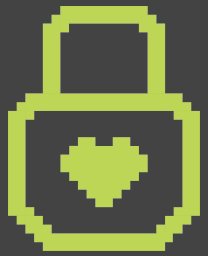
Threat Modelling

Cybersecurity for Sex Workers

Updated May 2020



Introduction to Threat Modelling

Threat Modelling

- Outlining and assessing the adversaries and threats you may face when participating in certain activities
- A way to prepare for your personal worst-case scenarios
- Method of figuring out which strategies are worth implementing

Threat Modelling

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.

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.

What do I want to protect?

- These are **ASSETS**

Examples: my identity; my money; my online following

Threat Modelling

Who do I want to protect it from?

- These are **ADVERSARIES**

Examples: the government; individuals who
Want to harass me, my personal circle

How bad are the consequences if I fail?

- These are **POTENTIAL THREATS**

Examples: physical safety is threatened;
payment apps or accounts get frozen

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.

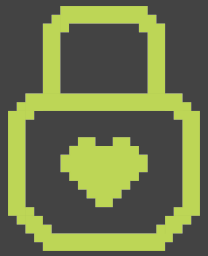
How much trouble am I willing to go through to try to prevent potential consequences?

- The last, most important threat modelling question!

This will help you assess what tools you will end up using

Your Digital Footprint

Cybersecurity for Sex Workers



Introduction to Your Digital Footprint: The Basics

What does it mean to be *cybersecure*?

Three important practices:

To ensure your digital footprint is as sparse and unconnected as possible, we will cover:

1. **SECURE ACCOUNTS**
2. **ENCRYPTION**
3. **ANONYMOUS BROWSING**

1. SECURE ACCOUNTS

1. Secure Accounts

Digital Mapping Exercise

Where do I exist on the internet?

Make a list of all the apps that you use to talk and communicate

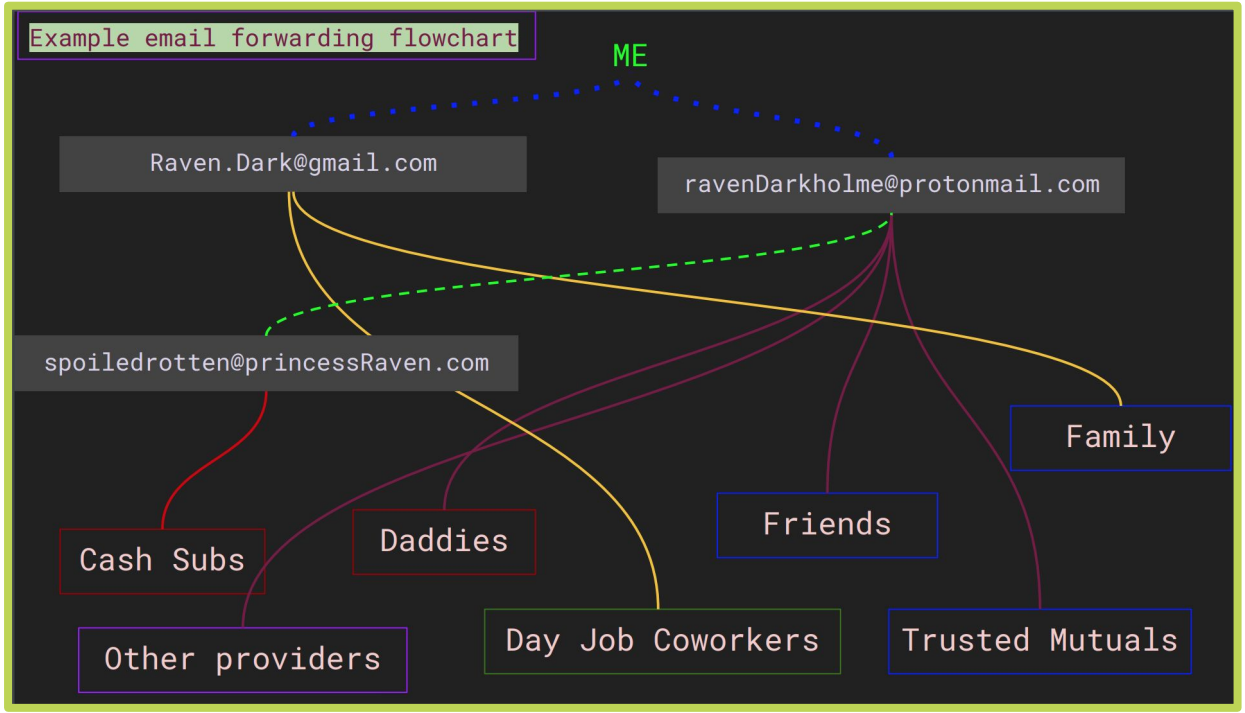
- (email, Facebook, Instagram, text message, etc)

Now write down all the groups you talk to

- (friends, family, cash subs, clients, dayjob coworkers, etc)

1. Secure Accounts

Account Separation



This image is from the Doxxing self-defense example diagram from Hacking//Hustling

1. Secure Accounts

Anatomy of an Account

- Password
- Name
- Phone number
- Email

Diversify these between accounts
so your identity remains anonymous.

1. Secure Accounts

Anatomy of an Account

What's the harm of reusing your identifying credentials?

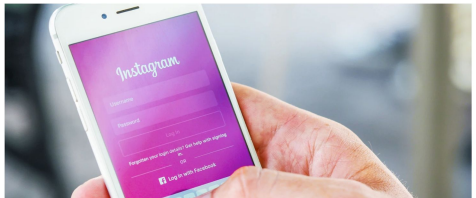
Example: If Instagram bans one of your accounts, they will target all your affiliated accounts through the same phone number or email.

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



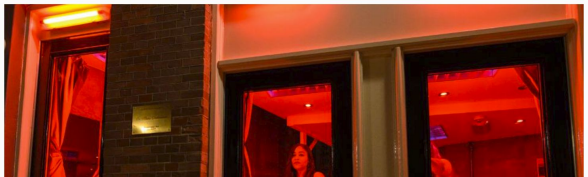
Related Articles

Sex Workers Bracing for Income Loss During Coronavirus Pandemic
ANYA ZOLEDZIOWSKI

An OnlyFans Leak Isn't Anything New
SAMANTHA COLE

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.



1. Secure Accounts

Passwords

The Dangers of Using Biometric Data Passwords

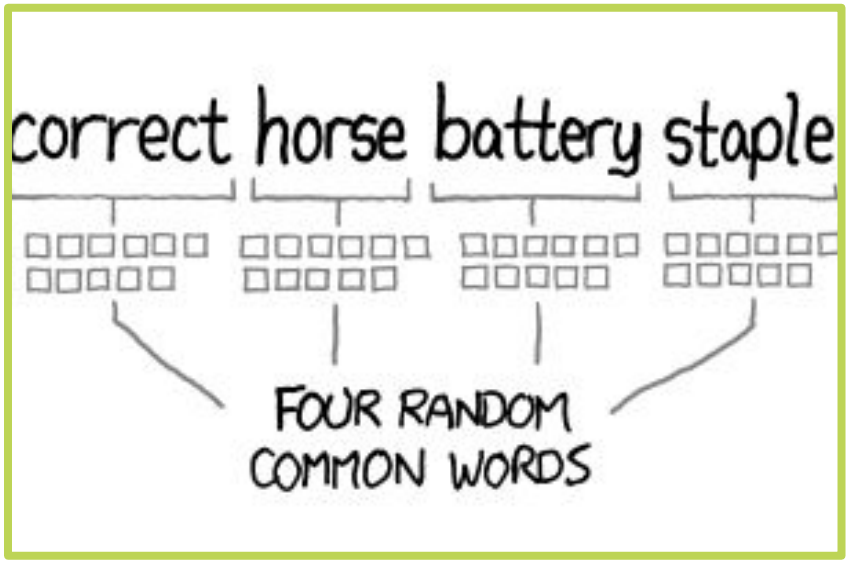
Ex: Facial recognition, thumb print, vocal recognition.

Physical force from law enforcement or clients pose a **huge threat to the security of your device**.
Use alpha-numeric passwords so you and only you can access your device.

1. Secure Accounts

Passwords

What makes a strong password?



- *Multiple words*
- *Long strings*
- *Easier for humans to remember but harder for computers to crack*

1. Secure Accounts

Passwords

Some experts recommend using the dice method to create these passwords.

11126	abase	11256	adam	11426	agony	11556	algal
11131	abash	11261	adams	11431	agree	11561	alger
11132	abate	11262	adapt	11432	ague	11562	algol
11133	abbas	11263	add	11433	agway	11563	ali
11134	abbe	11264	added	11434	ah	11564	alia
11135	abbey	11265	addict	11435	ahead	11565	alias
11136	abbot	11266	addis	11436	ahem	11566	alibi
11141	abbott	11311	addle	11441	ahoy	11611	alice
11142	abc	11312	adele	11442	ai	11612	alien
11143	abe	11313	aden	11443	aid	11613	alight
11144	abed	11314	adept	11444	aida	11614	align
11145	abel	11315	adieu	11445	aide	11615	alike
11146	abet	11316	adjust	11446	aides	11616	alive

1. Secure Accounts

Passwords

Password Managers: a single master password to access the “password vault” rather than attempting to memorize different passwords for all accounts

- Most password manager applications offer additional capabilities, like storage of credit card and frequent flyer information. .
- Password managers are often paid, with some exceptions. See a list and more information on both password managers and the diceware method in the Implementation Hub..

1. Secure Accounts

Getting Started:

Test your password!

Enter a fake password. Compare the strength to the “correcthorsebatterystaple” password example from the XKCD comic. This site shows both the strength of the password and how long it would take a computer to guess it.

https://howsecureismypassword.net/

1. Secure Accounts

Creating email accounts

Easily create **different emails** for different accounts:

- ProtonMail - end to end encryption when **both** parties are using
- Gmail - not encrypted

Be sure to check out the Implementation Hub for more email creation options.

1. Secure Accounts

Creating phone numbers

You can create **virtual phone numbers** as easily as email accounts:

- Google Voice
- Skype
- FreedomPop
- Textnow

****Be careful about texting/calling on these platforms, as many of them do not offer end-to-end encryption**** *Check out the Implementation Hub for more number creation options.*

1. Secure Accounts

Burner phones

Consider carrying **multiple phones, or using burner phones.** You can use fresh numbers in your ads, or avoid being found on Facebook if someone searches your number.

- Buy burner phones with cash
- Use “burner numbers” (previous slide) on your burner phone!
- Don’t use social media or Gmail on your burner work phone

1. Secure Accounts

Digital Mapping Exercise

- There’s a lot to keep track of when choosing certain services for certain purposes. On the next slide, there’s a table to fill out to help you clearly understand the limitations and capabilities of the platforms you might think about implementing.

- Think specifically about what services you might use for your specific line of work.

1. Secure Accounts

Digital Mapping Exercise

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				
...				
...				

1. Secure Accounts

Two factor authentication

Passwords are sometimes not enough to protect an account. Like an extra padlock, 2FA is a way to verify that ***you*** are the one accessing your account. Offered by many platforms, including Amazon, WhatsApp, Twitter.

- Avoid SMS (easy to steal number and trace back to you)
- Consider risks with clients or law enforcement if using fingerprint
- But…. better to have either of these as an extra padlockthan nothing at all!
- Best of all, get an authenticator app, like Google Authenticator

Additional Practices

And remember…

After all that work, **don’t include a link between work and personal accounts in your bios!**

2. ENCRYPTION

Now you have a secure ecosystem of accounts!

But what about the content that’s bouncing back and forth between them?

2. 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?

2. Encryption

Digital Mapping Exercise

What platform was that last message on?

Depending on the level of encryption used by your communication platform, these scenarios become more or less likely.

That’s where encryption comes in!

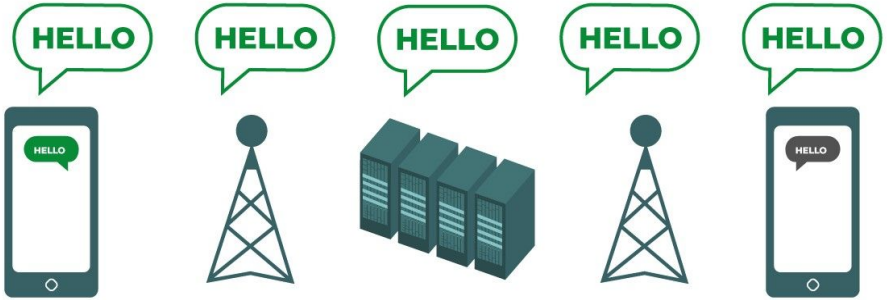
2. Encryption

What's Encryption

What happens when you send a message over a communication service platform? Who can see it?

Unencrypted data in transit:

- Like sending a letter without an envelope

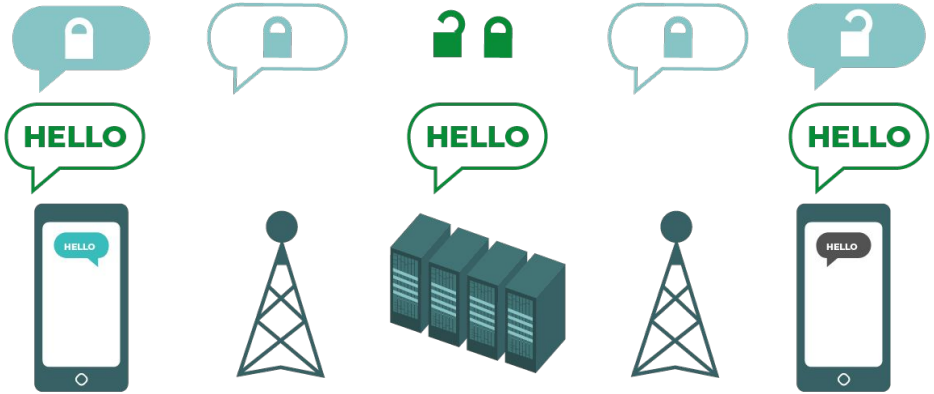


2. Encryption

What's Encryption

Transport layer security (TLS), used by most companies:

- Like sending a letter in an envelope that only the post-office can open
- TLS examples — Facebook & Gmail

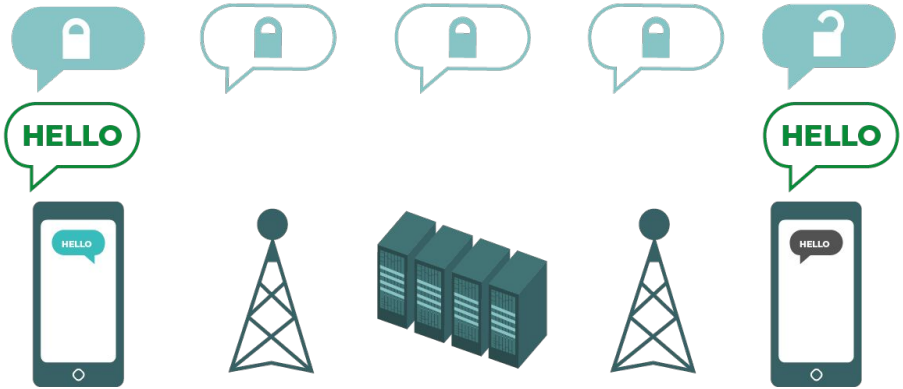


2. Encryption

What's Encryption

End-to-end encryption:

- Like sending a closed letter whose contents only you and receiver can see. Return address, date, etc. remain open.
- Encryption examples — Signal



2. Encryption

What's Encryption

When do you need end-to-end encryption?
Questions from the EFF:

- **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?**

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

2. Encryption

How Encryption Works

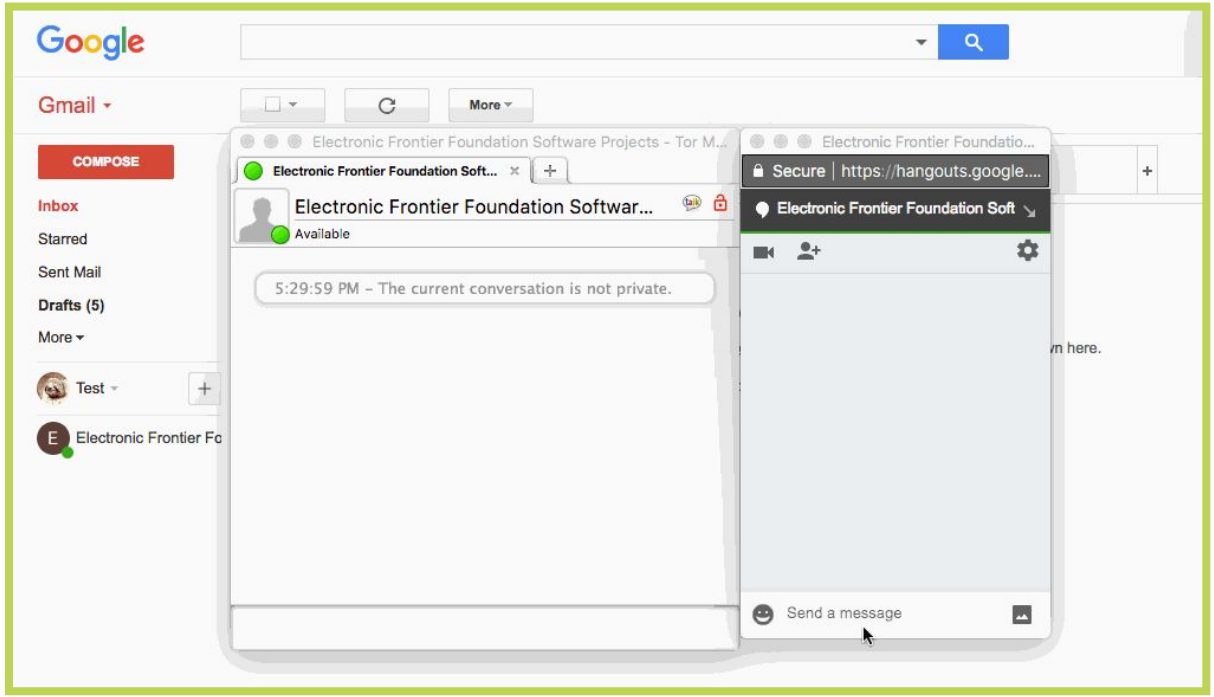
How to protect the content of my communications?

Encryption turns information into a secret message. In end-to-end encryption, only the original sender (first end) and the receiver (second end) have the key.

Even if your messages *are* intercepted, anyone reading them will see only gibberish.

2. Encryption

How Encryption Works



Here's what encryption really looks like in real time in this Google Hangout chat example from the EFF.

2. Encryption

Tools & Platforms to Use

You can use end-to-end encryption for **any communication,** including voice and video calls, messaging and chat, and email.

- ***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" (1).

- ***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.

Continued...

2. Encryption

Tools & Platforms to Use

- ***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.

- ***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.

- ***ProtonMail*:** offer end-to-end encrypted email messages. Like PGP, they use a key system to encrypt and unlock messages.

2. Encryption

Facebook : Chatting & Advertising

Consider these questions before using Facebook:

- 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: 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?
    - Assume that all the messages you send are **public**, even with Facebook's secret message service
- How do you maintain a brand safely with a fan page or a personal page?
    - Make sure you don't look like you're trying to sell sexual services on Facebook - be intentional about the platforms you link to

2. Encryption

Getting Started:

Install Signal

Signal is an encrypted messaging platform, widely used by sex workers. If you only take one step to safer messaging, let it be this one!

https://signal.org/download/

2. Encryption

When Encryption Fails

End-to-end encryption does not protect your **metadata:** everything *except* the content of the communication

- Subject line of an email
- Who you are communicating with, and when
- Time spent on a call
- Your location when you make a call
- The recipient

2. Encryption

Mobile Metadata

sexyselfie_03.JPG
Modified: Today 2:50 PM

More Info:

Dimensions: 3264x2448

Latitude: 36.1134

Longitude: -115.1724

Device model: iPhone 6

When you send a selfie, you're also sending supplemental metadata like date, time, camera settings, and your exact location.

Not good.

The illustration in this image was created by illustrator Laura Breiling.

2. Encryption

Mobile Metadata

You can’t prevent all metadata from being added to your photos. But there are a few other steps you can take:

- Prevent geotagging by turning it off in your camera app
- Turn off location tracking in your other phone apps
- Use apps like Obscura (iOS only) to remove metadata from your photos
- See our Implementation Hub to learn to remove metadata manually

2. Encryption

Non-digital Metadata

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**.”

- Check for visual background info that reveals your location
  street signs, address info, license plates)
- Encryption doesn’t work against insider threats! Make sure you trust your network

3. DECREASED SUREVEILLANCE BROWSING

3. Anonymous Browsing

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?

What did you do in this situation to get access to the content?

3. Anonymous Browsing

Virtual Private Network (VPN)

A VPN can get you around certain online barriers.

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.
- Keeps your browsing anonymous from your internet service provider.

Why Anonymous Browsing is Important

- 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 about **Incognito 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

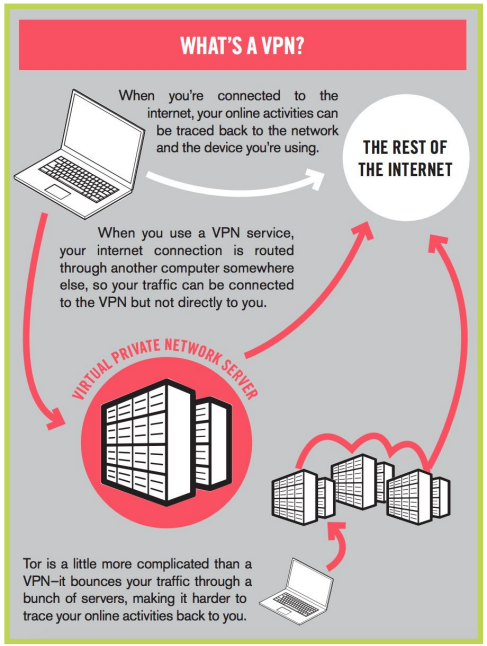
3. Anonymous Browsing

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)

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)

How and When to Use VPNs



This diagram was found in the guide Online Worker Safety Hazards and Cautions from Hacking//Hustling.

There are many reasons and situations to use a VPN as a sex worker. Post-SESTA/FOSTA, many erotic websites and sex worker-friendly platforms have **decided to avoid legal liability by blocking US visitors**. 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 and ISP
- Access geo-blocked websites
- Bypass internet censorship
- Download or torrent files

The limits of a VPN

- VPNs are businesses, and own their own servers to reroute your address.
- By using a VPN, you remain anonymous to ISP's, but **this doesn't guarantee you're anonymous to the VPN itself**.
- If the government has a reason to acquire your data, it can get a warrant from your provider OR a VPN to pursue legal action against you.

By using a VPN, **you transfer your trust from your ISP to your VPN**.

3. Anonymous Browsing

How and When to Use TOR (The Onion Router)

- 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. 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.

Using a Browser Extension

- **Hypertext Transfer Protocol Secure (HTTPS)** 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.

- The browser extension **HTTPS Everywhere** helps ensure the web pages you visit are encrypted. It will help keep you from visiting sites with expired or invalid security certificates.

3. Anonymous Browsing

Getting Started:

Install HTTPS Everywhere

- Let’s get started with secure browsing by installing HTTPS Everywhere
- HTTPS Everywhere is an extension to Chrome, Brave, Firefox, Opera and TOR browsers. If you have one of these, great! Let’s get started

HTTPS Set-Up Instructions

We've introduced a lot of tools & platforms.

Look out for our **Implementation Hub**, which will help you use and install all the resources mentioned in this workshop.

Thank you!

Cybersecurity for Sex Workers

Still have questions?
Drop them to
sw_cyberproject@protonmail.com
so we can keep improving this material.