Reverse Image Check & Digital Hygiene Kit

A Privacy Toolkit for Dommes & Online Sex Workers

Why This Matters

In an era of facial recognition, deepfake tools, and automated content scraping, protecting your identity and digital footprint is essential for sex workers. This guide will help you clean your files, track your image, and guard your likeness online.

1. Strip Metadata from Photos and Videos

- Use tools like ExifCleaner (Windows/macOS), ImageOptim (macOS), or mat2 (Linux) to remove hidden metadata such as location, camera model, or timestamps.
- Always export edited images through these tools before posting.
- Do not post screenshots directly from phone galleries - these often retain metadata.

2. Use Reverse Image Search Tools

- Run regular checks to ensure your content hasn't been reposted or misused:
  - PimEyes (facial recognition, paid tiers)
  - FaceCheck.ID (NSFW-friendly)
  - Google Images (drag and drop search)
  - Yandex Images (can find deeper web reposts)
- Search every few months, or after large content drops or viral tweets.

3. Track Reposts or Leaks with Watermarks

- Add subtle watermarks to photos or videos: e.g., initials, emojis, or your URL in a corner.
- Use dynamic watermarking tools like uMark or iWatermark Pro.
- For advanced use, add invisible watermarks using Digimarc or StegCloak.

4. Scrub Yourself from People-Finder Sites

- Use services like JustDeleteMe or PrivacyBee to mass-delete yourself from public databases.

- Manually opt out of people-finder and facial recognition databases.

- Use browser extensions like uBlock Origin to block web trackers.

5. Monitor for Deepfake Misuse

- Run your selfies and clips through FaceCheck.ID or PimEyes.

- If you find deepfakes or impersonations:

  - Screenshot everything.

  - File a report with the platform (label as deepfake or AI abuse).

  - Issue a DMCA takedown or content removal request.

  - Contact advocacy services like The Cyber Helpline or SWARM.

6. Extra Tips

- Use Firefox or Brave browser with strict privacy settings.

- Avoid uploading images with direct eye contact or flat expressions - these are easiest to deepfake.

- Disable auto-backups of media to Google Photos, iCloud, or Dropbox.

Recommended Tools & Resources

- PimEyes - https://pimeyes.com

- FaceCheck.ID - https://facecheck.id

- The Cyber Helpline - https://www.thecyberhelpline.com

- ImageOptim - https://imageoptim.com

- ExifCleaner - https://exifcleaner.com

- StegCloak - https://github.com/KuroLabs/stegcloak

- mat2 (Linux) - https://0xacab.org/jvoisin/mat2

- uBlock Origin - https://github.com/gorhill/uBlock

- JustDeleteMe - https://justdeleteme.xyz