ProCoRe

Outils pour la sécurité numérique des travailleur·se·x·s du sexe (TdS)

Facteurs de risque :

- Clients avec lesquels les TdS sont en contact direct et qui sont mal intentionnés.
- Harcèlement, outing, cyber-mobbing.
- Moyens de pression contre les TdS sans autorisation de séjour ou de travail.

Concepts de sécurité :

- Créer une identité professionnelle distincte de son identité civile.
  Ces deux identités ne doivent avoir aucun lien entre elles (par ex. ne pas être ami·e·x·s sur Instagram, …).
- Avoir deux téléphones portables : un pour le travail, un pour la vie privée.
  Consulter ses comptes professionnels (ex. Instagram) uniquement avec le natel professionnel.
- Créer différentes identités en ligne (avec différents comptes) pour le travail, la famille, les proches, les collègue·x·s, …
- Déterminer sur quels comptes des contenus érotiques peuvent être partagés et jusqu'à quel point.
- Publier des contenus sur plusieurs plateformes à cause de la censure et « canaliser » les clients via les médias sociaux vers des plateformes où les contenus érotiques sont autorisés (p. ex. Onlyfans, ManyVids).

Communication :

- Un téléphone uniquement pour le travail du sexe.
  Acheter un nouveau téléphone et une carte SIM anonyme. Contacter les clients uniquement avec son téléphone professionnel.
- Carte SIM anonyme : essayer d'acheter une carte prépayée dans un kiosque sans montrer sa carte d'identité. En Allemagne, en France ou au Portugal par exemple, il est facile d'acheter des cartes prépayées anonymes qui fonctionnent également en Suisse (par contre, un numéro étranger peut éveiller des soupçons de la part de potentiels clients).
- Adresses mail jetables (par ex. si besoin d'un courriel seulement pour ouvrir un compte) : yopmail.com ; temp-mail.com (pour se connecter, seuls un nom et un mot de passe sont requis).
- Services de messagerie sécurisés : tutanoata.com ; protonmail.com (si le client a aussi ces fournisseurs, on peut sélectionner que ses mails soient effacés après 1 ou 7 jours).
- Yahoo, Hotmail, Gmail sont des fournisseurs peu sûrs.
- Services de chat sécurisés : WhatsApp, Wickr, Signal, Telegram, Wire, Element (les deux derniers fonctionnent également sans carte SIM sur un téléphone).

Métadonnées :

- Photos : les métadonnées sont des informations en lien avec l'image (l'heure à laquelle la photo a été prise, le lieu (GPS), le nom du téléphone/de l'ordinateur, ...). Même si une photo est retouchée avec Photoshop, les métadonnées sont toujours

enregistrées. Il est de plus en plus facile de reconstruire des visages avec des logiciels, par exemple s'ils sont pixellisés.

- Cyberharcèlement : de plus en plus de personnes sont familiarisées avec le numérique et l'exercent. Grâce aux métadonnées, il est possible de relier différentes images comme une photo d'un chat sur Facebook avec une photo d'une TdS sur une plateforme si elles ont été prises avec le même téléphone.
- Outils pour supprimer les métadonnées : ScrambledExif, EXIF Purge, Metadata.systemli.org

Paiements :

- SI aucun lien ne doit être établi avec son propre compte :
  - De préférence, paiement en liquide.
  - Paiement par cartes prépayées (Ok-card) ou cartes-cadeaux (Amazon) (bémol : on ne connaît pas la somme qui se trouve réellement sur la carte).
  - Services de paiement anonymes : Wishlist, TransfertWise (une adresse mail est nécessaire. On peut payer ou être payé·e·x de manière anonyme. Wise s'interpose en quelque sorte entre le compte de la personne TdS et celui du client), Horizontl (plateforme en cours de construction pour TdS).

Mots de passe et utilisation d'Internet en toute sécurité :

- Mots de passe sûrs : un mot de passe différent pour chaque compte, au moins 10 mots choisis au hasard.
- Gestionnaires de mots de passe : pour smartphone KeepassDC (Android) et Keepassium (iphone), et KeepassXC pour ordinateur (ne sont pas sur le cloud, moins de risques d'attaques).
  Keepass crée aussi lui-même des mots de passe. Finalement, la personne ne doit retenir qu'un seul mot de passe très sûr pour Keepass.
- Pour l'authentification à deux facteurs : Free OTP
- Utilisation d'Internet plus sûre :
  - ⇒ Ne visiter que des sites web avec https (connexion cryptée).
  - ⇒ Installer un VPN : iPhone : Orbot ; Android : Riseup ; Laptop : Riseup (tous gratuits)
  - ⇒ Utiliser le navigateur Tor (torproject.org). Sur iPhone, il s'appelle Onionbrowser et nécessite l'installation d'Orbot. Il est important d'utiliser TOR dès le début et créer tous les comptes pour les annonces avec TOR Browser.

Construire son propre site internet sécurisé :

- Nom de domaine : njal.la (on peut le faire de manière anonyme).
- Hébergement : redumbrella.ch (par des TdS) ; abelohost.com (par des TdS) ; orangewebsite.com (sexwork-friendly).
- Redumbrella propose également de créer des sites et des profils.