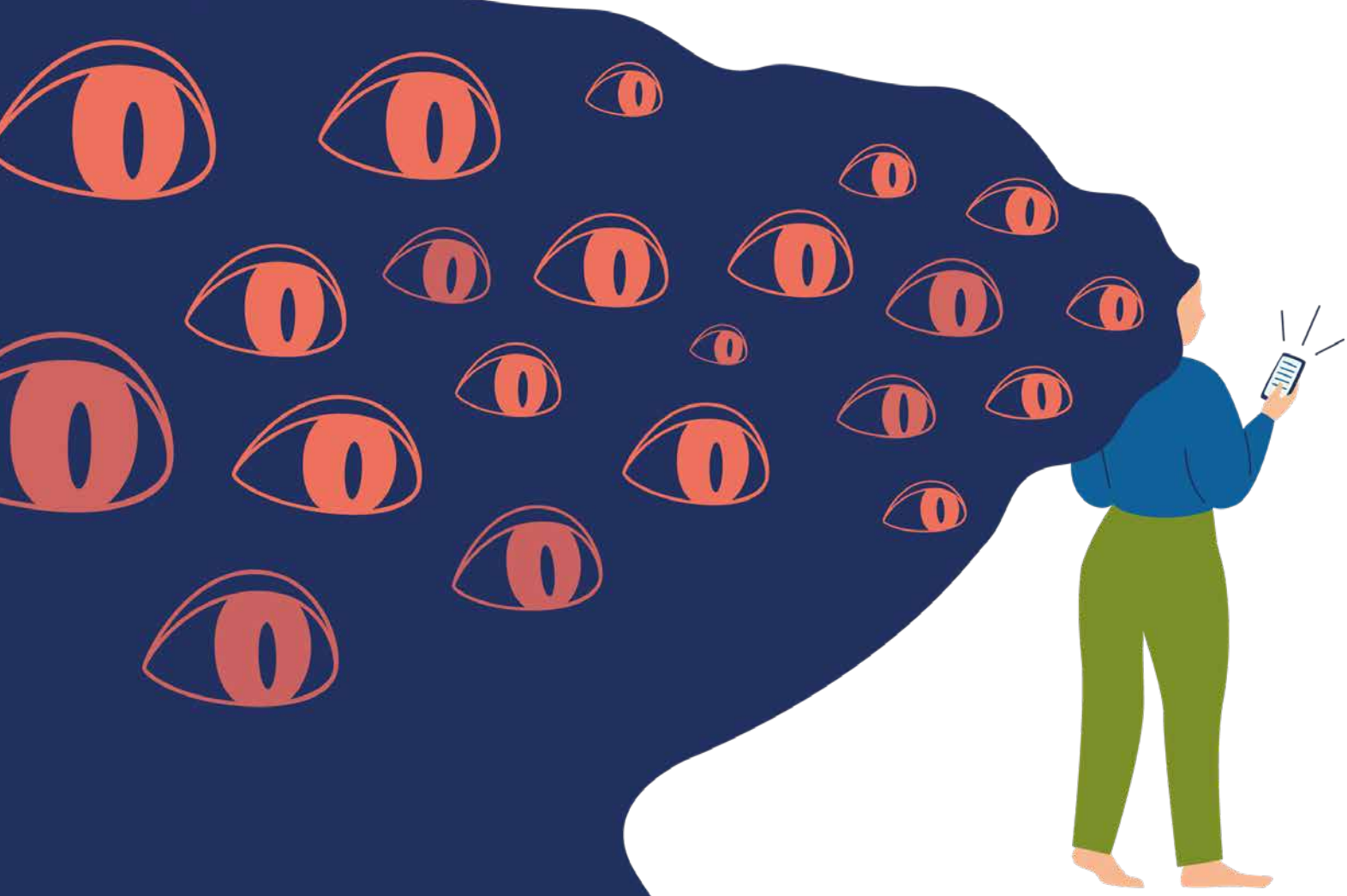

DeStalk TOOLKIT

per operatrici che lavorano con donne che subiscono violenza digitale

Blanquerna UNIVERSITAT RAMON LLULL
kaspersky
UNA CASA PER L'UOMO società cooperativa sociale
REGIONE DEL VENETO
www.work-with-perpetrators.eu

Supported by the Rights, Equality and Citizenship Programme of the European Union (2014–2020)

DeStalk Toolkit per operatrici che lavorano con donne che subiscono violenza digitale

Indice

UNA CASA PER L'UOMO
società cooperativa sociale

DeStalk: detect and stop stalkerware and cyberviolence against women
Una Casa per l'Uomo
Elena Gajotto – Chiara Moretti – Luisa Casagrande
Gennaio 2022
Rev. Ottobre 2022

Glossario dei termini sulla cyberviolenza

Nonostante la tecnologia sia parte integrante delle nostre vite, la prima definizione generale di cyberviolenza è stata introdotta da GREVIO solo nel novembre 2021:

Dimensione digitale della violenza contro le donne: riguarda una vasta gamma di atti commessi online o tramite strumenti tecnologici che sono parte del continuum di violenza che donne e ragazze subiscono per motivi legati al loro genere, anche nella sfera domestica, in quanto manifestazione legittima e ugualmente nociva della violenza di genere subita OFFLINE da donne e ragazze

Secondo questa definizione, la cyberviolenza viene rinominata "dimensione digitale della violenza contro le donne" e riguarda sia gli atti violenti commessi tramite siti web o tramite il reperimento o la pubblicazione di dati online, sia i comportamenti violenti agiti tramite strumenti tecnologici sia hardware che software.

È importante capire che la seguente lista di forme di cyber violenza non è esaustiva in quanto le forme di cyber violenza cambiano e si sviluppano seguendo il costante e rapido evolversi delle tecnologie digitali. Inoltre, una qualche forma di cyber violenza potrebbe variare nel modo di mostrarsi e quindi alcune caratteristiche potrebbero confondersi con quelle di altre forme. In aggiunta, può succedere che la stessa forma di violenza abbia un nome differente. Così come l'EIGE (2017) ha fatto notare, avere una definizione condivisa politicamente può facilitare un migliore coordinamento nei diversi livelli organizzativi. Data la complessità del fenomeno, la condivisione delle definizioni facilita la collaborazione multi agenzia tra centri antiviolenza, centri per il trattamento degli uomini autori di violenza e altri servizi.

Cyberviolenza è un termine ombrello che racchiude tutte le forme di violenza che si verificano con l'uso delle tecnologie informatiche. Le forme più comuni sono il cyber-bullismo, le molestie on line e la pubblicazione di immagini. Come afferma GREVIO al paragrafo 10 della raccomandazione citata sopra, da diversi anni le violenze di genere subite da donne e ragazze sono state amplificate e facilitate dalla tecnologia, che ha portato a un'escalation mai vista prima del fenomeno. La violenza agita online o tramite l'uso di tecnologie rappresenta un continuum delle forme di violenza "tradizionali" e non è quindi un fenomeno separato dalla violenza del "mondo reale", poiché spesso segue gli stessi schemi della violenza offline ed è associata sia a conseguenze negative psicologiche, sociali e peggioramento della qualità di vita che, spesso, a violenza fisica, psicologica e sessuale.

La cyberviolenza contro donne e ragazze include molte forme di violenza agite tramite strumenti informatici per motivi di genere o di genere e altri fattori (ad esempio, etnia, età, disabilità, orientamento sessuale, professione o credo personali).

Come specificato da EIGE[1] tutti gli atti di cyberviolenza contro donne e ragazze possono:

a. iniziare online e continuare offline, ad esempio nel luogo di lavoro, a scuola o a casa;
b. iniziare offline e continuare online tramite diverse piattaforme, come social media, email o app di messaggistica (es. whatsapp);
c. essere agite da un singolo o da un gruppo di persone, anonime e/o sconosciute alla donna;
d. essere agite da persona o gruppo di persone che la donna conosce, come ad esempio un (ex) partner, un compagno di classe o un collega;

Grazie alle molteplici possibilità offerte dalle tecnologie informatiche, la cyberviolenza può essere messa in atto attraverso un'ampia varietà di meccanismi, questa è una **lista che comprende le modalità più rilevanti tramite le quali viene agita cyber violenza di genere**.

1 EIGE (2022) *Cyber Violence against Women and Girls Key Terms and Concepts* **Cyber Violence against Women and Girls. Key terms and Concepts (europa.eu)**

Glossario dei termini sulla cyberviolenza

■ Cyber stalking

prevede comportamenti ripetuti e perpetrati dalla stessa persona e può includere: – Invio di e-mail, messaggi di testo SMS) con messaggi offensivi o minacciosi; pubblicazione di commenti offensivi su Internet; monitoraggio e tracciamento della vittima. Cyberstalking è il "tradizionale" stalking agito in modi nuovi e più efficienti, con le seguenti modalità:

- **Stalkerware:** sono delle app segretamente installate sul dispositivo della vittima/ sopravvissuta per monitorarla e tracciarla
- **Hacking o cracking:** accesso alle comunicazioni o ai dati registrati online (per esempio sul cloud) o su un dispositivo senza il consenso del proprietario. Questo include il controllo da remoto di webcam e l'uso di dispositivi "smart" (con tecnologia Alexa o Google Home) per ascoltare le conversazioni
- **Sorveglianza/tracciamento:** utilizzo della tecnologia per monitorare le attività, le interazioni sociali e i movimenti della donna. Ad esempio, i dispositivi di tracciamento (GPS) possono essere usati per monitorare i movimenti della partner tramite il proprio telefono o altro dispositivo wireless
- **Seguire** la donna **online**, monitorarne gli account social, rispondendo a tutti I suoi post, iscrivendosi agli stessi gruppi, taggandola ossessivamente. Questo può anche essere fatto con account falsi

■ Cyber harassment (molestie online)

è una categoria ampia al cui interno troviamo minacce o altri comportamenti aggressivi agiti da un singolo o da un gruppo di persone, mirati a offendere, denigrare o sminuire una persona tramite l'utilizzo di dispositivi digitali o tramite canali privati o pubblici. Le molestie online possono avvenire tramite:

- email o messaggi non desiderati
- Richieste offensive o inappropriate sui social media o nelle chat
- Minacce di violenza fisica o sessuale via email, messaggi o chat
- Hate speech, ovvero uso di linguaggio denigratorio, offensivo, minaccioso
- Commenti inappropriati o a sfondo sessuale su post o contenuti online

Alcune tipologie di cybermolestie sono:

- **Slander (diffamazione)** si riferisce all'azione di danneggiare la reputazione di qualcuno tramite la pubblicazione e condivisione di informazioni false (per esempio: pettegolezzi sui social media).
- **'Slut-shaming'** è l'atto di far sentire una donna colpevole o inferiore per determinati comportamenti o desideri sessuali che si discostino dalle aspettative di genere tradizionali.
- **Minacce online (threats)** di stupro, abuso o morte.
- **Body shaming**: ovvero deridere qualcuno per il suo aspetto fisico, spesso tramite commenti o post online.
- **Gendertrolling**: atti online dannosi che riguardano l'invio o la pubblicazione di email o post provocatori, che possono includere anche minacce di stupro e morte. Così come il trolling, il gendertrolling mira a fomentare liti e dibattiti e aumentare il seguito della disputa, incitando una arrabbiata o negativa da parte della vittima designata (EIGE, 2022)
- **Sexual solicitation/sexting non consensuale** ricevere richieste non desiderate di parlare di sesso o di compiere una qualche azione a sfondo sessuale in vari contesti online. Questa categoria include le richieste di condivisione di immagini sessualmente esplicite o l'avvio di interazioni sessuali tecno-mediate. Può portare alla ricezione di commenti misogini, molestie e minacce, in particolar modo quando la vittima rifiuta di eseguire le richieste

Glossario dei termini sulla cyberviolenza

Diffusione non consensuale di immagini intime

copre una vasta varietà di azioni che possono essere spiegate con la condivisione di immagini o video a sfondo sessuale condivisi oppure ottenuti **senza il consenso della persona**. Questa categoria include:

- **Sextortion**. Estorsione di denaro, di favori sessuali o altro ai danni di una persona, dietro minaccia di rendere pubblici contenuti personali compromettenti di natura sessuale (messaggi di testo, foto o video).
- **Diffusione non consensuale di immagini intime**. Distribuzione, o la minaccia di distribuire, tramite mezzi informatici, immagini/video intimi, privati e/o manipolati di una donna o ragazza senza il suo consenso. Immagini e video possono essere ottenuti in modo non consensuale, manipolati in modo non consensuale, o ottenuti consensualmente ma distribuiti in modo non consensuale. Questa forma di cyberviolenza è generalmente conosciuta come "revenge porn", termine incorretto che crea la falsa impressione che l'autore abbia agito per reazione ad una condotta posta in essere dalla persona offesa nei confronti del soggetto che diffonde il materiale sessualmente esplicito, colpevolizzando inconsciamente la vittima.
- **Creepshot voyeurism** (inclusi downblousing and skirting) si riferisce allo scattare foto o girare video di parti intime del corpo femminile (ad esempio: schiena, gambe, scollatura), senza il consenso della donna. Questo può anche essere fatto tramite telecamere nascoste, o quando la donna non ne è consapevole (nella doccia, mentre dorme ecc.).
- **Deepfake**. l'uso non autorizzato di immagini e foto di donne per realizzare filmati, quasi sempre a carattere pornografico, nei quali l'immagine della donna viene sostituita, tramite algoritmi digitali, a quella originariamente presente nell'immagine o video.
- **Cyberflashing**. invio non richiesto di immagini a contenuto sessuale – in genere, primi piani di genitali maschili ("dick pics"), tramite app di appuntamenti, social media, app di messaggistica, o tramite le funzioni AirDrop e Bluetooth dei telefoni

Limitazione dell'utilizzo della tecnologia

Si riferisce a tutte quelle forme di violenza che impediscono alla donna di utilizzare la tecnologia, con l'obiettivo di controllarla e isolarla. Questa categoria include:

- Limitazione o negazione dell'utilizzo di dispositivi (smartphone, tablet o pc)
- Limitazione o negazione dell'uso della connessione internet
- Limitazione o negazione dell'uso di app particolari
- Distruzione e danneggiamento di dispositivi

Alcuni esempi sono:

- limitazioni all'utilizzo di app bancarie: tale azione prevede l'impossibilità della donna di accedere liberamente alle risorse economiche proprie e/o familiari e, quindi, di poter essere maggiormente autonoma,
- rottura di dispositivi tecnologici come il telefono cellulare, il computer ecc. Molto spesso la donna non dispone di risorse economiche per acquistare nuovamente i dispositivi dovendo così rinunciare ad una connessione con l'esterno,
- Controllo da remoto della connessione: quando una donna non possiede dispositivi elettronici l'uomo può impedirle l'utilizzo del suo smartphone o computer per evitarle il contatto con l'esterno o le richieste di aiuto;
- limitazioni all'utilizzo di app/siti internet legati alla salute: ciò impedisce alla donna di prendersi cura della propria salute rimanendo intrappolata nella relazione maltrattante in quanto può accedere alle cure soltanto con la concessione del maltrattante.

Glossario dei termini sulla cyberviolenza

Altre forme

- **Doxing** (a volte scritto anche come doxxing) è l'azione di condividere informazioni riconoscibili e spesso private riguardo ad una persona (nome, numero di telefono, indirizzo e-mail, indirizzo di residenza ecc.) su piattaforme online senza il consenso. Dato che le Informazioni permettono di localizzare e rintracciare fisicamente la donna, il doxing può essere precursore di violenza "offline" (stalking, minacce, molestie, violenza fisica e psicologica). Solitamente il doxing avviene nel contesto di violenza nelle relazioni intime, IPV (EIGE, 2022).
- **Furto di identità**, usare le informazioni personali di qualcuno per fingersi quella persona ottenendo soldi o benefici in suo nome. Molte app gratuite permettono anche di agire lo spoofing, che sarebbe l'azione di falsificare le informazioni trasmesse durante una chiamata facendo apparire sul display della persona chiamata il numero di qualcun altro.
- **Tratta digitale**uso di Internet, social media e nuove tecnologie per reclutare e attirare le potenziali vittime, soprattutto donne e bambini, ai fini dello sfruttamento sessuale.

Guida per operatrici: Rilevazione, valutazione e piano di sicurezza informatico

La cyber violenza è un termine generale all'interno del quale esistono vari tipi e forme diverse di violenza di genere agita online, questa può essere suddivisa in varie categorie: cyberstalking (attraverso l'utilizzo di app per lo stalkerware o altri mezzi informatici), condivisione non consensuale di immagini molestie online. La violenza digitale rappresenta un continuum della violenza contro le donne, e molte forme di violenza digitale possono essere considerate l'estensione online di forma di violenza perpetrate nel mondo "offline", come ad esempio avviene con "cyber"-stalking e "cyber"molestie. In altri casi, invece, la tecnologia ha portato a nuove e diverse forme di violenza (come, ad esempio, il doxing o la condivisione non consensuale di immagini intime), che amplificano e aumentano l'impatto sulla vittima rispetto alla violenza agita nel mondo offline.

La violenza digitale può essere agita con diversi dispositivi (smartphone, pc, tracciatori GPS, smart home devices, fitness trackers, ecc.) e su diversi spazi online (social media, siti internet, app di messaggistica, account personali, ecc.), che sono in costante cambiamento ed evoluzione e che quindi possono dare luogo a nuove forme di violenza digitale. Data la molteplicità di forme e di mezzi, la violenza digitale può essere agita da tipologie diverse di autori, che possono essere conosciuti (es. (ex) partner, amico, collega, compagno di classe, ecc.) o sconosciuti, sia singolarmente che in gruppo.

Come sappiamo, gli spazi fisici (offline) e digitali (online) sono strettamente correlati e interconnessi, e, come già visto, ***la violenza digitale può essere precursore o estensione della violenza nel mondo fisico*** (EIGE 2022).

Per questo motivo, è necessario condurre un accurato assessment della cyberviolenza, e includere elementi di sicurezza digitale in tutti i piani di sicurezza.

Guida per operatrici: Rilevazione, valutazione e piano di sicurezza informatico

Assessment e valutazione

L'assessment ci aiuta a identificare eventuali forme di violenza tecnomediate, a discutere varie opzioni possibili con la donne, utili alla stesura di un piano di sicurezza digitale, e alla corretta raccolta di documentazione e prove.

La violenza digitale può essere opprimente e travolgente, perché può accadere in ogni momento, in ogni luogo e in molti modi diversi. L'assessment serve per validare l'esperienza della donna e a rassicurarla, fornendole anche informazioni utili ad aumentare la sua sicurezza digitale.

Struttura di valutazione della violenza digitale

Per un corretto assessment della violenza digitale, è necessario seguire i seguenti step:

- **Ascoltare l'esperienza della donna**
  - Cos'è successo?, quanto spesso?
  - Come pensa che sia successo?
- **Valutare quali informazioni sono state utilizzate**
  - Di quali informazioni aveva bisogno l'autore per fare quello che ha fatto?
  - Dove sono conservate queste informazioni?
  - Come possono essere ottenute?
- **Passare in rassegna dispositivi, account, persone e luoghi frequentati, tenendo in considerazione quali informazioni sono state utilizzate dal maltrattante**
  - account cloud
  - dispositivi "di famiglia" o dei bambini
- **Valutare l'accessibilità di dispositivi e account**
  - Quali sono ad accesso esclusivo della donna?
  - Quali sono condivisi con il maltrattante?
  - Quali sono condivisi con i figli o con altre persone?
- **Valutare la messa in sicurezza di dispositivi e account**
  - Possono essere aumentate le impostazioni di privacy senza mettere in pericolo la donna?
- **Pianificare i passi successivi**
  - Quali sono gli obiettivi della donna?
  - Come può raggiungerli in sicurezza?
  - Come raccogliere le prove in sicurezza?

Il piano di sicurezza IT

Il piano di sicurezza informatico (IT) non è diverso da quello che normalmente si fa nei centri antiviolenza, serve concentrarsi sulla donna e capire quali siano i suoi bisogni a breve termine e quelli a lungo termine e come la violenza digitale sta interferendo con la sua vita e obiettivi. Per definire il piano di sicurezza IT, le competenze tecnologiche sono utili, ma non sono indispensabili.

È importante che il piano di sicurezza informatica sia individualizzato e che fornisca direttamente alla donna strumenti ei strategie per monitorare rischi e sicurezza, creando empowerment.

Ricordiamoci che per eliminare la violenza digitale non è possibile eliminare la tecnologia, è necessario impostare il piano di sicurezza includendo la tecnologia stessa, restituendo alla donna il controllo e la possibilità di scegliere.

Come accennato in precedenza, nella definizione del piano di sicurezza IT è necessario innanzitutto considerare quali siano gli obiettivi immediati e a lungo termine della donna:

- **Interesse legale**
  - Raccogliere documentazione per una denuncia
  - Richiedere misure di protezione
  - Procedimenti civili: divorzio, affidamento minori, ecc.

Guida per operatrici: Rilevazione, valutazione e piano di sicurezza informatico

- **Aumento privacy**
  - Mantenere la comunicazione con il maltrattante aumentando la sicurezza
  - Migliorare la sicurezza di dispositivi e account
  - Creare nuovi account o attivare nuovi dispositivi
- **Interruzione della violenza**
  - Capire come viene utilizzata la tecnologia per agire violenza
  - Contrastare le forme di violenza digitale in atto
  - Usare la tecnologia per arginare/interrompere/prevenire la violenza

I pilastri del piano di sicurezza IT

Documentare il maltrattamento:

- tenere un registro/diario di quello che succede
- fare screenshot e foto
- non eliminare gli originali (e-mail, sms, audio vocali,app etc)
- utilizzare app che tengano al sicuro i documenti salvati
- vagliare opzioni legali

Verificare strumenti/modalità utilizzo:

- dispositivi
- account (e-mail, cloud, banking account, social media, ecc),
- Luoghi fisici frequentati e mezzi utilizzati per spostarsi

⚠ ATTENZIONE: è fondamentale conservare gli originali di e-mail, sms, audio vocali, e non cancellare dal dispositivo le app tramite cui sono stati inviati. Gli screenshot possono essere di supporto nella ricostruzione di quanto accaduto, ma possono non avere valore probatorio qualora in sede di giudizio venga sollevata un'eccezione di parte. In questo caso è necessaria l'analisi del dispositivo contenente l'applicazione originale, fatta da un perito informatico forense.

Elementi Per l'identificazione Del Rischio

Nella valutazione delle possibili fonti di rischio, è importante ricordare che le informazioni personali possono essere memorizzate in molteplici dispositivi, app e account a cui il maltrattante potrebbe avere accesso, come ad esempio:

- Social Network (Facebook, Instagram, Tik Tok, etc.)
- App di messaggistica (WhatsApp, Telegram, ecc.)
- Paypal o altri sistemi di pagamento elettronico
- App home banking
- App di servizi sanitari
- Amazon (Incluso Prime Video)
- App di consegna cibo (Foodracer, Glovo, JustEat, Deliveroo, ecc.)
- Spotify
- App di streaming (Netflix, Discovery+. Disney+, DAZN, ecc)
- App per gli allenamenti (Garmin, Fitbit, MiFit, Strava, Run Keeper, ecc.)
- App di viaggi (Booking, Trivago, TripAdvisor, ecc.)
- App per il dating online (Tinder, Bumble, ecc.)

Guida per operatrici: Rilevazione, valutazione e piano di sicurezza informatico

È quindi necessario considerare gli aspetti relativi a connessioni, informazioni e accesso:

- **Connessioni:**
  - A cosa sono collegati i dispositivi in uso? Altri dispositivi? App? Account online?
  - Come avviene la connessione? (wifi, bluetooth, altro)
  - Sono connessioni aperte o richiedono una password?
  - Chi controlla la connessione?
- **Informazioni:**
  - Quali informazioni sono condivise?
  - Quali altre info potrebbero essere condivise? (indirizzo IP, posizione, dati su abitudini di consumo)
  - Con chi vengono condivise queste info?
  - I produttori dell'app hanno delle regole sulla privacy?
  - Si possono mettere dei limiti nella condivisione?
- **Accesso:**
  - Chi ha accesso ai dispositivi o agli account?
  - Accesso da remoto o in presenza?
  - Chi altro della famiglia accede a questi?

Per facilitare il lavoro di assessment e pianificazione, è stata messa a punto una checklist ad hoc (***DeStalk Digital violence assessment checklist***), che include segnali di pericolo o campanelli d'allarme riguardanti le varie forme di violenza digitale, con relativi pericoli e possibili contromisure.

■ Misure di sicurezza

Quando c'è la possibilità che telefono della vittima/sopravvissuta possa essere monitorato o controllato, è prioritario co-costruire con la donna un **piano di sicurezza** informatico sicuro e chiaro. È necessario però ricordarsi che **cambiamenti improvvisi**, quali ad esempio il cambio delle password o la cancellazione di app sospette, possono mettere in allerta il maltrattante e creare **un'escalation di comportamenti aggressivi del maltrattante**.

Il piano di sicurezza informatico può essere costruito seguendo questi punti chiave:

- **Canale di comunicazione sicuro**
  Se il cellulare è tracciato, è importante non liberarsene o eliminare app sospette. Verificare se la donna può permettersi di comprarne uno nuovo, oppure farsene prestare uno: in entrambi i casi è necessario l'acquisto di una nuova SIM CARD. In alternativa, verificare se la donna può usare il dispositivo di una persona fidata o un computer pubblico (in biblioteca, per esempio).
- **Utilizzo di un dispositivo sicuro**
  Decidere insieme alla donna dove può nascondere un nuovo dispositivo e quando/come usarlo. La vittima/sopravvissuta dovrebbe usare il dispositivo "sicuro" per tutte le conversazioni di cui il maltrattante non deve venire a conoscenza (ad esempio: con il centro antiviolenza, avvocato, polizia, medico, ecc.), ma dovrebbe continuare ad usare il cellulare sotto controllo per le altre normali attività in modo da non creare sospetti nel maltrattante e per raccogliere prove.
  Discutere con la donna anche la necessità di mantenere nascosto il dispositivo sicuro dai bambini.

Guida per operatrici: Rilevazione, valutazione e piano di sicurezza informatico

- **Utilizzo di comunicazioni online e degli account dei social media**
  Se necessario, creare un nuovo indirizzo e-mail e cloud per lo scambio di informazioni con destinatari "sicuri" e per conservare documenti e prove. Discutere con la donna quali tipi di informazioni può condividere sui social media.

Controllare il dispositivo per la presenza di stalkerware

Se la donna che richiede il nostro aiuto ha la sensazione che il suo (ex)partner possa conoscere troppe sue informazioni nonostante non le abbia mai condivise con lui, potrebbe essere utile aiutarla a verificare l'eventuale presenza di stalkerware nel suo dispositivo.

- Controllare se ci sono segnali di pericolo (ad esempio legati al consumo della batteria o del traffico dati) è il metodo di verifica meno intrusivo, ma è anche quello che dà meno certezze, perché spesso lo stalkerware non lascia traccia.
- Usare un programma di antivirus per cellulari. Gli antivirus sono molto efficaci nella rilevazione dello stalkerware, ma è necessario prestare attenzione al fatto che lo stalkerware potrebbe allertare il maltrattante che è in uso un antivirus.
- Usare strumenti specifici per la rilevazione di stalkerware, come TinyCheck. Il maltrattante non verrà a conoscenza che questo strumento è stato usato, ma questo richiede che venga usato un secondo dispositivo per essere messo in funzione. (**https://github.com/KasperskyLab/TinyCheck**)

⚠ ATTENZIONE: quando si controlla il cellulare per verificare la presenza di app sconosciute, è importante ricordare che il sistema operativo installa di default diverse app che non ci sono familiari e che, se erroneamente, disinstallate, potrebbero compromette il funzionamento del dispositivo. Se si hanno dei dubbi, chiedere a un tecnico informatico di fiducia di fare il controllo.

È opportuno che operatrici di centri antiviolenza o altri servizi che lavorano con le vittime siano formati sulle modalità di controllo di un dispositivo ed eventualmente, sull'utilizzo di loro strumenti di verifica come TinyCheck.

Un'altra strategia utile potrebbe essere quella di creare delle collaborazioni con un tecnico informatico di fiducia a cui far controllare i dispositivi.

⚠ ATTENZIONE: se il controllo del dispositivo dà esito negativo, non significa che il dispositivo non abbia delle app installate. Il maltrattante potrebbe usare altri app o strumenti per monitorare/tracciare la donna. Per esempio, potrebbe avere accesso ai suoi account online, o potrebbe controllarle il cellulare mentre lei lo lascia incustodito, ecc.

Guida per operatrici: Rilevazione, valutazione e piano di sicurezza informatico

Misure di sicurezza quando c'è il sospetto che la vittima/sopravvissuta possa essere monitorata e/o tracciata

- ☐ Informarla che le app di stalkerware potrebbero registrare le sue conversazioni, suggerirle di lasciare il cellulare in macchina o fuori dalla stanza dove si effettuano i colloqui con le operatrici del centro o con medico, forze dell'ordine, avvocato, ecc.
- ☐ Controllare, anche tramite app apposite, se l'utilizzo di dati internet è aumentato senza una reale ragione (Lo stalkerware consuma molti dati per trasmettere le informazioni)
- ☐ Installare un'app di antivirus (NOTA BENE: come già detto in precedenza, le app di stalkerware possono allertare il maltrattante quando viene installato un antivirus)
- ☐ Cambiare frequentemente le password dei dispositivi e degli account, usare password non facilmente individuabili
- ☐ Cambiare le modalità di sblocco del cellulare, usare un PIN oppure una sequenza di sblocco invece dell'impronta digitale o del riconoscimento facciale
- ☐ Controllare quali app hanno l'autorizzazione alla posizione e alla fotocamera e revocarne il consenso se attivo
- ☐ Disconnettere WhatsApp Web e/o Telegram dal computer o altri dispositivi che sono facilmente accessibili al maltrattante
- ☐ Discutere con la donna della necessità di non far usare ai figli i dispositivi
- ☐ Cambiare le modalità di accesso all'account dell'online banking
- ☐ Chiedere ad un meccanico di fiducia di controllare e, possibilmente, disattivare il GPS dell'autovettura
- ☐ Spiegarle di non accettare richieste di amicizia o follower sconosciuti
- ☐ Controllare la lista di followers/amici in ogni social media e cancellare profili sconosciuti. Ricordarle che se il profilo/account è pubblico, chiunque può vederne i contenuti anche se non è un follower/amico
- ☐ Dire alla donna di non condividere sui social media o sulle storie di WhatsApp immagini o altri dettagli che possano rivelare informazioni su dove si trova/cosa sta facendo
- ☐ Indagare la possibilità che la donna possa avere altri account condivisi col maltrattante che possono sembrare "innocui" (vedi lista sottostante).

Misure di sicurezza quando si è certi che il cellulare/dispositivo è tracciato

Quando si è certi che il dispositivo sia tracciato tramite l'utilizzo di app di stalkerware o che il maltrattante stia monitorando la vittima/sopravvissuta con mezzi informatici, è importante fare i passaggi giusti per assicurare la sicurezza della vittima e per raccogliere le prove contro il maltrattante.

- ☐ Se si individua un'app di stalkerware, la vittima/sopravvissuta vorrà eliminarla immediatamente. È necessario spiegarle le conseguenze se si dovesse disinstallare (escalation di comportamenti violenti, distruzione di prove)
- ☐ Revisionare e rinforzare il piano di sicurezza informatico
- ☐ Ricordarsi che ripristinare il dispositivo alle impostazioni di fabbrica distruggerà le prove e potrebbe non essere efficace nei dispositivi più datati
- ☐ Aiutare la vittima/sopravvissuta ad attivare una nuova SIM card e nel ritrovare un dispositivo "sicuro"

Guida per operatrici: Rilevazione, valutazione e piano di sicurezza informatico

☐ Quando si re-installano le app su un nuovo dispositivo o su quello ripristinato ai dati di fabbrica, ricordarsi di scaricare le app direttamente dallo store ufficiale e non fare il backup per non scaricare nuovamente le app di stalkerware

☐ Creare un nuovo account Google o iCloud per il dispositivo "sicuro"

⚠ ATTENZIONE: creare un nuovo account Google o iCloud per l'attivazione di un nuovo dispositivo sicuro è fondamentale in tema di sicurezza informatica, in quanto questi account danno l'accesso a una varietà ampia di app e informazioni, come e-mail, file su cloud, mappe e posizioni, foto, contatti, ecc.

☐ Se non c'è nessuna app di stalkerware ma il maltrattante sta monitorando la donna tramite altri mezzi informatici (per esempio: ha accesso ai suoi account online, ecc.), è importante raccogliere informazioni sugli account/dati che vengono monitorati

☐ Anche se la vittima/sopravvissuta non è sicura di voler coinvolgere le forze dell'ordine, suggerire di tenere una cronologia degli eventi (incluse le date, gli orari, le posizioni, i testimoni se ce ne sono, le tecnologie che si pensa siano coinvolte -come il cellulare, l'email, ecc.-, e una breve descrizione di cosa il maltrattante ha fatto)

☐ Ricordarle di cambiare le password solo quando è sicuro farlo

☐ Discutere con lei di come utilizzare il dispositivo o l'account tracciato in maniera organizzata e controllata, in modo da evitare di condividere troppe informazioni con il maltrattante ma, allo stesso tempo, senza suscitare sospetti in lui.

■ Cosa fare in caso ci siano molestie online o condivisione non consensuale di immagini o informazioni

Nel caso ci sia il sospetto o la certezza della presenza di queste forme di cyber violenza, si può aiutare la vittima/sopravvissuta con i seguenti consigli e misure di sicurezza per prevenire altri danni e per raccogliere delle prove:

☐ È importante incrementare i livelli di privacy degli account dei social media che dovrebbero essere impostati sul livello più elevato possibile

☐ È possibile impostare un **Google Alerts** che monitori se vengono pubblicati online dei contenuti riguardanti la vittima/sopravvissuta. Google manderà un'email quando certi termini (come il nome della donna) appariranno in Google Search

☐ Per mantenere le prove delle molestie sui social media il primo passo è quello di fare degli screenshot della molestia/abuso. È necessario ricordare che gli screenshot non costituiscono una prova definitiva in tribunale e che devono essere acquisite anche le prove digitali.

☐ Discutere la possibilità di segnalare la molestia/pubblicazione di immagini al social media di competenza (da verificare le politiche di segnalazione di ogni social media **Facebook** | **Instagram** | **Twitter** | **YouTube** | **TikTok**) o del sito web. Se il contenuto segnalato viola i termini del servizio o le sue line guida, i social potrebbero rimuovere il contenuto. In questo caso, prima che il contenuto possa essere rimosso, è necessario raccogliere documentazione sull'abuso subito a mo' di prova. Si ricorda di controllare nella sezione sottostante come fare le segnalazioni su siti con contenuti per adulti.

Guida per operatrici: Rilevazione, valutazione e piano di sicurezza informatico

- ☐ A volte lo stesso contenuto potrebbe essere stato pubblicato su più di un sito web. In questo caso usare la funzione del motore di ricerca "reverse search" (ricerca per immagini) potrebbe aiutare. Per usare la funzione "reverse search" si dovrà caricare la foto sul motore di ricerca, e questo scansionerà il web per verificare la presenza di tale contenuto. È necessario ricordare che questo procedimento potrebbe recare molto stress nella vittima.
- ☐ Nel caso di telefonate moleste, queste possono essere registrate e tenute come prove.
- ☐ Nel caso la donna riceva telefonate in cui il maltrattante utilizza app di spoofing per sostituire il proprio ID chiamante, è importante tenere traccia delle chiamate scattando delle fotografie/screenshot del numero chiamante e registrarne sia la data che l'orario, così come serve mantenere un registro delle chiamate con i numeri, la data e gli orari.
- ☐ Se del contenuto è già stato pubblicato, questo può essere rimosso dal motore di ricerca: i residenti nell'EU hanno il diritto di chiedere che vengano rimossi da **Google** i link alle pagine web contenenti dati che sono superati, irrilevanti, eccessivi o inaccurati. Questo non prevede che vengano eliminate le pagine web, ma solamente che questi risultati non vengano mostrati nei risultati di ricerca di Google, in modo da ridurre le possibilità che le persone li trovino. Questo può essere richiesto anche a **Bing** e **Yahoo**.
- ☐ Monitorare i commenti e i feedback quando foto/video sono già stati pubblicati online potrebbe essere un'altra fonte di forte stress. Si può suggerire alla vittima che provi a non monitorare il contenuto online e i commenti annessi.
- ☐ Se il maltrattante ha minacciato di pubblicare contenuti private online su Facebook e Instagram, si può aiutare la vittima/sopravvissuta ad accedere al **Programma pilota sulle immagini intime non consensuali (NCII) di Facebook**. Questo programma può prevenire il fatto che certe immagini vengano pubblicate. La vittima/sopravvissuta dovrà contattare una delle organizzazioni partner del programma (vedi la lista **qua**) e fornire un'immagine originale da bloccare (non uno screenshot).

■ Rimozione di contenuti da siti per adulti

Se è stato pubblicato online del contenuto private su siti per adulti, la maggior parte di questi siti ha una procedura di "rimozione contenuti". Qui si possono trovare le pagine per la "rimozione contenuti" di alcuni siti **Pornhub** | **Xhamster** | **X videos** | **XXNX** (attenzione: questi link apriranno le pagine di siti per adulti).

Consigli utili per la segnalazione:

- ☐ Quando si fa una segnalazione, usare il browser in modalità in incognito
- ☐ Non usare l'indirizzo e-mail personale (crearne uno apposito per lo scopo)
- ☐ Non fornire una copia del proprio documento di identità al sito se viene richiesto
- ☐ Fornire l'esatto URL del video o della foto che si vuole rimuovere
- ☐ Richiedere che tutti i video e foto vengano rimossi, inclusi i thumbnails (immagini di anteprima)

Cyber violenza e stalkerware: consigli utili sulla tecnologia e social media per le sopravvissute

La tecnologia è una parte fondamentale delle nostre vite: è ovunque e la usiamo costantemente. È importante sapere come possiamo aumentare la nostra "sicurezza digitale" in modo da continuare ad usare la tecnologia e rimanere connessi.

Qui si possono trovare dei consigli utili su come incrementare la propria sicurezza digitale mentre si vive ancora con un partner maltrattante o dopo averlo lasciato.

- ☐ **Usa un dispositivo sicuro**, che è un dispositivo al quale il tuo partner non ha accesso. Potrebbe essere un nuovo dispositivo, uno pubblico, o quello di una persona fidata. Questo dispositivo sicuro va usato per tutte quelle informazioni e comunicazioni di cui il partner non deve essere a conoscenza. Questo include le comunicazioni con il centro antiviolenza, con le forze dell'ordine, con l'avvocato, con il medico, con la banca, ecc. Anche un vecchio telefono senza la connessione internet potrebbe essere una buona scelta.
- ☐ **Attiva un nuovo numero di telefono**: oppure usa un numero sicuro (ad esempio quello di un'amica o di una vicina di casa) per comunicare con la polizia, con il centro antiviolenza e con l'avvocato. Condividi questo numero solo con persone fidate.
- ☐ **Proteggi il tuo dispositivo con una password o PIN**: ogni dispositivo che hai, cellulare, computer o tablet, dovrebbe essere protetto con una password o PIN che solo tu conosci. Quando si impostano questi codici segreti, non usare la data del compleanno tuo o dei tuoi figli, nomi di animali domestici, o altre cose che ti piacciono (cibi, film, canzoni) in quanto potrebbero essere facilmente indovinabili. Non usare la stessa password o lo stesso PIN su ogni dispositivo.
- ☐ **Non condividere le password** con altre persone, neanche con i tuoi figli (potrebbero condividerle con il padre).
- ☐ **Non salvare le password** sul tuo computer o cellulare. Quando i browser come Chrome, Edge, ecc. chiedono se si vuole memorizzare la password per usi futuri: scegli "no". Se stai già usando già usando password salvate sul dispositivo per entrare nei tuoi account, il partner potrebbe essere in grado di accedervi. Non salvare le password su quaderni, agende o fogli di carta in casa o in ufficio. Si possono salvare in modo sicuro le password in app o dispositivi dedicati a questo scopo, che si chiamano "password manager"
- ☐ **Crea un nuovo account email** per gestire le comunicazioni. Questo account verrà anche usato per creare altri account (per la banca, servizi sanitari, assicurazioni, ecc.) e quando servirà un altro indirizzo email per verificare la tua identità. Se possibile, non usare il tuo nome/cognome per l'email, ma scegli un altro nome (per esempio Qualcosaqualcosa@email.com invece di Tuonomecognome@email.com).
- ☐ **Crea un nuovo account Google o iCloud** per il tuo dispositivo sicuro. È importante ricordare che l'account Google o iCloud memorizza informazioni su di te e sulla tua vita, come foto, email, contatti, file, ecc. Quindi è importante proteggere questo account con una password difficile da individuare e che questa non venga condivisa con nessuno.
- ☐ **Disabilita la geolocalizzazione** del tuo telefono o tablet, perché se è attivata il dispositivo registra tutti i tuoi spostamenti e li conserva nel tuo account Google o iCloud.
- ☐ **Disattiva dispositivi smart in casa** come "google nest" o Alexa, che potrebbero essere usati per ascoltare le conversazioni a distanza da chiunque ne abbia le credenziali di accesso.
- ☐ **Usa la modalità in incognito del browser** quando navighi sul web, sia da cellulare che da tablet e pc, così non restano tracce dei siti web visitati.

Cyber violenza e stalkerware: consigli utili sulla tecnologia e social media per le sopravvissute

- ☐ Prima di spegnere il dispositivo, **scollegati ed esci** dai siti e dagli account, specialmente quelli dei social media e email. Chiudere la finestra web non ci disconnette dai siti, e chi usa il dispositivo dopo di noi può facilmente avere accesso ai nostri account.
- ☐ **Controlla le impostazioni di privacy** dei social media e impostarli sul livello più alto di privacy. Fare lo stesso con gli account dei figli.
- ☐ **Fai attenzione a ciò che posti online**, evita di postare qualunque informazione che possa rivelare i tuoi spostamenti, o che possa danneggiare la tua reputazione o che possa essere usata contro di te. Fai attenzione a chi può visualizzare i tuoi post e ricordati che amici e followers possono fare screenshot delle tue immagini e dei tuoi post e condividerli con altri. Come norma:
  - Non condividere informazioni personali
  - Non taggare le foto con il luogo in cui ti trovi
  - Chiedi ai tuoi parenti e amici di non postare foto tue e dei tuoi figli e non che non ti tagghino nelle foto

Cerca di essere selettiva con le richieste di amicizia e con i followers sui social media. Aggiungi solo persone fidate che non comunicheranno con il maltrattante.

Checklist per operatrici che lavorano con donne che hanno subito violenza digitale (DeStalk *Digital violence assessment checklist)*

Quando si parla di violenza online e di dispositivi elettronici, ci sono alcuni segnali di pericolo che possono avvertire la vittima/sopravvissuta e i professionisti che lavorano nei servizi di supporto riguardo alla potenziale presenza di stalkerware o altre forme di cyber violenza.

Molte volte, la vittima/sopravvissuta potrebbe non essere a conoscenza di tutti i modi in cui la cyberviolenza può essere agita. È importante essere attivi e verificare la possibilità che siano presenti forme di cyber violenza anche se la donna non dimostra preoccupata o sospettosa al riguardo. La donna potrebbe non essere a conoscenza di ciò che sta succedendo o potrebbe non considerarlo un problema.

Questo strumento non è da intendersi come una lista di domande da porre direttamente alla vittima/sopravvissuta, ma è piuttosto una lista di "segnali di pericolo" che potrebbero segnalare la presenza di stalkerware o altre forme di controllo agite tramite l'utilizzo di mezzi informatici.

È importante ricordare che la cyber violenza non si limita al cyber stalking, ma include altre forme di violenza, come le molestie online, la condivisione non consensuale di immagini.

Lo strumento fornisce una lista di segnali di pericolo divisi in quattro gruppi:

- Segnali di pericolo tecnici in relazione agli smartphone (o altri dispositivi)
- Segnali di pericolo relativi all'utilizzo di dispositivi e account
- Segnali di pericolo riguardanti il comportamento del partner/maltrattante
- Segnali di pericolo riguardanti i social media

Per ogni segnale di pericolo si elencheranno i pericoli connessi, la possibile forma di cyber violenza e cosa è possibile fare a riguardo.

⚠ ATTENZIONE: prima di effettuare qualsiasi azione della lista sottostante, la priorità è quella di creare un **piano di sicurezza informatico** chiaro e preciso con la donna (vedi guida per operatrici). Ricordarsi sempre che cambiamenti improvvisi possono portare ad un'escalation del comportamento aggressive del maltrattante.

Segnali di pericolo tecnici in relazione agli smartphone o altri dispositivi

SEGNALI DI PERICOLO	Sì	No	Pericolo	Forma di cyberviolenza	Se presente, cosa può essere fatto?
Il dispositivo è scomparso per un periodo di tempo e all'improvviso è riapparso			Questi sono segnali che un'app di stalkerware può essere stata installata sul dispositivo	Cyberstalking, stalkerware	Controllare che non sia stato installato stalkerware da parte del maltrattante. Se ne viene confermata la presenza, allora bisogna pianificare i passi successivi in modo attento. Si ricorda di tenere a mente tutti i dettagli relativi alla sicurezza in casi di stalkerware
Il cellulare / tablet / computer viene usato anche dal partner					
La batteria del cellulare si scarica più velocemente di prima					
C'è un'icona di un'app che la vittima/sopravvissuta non riconosce					
Il cellulare consuma più dati mobili di prima					
Il maltrattante ha regalato nuovi dispositivi alla vittima/sopravvissuta o ai figli					
Nel cellulare c'è un'app chiamata "Superuser" (per Android) o "Cyndia" (per iOS)			Queste app permettono l'installazione di software di terze parti nel cellulare		
Alcune app hanno i permessi relativi alla posizione e/o l'accesso alla fotocamera o al microdono anche se non erano stati concessi inizialmente			Possono esserci delle app che condividono informazioni sulla posizione, o che utilizzano fotocamera e/o il microfono senza che la donna ne sia consapevole	Hacking, cyberstalking, condivisione non consensuale di immagini	Controllare periodicamente che questi permessi siano revocati
La donna ha recentemente cambiato il cellulare senza cancellare i dati da quello vecchio			Il maltrattante può avere accesso al Vecchio cellulare, ai dati contenuti in esso e agli account delle app (email, social media, ecc.)		Cancellare tutti i dati dal vecchio cellulare

Segnali di pericolo relativi all'uso di dispositivi e account

SEGNALI DI PERICOLO	Sì	No	Pericolo	Forma di cyberviolenza	Se presente, cosa può essere fatto?
I dispositivi non hanno un blocco di sicurezza, o la password del dispositivo/ account è semplice ed è la stessa per vari dispositivi o account			Il maltrattante può aver accesso al dispositivo o ad altri svariati account online		Cambiare le password regolarmente, scegliendone di più complesse
Le password sono memorizzate nel computer/ dispositivo accessibile al maltrattante					
La donna usa l'impronta digitale o il riconoscimento facciale per sbloccare il dispositivo			Il maltrattante può avere la possibilità di sbloccare il dispositivo mentre la donna sta dormendo	Cyberstalking, condivisione non consensuale di immagini	Cambiare il blocco schermo inserendo un PIN o sequenza. Ricordarsi che il PIN non è comunque sempre sicuro, può essere facilmente visto e ripetuto
Le app di messaggistica come Whatsapp Web o Telegram vengono installare sui computer o tablet accessibili anche da altre persone			Il maltrattante può essere in grado di leggere le conversazioni e vedere sia foto che video		Disconnettere e revocare gli accessi delle app di messaggistica (questo può essere fatto dal cellulare). Evitare di usare queste app su dispositive condivisi.
I partner si scambiano le password di social media o di altri account					Cambiare le password
Il dispositivo è usato anche dai figli della coppia			Il padre può aver chiesto ai figli di riferirgli il contenuto dei messaggi del scambiati dalla madre	Monitoraggio, cyberstalking	Cambiare le password ed evitare che i figli abbiano accesso agli account della madre
Il partner ha accesso ai dettagli bancari della donna			Il maltrattante può controllare I movimenti bancari e autorizzare trasferimenti di soldi	Cyberstalking, violenza economica	Cambiare i dati per l'accesso all'online banking
La macchina della donna ha il sistema GPS integrato			Il maltrattante può rintracciare le destinazioni e strade percorse dalla vittima/ sopravvissuta	Tracciamento, cyberstalking	Parlare con un meccanico di fiducia riguardo alla possibilità di interrompere le funzioni GPS dell'auto
Il maltrattante ha accesso all'account Google della donna			Attraverso l'account Google, il maltrattante può rintracciare la posizione del cellulare Android della donna in qualsiasi momento, così come controllare lo storico delle posizioni (cronologia di Google maps)		Disattivare la localizzazione e lo storico delle posizioni nel cellulare, cambiare password.
Ci sono dispositivi "smart" in casa (come Alexa, Google home, Google nest, etc.)			Questi dispositivi possono essere hackerati per ascoltare le conversazioni da remoto o per fare cyberstalking	Monitoraggio, cyberstalking	Disattivare I dispositive o, almeno, rimanere vigili riguardo alla loro presenza

Segnali di pericolo riguardanti il comportamento del partner / maltrattante:

SEGNALI DI PERICOLO	Sì	No	Pericolo	Forma di cyberviolenza	Se presente, cosa può essere fatto?
A volte il maltrattante conosce alcune informazioni che non erano state discusse o condivise con lui			Il maltrattante potrebbe avere sotto controllo il cellulare della vittima/sopravvisuta, oppure avere accesso ai suoi account	Monitoraggio, stalkerware	Controllare il dispositivo per app di stalkerware
Il maltrattante è stato avvistato in alcuni luoghi normalmente non frequentati dalla donna (la donna non aveva condiviso i suoi spostamenti con lui)			Il maltrattante potrebbe avere sotto controllo il cellulare o l'auto della donna	Tracciamento, stalkerware	Verificare la presenza di stalkerware nel dispositivo, disattivare il GPS dell'auto
Lui cita parti di messaggi / conversazioni telefoniche che la donna ha avuto con altre persone			Il maltrattante potrebbe avere sotto controllo il cellulare della donna, o avere accesso alle app di messaggistica o ai suoi account	Monitoraggio, stalkerware	Verificare la presenza di stalkerware nel dispositivo, cambiare le password degli account
Lei è sicura che lui non la stia seguendo, ma pensa che il suo partner conosca troppo bene i suoi spostamenti			Il maltrattante potrebbe avere sotto controllo il cellulare della vittima/sopravvissuta	Tracciamento, stalkerware	Controllare il dispositivo per app di stalkerware
Il partner della donna ha smesso di chiederle di visionare il cellulare o di avere le sue password			Il maltrattante potrebbe aver installato delle app di stalkerware sul cellulare di lei		
Lui vuole avere rapport sessuali nello stesso posto della stanza e con condizioni particolari			Potrebbero esserci dei dispositivi di videoregistrazione nascosti nella stanza	Condivisione non consensuale di immagini, doxing, sexting, revenge porn, sextortion	Controllare se sono presenti dispositivi che possano registrare, se possibile, coprirli con indumenti/coperte

Segnali di pericolo riguardanti i social media:

SEGNALI DI PERICOLO	Sì	No	Pericolo	Forma di cyberviolenza	Se presente, cosa può essere fatto?
La donna è stata contattata da estranei sui social media			Il maltrattante può aver creato un profilo falso per monitorare la donna; le informazioni di contatto di lei possono essere state condivise dal maltrattante	Monitoraggio, molestie online, sexting, doxing	Controllare se il profilo sconosciuto ha foto, post, followers, contatti in comune
Spesso lei condivide immagini e dettagli di dove si trova sui social media o nelle storie WhatsApp			Questi dettagli possono essere usati per rintracciarla e monitorarla. Le storie WhatsApp possono essere visualizzate anche da persone che non fanno parte della propria rubrica	Monitoraggio, cyberstalking, condivisione non consensuale di immagini	Discutere con la vittima/sopravvissuta riguardo l'importanza di valutare l'impatto di ciò che condivide
Lei ha condiviso le password degli account dei social media con il partner			Il partner può accedere agli account di lei, monitorarne le conversazioni, vedere gli amici/followers, acquisire immagini		Cambiare le password. Discutere dell'importanza di non condividerle con altre persone, nemmeno in situazioni di "emergenza".
L'email per il recupero della password è accessibile anche al partner			In questo caso, se la donna cambia la password, il maltrattante può facilmente notarlo. Può inoltre cambiare lui stesso la password, bloccando alla donna l'accesso ai suoi account	Monitoraggio, cyberstalking, furto di identità	Modificare l'indirizzo per il recupero della password prima di cambiarla
La donna ha notato attività strane sui suoi account social come se qualcun altro avesse avuto accesso			Qualcuno, non necessariamente il partner, può avere accesso agli account	Cyberstalking, furto di identità, condivisione non consensuale di immagini	Cambiare le password
La donna ha ricevuto chiamate di "apprezzamento" o messaggi da estranei			È possibile che le informazioni di contatto della donna e sue immagini private siano state condivise online	Doxing, sexting, condivisione non consensuale di immagini, molestie online, revenge porn	Tenere tracciabilità delle chiamate/messaggi, impostare un Google alert, richiedere ai motori di ricerca la rimozione del materiale
La donna riceve chiamate da numeri contenuti nella sua rubrica, ma quando risponde si rende conto che è il maltrattante			Il maltrattante potrebbe usare app falsificano il suo ID chiamante	Spoofing, molestie	Tenere tracciabilità di queste chiamate insieme al registro chiamate del cellulare