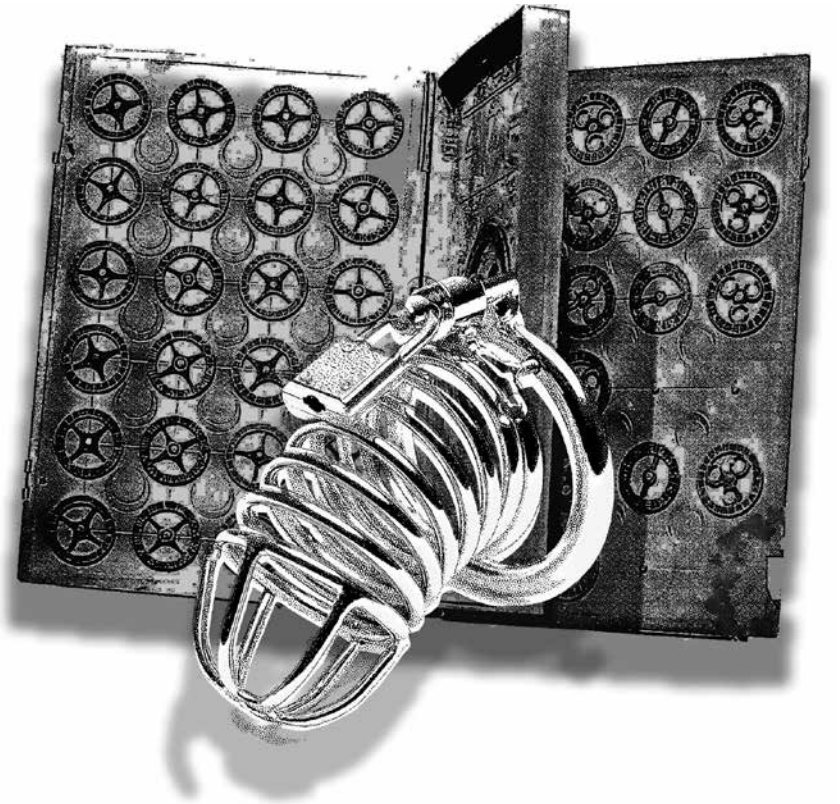
Dealing with Clients

Finally, Plaise 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, Plaise never uses their own credit card. Plaise instead asks the client to pay if a credit card is needed.

Plaise also knows that infecting a smartphone or another electronic device with spyware is cheap and easy, 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.

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.



6

Digital Self-Defense Guide: Context-specific Modules

This chapter includes modules that should be chosen based on the needs and goals of the community addressed by your digital self-defense guide. These should not be translated literally but adapted through interviews, focus groups and workshops with people from the target community. To learn more about the process, see Chapter 3 on Methods.

Introduction: The Persona

Creating a persona for each guide helps define the needs and goals of your target readers as well as make the usage of the guides more compelling. For more information, see "Persona-based Design" in Chapter 3.

Eve Pentest: The American Pro Domme

Eve Pentest is a digital security dominatrix who knows how to secure boundaries and create a safer space to play. Eve knows a lot about technology and how the internet operates. She uses many online services for her work and knows how to protect herself against potential stalkers, hackers and haters. She works in a dedicated dungeon and keeps her private life completely separated from her work life.

When FOSTA/SESTA was passed, and online services abruptly started locking down or deleting accounts without any warning, one of her accounts was deleted but she didn't lose her data because she had backed everything up and is now advertising her services on a more reliable platform that recognizes her right to anonymity as the ultimate protection against many threats she faces.

Ava Tarnung: The Sex Worker Registered in Berlin

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 different online activities. They think that knowing how to perform different personas both off and online is one of the keys to secure their life from stalkers and haters as well as to enjoy their multifaceted life.

Ava is a nerd. After some years of explorations on the Web they've learned quite a lot about technology and how online platforms operate. This knowledge, together with the close-knit contacts they have 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).

Anne Onimas: The Unregistered Sex Worker in Berlin

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. Anne makes sure, for example, to hide the IP address of her home connection as much as possible, which for the authorities (and for hackers) could lead directly to her official name and home address.

Plaise Filler

As discussed in Chapter 3, for this manual on how to create new digital self-defense guides we have created a placeholder persona called Plaise Filler. This persona does not have a back story as it is supposed to be replaced with the new personas that will be created for new guides.

Takedown Requests

This module should be adjusted depending on the privacy and copyright laws of your country. For example, in the European Union the General Data Protection Regulation (GDPR) gives individuals the right to ask organizations to delete their personal data (generally referred to as the "Right to be forgotten"), while in the United States and other non-EU countries it is best to refer to copyright regulations such as the Digital Millennium Copyright Act (DMCA) when requesting to have copyrighted information removed.

When Plaise 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, Plaise also did another name search inspired by this self-doxing guide.

++

Access Now Digital Security Helpline: Self-Doxing Guide

https://guides.accessnow.org/self-doxing.html

++

In their previous life, Plaise was not trying to protect their privacy so they didn't pay that much attention when people posted their picture online. Therefore, Plaise 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 that connected 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 this guide on how to document online harassment.

++

Digital First Aid Kit: Documenting Digital Attacks

https://digitalfirstaid.org/documentation/

++

The following paragraph only applies to EU citizens so we have used the persona Ava Tarnung from the guide for Berlin-based sex workers rather than to our default persona Plaise Filler.

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

++

Google: Personal Data Removal Request Form

https://reportcontent.google.com/forms/rtbf

++

The following paragraph applies everywhere.

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

++

Facebook: Report a Privacy Violation

https://www.facebook.com/help/contact/144059062408922

X (Twitter): Safety and Sensitive Content

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

Cyber Civil Rights Initiative Safety Center

https://cybercivilrights.org/ccri-safety-center

Without My Consent: Take Down

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

++

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

Plaise wants to be sure that their work identity can never be connected to their official one—not by stalkers, or neighbors, or even by state authorities. Plaise 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 phone with a new pre-paid SIM card for their new identity.

++

EFF Surveillance Self-Defense: The Problem with Mobile Phones

https://ssd.eff.org/module/problem-mobile-phones

++

Add an explanation here on how sex workers can acquire SIM cards that are not registered under their official name in the specific context of your guide. In the country you are writing for it may even be impossible to acquire a SIM card without documents. In these cases, sex workers may have found other ways of separating devices or you might explore the possibility of paying for an online service that gives out phone numbers such as Google Voice or Twilio.

Plaise 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 they leave their personal phone at home.

Plaise 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.

Tools for Secure Identity Management

We did not include this section in previous Cypher Sex guides as we thought these tools may be too complex to be of use to most basic users. However, depending on how tech-savvy your community is, you may decide to include them in your guides.

Ideally, Plaise knows that the best solution to separate their identities would be to have different devices for each of them. However, Plaise manages several identities and can't afford to buy so many devices!

In the beginning, Plaise's solution was to create different user accounts on their computer and just keep a separate phone for work. This was a good solution to avoid making mistakes, such as using the wrong email address to write to clients, but they knew that if their computer was ever hacked it would be easy to connect their many different life domains.

Then Plaise found out that they could learn to protect their multiple identities much better by installing a special operating system that is particularly useful to keep life domains separated.

Qubes OS

Plaise's computer runs on Qubes OS, an operating system focused on security and privacy that allows them to easily manage all their different identities and activities while keeping them separated from each other.

++

Qubes OS

https://www.qubes-os.org

++

After reading the *Organize the Revolution while Browsing Porn* zine and checking out how Qubes OS may be used by other kinds of persons in the Qubes OS How-To Guide on "How to organize your qubes," they decided that this would be a perfect tool to keep their sensitive information safe from any unwanted intrusion.

++

Qubes OS: How to organize your qubes

https://www.qubes-os.org/doc/how-to-organize-your-qubes

++

Plaise had to study the documentation a bit, since Qubes OS is very different from any other operating system (Windows, macOS or Linux), but in the end they concluded it wasn't so hard and went on to install Qubes OS and create a qube for each of their sensitive activities and different life domains. Now these qubes are running on their Qubes OS machine:

- **Personal:** for social networking platforms, email and messaging apps they use to communicate with friends and family.
- **Work:** for platforms they use for their sex work ads and for email and messaging apps they use with clients. *In countries where sex work is illegal, you may want this qube to connect through Tor to anonymize work activities.*
- **Banking:** for only accessing their online bank account and other payment platforms.
- **Bureaucracy:** for storing their official documents and accessing government platforms where they have an account.
- **Vault:** a qube disconnected from the internet used to store their passwords in a secure password manager.
- **Media:** a qube disconnected from the internet where they store all their work images and videos.

They also use "disposable" qubes to access insecure websites and have set up a VPN qube to connect safely to the internet from cafes and hotels.

Tails

When Plaise is travelling to work in countries where sex work is illegal they leave their computer at home and just bring a Tails USB stick with them. They additionally use the Persistent Storage feature to keep their most important work data in an encrypted folder within that USB stick.

When they reach their destination, Plaise then asks a friend to use their PC and boot it with their Tails stick to use it as a normal computer. This way Plaise can navigate the web and access their own accounts through a secure anonymous connection while keeping their data secure at the same time.

++

Tails, a portable, secure and anonymous operating system

https://tails.net

++

Secure Connections

Securing Connections When Using Public Wireless Networks

In some contexts, using public wireless networks (Wi-Fi) may be extra risky or not even possible. These tips should be reviewed in light of the applicable local laws on the usage of encryption tools and on internet connection. Also, in certain countries there may be VPNs that work better and it is worth checking them and including them in this module.

Plaise tries whenever possible not to use untrusted internet connections like the free wireless networks (Wi-Fi) they find in coffee shops, railway stations and hotels. They know that the owners of these networks (or worse hackers) might spy on them while they're connecting to the internet. Instead, they prefer to use data on their phone and do most of their sensitive work through their home connection.

Still, sometimes using these connections is easier and cheaper so Plaise'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 free Wi-Fi access points.

Plaise keeps note of VPNs that are reliable, to share with 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.

++

NYT Wirecutter Guide to VPN Services

https://www.nytimes.com/wirecutter/reviews/best-vpn-service

++

Anonymous Connections

We recommend only using anonymous connections in cases where there is a need to hide from State authorities. This is why we suggest anonymization tools in the guide for the United States (where sex work is mostly illegal), but in the guide for Berlin we only recommend them for unregistered sex workers. On the other hand, in some countries the usage of anonymization tools might be illegal and other solutions may be needed—such as connecting from public Wi-Fi networks where no registration is required.

When Plaise connects to the internet for their work they prefer to leave as few traces as possible; for example, the IP address of their home connection which can lead authorities and hackers directly to their official name and home address. Therefore, when they created their work accounts (email, sex work platforms, social media, etc.) they used Tor Browser and they only access these work accounts through their work phone or when using the Tor Browser on their computer.

++

Tor Browser

https://www.torproject.org

++

Online Accounts

To advertise their services, Plaise uses both mainstream and specialized social networking platforms. At the same time, they use different accounts on many of 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.

Edit the following table to reflect the platforms that your community actually uses.

Plaise has the following accounts:

Platform	Contacts	Real or Fake Name	Trust in Contacts	NSFW?	Disposable Account
Facebook	Friends	Realistic Fake Name 1	High	Yes	Yes
Facebook	Family	Family Name	Medium	No	No
Instagram	Friends	Realistic Fake Name 1	High	Yes	Yes
Instagram	Work	Work Name	Low	OFC!	Yes
X (Twitter)	Public	Work Name	Low	Yes	Yes
[platform]	--	--	--	--	--

Plaise considers all accounts on services that require official names or restrict adult content or sex work as disposable (see the section on "Terms of Use" in Chapter 5). For example, they try to use a realistic name on Facebook (to avoid being spotted by Facebook's bots 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, Plaise never takes for granted that these disposable accounts will last very long and makes a backup of everything they want to keep on their local machine and in an external hard drive.

To keep their accounts really separated, Plaise avoids connecting accounts to their official identity unless they have decided to or have to use it 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-worker friendly space like Tryst or commercial sex work platforms—and tells their contacts that they can find them on those more stable accounts if their other accounts are suddenly deleted or blocked.

Add any further solutions your community may have found to keep stable accounts online here.

++

Tryst

https://tryst.link

++

Payment Methods

Depending on the solutions found by your community, you may want to remove, add or change some of the recommendations listed here.

Plaise 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.

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

++

Sex Worker Helpfuls: Sex Work Approved Payment Options

https://sexworkerhelpfuls.com/payment-options
(last updated November 2018)

++

Sometimes Plaise also asks clients to recharge their bank account at a supermarket and for that they have an online bank account that offers the possibility of sending cash through a bar code. For example, Plaise can make a screenshot of the bar code in their phone banking app and send it to a client who can then go to a supermarket and pay the money by having the barcode scanned at the checkout counter.

Another option Plaise has considered is paying for a Wise (formerly TransferWise) business account which gives the possibility of having money wired to an email address.

Some of Plaise's colleagues also have their clients send money through a standard wire transfer to their bank account by giving them their bank account number without their name. Even if this can work, this is riskier because the client will see their official name appear in their bank statement.

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

Communicate with Clients

First Contact

This module should be adapted to the platforms used most by your community.

Plaise has several ways they can be reached by new clients. New clients can write to them through a form on their website, on dedicated platforms such as Tryst or *[add platforms used most by your community here]*.

Add more tips here on how sex workers advertise their services online in your area.

On all of these platforms, Plaise 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.

Please consider that in some countries where sex work is illegal and cracked down upon having dedicated pictures for sex work may be incriminating. In such cases, the strategy described in the following paragraph should be changed to something that works best for your community.

Often potential new clients will ask Plaise for more pictures so they have a portfolio of images created precisely for this purpose that are only shared via dedicated work accounts.

Advance Payments to Improve Security

This module only applies to situations where sex work is illegal and police investigations are strictly regulated by the rule of law. To create a better example, here we have used the secondary persona Anne Onimas from the guide for Berlin-based sex workers rather than our default persona Plaise Filler.

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 who 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.

Staying in Touch with Clients

In the following examples we list a strategy used by professional dominatrixes (who have more leverage on their regular clients) and a few strategies used by escorts (who have less power and generally cannot tell clients what apps they should install). It is worth discussing various strategies with your community to see what works best in their specific case. Depending on your constituency, these solutions may change a lot.

A Strategy for Professional Dominatrixes

Once Eve has decided to arrange a session with a new client, she asks them to establish a more secure communication channel than regular email. In her reply email, Eve writes:

> Hi dear,
>
> I would be happy to make plans for a session but first it would be good to establish a more trusted communication channel - both for your safety and mine.
>
> We can keep talking on one of the following platforms - just let me know which one you prefer:
>
> If you want to keep using emails, you can create an account on Protonmail: https://protonmail.com
>
> Once you've set it up, you can contact me on this address from that account.
>
> If you prefer to use a phone, we can use one of the following tools:
>
> Wire - https://app.wire.com - you can create an account with your computer and then install the app in your phone, logging in with the account you created.
>
> Signal - https://signal.org - this is also a good solution if you don't mind using your phone number. Of course, you could also get a different phone number to create an account.
>
> Let me know,
> Eve

If the client chooses Wire or Signal, Eve then sets the messages to disappear within one day so that even if she or the client loses their device the messages cannot be seen by anybody else because they will have already disappeared.

Possible Strategies for Escorts

Once they have established first contact with a new client, Plaise asks them to switch to an instant messaging (IM) app such as WhatsApp, Telegram, Signal, or Wire.

In each case, Plaise has created a dedicated account with their work phone number—or when possible only their work email. Plaise then only accesses these accounts on their work phone or through a dedicated browser (such as Tor Browser) on their computer.

When sending pictures or other sensitive information to a client, Plaise sets the messages in the conversation to disappear as soon as possible so this information won't stay forever in the client's device. Unfortunately, not all apps offer the possibility of setting a very short time frame for disappearing messages; for example, WhatsApp or regular Telegram chats will not let users have a message disappear after some seconds—which is a very useful function when sending erotic pictures that Plaise would not like clients to screenshot or save. This is why whenever possible Plaise opts to use Telegram's secret chat option, Signal, or Wire for instant messaging—and prefers not to use WhatsApp.

Online Work

While this advice should apply to any situation, if online sex work is illegal in the country you are writing for it would be worth repeating or moving advice on how to secure online connections here.

Videochat

Recently, Plaise and their colleagues started exploring ways of earning money through online work. What worried Plaise 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 Skype (which has a history of not protecting its users' privacy) but also even more privacy-friendly platforms such as Jitsi, which cannot stop users from taking screenshots or recording video calls.

In the end, Plaise decided to create an account on a platform that has been created specifically for cam work and protects sex workers from many possible threats—including clients taking screenshots. They now do their online sessions on Manyvids (manyvids.com), which puts protections in place to reduce the risk of clients exploiting their content.

Selling Pictures and Videos

Plaise also gets a small income from selling videos and pictures online. To be sure nobody can resell this content without their permission, they always add a watermark to all of them. To better plan the creation of their content, Plaise followed the tips in "A Guide for Adult Content Creators" below.

++

A Guide for Adult Content Creators

https://letagparfait.com/en/2020/12/07/a-guide-for-adult-content-creators
(last updated December 2020, see PDF link)

++

Work Websites

While this advice should apply in any situation, there may be some local regulations on the management of websites owned by citizens of your country that you would also include here.

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

Registering Domains

When Plaise decided to buy a domain for their website they looked for hosting providers that included domain privacy protection in their basic package but then they found an even better option—even if a bit more expensive. Plaise ultimately registered their domain with the anonymous domain name provider Njalla which accepts encrypted anonymous requests to register a domain and payments made with a variety of platforms including cryptocurrencies.

++

Njalla

https://njal.la

++

Hosting Providers

Because Plaise 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 (found in Chapter 5) they also want their clients to be free to stay anonymous when visiting their site. Therefore, Plaise only considers hosting providers that offer ways of implementing HTTPS (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.

Plaise's website is hosted by Red Umbrella, a provider run by sex workers for sex workers. Additionally, the following list includes hosting providers that are not based in the United States and, therefore, not bound to enforce American laws related to SESTA/FOSTA, and do not implement practices (such as banning "adult content") that can harm sex workers:

Red Umbrella: https://redumbrella.ch
- Owned and operated by sex workers
- Icelandic servers
- Free SSL certificate
- WordPress support

Orange Website: https://www.orangewebsite.com
- Anonymous sign-up (email only)
- No logging
- 2-factor authentication
- 100% green energy
- Accepts bitcoin

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

RESOURCE LIST

Access Now Digital Security Helpline: Self-Doxing Guide
https://guides.accessnow.org/self-doxing.html

Access Now Digital Security Helpline: Secure Survey Tools
https://communitydocs.accessnow.org/284-Secure_survey_tools.html

Cyber Civil Rights Initiative Safety Center
https://cybercivilrights.org/ccri-safety-center

Digital First Aid Kit: Documenting Digital Attacks
https://digitalfirstaid.org/en/documentation

A DIY Guide to Feminist Cybersecurity
https://hackblossom.org/cybersecurity

EFF Surveillance Self-Defense
https://ssd.eff.org

Gendersec Guide to Multiple Identity Management
https://gendersec.tacticaltech.org/wiki/index.php/Step_1

KeePassXC: Cross-platform Password Manager
https://keepassxc.org

Organize the Revolution While Browsing Porn
https://archive.org/details/queer-online-zine-2017

Privacy-Conscious Email Services
https://prxbx.com/email

Qubes OS
https://www.qubes-os.org

RiseupVPN
https://riseup.net/en/vpn

Security In-a-Box
https://securityinabox.org

Tails
https://tails.net

Tor Browser
https://www.torproject.org

Tryst
https://tryst.link

Without My Consent: Take Down
https://withoutmyconsent.org/resources/something-can-be-done-guide/take-down

BIBLIOGRAPHY

Kendra Albert, Elizabeth Brundige, and Lorelei Lee, "FOSTA in Legal Context," *Columbia Human Rights Law Review*, Issue 52.3, https://hrlr.law.columbia.edu/hrlr/fosta-in-legal-context/.

Jessica Betancourt, "Digital harm Reduction," LinkedIn, September 28, 2020, https://www.linkedin.com/pulse/digital-harm-reduction-jessica-bari.

Kim Burton and Anqi Li with Michael Carbone and Flo Pagano, *A First Look at Digital Security* (Access Now, 2018), available at https://www.accessnow.org/wp-content/uploads/2018/03/A-first-look-at-digital-security-digital-copy.pdf.

Michael Carbone and Flo Pagano, *Organize the Revolution While Browsing Porn* (2017), https://archive.org/details/queer-online-zine-2017.

Daniel Ó Cluanaigh, et al, *Holistic Security. A Strategy Manual for Human Rights Defenders* (Tactical Technology Collective, 2016), available at https://holistic-security.tacticaltech.org.

Samantha Cole and Emanuel Maiberg, "Anti-Porn Lobbyists Pressure Reddit to Shut Down Its NSFW Communities," *Motherboard*, vice.com, May 1, 2023, https://www.vice.com/en/article/m7bvbv/anti-porn-lobbyists-pressure-reddit-to-shut-down-its-nsfw-communities.

Alan Cooper, et al, *About Face: The Essentials of Interaction Design*, 4th ed. (Indianapolis, IN: John Wiley & Sons, 2014).

Bishakha Datta and Zarah Udwadia, *Hacking Digital Gender Norms* (Point of View, 2019), available at https://pointofview.org/wp-content/uploads/2023/01/Hacking-Gender-Norms_Web.pdf.

Lorenzo Franceschi-Bicchierai and Joseph Cox, "Inside the 'Stalkerware' Surveillance Market, Where Ordinary People Tap Each Other's Phones," *Motherboard*, vice.com, April 18, 2017, https://www.vice.com/en/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x.

Electronic Frontier Foundation, "Infographic: Why Section 230 Is So Important," https://www.eff.org/issues/cda230/infographic.

Electronic Frontier Foundation, "Section 230," https://www.eff.org/issues/cda230.

Gennie Gebhart, "The 12 Days of 2FA: How to Enable Two-Factor Authentication For Your Online Accounts," Electronic Frontier Foundation Deeplinks Blog, eff.org/deeplinks, December 8, 2016, https://www.eff.org/deeplinks/2016/12/12-days-2fa-how-enable-two-factor-authentication-your-online-accounts.

Melissa Gira Grant, "The Real Story of the Bipartisan Anti–Sex Trafficking Bill That Failed Miserably on Its Own Terms," *The New Republic*, newrepublic.com, June 23, 2021, https://newrepublic.com/article/162823/sex-trafficking-sex-work-sesta-fosta.

Harm Reduction International, "Fact Sheet: Sex Work & Harm Reduction," https://harmreduction.org/issues/sex-work/harm-reduction-facts.

David Huerta and Yael Grauer, "The Best VPN Service," *New York Times*, nytimes.com, last updated March 14, 2023, https://www.nytimes.com/wirecutter/reviews/best-vpn-service/.

Laura Jarrett and Sara Ashley O'Brien, "Justice Department seizes classified ads website Backpage.com," *CNN*, cnn.com, last modified April 6, 2018, https://edition.cnn.com/2018/04/06/politics/backpage-doj-seizure/index.html.

Duncan Ki-Aries and Shamal Faily, "Persona-centred information security awareness," *Computers & Security*, Vol. 70, September 2017, 663-674, https://doi.org/10.1016/j.cose.2017.08.001.

Sarah Jamie Lewis, ed., *Queer Privacy* (Mascherari Press, 2017), available at https://leanpub.com/queerprivacy.

Shannon Liao, "Tumblr will ban all adult content on December 17th," *The Verge*, theverge.com, December 3, 2018, https://www.theverge.com/2018/12/3/18123752/tumblr-adult-content-porn-ban-date-explicit-changes-why-safe-mode.
_____,"Tumblr's adult content ban means the death of unique blogs that explore sexuality," *The Verge*, theverge.com, December 6, 2018, https://www.theverge.com/2018/12/6/18124260/tumblr-porn-ban-sexuality-blogs-unique.

Declan McCullagh, "From 'WarGames' to Aaron Swartz: How U.S. anti-hacking law went astray," *CNET*, cnet.com, March 13, 2013, https://www.cnet.com/tech/tech-industry/from-wargames-to-aaron-swartz-how-u-s-anti-hacking-law-went-astray.

US Department of Justice: Office of Public Affairs, "Justice Department Leads Effort to Seize Backpage.Com, the Internet's Leading Forum for Prostitution Ads, and Obtains 93-Count Federal Indictment," last modified April 9, 2018, https://www.justice.gov/opa/pr/justice-department-leads-effort-seize-backpagecom-internet-s-leading-forum-prostitution-ads.

Norman Shamas, "A Brief Introduction To FOSTA-SESTA," *GenderIT*, genderit.org, November 2, 2018, https://www.genderit.org/resources/brief-introduction-fosta-sesta.

Julia Slupska, Scarlet Dawson Duckworth, Linda Ma, and Gina Neff, "Participatory threat modeling: Exploring paths to reconfigure cybersecurity," Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems, Article: 329, May 2021, 1-6, https://doi.org/10.1145/3411763.3451731.

Netzpolitik, "Why chat control is so dangerous," EDRi20, edri.org, November 17, 2021, https://edri.org/our-work/why-chat-control-is-so-dangerous.

Paz Peña Ochoa and Francisco Vera Hott, "Pornografía no consentida: ¿Cómo responden las plataformas privadas de internet a las usuarias de América Latina?," acoso.online, 2017, available at https://acoso.online/biblioteca.

Nitasha Tiku, "Craigslist Shuts Personal Ads for Fear of New Internet Law," *Wired*, wired.com, last updated March 23, 2018, https://www.wired.com/story/craigslist-shuts-personal-ads-for-fear-of-new-internet-law.

OH Yes Please, "Acronyms Models for Consent," https://ohyesplease.org/lessons/acronyms-models-for-consent.

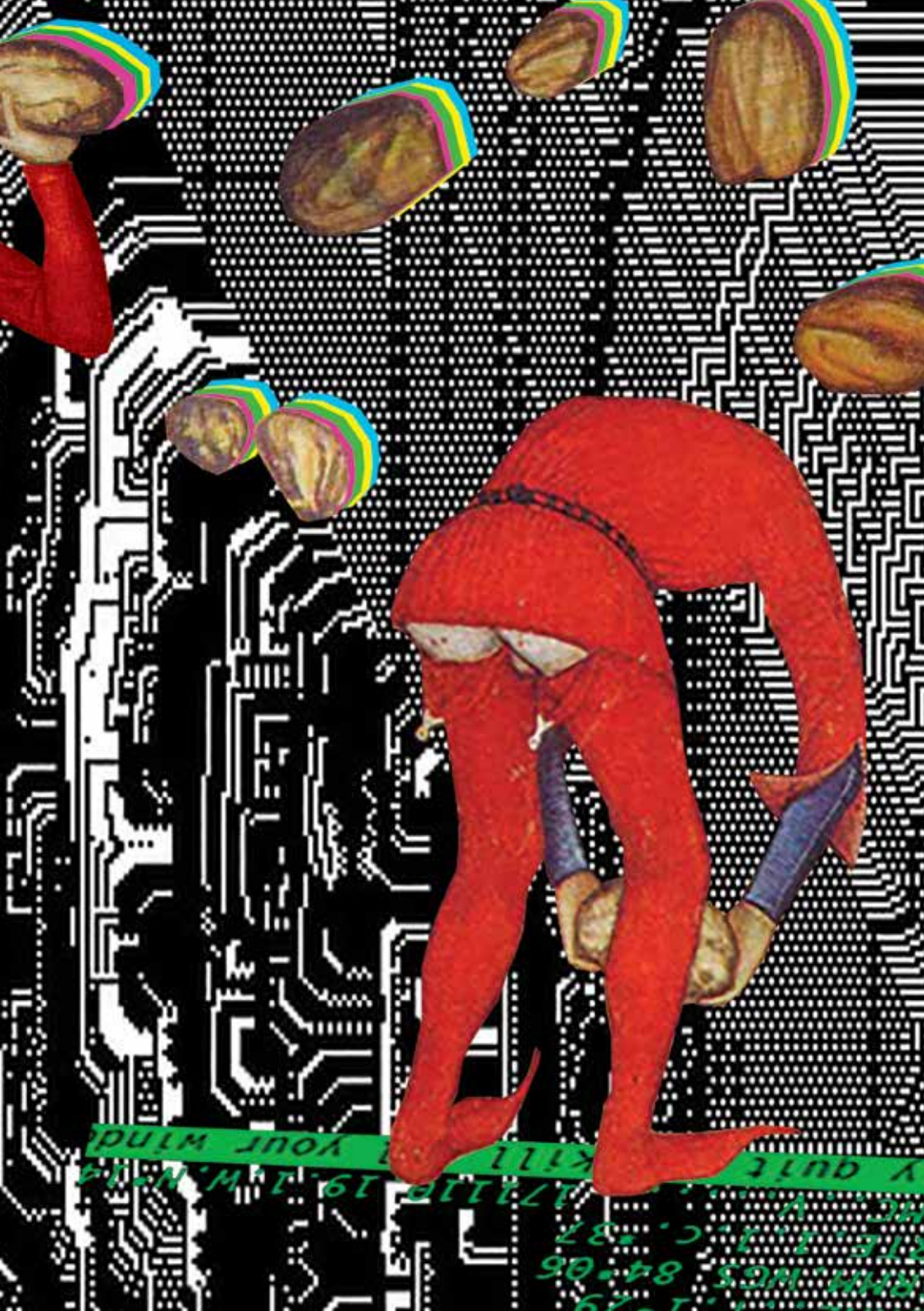
Estrella Soria and Luisa Ortiz Pérez, *Hacks de Vida: Consejos prácticos para la atención a personas que enfrentan violencias de género en línea en América Latina* (Institute for War and Peace Reporting, 2018), available at https://iwpr.net/global-voices/print-publications/hacks-de-vida-life-hacks.

Subha Wijesiriwardena, "Private Parts: Obscenity and Censorship in the Digital Age," *GenderIT*, genderit.org, June 24, 2019, https://www.genderit.org/feminist-talk/private-parts-obscenity-and-censorship-digital-age.

"Self-managed social centres in Italy: Bologna," Wikipedia, last updated September 10, 2023, https://en.wikipedia.org/wiki/Self-managed_social_centres_in_Italy#Bologna.

McKenzie Wark, *Raving* (Durham, NC: Duke University Press, 2023).

Yale Global Health Justice Partnership, "The Law and Sex Work: Four Legal Approaches to the Sex Sector," April 2020, https://law.yale.edu/sites/default/files/area/center/ghjp/documents/the_law_and_sex_work.pdf.



HOW TO CYPHER SEX is a manual for collectively writing localized digital self-defense guides that advocates self-empowerment through the use of online identity management and other digital self-defense strategies.

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

HOW TO CYPHER SEX is available online as a shareable PDF with hyperlinks at cyphersex.org.

Cover design and illustrations by Bella Merda Design.
This publication has been made possible with support from Constant.