Navigare protette

La tecnologia digitale è una parte fondamentale delle nostre vite: è ovunque e la usiamo costantemente. È importante sapere come possiamo aumentare la nostra sicurezza online in modo da continuare a **navigare sentendoci libere e al sicuro.**

95% degli abusi online avviene contro le donne, soprattutto da parte di partner o ex

58% delle adolescenti e giovani subisce molestie sui social media quasi quotidianamente

70% delle donne che subiscono cyber-violenza subiscono anche violenza fisica o sessuale[1]

71% degli autori di violenza all'interno di una relazione controlla i dispositivi delle partner

Se pensi che sia normale. O se hai la sensazione che non lo sia ma non sapresti dire come mai.

Se pensi che a te non capiterà. O se senti che forse potresti essere a rischio ma non sai bene in che modo.

Se vuoi saperne di più perché, è vero, viviamo connesse. O se ti trovi in difficoltà, per te stessa o per la tua amica, sorella, collega, vicina, mamma, figlia.

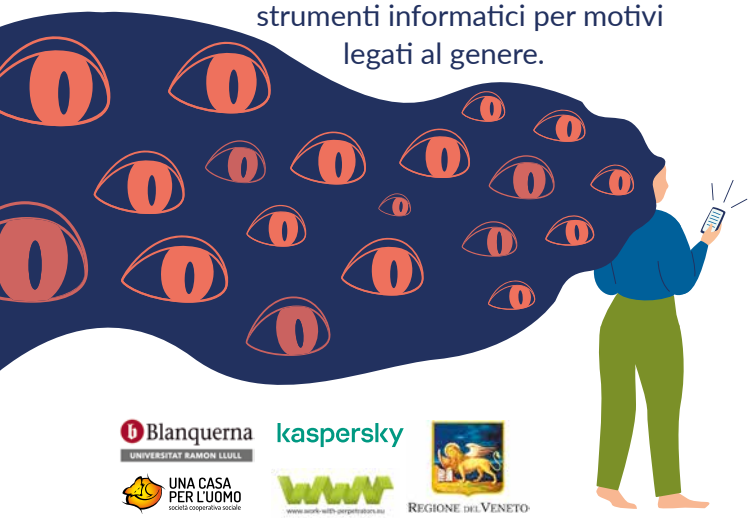
Questo prontuario ti è utile per:

- Sapere come **tutelarti**
- Poter **aiutare** altre donne a te vicine
- Anche se tutto va bene, farti **riflettere**

Le forme di violenza digitale contro le donne

La **dimensione digitale della violenza contro le donne**[2] comprende sia gli abusi che accadono online, sia quelli che sono facilitati dalla tecnologia, ed esiste una continuità tra online e offline. Il mezzo è virtuale, ma l'abuso è reale e i suoi effetti sono concreti.

La cyberviolenza contro donne e ragazze[3] include **molte forme** di violenza agite tramite strumenti informatici per motivi legati al genere.



Gli atti di cyberviolenza contro donne e ragazze possono

- iniziare online e continuare offline, nei luoghi fisici, ad esempio sul posto di lavoro, a scuola o a casa;
- iniziare offline e continuare online tramite diverse piattaforme, come social media, email o app di messaggistica;
- essere agiti da una persona (o da un gruppo di persone), anonima o sconosciuta alla donna;
- essere agiti da una persona (o un gruppo di persone) che la donna conosce, come ad esempio un (ex) partner, un compagno di classe o un collega.

Blanquerna Universitat Ramon Llull · kaspersky · UNA CASA PER L'UOMO società cooperativa sociale · www.work-with-perpetrators.eu · Regione del Veneto

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

Le forme di violenza digitale contro le donne

LIMITAZIONE DELL'ACCESSO AL DIGITALE

Impedire o limitare l'utilizzo di dispositivi come telefono, pc o tablet, di app o di connessione internet, con lo scopo di controllare o isolare una persona, o la minaccia di farlo, con lo scopo di manipolarla.

CYBERSTALKING E CYBERSORVEGLIANZA

Uso di strumenti informatici per molestare, intimidire, spiare una persona, facendola sentire minacciata e insicura.

Questo può avvenire con l'accesso a dispositivi e account tramite

- Richiesta di uso del dispositivo
- Uso di password condivise o sottratte
- Accesso a dispositivi condivisi o non protetti
- Installazione di app spia (stalkerware)
- e/o mediante l'utilizzo di dispositivi quali
- GPS dell'auto o dispositivi di tracciamento
- Impianti di videosorveglianza
- Dispositivi smart home (es. Google home o Alexa)

CYBERMOLESTIE E CYBERBULLISMO CONTRO DONNE E RAGAZZE

Molestie tramite email e messaggi, profili online e pagine internet, con lo scopo o l'effetto di creare per la vittima un ambiente intimidatorio, ostile, degradante, umiliante o offensivo.

Si tratta di:

- 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

USO NON CONSENSUALE DI CONTENUTI PERSONALI E INTIMI

Abuso relativo alla circolazione, o alla minaccia di far circolare tramite mezzi informatici, di 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,
- ottenuti consensualmente ma condivisi in modo non consensuale

Blanquerna Universitat Ramon Llull
kaspersky
UNA CASA PER L'UOMO società cooperativa sociale
Regione del Veneto

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

Consigli utili per aumentare la sicurezza digitale

Per tutte, tutti i giorni

Proteggi il tuo dispositivo con una password o un PIN: ogni dispositivo che hai, cellulare, computer o tablet, dovrebbe essere protetto con una password o PIN che solo tu conosci.

Quando scegli una password o un PIN, **non utilizzare parole o codici facilmente indovinabili**, come compleanni, nomi di animali domestici, o altre cose che ti piacciono. Non usare la stessa password o lo stesso PIN su ogni dispositivo.

Non condividere le password dei tuoi dispositivi e dei tuoi account e profili con altre persone, neanche con il tuo partner o con i tuoi figli.

Non salvare le password sul tuo computer o cellulare, né 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, che si chiamano "password manager".

Disabilita la geolocalizzazione del tuo telefono o tablet quando non ti serve.

Prima di spegnere un dispositivo condiviso con altri, **scollegati ed esci** dai siti e dagli account e durante l'utilizzo usa la modalità incognito.

Controlla le impostazioni di privacy dei social media scegliendo il livello più alto di privacy.

Fai attenzione a ciò che posti online, soprattutto se si tratta di contenuti che possono rivelare i tuoi spostamenti o altre informazioni o immagini che potrebbero essere sfruttate per danneggiare te o la tua reputazione.

In generale, **non condividere pubblicamente online informazioni** personali (nome, indirizzo, data di nascita, codice fiscale, numero di telefono, numero carta di credito, etc).

Quando sospetti o sei certa che qualcuno ti stia controllando

Usa un dispositivo sicuro, al quale il tuo (ex) partner non ha accesso. Potrebbe essere un nuovo dispositivo, uno pubblico, quello di una persona fidata, o un vecchio telefono senza internet. Il dispositivo sicuro va usato per tutte le comunicazioni con il centro antiviolenza, con le forze dell'ordine, con l'avvocato, con il medico, con la banca, ecc.

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.

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. Quando crei il nuovo account, segui le regole indicate sopra per avere password sicure.

Disattiva dispositivi smart in casa come "google nest" o Alexa, che potrebbero essere usati per ascoltare le conversazioni a distanza.

Usa la modalità in incognito del browser quando navighi in internet, così non restano tracce dei siti web visitati.

Blanquerna Universitat Ramon Llull · kaspersky · UNA CASA PER L'UOMO società cooperativa sociale · Regione del Veneto

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

ATTENZIONE!

- Se scopri di avere una app spia installata sul tuo dispositivo NON rimuoverla.
- Se ricevi messaggi di minaccia, offesa o altro, NON cancellarli.
- E in generale, se ti trovi vittima di un abuso NON cercare di risolvere da sola!

Oltre a eliminare o confondere le prove e il materiale per un'eventuale azione legale presente o futura a tua tutela, questo potrebbe metterti in pericolo: sapendo di essere stato scoperto, l'autore dell'abuso potrebbe peggiorare il suo comportamento.

Invece, tutelati così:

Rivolgiti alla **Polizia Postale**, è possibile farlo anche in anonimato e senza l'obbligo di sporgere denuncia.

Contatta un **centro antiviolenza** per essere supportata e informata sulle diverse possibilità che hai di sottrarti alla violenza e tutelarti.

E ricorda, cerca aiuto usando **dispositivi sicuri**!

Contatti:

- Portale web della Polizia Postale e delle Comunicazioni: **www.commissariatodips.it**
- Numero verde anti violenza e stalking: 1522
- Sito della rete nazionale dei centri D.i.Re Donne in Rete contro la violenza: **www.direcontrolaviolenza.it**

Desideri saperne di più? Clicca qui per trovare materiali, video, news e contatti di approfondimento.

www.work-with-perpetrators.eu/destalk-it/campaign

Riferimenti

1 European Institute for Gender Equality. (2017, June 19) Cyber violence is a growing threat, especially for women and girls. https://eige.europa.eu/news/cyber-violence-growing-threat-especially-women-and-girls

2 CoE GREVIO (2021) General Recommendation No.1 on the digital dimension of violence against women https://www.coe.int/en/web/istanbul-convention/-/grevio-publishes-its-general-recommendation-no-1

3 EIGE (2022) Cyber Violence against Women and Girls Key Terms and Concepts https://eige.europa.eu/sites/default/files/cyber_violence_against_women_and_girls_key_terms_and_concepts.pdf

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