DIGITAL PROTECTION FOR SEX WORKER RIGHTS DEFENDERS

Developed for

APNSW
ASIA PACIFIC NETWORK OF SEX WORKERS

in Consultation with

FRONT LINE DEFENDERS

DIGITAL PROTECTION FOR SEX WORKER RIGHTS DEFENDERS (SWRDs)

Developed for

APNSW
ASIA PACIFIC NETWORK OF SEX WORKERS

in Consultation with

FRONT LINE DEFENDERS

July 2022

Table of Contents

Fundamentals of Digital Protection

Addressing Common Threats to SWRDs

Introduction

> *ICT (information and communication technology) refers to technology (mobile phones, tablets, computers) used to connect and communicate with other people. This includes the internet, dating sites, escort sites, smartphone apps (e.g., Tinder, Grindr, WhatsApp), social media platforms (e.g., Facebook, Twitter, Instagram) and many more. ICT is profoundly transforming how sex workers communicate, organise, socialise, and work...and the COVID-19 pandemic has significantly expanded the digitalisation of public and private spheres.*
>
> (NSWP: Global Network of Sex Work Projects 2021)

Sex worker rights defenders (SWRDs) are challenged on two fronts: Not only are they human rights defenders, they are also sex workers. With both these identities being deeply marginalised, stigmatised and criminalised around the world, the severity of their risks increases manifold.

> *An HRD was sexually assaulted by a client with whom he had worked for years without a violent incident. Police and hospital staff both commented that the attack was to be expected, given that the HRD was a sex worker. A detailed testimony of the attack given to Front Line Defenders, however, shows that throughout the sexual assault, the perpetrators repeatedly threatened the defender to stop hosting human rights trainings and doing public advocacy. The attack occurred only after the long-term client became aware of the HRD's activism.*
>
> (Kilbride 2021, 8)

Digital protection of SWRDs must be seen from a holistic perspective. Much of the violence and intimidation they experience is a consequence of being so present and engaged (i.e., on location), or can be traced back to their high-visibility. Its perpetrators are not only clients and members of the general public but, primarily, law enforcers. (Kilbride 2021) Still, **there are many useful practices that can be adopted to reduce technology-driven abuse and violence**, and this document offers strategic and tactical guidance. It is indebted to conversations in digital security trainings with SWRDs, and the body of work created around this subject.

FUNDAMENTALS OF DIGITAL PROTECTION

1. The Holistic Protection Lens

'Holistic protection' is the acknowledgement that health and safety have multiple interconnected aspects: Physical protection, digital protection, and mental wellbeing (which impacts behavioural change).

When we hear the words 'security' or 'protection', we often think of worst-case situations such as bombs and terrorism. However, we apply principles of security and protection even in simple aspects of our lives. For instance:

We brush our teeth daily to secure their physical health. Since toothache can compromise other aspects of life—sleep, decision-making, memory, behaviour towards others—it makes sense to think of brushing teeth as a means of holistically protecting one's wellbeing.

1.1. Context Determines Effectiveness

Consider the following scenario:
Hema is a sex worker and vocal advocate for the rights of her community. After attending a digital security session at a local SRHR workshop, she sets a screen-lock on her phone for the first time. Making sure to create a strong passcode, she believes the data on her device is now fully protected. However, she continues working from busy coffeeshops where anyone behind can see what is on her screen. She also connects to the internet using public Wi-Fi networks, and leaves the phone with friends during toilet breaks.

Hema must understand that for her digital protection practice to be effective she must also (a) consider sitting with her back to a wall, (b) never leave the phone unattended, and (c) connect to the internet using a password-protected connection belonging to her, or one secured by a VPN.

To devise a holistic digital protection strategy, one's awareness of context and surroundings is essential. This can be addressed through the application of not just tools or skills-based solutions, but also behaviour-based solutions.

1.2. The Protection Landscape

The protection landscape consists of the myriad resources and avenues of support available when you wish to learn more about security, or are in trouble and need help.

1.2.1. Landscape Mapping

The practice of protection is a very personal experience. The more aware you remain of your personal environment and its realities, the higher your chances of being able to protect yourself holistically.

Ask yourself the following questions (from a digital perspective) to understand your protection landscape:

- What are my…
  - **Assets**; what should I protect?
  - **Adversaries**; who can cause me harm?
  - **Threats**; in which ways can I be harmed? (Hacking//Hustling n.d.)
- What is the **likelihood and scale of impact** of each threat?
- **How many devices do I own or share** that (a) store my information and/or (b) connect to the internet or other devices? [E.g., mobile phones, flash drives, Wi-Fi routers, smart TV, fitness trackers etc.]
- **Other essential questions about apps, platforms, and devices**:
  - What apps are on these devices? Are there any unused or unnecessary ones?
  - Through which channels am I communicating?
  - What accounts are open (or what services are being used)?
  - Where is information stored—both digital (e.g., cell phone, flash drive) and physical assets (e.g., handbag)?
  - What information is public; private (e.g., ID card); and sensitive (e.g., intimate pictures)—what should be protected, and from whom?

How did I acquire these devices? Did I buy them new—or did someone gift/sell a used device to me? Who all has **access to these devices** and the data stored on them?

- What **networks and social circles** am I part of? What is each network's perception of me?
- What **risks** do I take with my digital devices and data? What are external threats out of my control (e.g., weather, crime, surveillance) that could affect my wellbeing?
- If I have any existing **protection practices**, what are they? What do I do well? What would I like to do differently?

1.2.2. Context-Specific Threats

Here are examples revealed during trainings with SWRDs, of situations that extended far beyond digital risks to physical and psychological risks.

1. **During COVID, SWRDs have had to rely on connecting online more than before.** Potential clients requested pictures and, once these were shared, some of them:
   a. Used these pictures to created fake accounts, or even impersonate these SWRDs
   b. Blackmailed/doxed them

- This resulted in not just disruption of advocacy and business but increased physical and legal risks as well. It also deeply affected psychological wellbeing (depression, paranoia etc).

2. In the case of some LQBTQIA+ individuals, **being outed resulted in more layers of violence** impacting their work and well-being.

3. Some **SWRDs were gifted mobile phones by intimate partners**, who then felt entitled to access these devices, read chats, and committed violence out of jealousy; issues of interpersonal boundary-making can also be exacerbated by technology.

4. **SWRDs are vulnerable to social engineering frauds**, even those not designed explicitly for them, because:

    a. Many struggle with low digital literacy

    b. Seeking clients brings them into a wider range of online spaces, and more frequently

    c. Many belong to low-income households, which makes these fraudulent promises particularly attractive (SWRDs across Asia reported people losing money to online gambling and easy-loan ads). Since finance plays an important role in their well-being and security (access to care and housing), SWRDs need to **be careful of scams that can lead to financial loss**—often affecting their entire activism collective.

2. Social Engineering & Other Threats

> *Social engineering is the term used for a broad range of malicious activities accomplished through human interactions.* ***It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.***

(Imperva, N.D)

- Social engineering can be **in-person**; e.g., a stranger approaches you, says their wallet was stolen, then asks for cash to pay for transport home.

- It can be **automated**; e.g., you visit a website and a pop-up ad claims your system has performance issues that can be fixed by clicking on the ad and downloading software.

- It can be **hybrid**; e.g., you receive an SMS offering a low mark-up rate loan if you reply with 'Yes' in the next three hours—following which, a salesperson calls back attempting to sell you the offer for a small fee.

2.1. Phishing

Phishing is an attack carried out by cybercriminals pretending to be reputable companies, friends or acquaintances. They try persuading you to give up money, identity, or other personal information (e.g. credit card numbers, bank information, or passwords). (Microsoft n.d.)

Some basic ways to identify such scams:

- **Be careful with all links and attachments** in incoming emails, SMSes or forwarded messages. This includes website addresses (especially short links like bit.ly), hyperlinks, and attached files. **Before clicking or accessing, verify with the sender** whether this was intended for you and safe to open. You can check short links by expanding them using services such as https://unshorten.it/

- **Reread links from right to left** : https://google.drive.differentsuspiciousdomain.com will take us to differentsuspiciousdomain.com, not Google Drive.

- **Examine details** such as CC and BCC fields, subject lines, and timestamps to spot inconsistencies.

- **Fraudulent messages are often unprofessionally written** and contain language errors and poor-resolution graphics and logos.

- **Be aware of your feelings.** Phishing messages are often designed to stir one or more uncomfortable feeling, such as fear, paranoia, shame, guilt.

- **Be wary of calls for action.** Phishing messages may contain high-value offers, unexpected communication, or threats of negative consequence.

Interactive Phishing Quiz

- https://phishingquiz.withgoogle.com/

Further Reading

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

2.2. Other Forms of Attack

These include **identity theft**, the cloning of credit cards, and non-consensual filming/ photography of unsuspecting targets. Identity theft, also known as impersonation, is a targeted form of phishing. In it, the attacker assumes the SWRD's identity and uses it to gain unfair advantage over their friends and family. The process often involves hijacking social media/email accounts, or creating fake ones; or through data collection. (See Section 4.3: Securing Social Media, Clouds, and Other Online Accounts)

Someone simply walking past you with a **card cloning** device can steal information off its magnetic strip. Keeping cards in a Faraday's (RFID/signal-blocking) bag, or wrapped in aluminium foil, can prevent this. Also, activate SMS/email notifications to catch and report misuse ASAP: Most banks can send these (stating purchases/withdrawals from accounts and bank cards) and this is essential information for catching misuse and blocking card(s) promptly.

(For non-consensual filming see Section 9.2: When Stepping Out for Work)

2.3. Doxing

Doxing is a form of cyberbullying that involves making an SWRD's personal information widely available to the public, often through the internet. **E.g., leaking a home address or phone number, subjecting the SWRD to harassment.**

You can prevent or minimise such attacks by employing these data safety practices:

- **Mindful data** sharing with people you don't fully trust

- **Keeping sensitive data encrypted** and inaccessible to strangers

- **Securing social media accounts** (See Section 6: Email and Social Media)

- **Editing photos and documents before sharing** e.g., reducing image quality; or marking it with the name of the receiver or purpose (making the recipient responsible for protecting it)—such as recommended in some countries when submitting ID copies to accompany other documents (See Section 7.2.1: Concealing Personal Details)

Further Reading

- https://www.fortinet.com/resources/cyberglossary/doxing

3. Digital Hygiene and Other Fundamentals

Digital hygiene consists of practices that improve the health of devices, avoiding the stress and paranoia of wondering 'What happened?'

Further Reading

- https://securityinabox.org/en/phones-and-computers/windows/

3.1. Physical Security of Digital Devices

Often, physical neglect of digital devices results in malfunction.

Avoid exposing devices to **extreme temperatures**, such as leaving them in the sun or working from the kitchen,

Keep devices away from **excessive moisture**.

Don't let **dust** accumulate around openings,

Avoid placing **weight** on devices, or packing them with other things that put excessive stress on their screens or circuits.

Keep devices away from strong **magnets or electric currents.**

Further Reading

- https://securityinabox.org/en/phones-and-computers/physical-security/

3.2. Cracked Software

"Cracked" software is that which has been modified (by an unauthorized person) to disable its ability to ask for a user license key. One analogy is breaking a door-lock for easy access: This may be convenient for some but creates an opportunity for undesired access. Similarly, cracked software may have 'backdoors'/vulnerabilities that make devices susceptible to hacking/malware/malfunction.

A safer alternative to cracked software is FLOSS (free, libre and open-source software):

- **Linux Ubuntu**: This operating system allows you to enjoy similar productivity and entertainment features as Microsoft Windows and Mac OS.

- **GIMP**: Prepare basic illustrations and edit photos on this (instead of Adobe Photoshop)

- **Libre Office Suite**: Use this to write, edit and format reports and articles; create multimedia presentations; and prepare spreadsheets (instead of Microsoft Office); Libre Office also works across Windows, Mac OS and Linux without compromising functionality, and can read and save files in popular formats such as *.doc(x) and *.xls(x).

3.3. Updates & Upgrades

Accept operating system and software updates as they arrive. They contain important patches and fixes for hardware and software vulnerabilities, such as bugs and backdoors. If this feels inconvenient, setting your device to update as you sleep may help.

3.4. Password Management

Like locking a metal safe, **passwords are your data's primary defence.** Some recommended best-practices:

- **Avoiding names/dates/etc that anyone can guess** are important to you
- **Keeping it long** (e.g. 16 characters or more)
- **A combination** of CAPITAL letters, small letters, numerals (0,1,2,...,9), special characters (!@#$%^&*), and empty spaces
- **A passphrase (or sentence) instead of a word**—see Diceware: https://diceware.dmuth.org/
- **Different passphrases** for different accounts
- **Using a FLOSS password manager** such as:
  - KeepassXC (Windows, Mac OS, Linux)
  - KeepassDX (Android)
  - StrongBox Password Safe (Mac OS, iOS)
  - BitWarden (Cloud-based)
- **Enabling two-factor authentication with an app** such as Aegis or Google Authenticator. Using an authentication app ensures that you can access your verification codes even when your SIM is not working, and that your codes don't arrive via unsecure SMS.

Further Reading

- https://securityinabox.org/en/passwords/passwords-and-2fa/

3.5. Protection from Malware

Malware is software designed to cause harm (device malfunction, data theft, privacy violations etc). Some common types are viruses, trojans, spyware and ransomware. Malware can enter devices from many sources, such as malicious email attachments or website links that navigate to dubious app downloads. It can spread across devices through the intentional/unsuspecting use of infected external hard drives / memory sticks. (See **'Baiting'** and **'Scareware'** here: https://www.imperva.com/learn/application-security/social-engineering-attack/) It can also be injected into unsuspecting users' devices by hackers manipulating public Wi-Fi networks.

The following precautions are effective:

- Install **anti-malware software** on laptops, desktops and smartphones, and update it regularly. While paid anti-malware offers proactive and better protection, it is best to always have it rather than not so even a free one will do. Recommended ones:
  - **Windows**: Microsoft Defender

Antivirus (formerly Windows Defender) supplemented by Malwarebytes

  - **Macs OS**: Malwarebytes, Avira, or AVG

- **Check with source** before clicking on unknown links or downloading dubious attachments.

Further Reading

- https://securityinabox.org/en/phones-and-computers/physical-security/

4. Secure Internet Usage

The internet is an essential tool for remaining updated on world affairs, staying in contact with loved ones, and conducting business. In the process, **we often end up giving up personal information with or without consent that can result in information leakage**. (See Section 6.1: Digital Footprints and Legal Considerations)

4.1. Internet Browser Security

Some browsers (Brave, Mozilla Firefox, and Tor) are more secure than others (Google Chrome, Microsoft Edge, Safari, and Opera). However, **nearly all browsers offer basic settings that reduce the amount of data they store or share with advertisers.**

- Avoid allowing the browser to remember important passwords, home/office addresses, and online transaction information. This "**auto fill**" setting can be disabled from inside the browser's privacy and security settings (see links below).

- Clear **browsing history and other data** regularly. To prevent the browser from recording history (i.e., which sites have been visited), use the "Private" or "Incognito" mode—however, your internet service provider will still record website addresses. (See Section 4.2: VPNs: Accessing Blocked Websites and Enhancing Anonymity)

- Disable third-party cookies; and set the browser to delete cookies once it is closed.

- Set Permissions (for camera, microphone, location etc.) to always ask before accessing.

- Disable automatic downloads, and know where downloaded files get saved.

- Install privacy- and security-enhancing browser extensions e.g. Privacy Badger, Facebook Container, Ublock Origin.

Further Reading

- https://securityinabox.org/en/tools/firefox/
- https://privacyinternational.org/guide-step/4326/chrome-adjusting-settings-enhance-your-online-privacy
- https://support.mozilla.org/en-US/products/firefox/privacy-and-security
- https://its.ucsc.edu/software/release/browser-secure.html

4.2. VPNs: Accessing Blocked Websites & Enhancing Anonymity

A VPN (virtual private network) is a tool used for bypassing online censorship and surveillance and proxies. In countries where dating apps such as Tinder and Grindr are blocked, SWRDs report that community members often use unsafe means to access these apps to network and meet new clients (such as VPNs that have neither been security-audited and cleared, nor have a good track record for protecting user privacy). **A reliable VPN ensures a secure resumption of business at non-disruptive internet speeds.**

VPNs and other anonymity-enhancing technologies with a track record of exhibiting care towards user privacy:

- **Psiphon** *(free)* | https://psiphon.ca/
- **Proton VPN** *(free)* | https://protonvpn.com/
- **TunnelBear** *(free 0.5–1.5 GB/month; more in some countries)* | https://www.tunnelbear.com/
- **Tor Browser** *(free; only anonymizes website traffic that passes within the browser window)* | https://www.torproject.org/
- **NordVPN** *(paid)* | https://nordvpn.com/
- **Mullvad VPN** *(paid)* | https://mullvad.net/en/
- **TorGuard** *(paid)* | https://torguard.net/

Further Reading

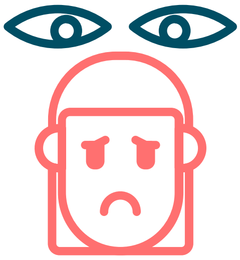
- https://securityinabox.org/en/internet-connection/anonymity-and-circumvention/
- https://ssd.eff.org/en/module/choosing-vpn-thats-right-you

4.3. Securing Social Media, Clouds, and Other Online Accounts

Here are good practices to **reduce the possibility of social media accounts being "hacked"** (more accurately, "cracked"), i.e., being hijacked by attackers:

- **Keep strong passphrases and use multifactor authentication** (See Section 3.4: Password Management)
- **Ensure the primary email to which your account is linked is in your control** (i.e. not shared or, if hacked, retrievable through another linked email account or phone number) See Section 8.1: Online Violence, Stolen ('Hacked') Accounts, and Other Challenges
- **To secure specific platforms**, refer to checklists at: https://securityinabox.org/en/communication/social-media/

ADDRESSING COMMON THREATS TO SWRDS



5. Protecting Data on Devices

The information SWRDs store includes evidence of human rights violations, arrests, and testimonies; as well as details of community members, and interactions with clients. Protecting this data—which may be confiscated and used to harness/deter them or community members—is crucial.

5.1. Disguising Contacts

> *"Police threaten sex workers with higher jail sentences if they seek help from SWRDs...Sex workers pretend to be calling a family or friend when they ring the (SWRD's) emergency hotline."*
>
> (Kilbride 2021, 93)

- **Save numbers under names that protect you and community members.** Where applicable, avoid display pictures that reveal identity.

5.2. Hidden/Encrypted Storage

- Know **where photos, screenshots, etc are stored on your phone**. Are they backed up online? Are other apps on your phone, like Google Photos, also copying (syncing/backing-up) your photos? Review your photo-taking and storage practices and know exactly where everything is. Also, be sure to tidy up your devices often. Delete your lewds, or move them to secure storage. (Duffy and Eddy 2019)

- Activate the **Secure Folder** feature in your phone (if available), and customise and/or hide its icon. It is protected with a passcode or biometrics, and contacts, photos, etc can be moved to it directly from Gallery or by going through My Files.
    - In Samsung devices, look under Settings>>Security>>Secure Folder.
    - Google offers a similar **Safe Folder** on phones with Android 8.0-onward operating systems.
    - On iPhones you can 'hide' albums but they are not password protected. For that, download an app such as **Folder Lock.**
    - Consider using **Tella,** an app that makes it safer to record and store sensitive data, including photos, videos and documents pertaining to human rights work—or anything more personal that could affect the SWRD's work and security. | https://tella-app.org/

5.3. Backing Up Data

To avoid data loss, back it up often. This means copying it from the first location (device storage, external hard drive, memory stick, online) and pasting it in another **secure** location, so that it starts 'living' in two places instead of one. This way, if one copy gets lost, there will always be another copy of your data somewhere.

The following practices make data backup successful:

- Store the backup in a **physically separate location** so that in case of theft/fire/etc, the backup remains accessible
- Frequently **replace old backup with new backup**, especially if changes have been made to the original files (do not work on backed-up files)
- The more precious your data, the **more copies** you should make
- Clearly **label and date each backup** to avoid confusion

Free options for data backup through a cloud service:

- **Sync—5 GB free** | https://www.sync.com/
- **Google Drive—15 GB free** | https://www.google.com/intl/en/drive/

6. Email & Social Media

> *Becoming the victim of a crime is obviously never someone's fault, but (is sufficient) cause for everyone to take a look at how we can be proactive about our safety when using online dating apps...though...it's important to remember that screening is a privilege not every sex worker is afforded*
>
> (Tierney, 2018)

Registering for most social media services requires you to give them consent to collect, use and share your personal data for business gains. **Despite the challenges data collection presents to your privacy, it is possible to limit this violation** by making use of safety features built into the platform. (See Section 4.3: Securing Social Media, Clouds, and Other Online Accounts to learn how to limit other users' access to your personal data.)

6.1. Digital Footprints and Legal Considerations

A digital footprint/shadow refers to the trail of data you leave when using the internet (Kaspersky n.d.) and digital devices.

- SWRDs already face issues of receiving justice. Please be aware of the **legal status** of content shared/stored (e.g., laws around sex work, same-sex activity, pornography, and age of consent). If possible, use online search engines to understand more about local laws.

- Be aware of all **potentially incriminating data** on devices—not only that which is stored but that which passes though. Balance the convenience of keeping everything at hand with archiving/deleting content when the need arises.

- **SMS travels in plain text** (i.e., unencrypted); the network service provider and authorities can access it.

- Data in chatting apps, photo galleries and other locations on the phone/computer can be accessed through **legal means or coercion.**

- Each platform has its own **Privacy Policy** which covers what it might share with authorities

6.2. Secure Email Services

Whether or not you are an active email user, most social media accounts are registered against an email address.

- **Tutanota** and **ProtonMail** provide fool-proof security. **Gmail** and **Microsoft** also offer strong security features.

- Whatever service you prefer, ensure you

create strong passphrases and keep two-factor authentication always turned on.

- Some people keep an **anonymous/ secondary email account** to register for digital platforms.

6.3. Dating Apps and Social Networks

"One of our Yangon staff got sexually harassed on Facebook. They knew she was working for AMA—it's in her profile so sex workers can contact her for help—and so men assume she will be easy to have sex with. There is an assumption that sex workers, especially public ones like our staff, are easy to have sex with."

(Kilbride 2021, 88)

Points to consider when setting up accounts:

- **Which platform(s)** and why (e.g., OKCupid, Tinder, Grindr, Facebook, Instagram, Twitter etc)

- **Alternative platforms** such as Facebook and Instagram have more users—but they were not conceived as dating apps so their community guidelines are not structured to protect the rights of people using them as such; they also restrict the type of content that can be shared publicly

- **Check which information on your profile is publicly visible** (e.g., Facebook allows you to 'lock' your profile) | https://securityinabox.org/en/communication/social-media/

- **Avoid including personal details** (e.g., your full name or phone number—and consider using a pseudonym)

- If sex work is not legal in your country/ on the app, **be creative about how to communicate your business** without raising suspicion

- If the app allows, **hide your distance** to reduce the possibility of being tracked down

- **Avoid linking work and personal profiles,** or using the same display picture.

7. Secure Communication

For SWRDs, communication includes engaging with vulnerable sex workers, undertaking advocacy, mobilising community members and much more, in addition to maintaining relationships with clients.

7.1. Chat Apps,Screenshots and Disappearing Media

> *"The (police) officer took screenshots of (WhatsApp) conversations related to (the collective's) work...in which activists were planning upcoming activities and distributions of health rights information."*
>
> (Kilbride 2021, 95)

Signal Private Messenger is the gold-standard for secure messaging, and is highly recommended. Other apps SWRDs use have varying levels of security—e.g., WhatsApp, Telegram, Snapchat, Instagram, Facebook Messenger, Line, imo, Viber, and BiP. **Whichever app you choose, utilise its privacy and security settings to the maximum.**

Quick Suggestions:

- **Avoid using modified versions of WhatsApp** and other apps (only download from the Play Store/App Store),
- Use **disappearing messages** with a quick expiry time; or delete sensitive chats regularly.
- Signal, WhatsApp, Instagram, Messenger, etc have a **recall** facility—allowing you delete messages at both ends (within a short time period).

7.1.1. Useful Security Features in Popular Apps

- **Offers Disappearing Messages**
  - Signal
  - WhatsApp
- **Does not permit screenshots**
  - Grindr
- **Notifies you if a screenshot is taken**
  - Snapchat
  - Instagram (for media sent in 'View Once' mode)
  - Telegram (in 'Secret Chat' mode)
- **Does NOT notify you about screen recordings**
  - Almost every other app
- **Has a screen lock/inactivity time-out setting**
  - Signal
  - WhatsApp
  - Telegram
- **Does not easily cooperate with authorities**
  - Signal

7.2. Safer Sexting: Photos and Videos

Often, the greatest threat to personal security is when intimate/sexual content featuring you is leaked. A situation like this can be psychologically and socially devastating, even dangerous. Depending on local laws, it may become a serious legal concern.

Digital media is endlessly reproducible.

> *"If you're going to be sexting, you are assuming the risk that someone might copy your text, images, and videos. It's an unavoidable risk."*
>
> (Duffy and Eddy 2019)

Devices allow users to record directly through in-built features and apps (e.g., screenshots, video recordings, audio recordings of calls). **Anything can be forwarded without your consent; or even digitally manipulated.**

Since this line of work relies heavily on visual appeal, there will always be some risk involved. Below are ways to minimise that.

7.2.1. Concealing Personal Details

1. If you fear losing control of a photo of yourself unclothed, there are other ways to protect your business. **Experiment with the right body language, facial expression, and type of clothing for yourself.**
2. If you want to send something unclothed, be strategic:
   a. **Send face and body pictures separately.**
   b. **Crop out** all or part of the face/private parts.
   c. **Place a playful emoji/sticker** over the face/private parts.
   d. **Conceal recognisable physical features**, moles, tattoos, birthmarks—any details that may prove your identity even when you think the photograph has been anonymised.
3. **Be aware of what is in the background.** Scan the image for visual information that might give away clues to your identity/personal details/location.
4. **If you videocall or use a webcam,** remember it is easy for the other user to make a recording. Check what is in your background, and try to keep your head out of view (you might even go as far as disguising yourself with a mask, wig or makeup etc.)

   - You may be tempted to make a recording from your end, to protect yourself. Please remember this might not only endanger an innocent client, it could also be legally used against you.

NB: SWRDs sometimes use fake photographs in their profiles. If you choose to do this, please make sure the photograph is NOT of someone who did not give consent for it to be used; there can be legal implications. From the perspective of physical safety, also consider what reaction

the receiver may have to learning the photo was fake.

7.3. Screening Contacts for Work

SWRDs walk a fine line between making a living and advocating for human rights. These two aspects of their work directly impact each other.

Private photos: If the app allows sharing them in the chat, apply the suggestions in Section 8.2.1: Concealing Personal Details

- **Do not harass/cyberstalk**: Continuing to message someone when they do not seem interested can come across as alarming, annoying, or even tormenting. This will compromise their goodwill and your credibility, affecting advocacy efforts.
- **Sharing numbers/Moving conversation to another app**: Some SWRDs use a separate SIM for business purposes, not their personal one. Others prefer to conclude business in the original app (although having the client's number is a good security measure). Although, as an SWRD explained,

  "I can't change my phone number because I have to connect with the sex workers I help. They have my number and call it in emergencies."

  (Kilbride 2021)
- **Video call:** One step closer to meeting, this provides a way to verify identity and build rapport. Remember the client often needs to trust you as much as you need to trust them. Also, **trust your instinct and experience.**
- **Social media profiles:** If you get the opportunity, screen them by having a look at their Facebook, Instagram, etc. Remember, **be responsible with personal information you find.**
- **Catfishing and other scams:** Some create false profiles for attention and connection; others, to extract money.

Further Reading

- https://www.vice.com/en/article/qve4gq/what-everyone-can-learn-from-sex-workers-about-how-to-screen-dates
- https://www.pcmag.com/news/your-guide-to-safer-sexting
- https://www.rainn.org/articles/online-dating-and-dating-app-safety-tips

8. Helplines, Online Violence, and Lost Accounts and Devices

8.1. Online Violence, Stolen ('Hacked') Accounts, and Other Challenges

Targetted online abuse and defamation is a serious barrier to successful advocacy and wellbeing. Take screenshots of all forms of hate speech, falsified images, and online threats; and save links where possible. Report directly through digital protection helplines at the earliest.

- **Bumble** | https://bumble.com/en/help/privacy-and-safety
- **Facebook |** https://www.facebook.com/help/181495968648557
- **Grindr |** https://help.grindr.com/hc/en-us/articles/1500008659902-Blocking-reporting-profiles
- **Instagram** | https://help.instagram.com/547601325292351
- **OKCupid |** https://help.okcupid.com/hc/en-us/sections/5220623127181-Rules-and-Reporting
- **Tinder** | https://www.help.tinder.com/hc/en-us/categories/360006058312-Safety-Reporting
- **Twitter |** https://help.twitter.com/en/rules-and-policies/violent-threats-glorification

8.2. Managing Stolen/Lost Devices

8.2.1. Phone

Android

- https://support.google.com/accounts/answer/6160491

iPhone

- https://support.apple.com/en-us/HT210400
- https://www.icloud.com/find

8.2.2. Laptop or Desktop Computer

Windows

- https://support.microsoft.com/en-us/account-billing/find-and-lock-a-lost-windows-device-890bf25e-b8ba-d3fe-8253-e98a12f26316

MacOS

- https://support.apple.com/guide/findmy-mac/set-up-fmm53101237/mac
- https://www.icloud.com/find

Linux

- Prey Project | https://preyproject.com/

9. Digital Aspects to Real World Security Risks

9.1. Before Meeting Anyone

- **Share relevant information** with a trusted person, in case of danger or disappearance.
- If meeting online contacts for the first time, **screen profiles for health and safety information.** Sometimes, information shared (or deliberately withheld) can guide decision-making.

9.2. When Stepping Out for Work

- **Share your live location** with a friend (e.g., through Google Maps, WhatsApp); also, ask them to check on you at a given time. (There have been cases of SWRDs detained by police for a week without anyone knowing.)
- **Keep an eye out for hidden or visible cameras** in homes, hotels, public restrooms, offices.
    - **Use the phone's flashlight** to inspect suspicious holes and openings; a spy-cam's lens usually reflects light back.
    - **Observe crevices through your phone camera.** It is more likely to pick up night vision (infrared) cameras than the naked eye.
    - More tips: https://www.youtube.com/watch?v=y_3ZdpqHg18

  A related danger is **cybersex trafficking**, in which rogue clients or authority figures record/livestream criminal sexual activity with a hostage.

- Some trans SWRDs have swiftly informed their networks of abusive/complicated/dangerous situations by activating social media livestreams. This may serve as a deterrent in the moment, and later, as evidence. (However, it may invite retaliation from the abuser—or expose unsuspecting viewers to sensitive content, or even open the door to vigilantism—so it should be used mindfully.)
    - **Twitter (Camera icon>>Live>>Go Live)**
    - **Facebook (Create Post>>Live Video)**
    - **Instagram (temporary broadcast—recorded if saved immediately after)**

9.3. 'Revenge Porn' and Sextortion

'Revenge porn' is a common term for NCSII (non-consensual sharing of intimate images) and, despite your best efforts, you may find yourself dealing with such a situation. It is used for blackmailing or otherwise harming individuals and their loved ones. **This may be the outcome of content shared online with potential clients—or other media recorded with or without your consent.**

Electronic media is very easily reproduced and disseminated, so this can become extremely complicated and stressful, depending on your personal circumstances/vulnerabilities and the other person's intentions and determination. Protection remains the first line of defence, such as handling explicit media—Section 7.2: Safer Sexting: Photos and Videos—or looking for hidden cameras—Section 9.2: When Stepping Out for Work.

Second line of defence:

- **Contact the relevant helplines** in Appendix: Protection Helplines and Emergency Grants

- **Non Consensual Porn** – Online Removal Guide | https://cybercivilrights.org/online-removal/

- **Helpful Tips for Victims of Revenge Porn |** https://rcjlawgroup.com/2013/02/12/helpful-tips-for-victims-of-revenge-porn/

Other forms of revenge can include doxing. (See Section 2.3: Doxing)

Appendix: Protection Helplines | Emergency Grants | Further Research and Resources

Helplines

- *(Holistic)* **Front Line Defenders |** https://www.frontlinedefenders.org/en/emergency-contact
- *(Digital)* **Access Now |** https://www.accessnow.org/help/
- *(Digital)* Locate another nearby **CiviCERT organisation |** https://www.civicert.org/

Grants

- **Front Line Defenders |** https://www.frontlinedefenders.org/en/programme/protection-grants
- **Digital Defenders Partnership Incident Emergency Fund |** https://www.digitaldefenders.org/funding/incident-emergency-fund/
- **Urgent Action Fund for Women's Human Rights |** https://urgentactionfund.org/apply-for-a-grant/
- **ProtectDefenders.eu |** https://protectdefenders.eu/protecting-defenders/

Research and Resources

- **Hacking//Hustling|** https://hackinghustling.org/resources/
- **What is the Relationship Between Online Sex Workers and Cybersecurity?** | https://journals.sagepub.com/doi/pdf/10.1177/1071181321651304
- **Sex Worker Rights Defenders at Risk |** https://www.frontlinedefenders.org/sex-worker-rights-report/fullreport.html
- **Smart Sex Worker's Guide to Digital Security |** https://www.nswp.org/resource/nswp-smart-guides/smart-sex-workers-guide-digital-security

Citations

Duffy, Jill, and Max Eddy. 2019. *Your Guide to Safer Sexting*. Accessed 2022. https://www.pcmag.com/news/your-guide-to-safer-sexting.

Hacking//Hustling. n.d. *Threat Modeling*. Accessed 2022. http://soph.info/hh/Threat-Modeling.pdf.

Imperva. n.d. *Social Engineering*. Accessed 2022. https://www.imperva.com/learn/application-security/social-engineering-attack/.

Kaspersky. n.d. *What is a Digital Footprint?* Accessed 2022. https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint.

Kilbride, Erin. 2021. *Sex Worker Rights Defenders at Risk*. Accessed 2022.

https://www.frontlinedefenders.org/sites/default/files/fld_swrd_final_english.pdf.

Microsoft. n.d. *Protect Yourself From Phishing*. Accessed 2022. https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44.

NSWP: Global Network of Sex Work Projects. 2021. *"Smart Sex Worker's Guide to Digital Security." Global Network of Sex Work Projects*. 10 21. Accessed 2022. https://www.nswp.org/resource/nswp-smart-guides/smart-sex-workers-guide-digital-security.

Tierney, Allison. 2018. *What Everyone Can Learn From Sex Workers About How to Screen Dates*. February 5. Accessed 2022. https://www.vice.com/en/article/qve4gq/what-everyone-can-learn-from-sex-workers-about-how-to-screen-dates.