Cybersecurity for Sex Workers

— Workshop Curriculum —

Updated May 2020

Workshop Table of Contents

Slide Deck —

We put together several slide decks that you can present at your workshop to help guide participants through the content.

Implementation Hub —

In addition to this curriculum, we created a document that gets you started on installing some of the tools we talk about in the workshop.

Welcome!

What is this —

This is a **curriculum guide** built to give you an understanding of your digital footprint, and share safer practices with your community. Our goal is to provide easily accessible materials to help you run workshops that teach sex workers how, why, and when to use cybersecurity tools & strategies to protect themselves and their careers. We've done our best to gather suggestions for safer online practices – check out the section "Who's it for (and who's it by)" to read more about our sources. The strategies and suggestions in this guide reduce risk. They do not eradicate it. We can't ensure that, even if you implement everything to a T, you will be 100% safe online. But, we can promise that implementing just some of these strategies will leave you in a better position to track your digital footprint.

Mantaining an online prescence as a sex worker has always come with challenges, and the risks have only grown after 2018's SESTA/FOSTA laws. In the digital landscape post-SESTA/FOSTA, platforms that were previously friendly to sex workers are tightening their content regulations, which robs many of the basic protections and opportunities that other communities are afforded online. Now more than ever, we hope this curriculum will be used as a community resource to help you keep your accounts, browsing history, and personal life more secure from bad actors, information leaks, and increasingly common legal crackdowns.

Here you'll find:

1) A **Curriculum Guide** of cybersecurity strategies for safer sex work. This is a compilation of our research, laid out for you to jump straight into learning and teaching.

2) An accompanying **Slide Deck** that will aid you in running workshops on these topics. All sections in this curriculum have corresponding slides, which you can see below.

3) An **Implementation Hub** with a list of links and resources for how to use / install all of the tools mentioned throughout this curriculum. Since you might not be able to lead workshop participants in the installation process for all of these tools, we've compiled these services' installation guides for participants to use on their own after the workshop. Feel free to provide this link to all of your participants at the end of your time together.

Who’s it for (and who’s it by) —

We’ve built this for sex workers, educators, advocacy groups and allies that are looking to protect their online work. Whoever you are, you don’t need a sophisticated tech background to use this curriculum. If you run any part of your business on online platforms, or know those that do, this curriculum is for you. We got our info from public domain sources, including sex worker outreach projects, blogs, forums, interviews, and cybersecurity orgs.

The authors (us)

This curriculum was put together by Franky Spektor and Annalise Kamegawa. They met through the design community at UC Berkeley and have become collaborators on several human-centered design projects at the intersection of technology and ethics. In the last year, their focus has been on developing this workshop curriculum in collaboration with SWOP LA, and developing a tactile sex education model with a community of blind and visually impaired folks (BVI) in the Bay Area.

Franky is a design researcher working with communities at the margins and messy intersections. Her work focuses on co-creating accessible tech with local disability leaders, and designing against a variety of platform abuses. She is also currently involved in menstrual technology research, seeking to actively change the discourse around disability, sexuality, and tech development. In fall of 2020, she’s starting a PhD to continue building better fem tech.

Annalise is a designer who has leveraged modern technology to reimagine the potential for tech products and educational curriculum. She also graduated from UC Berkeley with a degree in Cognitive Science, focusing on the implementation of human centered design methods as a means of incorporating science and technology into community-driven products. Her driving design philosophy is to make real things that real people really need to use. Next year, she will be pursuing a masters in product development for emerging technologies.

To sex workers (who might also be educators)

Whether this is your first time looking into the world of cybersecurity, or you’re a seasoned expert, we hope that this guide can help you feel more secure in how you operate online. Our work was greatly supported by the folks at Sex Workers Outreach Project in Los Angeles (SWOP LA), a chapter of SWOP USA. Our work also builds on resources created by Danielle Blunt’s project Hacking//Hustling. In addition to Mistress Blunt, there are many amazing people who are contributing information to the world of online sex work like @sxnoir, the VP of @womenofsextech, Isobel Andrews, the folks who put together SexWorkHelpfuls, and all the sex workers who have shared their stories and experiences online.

To educators (who might also be sex workers)

Thank you for helping lead the spread of this information. The content here acts as a guide to help you lead workshops. If you are looking for more information on best practices for leading workshops, check out Our Data Bodies' work. They created a great guide called the Digital Defense Playbook that looks at the ethics and nuances of running workshops that tackle topics at the intersection of identity and technology. We've also drawn from the work of cybersecurity organizations, including the Surveillance Self-Defense project by the Electronic Frontier Foundation, and SimplySecure. Both these organizations have published their own curriculum guides on topics ranging from VPNs to Threat Modelling How-To's to a Security Education Companion for first time teachers.

To allies

If you're an ally, great! Thanks for using this resource too. Check out "85 Ways to Make Sex Workers' Lives a Little Easier" by Femi Babylon for other ways to be a more informed ally.

Further Research —

While we did our best to put together the most up-to-date information for you, best practices in cybersecurity change every day. **These implementation instructions were put together in the spring of 2020**. Between the publishing date of this guide and now, better software may have been released or more secure platforms may have been developed. **Before implementing any of the tools below, we encourage you to do your research about any of the mentioned platforms or methods to get the most up-to-date information.**

The Electronic Frontier Foundation (EFF) updates their site regularly and the people / communities we mentioned above also contribute more work to the field everyday — these are fantastic, reliable places to start your research.

Workshop Curriculum

Section 1.0 Building a Security Plan —

Introduction to Building a Security Plan, or “Threat Modeling”

As a sex worker who conducts business online, your data and privacy are open to several unique risks. In order to work through these risks and how to begin implementing solutions we’re going to do an exercise around **Threat Modeling.**

Threat modeling is a way of outlining and assessing the adversaries and threats you may face when participating in certain activities. It will also help you know how to prepare for your personal worst-case scenarios, and think through which strategies are worth implementing.

Digital Mapping Exercise

Let’s start by defining what a personal cybersecurity strategy looks like for each of us. The following are 5 main questions to consider when creating a threat model for your online presence. As you go through the questions, ask participants to write down or call out examples for each category. **Encourage folks to draw from their own experiences, or the experiences of people in their community.**

We’ve started with a few examples below as prompts.

The following questions are taken from the EFF’s activity, “Your Security Plan”. The version below comes from a version that was last updated on January 10, 2019. It’s part of their bigger cybersecurity project “Surveillance Self-Defense”. We’ve added it here with a few examples that might help you contextualize these questions for your niche in the industry.

If you’re looking for a tangible resource to guide your workshop, the EFF’s Threat Modeling Activity Handout (English, Spanish) offers a printable & editable worksheet that you can bring to your workshop.

Question 1 / What do I want to protect?

- **These are ASSETS**
  Examples: my identity; my money; my online following

Question 2 / Who do I want to protect it from?

- **These are ADVERSARIES**
  Examples: the government; individuals who want to harass me, my personal circle, local law enforcement, ICE, abusive ex-partners

Question 3 / How bad are the consequences if I fail?

- **These are POTENTIAL THREATS**
  Examples: physical safety is threatened; payment apps or accounts get frozen, exposure to friends and family, child protective services, getting scholarships revoked, being unable to post on social media, pseudonym leads back to your real name, revealing information about friends and family

Question 4 / How likely is it that I will need to protect it?

- **These are ADVERSARIES' CAPABILITIES**
  This is the big unknown for many! For instance, doxxing may be fairly uncommon, but have huge consequences. Being shadowbanned might be much likelier, but with lower overall risks. These trade-offs are something that we'll continue thinking through here.

Question 5 / The last, most important threat modelling question:

- ***How much trouble am I willing to go through to try to prevent potential consequences?***

With each cybersecurity section we go through, we'll be using this kind of threat modeling to determine what tools to use, when, and against what. This next section will discuss your digital footprint, and some of the ways your online activities can be made safer.

Section 2.0 Your Digital Footprint—

Introduction to Digital Footprint Basics

What does it mean to be cybersecure? To begin answering this question, we first need to look at our **digital footprint**, or the trail of **personal information** that's left by your **browsing, posting, and messaging**. Understanding where you are on the internet can help you target your adversaries which can range from a personal stalker to third-party trackers that can follow you across websites.

Here we introduce the three most important practices you can take to ensure your digital footprint is as sparse and unconnected as possible — so that your identity stays safe under your online activity.

To minimize your digital footprint, we'll be teaching you how to 1) **separate your accounts**, 2) **use encryption**, and 3) **use anonymous browsing**.

The first practice is to maintain **(1) SECURE ACCOUNTS:**

Digital Mapping Exercise

Ask participants, "Where do you exist on the internet?" Please make a list of all the apps that you use to talk and communicate (email, Facebook, Instagram, text message, etc).
Now write down all the groups you talk to (friends, family, cash subs, clients, dayjob coworkers, etc). **Encourage folks to draw from their own experiences, or the experiences of people in their community.**

Thinking about the threat models we just made, what happens if these groups cross? Is your identity leaked in potentially dangerous ways? Some platforms, like Facebook, make this leakage all too likely by showing your connections and suggesting potential friends.

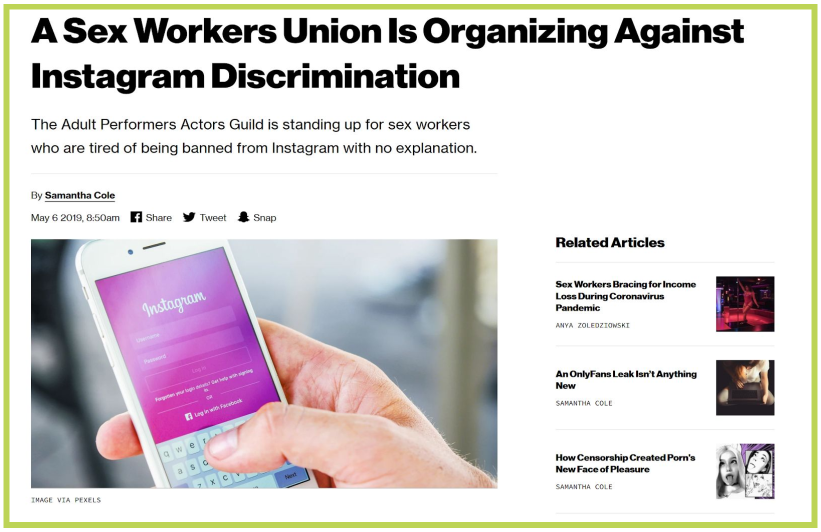
These communication examples come from the Doxxing Self Defense guide, created by Hacking//Hustling.

Account Separation Intro /

To keep this from happening, one of the best things you can do is **maintain different accounts** for your communications between your work communities and personal communities. Separating your email accounts is a great way of making sure your personal life stays separate from your work life.

How to Keep Accounts Secure: Now that we're separating our accounts, how can we make those separate accounts as secure as possible? The answer is to **make sure those accounts can't be linked with similar data.** The more different your information across separate accounts is, the better.

What's the harm of reusing your identifying credentials? If Instagram bans one of your accounts, they will target all your affiliated accounts through the same phone number.



A Sex Workers Union Is Organizing Against Instagram Discrimination

The Adult Performers Actors Guild is standing up for sex workers who are tired of being banned from Instagram with no explanation.

By Samantha Cole

May 6 2019, 8:50am Share Tweet Snap

IMAGE VIA PEXELS

Related Articles

Sex Workers Bracing for Income Loss During Coronavirus Pandemic
ANYA ZOLEDZIOWSKI

An OnlyFans Leak Isn't Anything New
SAMANTHA COLE

How Censorship Created Porn's New Face of Pleasure
SAMANTHA COLE

A Sex Workers Union Is Organizing Against Instagram Discrimination: "Suz Ellis['s]… first Instagram account, devoted to body-positivity, was deleted in 2015. In 2018, an Instagram account she made for her sex writing blog was removed at 14,000 followers." Accounts are taken down everyday for what Instagram deems as "inappropriate content." Although shadow banning is sometimes unavoidable, you can take steps to protect your accounts. This is an example to help contextualize this work. Feel free to use this in your workshop or ask for an example from your group.

Separate Accounts, trackers & browsers /

We are about to go into why it is important to have separate accounts for your work and personal life. At the end of all this, even though you can have completely different accounts with completely different sets of credentials, if you are using the same browser to do both personal and work related tasks, your information could still get linked through third-party trackers.

Consider using separate a separate browser for your work to avoid this linkage. For example, conduct all personal matter through Chrome, but do your work through Firefox.

If using two different browsers seems like a big hassle, consider Firefox's Multi-Account Containers.

Anatomy of an Account /

Using the same credentials across accounts, such as your email and phone number, allow for bad actors or platforms to connect your accounts. Often, the consequences can be worse than just being booted off Instagram, particularly when leaked data reveals aspects of your personal life.

Getting Started: Have you been part of a data leak?

If you have the time and resources to do so, look and see if any of your emails have been part of a mass data breach. Haveibeenpwned.com looks at what data breaches your email is attached to while also revealing what kind of data is associated with that email address.

Activity: haveibeenpwned.com

Dutch Prostitution Site Hookers.nl Hacked—250,000 Users' Data Leaked

Thomas Brewster Forbes Staff
Cybersecurity
Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

In 2019, a hack on the website Hookers.nl led to a security breach for its users. Forbes reported that "'...a data breach has occurred and the email addresses have been stolen from all users.' They claimed the email addresses were being offered for sale online by the hackers and recommended users change their login details." Ask the group to talk *about some unintended consequences they've experienced or heard of in regards to not separating email accounts.*

By differentiating your credentials across accounts, you are taking an important step to prevent doxxing.

Let's go through the **anatomy of an account** to learn how to make your credentials as differentiated as it can be. Here we'll learn about everything that goes into an account, such as how to **create secure passwords** for each of your profiles, **use multiple emails**, and **make new phone numbers.** Using these tools, you can make sure you never use the same email address or phone number twice when signing up for services.

Passwords /

For both your online presence and communications accounts, **password management** is essential. Using multiple privacy tools and keeping track of so many accounts is a lot to handle, and it might be tempting to share passwords between them. However, this is one of the most important ways that you can make sure your hard work stays protected!

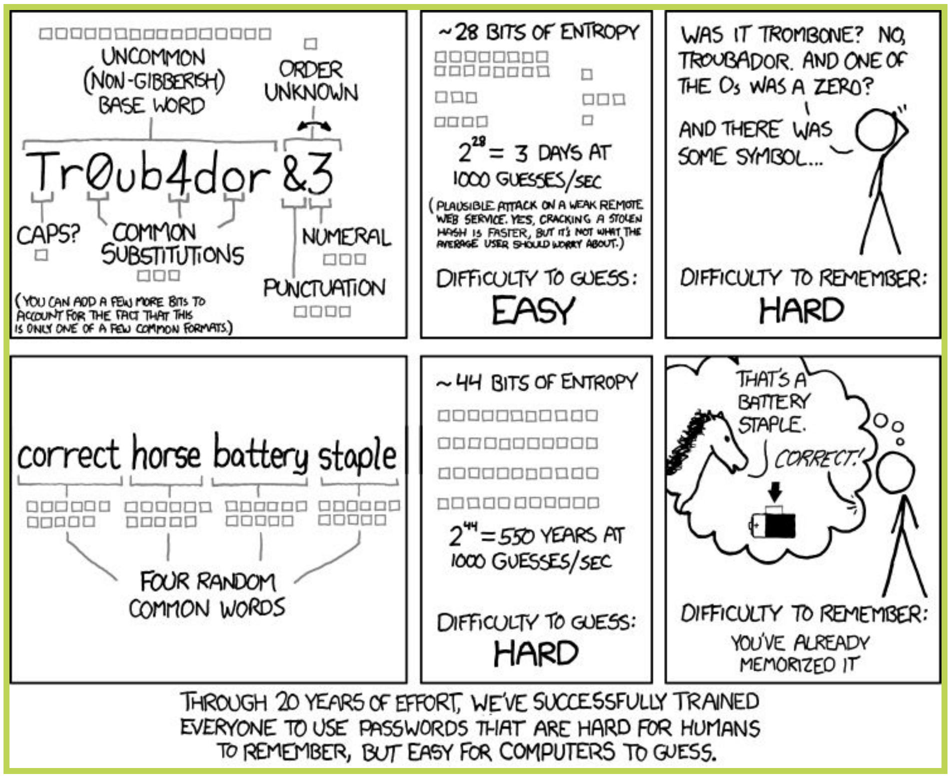
💡 **The Dangers of Using Biometric Data**

Why use a password as opposed to fingerprint/ facial recognition?

If you use a biometric data-based method (facial recognition, thumb print, vocal recognition) to secure your devices, a face or thumbprint is all that's needed to access your device, **posing a huge threat to the security of your device**. Now, law enforcement or clients have an easy way of accessing your device without your explicit consent. It should be noted that it is illegal for law enforcement to force you to unlock your device, but this hasn't stopped them in the past.

It is recommended that all your passwords are alpha-numeric based so you and only you can access your device. Some people might have issues with spelling for randomly-generated passphrases. Try and devise a passphrase that can be memorized and easily spelled.

What makes a strong unique password? ***Multiple words for a long but simple password are often best.*** *See this great example about what makes a secure* *password from an (XKCD) comic below. Complicated letter and symbol combinations end up being hard for humans to remember, but easy for computers to guess.*


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Some experts recommend using the diceware method to create multiple-word passwords. The diceware method uses only a dice and the word list provided on www.diceware.com. For more information on how to create passwords with the dice method, check out our take-home Implementation Hub.

These methods are a great start, but for the best protection, consider using a **Password Manager.** Password managers can automatically generate and fill in strong, unique passwords for all your accounts. All you need to remember is a single master password to access the "password vault" rather than attempting to memorize a bunch of multi-word passwords for all your accounts. Most password manager applications offer additional convenient capabilities, like auto-filling your credit card and frequent flyer information. Some browsers offer a password manager. This can help you avoid phishing attacks because a browser is able to remember where a password and username were assigned whereas humans can often fall prey to deceptive mimicry.

The only downside: password managers are often paid, with some exceptions. PCMag put together two lists that talk about their favorite password managers — paid services and free services. Read them through to choose the best one for you. The EFF also gives you in-depth instructions on how to implement KeePassXC. They chose this because it is a free password manager and "more actively developed than some of the alternatives."

For teachers: You may hit a lot of roadblocks in getting your students to incorporate a password manager into their workflow. Here's a guide from the EFF (Password Managers) that can help you guide your students into implementing a password manager. It contains a helpful FAQ and additional readings that will give you a better grasp on this ins and outs password managers. See more information on both password managers and the diceware method in the Implementation Hub.

Getting Started: How Strong is your Password

If you have the time and resources to do so, we recommend helping your participants get started with password security by going to the below link and having participants enter a couple fake passwords. Try comparing to the XKCD comic password "correcthorsebatterystaple". The site shows both the strength of the passwords and how long it would take a computer to guess it.

Activity: https://howsecureismypassword.net/

Haven't had enough of passwords? The EFF created a quick guide that summarizes what a weak and strong password look like

Creating temporary or placeholder emails /

Now that you've got super strong passwords, let's look at the other big two pieces of account anatomy: your **email and phone number**. There are lots of services out there that let you make as many emails and phone numbers as you want, to make sure that every account you make is unique and isn't traced back to a digital footprint that points directly back to you. We're listing a few tools below, but be sure to check out the Implementation Hub for more details about their features and how to install them.

Email Accounts: For email accounts, you can use **ProtonMail** (or even **Gmail**) to create as many accounts as you want. Consider encryption as one of the factors when choosing an email service — we will cover exactly what encryption is and why it matters in the next section.

- ProtonMail: end-to-end encryption when **both parties** are using it
- Gmail: uses encryption in transit (HTTPS and STARTTLS), but it's not end-to-end encrypted, so communications are visible to the company.

*As a reminder - *look at what kind of information you'll be revealing when starting an account.* Sometimes you will need to provide a phone number or a user name. Keep in mind how this type of info might link your identity to multiple accounts.

Temporary or Placeholder Phone Numbers /

Virtual Phone Numbers: You can create virtual phone numbers as easily as email accounts. Below are some of the platforms that offer virtual phone number creation.****Be careful about using the following services for texting/calling as many of them do not offer end-to-end encryption**** These services will only protect you from clients or platforms **knowing your real phone number — NOT keeping your activity safe from law enforcement.**

- Google Voice
- Skype
- FreedomPop
- Textnow

Use the above platforms to screen clients, or set up an appointment. For sensitive information (like payment), never use unencrypted text services.

In certain high risk situations, you may also consider carrying multiple phones, or using burner phones. According to Cathy Reisenwitz's blog, one reason you may want a burner phone is so you can use "fresh phone numbers in your ads. The more places you use the same number, the easier it is to connect your work to your identity." We've already seen that social media apps often cross-list your info. For instance, **searching a cell phone number on Facebook brings up your full name and profile picture**. Reisenwitz suggests, "For extra security, **use cash to buy your prepaid phone**."

In lower risk situations, if you're just looking to give a new number to a client, you can create a dummy number on Google voice and register it with a Signal account. This way, you get to end-to-end encryption and a new number without having to get a whole new phone.

Even with burner numbers, there are still risks if you use a burner app on a phone tied to your real ID. Law enforcement can compel burner phone applications to turn over their records, and their information will directly tie you to every ad you've ever placed. Reisenwitz says your best best is to use burner apps on a burner smartphone!

Digital Mapping Exercise

Below is a table we encourage you to fill out with your participants. There's a lot to keep track of when choosing certain services for certain purposes. The categories laid out below help to clarify the limits of each service

GOAL: By completing this exercise, participants are left clearly understanding the limitations and capabilities of the platforms they are thinking about implementing. They come out with a better understanding of what services they can use for the specific needs of their work.

The Service(s)	**The Service's Function**	**What to Use it For**	**What Will it Protect you From**	**What it Won't Protect you From**
Example: Google Voice, Skype, FreedomPop, Textnow	These services will generate new phone numbers for you	Use these "fake" numbers to sign up for new accounts; upon an **initial** screening of a client	Having to connect your real phone number across multiple accounts; Client knowing your real phone number	These services are not encrypted, so they will be able to access your conversations or supply them to law enforcement
Burner phones				
Burner apps				
...				
...				

Set up two-factor authentication:

Okay, one last thing. Passwords alone are sometimes not enough to protect an account. If your password is leaked in a data breach or an adversary gets a hold of your account information, your password becomes a useless form of protection. **Two-factor authentication (2FA)** is an additional method of verification that is used in combination with your account's password password to create an extra barrier to entry for your accounts. It's essentially a way of telling your account, "hey! This is really me" after a password has been entered.

Many internet services and platforms offer 2FA, from Amazon to WhatsApp to Twitter. You might have also seen your email provider prompt you to use 2FA, or needed to use 2FA as part of an organization or school.

“As PCMag's lead security analyst Neil J. Rubenking puts it, "there are three generally recognized factors for authentication: ***something you know*** *(such as a password),* ***something you have*** *(such as a hardware token or cell phone),* ***and something you are*** *(such as your fingerprint). Two-factor means the system is using two of these options."*

As you first venture into 2FA, the way you will verify your identity after entering a password will typically fall in the “something you have” category. From most ideal to least ideal, this can be hardware tokens, authentication apps, or an SMS message.

When choosing a method of 2FA, think about who you’re protecting your data from. Have your phone on you while meeting with clients? You may think about using an app-generated code over biometric data like a thumb print. The same vulnerability may be present when interacting with police, who could force your hand on your phone.

It is also recommended by the cybersecurity field to avoid using SMS (when you’re texted a code) because of the potential vulnerabilities from hackers, who only need to know your phone number to nab your code. This is recommended because the practice of “SIM jacking” has become a common way for hackers to access accounts. SIM jacking is not a rare occurrence, but it’s better to have SMS as an extra padlock than not use 2FA at all. If you do find yourself using SMS verification often, secure your cell account by setting up a passcode with your cellphone service provider. SMS verification aside, adding an extra layer of security to your cell service provider is just good practice considering the frequency of SIM jacking.

What should you use instead? It’s often recommended to get an authenticator app such as Google Authenticator, Authy, or Duo. However, it’s better to use 2FA with SMS than to not use 2FA at all! Check out the Implementation Hub for more resources on 2FA from this EFF article, which links you to instructions on how to set up 2FA on popular platforms. The EFF also provides a worksheet that guides users through the nitty-gritty of setting up and using 2FA.

Additional practices:

Following these guidelines on differentiating the anatomy of your accounts will go a long way to protect your privacy and livelihood. In addition to technical resources, make sure that you’re also being careful not to let sensitive information leak in the content of your communications. After all that work, don’t include a link between your personal and work accounts in your bios! Don’t use a work email for a personal instagram account.

💭 **Remaining Questions**

Despite the research in this document and our conversations with experts, you might encounter some remaining questions. For instance, how am I supposed to create a brand? Can I use the same username for all my accounts? What kind of personal information ***can*** I share without being tracked? We'd love crowdsourced insights for these or other questions as you run workshops. If you have any suggestions on these topics or further questions, reach out to us at sw_cyberproject@protonmail.com.

The second practice is to maintain **(2) ENCRYPTION:**

Now you have a secure ecosystem of accounts! But what about the content that's bouncing back and forth between them? After learning the basics of keeping a safe account, we can talk about the second big practice in cybersecurity, **encryption**.

Digital Mapping Exercise

Look at the last message you sent to a client. What would it mean if...

- Your day job employer
- Your landlord
- Law enforcement

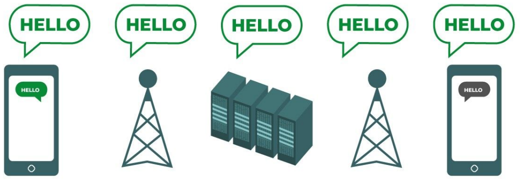
...read that message? What platform was that message on? Depending on the level of encryption used by your communication platform, these scenarios become more or less likely.

Encryption is an important part of making sure the recipient of your message, and only the recipient, is able to read what you sent. In this section, we're going to learn about different levels of encryption, so you know what platforms to use for different kinds of communication.

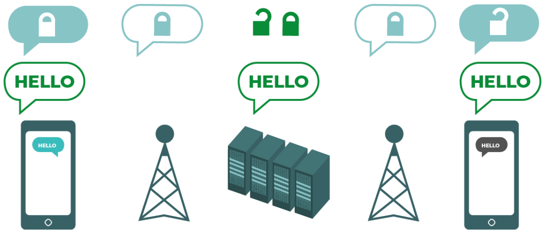
What is Encryption in Transit? /

Encryption is a way of scrambling data so only certain parties can read or interpret it. There are various types of encryption and different degrees to which your data could be scrambled. To start, let's think about what it means to send a digital message.

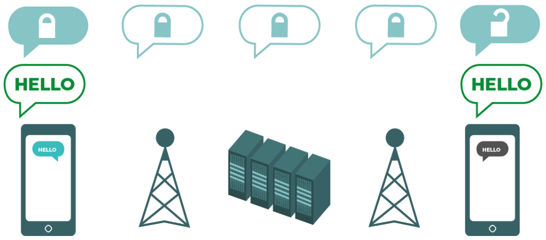
Sending a message over a communication app is a lot like sending a letter. But unlike using the post office, your message's digital journey can be filled with many more prying eyes. What happens when you send a message over a communication service platform? Who can see it? Below is a look at unencrypted data in transit, moving from your device to another person's through an app-owned server. Talking over some unencrypted communication apps is like **sending a letter without an envelope** — everyone from the company, to bad actors on your local network, to your internet service provider has access to your private content.



Many companies use transport-layer security (TLS), which protects your data as it travels to and from the company's servers. This is like sending a letter in an envelope that only the post-office can open and read before forwarding it to your recipient. When you use platforms like Facebook messenger or Gmail, you're using TLS. These companies can fully see, store, and sell your conversations. **What content would it be ok to send this way?**



Is there content that wouldn't? If so, there is a third even more secure option, called end-to-end encryption. No one, including the app or platforms you're using, can see your information except you and the receiver. That's what you're getting when you use platforms like Signal. But, just like when you send a letter in a sealed envelope, the post office (and platform) can still see your message's destination and sender address, the time it was sent, how big the package is, etc.



When do you need end-to-end encryption for your communication? The EFF Surveillance Self-Defense guide provides the following guiding questions:

- **Do you trust the app or service you are using?**
- **Do you trust its technical infrastructure?**

- **How about its policies to protect against law enforcement requests?**

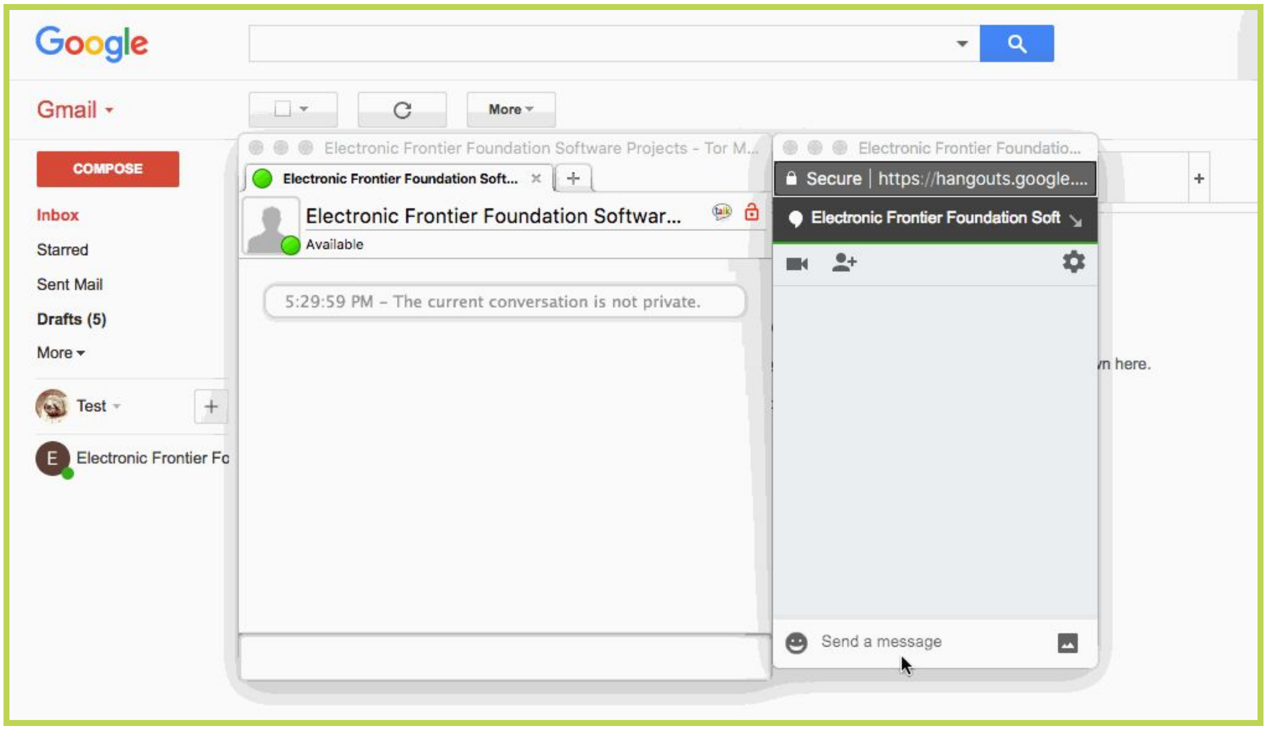
According to the EFF, if you answer “no,” to even one of these questions, then you might need to use encrypted platforms for your communications.

The diagrams above and part of this curriculum draw from the EFF’s Surveillance Self-Defense Guide’s section on Encryption Basics.

How Does End-to-End Encryption Work & Why should I use it? /

“Information is turned into a secret message by its original sender (the first ‘end’), and decoded only by its final recipient (the second ‘end’). To be truly secure, only the ‘ends’ of the conversation should have the keys that let them encrypt and decrypt” (EFF). Importantly, this means that **if you’re using a platform with “end-to-end” encryption, not even that platform will be able to view your content**.

As we saw from our diagrams, it is easy for messages to be intercepted. Using encrypted platforms for your communications is one easy way to make sure that even if your messages *are* intercepted, anyone reading them will see only gibberish.


Google
Gmail
More
COMPOSE
Inbox
Starred
Sent Mail
Drafts (5)
More
Test
Electronic Frontier Fo
Electronic Frontier Foundation Software Projects - Tor M...
Electronic Frontier Foundation Soft...
Electronic Frontier Foundation Softwar...
Available
Electronic Frontier Foundatio...
Secure | https://hangouts.google....
Electronic Frontier Foundation Soft
Send a message
n here.

5:29:59 PM – The current conversation is not private.

Here’s what end-to-end encryption really looks like in real time in this Google Hangout chat example from the EFF.

Tools & Platforms to Encrypt Your Messages /

What platforms can I use? You can use end-to-end encryption for any communication, including voice and video calls, messaging and chat, and email. We've included a basic overview of your options. While these apps encrypt the messages while getting from your phone to a client's, the messages will still exist on both devices once it's sent.

Please prompt participants to read more about how to use each tool in depth in the Implementation Hub.

Signal, ProtonMail, What's App, Wire, PGP (Pretty Good Privacy)

- *Signal: "*Can be used as an end-to-end encrypted option if both sender and recipient are using it, but the app also allows for others to receive messages as unencrypted SMS." Signal is lauded as one of the best security protocols out there, and their open source platform has been implemented by other services including Facebook's Secure Messenger option. The source code is open source, meaning it is publicly available to be audited by the wider security community. Although the developers have announced plans to move toward a username based registration model, a user must register a new account with a phone number.

- *WhatsApp*: Provides end-to-end encryption, which means both the sender and the recipient's messages are secured. It provides the same automatic encryption for calls. Word of caution: now owned by Facebook: any precautions you can and should take with Facebook messenger should be applied to WhatsApp. WhatsApp uses the Signal protocol.
    - Facebook encrypted messaging:
- *Wire:* A messaging app that offers end-to-end encryption of messages, calls, and shared files. *Doesn't require a phone number to use it. You can also send self-destructing messages. The other party also has to have wire to message them.
- *Keybase:* Keybase is another app for encrypted messaging and filesharing. It can be used on both mobile and desktop devices. Many find it easier to handle larger group messaging on Keybase.
- *PGP (Pretty Good Privacy)*: This is a tool used for encrypting emails through any email platform/service. Both the sender and the receiver need a key to be able to send and read the messages. Although PGP can be quite effective, many find it to be technically difficult to implement.
- *ProtonMail*: supposedly offer end-to-end encrypted email messages. Like PGP, they use a key system to encrypt and unlock messages. However, ProtonMail

has lately come under attack for not being as secure as they advertise. Some cybersecurity experts maintain that Gmail is actually still the safest bet.

A Note on Facebook as a Method of Communication & Advertising:

Some sex workers prefer not to use any mainstream social media platforms at all; others find that advertising their public persona with Facebook is a great way to connect with fans and drive business towards *legal* revenue streams such as their OnlyFans or ManyVids, or their modelling.

Your risk tolerance with Facebook is a personal decision. As you consider your threat model for this platform, take a look at the following considerations:

- What part of your work are you trying to keep private?
- What parts of your work are you trying to advertise?
- Absolutely avoid working on Facebook
    - This includes communicating with clients and discussing illicit service through the platform

- Are you comfortable communicating to your friends, community, or fans about the work you do?
    - Be judicious and careful about what you say
    - Make the assumption that what you're saying in a chat/comment is **public**
    - While Facebook messenger offers end-to-end encrypted messaging services through their "secret messages" service, beware that the message exists on your device and the receiver's device (Facebook Secret Conversations). Messages must be deleted on both sides for it to be gone. Additionally, your communications are subject to an enormous amount of metadata from your targeted advertisements and friend profiles.

    - If you're looking for a more usable encrypted messaging system**, we suggest using Signal** whenever possible instead

- How to maintain a brand safely (fan page, personal page)
    - Be intentional about what platforms you're advertising through Facebook. Be careful to only link legal platforms and services — and never link to illegal activity
    - Make sure you don't look like you're trying to sell sexual services on Facebook

Getting Started: Install Signal

Signal is an end-to-end encrypted messaging platform, widely used by sex workers. If you have the time and resources to do so, we recommend helping your participants get started by installing Signal as part of the workshop. If this ends up being the only end-to-end encrypted messaging tool you use, you're well on your way to having a more secure digital footprint.

Once information is on your phone, it's available for others to see if they have access to your device. Enable message deletion, or periodically go through your messages and delete them

Signal works through your phone number, so make sure to install it on your phone first. Then you can have the convenience of receiving messages in a desktop app.
https://signal.org/download/

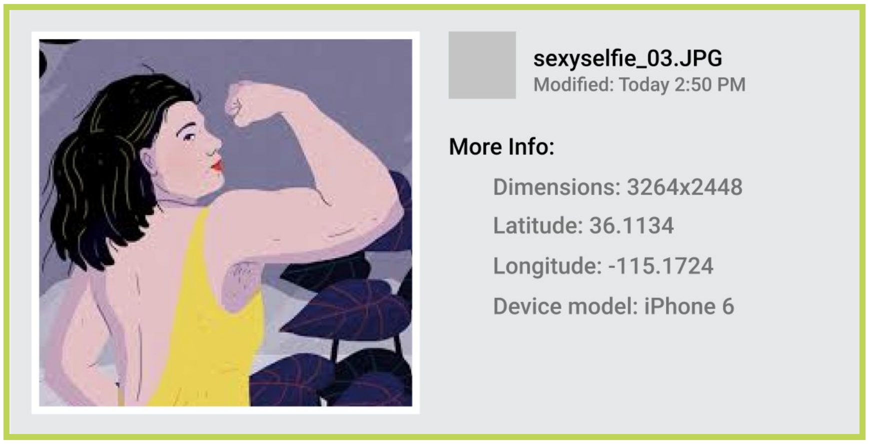
When Does Encryption Fail /

Though encryption can go a long way to protect you, it's not airtight. There are a few ways that encryption can fail, or situations where it doesn't cover what you think it might. End-to-end encryption "only protects the content of your communication, not the fact that you are communicating in the first place. It does not protect your **metadata:** everything *except* the content of the communication.

This includes the subject line of an email, who you are communicating with, and when. Time spent on a call, your location when you make a call, when a call took place, the recipient — all this is metadata.

Also consider: do you trust the person you are communicating with? It could be the case that they're taking screenshots of your correspondence. What if their device is compromised? Malware or phishing can pose a threat to your communication.

Removing Mobile Metadata



sexyselfie_03.JPG
Modified: Today 2:50 PM

More Info:

Dimensions: 3264x2448
Latitude: 36.1134
Longitude: -115.1724
Device model: iPhone 6

All digital photos, including the ones taken on your phone, have a file attached to it called an Exchangeable Image File Format (EXIF) File. "In addition to all the bits dedicated to the actual picture, it records a considerable amount of supplemental metadata … [including] date, time, camera settings, and possible copyright information." The illustration in this image was created by illustrator Laura Breiling.

According to How To Geek, "You cannot stop EXIF metadata from being added to your photographs, though you can **prevent geo tagging by simply turning it off in your camera or camera app.**" In in awesome article by Unbound Babes called How to Store Your Nudes & Other Advice from a Cyber Security Expert, the author similarly advises **turning off location tracking services on your other phone apps** so the geo tagging metadata isn't stored.

Here's some advice they gave on removing metadata via your mobile device: "On a phone, **Fluntro or Photoexifeditor** are useful." Learn how to scrape metadata from your photos manually in the Implementation Hub.

Non-digital Metadata

File metadata isn't the only kind to pay attention to. Also make sure that any images you send don't have any background information that could reveal where you're located (street signs, address information, license plates, etc.) The EFF suggests, "The best thing you can do is to be aware of **what metadata** you transmit when you communicate, **who can access** that information, and **how it might be used**."

A parting note: Encryption doesn't work against insider threats! You may have protected your content from external actors, but make sure you can also trust the people you are interacting with.

Remaining Questions

Participants may wonder, How do I ask a client to use the same service that I am using? A few strategies here could include asking clients to create accounts upon agreement of service. "Create a ProtonMail account to talk to me, it's for **your own safety**!" You might mention legal ramifications, or suggest it so a spouse won't be able to see.

Another question is, How do I know if someone has taken a screenshot of something I sent? Some platforms don't allow this, such as OnlyFans. This one's tougher to answer for every platform, especially if it's being accessed through a VPN. We'd love crowdsourced insights for these or other questions as you run workshops. If you have any suggestions on these topics or further questions, reach out to us at sw_cyberproject@protonmail.com.

The last practice to implement is **(3) DECREASED SURVEILLANCE BROWSING**:

Keeping **accounts separate** and **content encrypted** are two very important ways of keeping yourself anonymous. However, your computer's **IP address** is one identifier we often overlook — this last section shares a few ways of continuing to keep yourself safe online by anonymizing your IP address as you browse the internet. Besides your IP address, web applications are often riddled with fingerprinting mechanisms that advertisers and other third party trackers use to identify you and your habits. These can be piecemealed together across your entire browsing history to identify who you are and what you're up to online. Without the proper protections in place, this is how different accounts and applications you use can begin to "learn" things about each other.

Digital Mapping Exercise

Have you ever tried to read an article, watch a TV show, or play an online game on a network that wouldn't let you? For example, Netflix won't let you stream in another country. Ask participants, What did you do? In such cases, maybe you tried the mobile site, tried the site with a different country URL at the end… or used a VPN.

A **Virtual Private Network (VPN)** is software that masks your IP address and makes it look like you're coming from somewhere else, by routing your Internet activity through a private server. It is often used for censorship circumvention—for example, when you are using a school's censored Internet connection or in a country that blocks content. It also keeps your **browsing anonymous from your internet service provider**.

Why decreased Surveillance Browsing is Important /

Sex Workers Are Moving Online, Supporting Each Other During Coronavirus

By Nastia Voynovskaya Mar 25

With more sex workers moving online because of Coronavirus, it's important to incorporate cybersecurity into your practices. The piece "Sex Workers Are Moving Online, Supporting Each Other During Coronavirus" provides more tips and community orgs that can help you make the move to onlline work.

What are the potential threats of browsing? Let's get into a brief intro to **ISP's (Internet Service Providers)**, and your computer's **IP address** versus external servers. You don't need to remember all of this jargon, but the relationship is pretty simple.

Your IP address: The "IP" part of IP address stands for "Internet Protocol." The "address" part refers to a unique number that gets linked to all online activity you do, like a return address on a letter you'd send out.

Internet Service Providers, or ISPs: XFinity, AT&T, Verizon are examples of ISP's. They are the ones that give you an IP address based on your location and what network you're using. ISP's are able to see valuable information when you connect to a WiFi network. What are some examples of what they can see? If your data is not encrypted, potentially your email, your passwords, every single site you've visited… that's pretty bad if the government asks your ISP to release potentially illegal activities.

💡 Who's Responsible? ISPs & SESTA/FOSTA

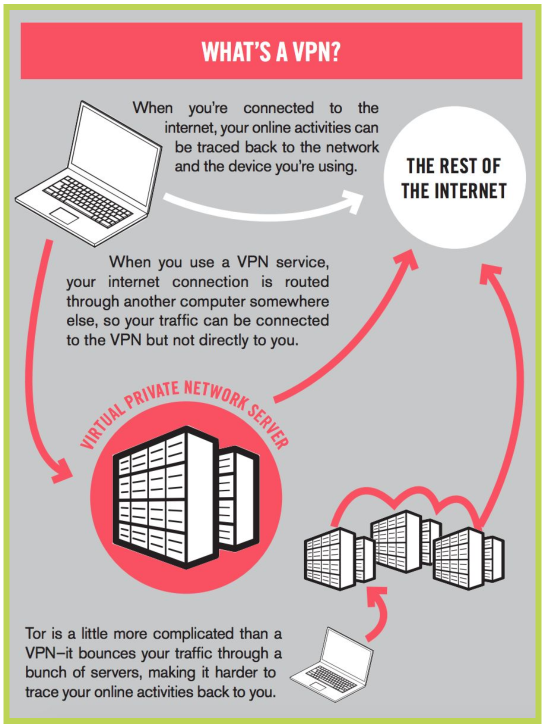
In 1996, the online community rallied to include section 230 into the Communications Decency Act (CDA). This important portion of the CDA says that ISPs are not considered "publishers" of information. Therefore, they are not held accountable for the website & content they provide access to. (Section 230 of the Communications Decency Act, The EFF)

In 2014, when Redbooks.com was shut down for hosting services related to sex work and prostitution, the US government decided to hold ISPs more accountable for their content. In the coming years, the development of SESTA/FOSTA would target the criminalization of child trafficking organizations and to more heavily criminalize online sex work.

SESTA/FOSTA makes amendments to CDA 230 in an attempt to hold ISPs accountable for hosting a service that "promotes or facilitates prostitution and sex trafficking or advertises sex trafficking," (*All Sex Workers Deserve Protection: How FOSTA/SESTA Overlooks Consensual Sex Workers in an Attempt to Protect Sex Overlooks Consensual Sex Workers in an Attempt to Protect Sex Trafficking Victims Trafficking Victims*, Heidi Tripp).

Knowing what an ISP is and how to navigate one is so important because it plays a central role in SESTA/FOSTA legislation.

How and When to Use VPNs /



WHAT'S A VPN?

When you're connected to the internet, your online activities can be traced back to the network and the device you're using.

When you use a VPN service, your internet connection is routed through another computer somewhere else, so your traffic can be connected to the VPN but not directly to you.

Tor is a little more complicated than a VPN–it bounces your traffic through a bunch of servers, making it harder to trace your online activities back to you.

This is a fantastic, simple diagram representing the relationship between your computer (IP address), your ISP — shown here as "the rest of the internet" — and a VPN. VPNs are like tunnels that route your address to a single private server (owned by the VPN company) before accessing the internet. TOR works much the same way, but moves your info through at least three different volunteer servers. This diagram was found in the guide Online Worker Safety Hazards and Cautions from Hacking//Hustling.

While you don’t need to use a VPN for all your browsing, it can be helpful to:

- Hide your browsing activity from your local home network or public networks, such as public wifi in a cafe
- Access geo-blocked websites, from Netflix to the Erotic Review
- Bypass internet censorship
- Download or torrent files

To learn more about the details of how a VPN works, we recommend looking at this EFF intro guide to VPNs. Some VPNs are paid, while others are free. The EFF suggests using this article from *That One Privacy Site* to gage the pros and cons of various VPN services. There is no one size fits all for your VPN so you need to assess your own risks and what you want to protect before choosing one to implement.

One easy place to **begin** your research is with ProtonVPN, created by the same company that produces ProtonMail. This company is quite aware of their sex worker client base, and will often tailor their products to worker needs.

The limits of a VPN: By using a VPN, you remain anonymous to ISP’s, but this **doesn’t guarantee you’re anonymous to the VPN itself**. If law enforcement suspects that you’ve been conducting illicit activities online, they could ask your ISP for your internet traffic. This is because under SESTA/FOSTA, ISPs are also held liable by the government for hosting sexual content. So, while using a VPN can help to hide your activity from your ISP, just remember that doing so transfers your trust from your ISP to your VPN.

While VPN traffic is much harder to pin down by law enforcement, VPN’s are still susceptible to warrants from the police. VPNs are businesses first and foremost, and own their own dedicated servers to reroute your address. This makes tracing back your history as simple as a quick search in a server log.

💡 Camming & your IP address

Much like sending nudes, camming can expose you to risks of being doxxed. When you send a nude, an Exchangeable Image File Format (EXIF) file is attached that could reveal your location. When streaming on a platform, your IP address could expose similar location data. The following are steps you can take to keep your personal information safe:

- Use a VPN (virtual private network) whenever you can to protect your IP address from revealing your location
    - Sites like Chaturbate, LiveJasmine & Camsoda collect your IP address and share it with third-party organizations. Using a VPN will give these platforms an IP address that doesn't link to your physical location
        - Chaturbate privacy & cookies Policy
        - Cam Soda Privacy
        - LiveJasmine Privacy Policy
    - Skype now hides your IP address by default, but it once released user IP addresses that were easily readable. Check how services handle IP addresses before using streaming platforms and web-based chatting services.
    - Some VPNs are slower than others. Think about the resolution and speed you want to stream at when choosing a VPN.
    - Some camming sites won't allow you onto their platform, or even ban you, if they detect that you are using a VPN. Check the platform's policy before logging on with a VPN.
- Look at the kinds of geoblocking services your cam site offers
    - Ex: Cam4 allows you to block select "countries, States or Provinces from viewing your profile."

Your IP address is only one way your location can be revealed. The following are other things to consider when interacting with clients you meet in a chat room

- Be careful about the information you reveal with your background and conversations
    - Be careful to hide any products or objects in the background of your chats that could clue the audience in to where your located
        - Ex: flyers, take-out boxes, and school materials can give clues to where you live
    - Avoid speaking about events, landmarks, or businesses that are specific to your area
- Your Amazon wishlist may be revealing your home mailing address.

- Sounds & conversations in the background of your stream, such as your housemates or partner(s), have the potential to reveal personal information about yourself.

Check out Cam4's quick guide to maintaining your privacy for other precautions to take while camming.

Choosing the right browser /

Choosing the right browser can do a lot to mitigate your concerns around security and privacy. Like with many of the tools you choose, there is a negotiation between privacy, security, and convenience. Chrome Browser, being developed by Google, is a fast and secure browser that protects users from many security concerns that other browsers may face. But being made by Google, it is no surprise that its privacy standards are pretty dismal. Firefox, on the other hand, is built with users' privacy in mind. Another option is the Brave browser. Like Firefox, the browser holds user privacy at the center of its mission. It aggressively blocks ads and works to stop ad tracking across platforms. Additionally, it's a super fast browser that's built on Chromium, an open-source project run by Google that makes up the nuts and bolts of Chrome. These three options are easy to use, but neither are as privacy oriented as the Tor browser.

No matter which browser you choose, it's always worth stepping into the settings of that browser to enhance the privacy and security settings that come out-of-the-box.

What about Incognito or Private Browsing Mode? Incognito mode is **NOT ENOUGH** to really keep you anonymous online. It doesn't mask your IP address, and only prevents your browser from storing your search history or cookies. In Incognito Mode, your activity is still perfectly visible to your ISP.

How and When to Use Tor/

You may have also heard of a service called Tor, The Onion Router. To access the Tor network, you need to install the Tor browser. Tor performs a similar function to a VPN, but is arguably more secure at protecting both your privacy and anonymity than a VPN. Unlike VPNs, Tor is a non-profit open source project. Because the Tor project doesn't make any money or own any of their own servers, it uses something called a "trustless network," which means that no one individual or actor *could* reveal your data even if asked by the government. It does this by routing your information through 3 randomly chosen volunteer servers, rather than a single server owned and paid for by the VPN. No one single volunteer server has all the information to retrace your identity. **This means**

that if you're trying to protect yourself specifically from government surveillance, it is the safer choice.

The downside is that it is always a bit slower to have your information move through 3 nodes (rather than just one for VPNs) and that it's generally **more of a technical challenge** to use outside of just a browser. Lastly, **Tor is not for torrenting** — they will disable Flash, Quicktime, and RealPlayer.

Using Browser Extensions to Increase Privacy and Security /

https://www.google.com

You're familiar with the HTTPS at the start of your web addresses. Hypertext Transfer Protocol **Secure** (HTTP**S**) is a modern extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet.

We'd recommend getting HTTPS Everywhere, a browser extension developed by the EFF and the Tor Project, will help keep you from visiting sites with expired or invalid security certificates. It's a safety measure which provides authentication of the website's identity and connection, and also encrypts the information shared between you and that website from unauthorized viewing. This means protection from hackers on your local network and viruses. If you remember transport layer security (TLS) from the Encryption section, HTTPS Everywhere basically guarantees that for all the sites you visit! Some browsers enable this by default, though it's nice to have some peace of mind that you have an extension in place to ensure you're protected!

Third party tracking and fingerprinting mechanisms are in place in nearly every website you visit. These things are silent but deadly, using increasingly sophisticated techniques to track you across websites and sell that data to the highest bidder. Thankfully, there are some browser extensions built specifically to prevent these nasty trackers from doing that! Privacy Badger is another extension developed by the EFF. It uses "heuristics" to detect tracking behaviors on websites you visit, attribute those behaviors to the different trackers that are doing them, then prevent those trackers from tracking you on any site you visit. Though there are other great tracker blocking extensions on the market, Privacy Badger is different in that it gets smarter over time, learning about more trackers as you browse the web. Also, it is open source, so the code itself is publicly available to read and audit.

For a more concerned threat model, you can disable Javascript altogether on your browser. NoScript is a browser extension that does just that. Although it will break the functionality of many sites you visit, it can greatly increase your security posture.

Getting Started: Install HTTPS Everywhere

If you have the time and resources to do so, we recommend helping your participants get started with secure browsing by installing HTTPS Everywhere as part of the workshop. This is a good way to start browsing more securely on the internet.
HTTPS Everywhere is an extension to Chrome, Brave, Firefox, Opera and Torbrowsers. Make sure that one of these browsers are set up first before doing the activity.

Set up instructions: https://www.eff.org/https-everywhere

Remaining Questions

Participants may wonder, How do I check a VPN's policy? How do they make money if they're free — with my data? In large part, the answer to this question is yes. Try to choose VPNs that are made for public service, such as ones developed by security organizations. If you have any suggestions on these topics or further questions, reach out to us at sw_cyberproject@protonmail.com.

Thank you!

Thank you so much for taking the time to look at this **curriculum guide**. We hope it has equipped you with some basic tools for a robust understanding of your digital footprint!

Though these recommendations will go a long way, just know that there is no way to be 100% safe online. Please stay vigilant, and work with us to help improve this curriculum. We encourage you to contact sw_cyberproject@protonmail.com with any questions, additions, or changes you'd like to see for this toolkit.

Hey! You didn't answer *this* question —

Hopefully in our future projects we can cover that topic! Send us an email at sw_cyberproject@protonmail.com and we can look into it for future workshops.

In the meantime, we encourage you to look for answers on your own. Through our research, we discovered a bunch of folks who are creating a lot of cool work at the intersection of sex work and technology. If your question can't be answered with a Google search, you can try to post to Switter "a sex worker-friendly social network." You can also check out the site Sex Worker Helpfuls, and particularly the Tumblr they run. When looking for online communities, look for platforms that are made and maintained by sex workers.

What's next —

This is just the beginning. We're currently working on creating several short educational modules around the specifics of sex work + cybersecurity.

In the near future, we aim to cover topics including:

- What to do when you're doxxed
- How to safely maintain social media accounts
- How to choose an online sex work platform that you can protect yourself on
- covering device encryption (eg preparing for an instance where your phone is seized -- particularly in the section about passcodes)
- threat modeling for backups and account recovery (what to do if you lose access to files)
- resources on opsec with regards to digital security

Drop us a line to let us know what you'd like to learn!