How to Stay Safe Online

For Dominatrices and Sex Workers

Introduction

Staying safe online is critical for dominatrices and sex workers due to the risks of stigmatisation, harassment, doxxing, violence, cyberflashing, and non-consensual recording of private sessions. Below are practical tips to protect your privacy, maintain anonymity, and ensure digital security, tailored to your profession, with specific guidance on Amazon Wish Lists, posting receipts safely, handling unsolicited explicit media, addressing non-consensual recording, and securing device control sessions.

1. Maintain a Separate Work Persona

- Use a stage name or pseudonym for all professional activities.
- Create separate emails, phone numbers (e.g., Hushed, Google Voice), and social accounts for work.
- Avoid cross-posting photos or using tattoos, locations, or metadata that could link your identities.
- Use tools like ImageOptim or EXIF Purge to strip geotags and metadata from images.

---

2. Secure Communication Channels

- Use encrypted apps like Signal or WhatsApp (with end-to-end encryption).
- Avoid using standard SMS.
- Use a VPN (e.g., NordVPN, Surfshark, Mullvad) to hide your IP address when online.

---

3. Use Separate Devices and Accounts

- Ideally, use a dedicated phone/laptop for work — password protected and secured.
- Store all passwords in a password manager like 1Password or Bitwarden.
- Enable two-factor authentication (2FA) for all your work-related logins.

---

4. Protect Against Doxxing and Privacy Breaches

- Never post identifiable info: no full names, addresses, or tagged locations.
- Use strong privacy settings on social platforms.
- Use email aliases through services like ProtonMail or Fastmail.
- Posting Receipts Safely: Blur all location, time, and business details before posting. Wait until you've left the area to share anything.

---

5. Screen Clients Thoroughly

- Use platforms like National Ugly Mugs (UK) to flag risky clients.
- Ask for ID or references before any booking.
- Trust your instincts — if a client's behaviour raises red flags, walk away.

---

6. Secure Financial Transactions

- Take all payments upfront.
- Use secure and anonymous options like Bitcoin, Throne, or gift cards.
- Avoid services like PayPal, Google Pay, and Square — they often ban sex worker accounts.
- Amazon Wish List Warning:
    - Disable third-party shipping to prevent revealing your real name/address.
    - Use a pseudonym as the list name (e.g., "Mistress X's Gifts").
    - Consider a PO Box or Amazon Locker for deliveries.

7. Secure Device Control and Cam Sessions

Device Control Sessions

- Use a separate work device with no personal content.
- Restrict access — turn off file sharing or clipboard functions.
- Use temporary one-time access codes (never reuse them).
- Monitor sessions closely and terminate if suspicious behaviour occurs.
- Protect yourself with firewalls, antivirus, and disk encryption (BitLocker, FileVault).
- Run sessions inside a virtual machine (VM) for isolation.
- Ban recording explicitly in your session terms. Use tools like ScreenShield to detect screen captures.

Private Cam Sessions

- Use platforms that support your boundaries (e.g., OnlyFans, Chaturbate, ManyVids).
- Watch for signs of recording (clients adjusting screens, odd pauses).
- Add subtle watermarks to your content.
- Blur or remove personal décor/backgrounds in cam sessions.
- If you are recorded without consent:
    - Save all evidence (screenshots, links, usernames).
    - Report to the platform.
    - File a police report (in the UK, this falls under intimate image abuse, Online Safety Act 2023).
    - Contact The Cyber Helpline, National Ugly Mugs, or a solicitor.

8. Handle Unsolicited Explicit Media (Cyberflashing)

- Cyberflashing is illegal in the UK under the Online Safety Act 2023.
- Do not reply. Block and document everything (screenshots, names, dates).
- Report to:
    - The platform (e.g., Instagram, WhatsApp, Twitter/X).
    - Your local police (via 101 or 999).
- Use support from Beyond the Gaze, The Cyber Helpline, and SWARM.
- Add clear no-tolerance warnings to your forms or profiles.

---

9. Leverage Technology for Safety

- Enable full disk encryption on your devices.
- Use privacy-focused browsers like DuckDuckGo, Firefox, or Brave.
- Block ads and trackers.
- Use Ugly Mugs, Red Umbrella, or Sex Work Alert Networks to check for unsafe clients.

---

10. Prepare for In-Person Safety

- Use a buddy system — tell someone where you'll be and when you'll check in.
- Set expectations and limits in advance.

- Carry a personal alarm or safety tool.
- Always have a charged phone and a backup contact.

---

11. Combat Online Harassment and Intimate Image Abuse

- Screenshot, record, and archive all harassment, doxxing, or leaks.
- Report content leaks to platforms and file DMCA takedown notices.
- Use legal frameworks under the Online Safety Act or UK harassment laws.
- Work with advocacy orgs: The Red Project, Beyond the Gaze, The Cyber Helpline.

---

12. Stay Informed and Connected

- Join peer forums like Tryst.link, Hacking//Hustling, or SWARM.
- Stay up to date on privacy laws and tech trends.
- Keep adapting your safety plan as tools and threats evolve.

---

13. Stay Safe from AI Manipulation and Deepfakes

The Threat

- Deepfake tools can simulate your face, voice, and likeness in fake porn, cam videos, or audio messages.

- These can be used to harass, blackmail, or impersonate you — with real consequences.

What You Can Do

- Add watermarks to all visual content.
- Avoid posting plain, expressionless selfies — they're easiest to fake.
- Run regular reverse image searches with tools like PimEyes, FaceCheck.ID, or Google Images.

If You're Targeted

1. Document everything — screenshots, URLs, file downloads.
2. Report to the platform and label it as "deepfake abuse" or "synthetic image abuse".
3. File a police report under UK intimate image abuse law (Online Safety Act 2023).
4. Send DMCA takedowns and request platform removals.
5. Contact advocacy/legal orgs like:
    - The Cyber Helpline
    - National Ugly Mugs
    - a digital rights solicitor

Prevention Tips

- Avoid giving out unedited video or high-resolution images.
- Keep a record of what content you've published and when.
- Include anti-AI or deepfake usage clauses in your booking terms and content distribution agreements.

Additional Notes

- Amazon Wish List Caution: Disable third-party shipping to avoid your name/address being shown to buyers.
- Image Abuse: Use takedown tools like Red Points, DMCA.com, or content removal services if content is leaked.
- Mental Health: Build in rest and aftercare after heavy scenes, control sessions, or harassment. Support yourself like you'd support a submissive.
- Legal Support: Keep your local laws saved and know your rights. UK residents can cite the Online Safety Act 2023 when reporting cyberflashing, image abuse, or AI manipulation.

Resources:

- Beyond the Gaze
- National Ugly Mugs
- The Cyber Helpline
- SWARM