Centro Antiviolenza
"Centro Aiuto Donna"
FONDAZIONE CITTÀ SOLIDALE ONLUS

Fondazione Città Solidale onlus
www.fondazionecittasolidale.it

AUTODIFESA *virtuale*

Una guida per mettere in sicurezza i principali account social e servizi più utilizzati in rete

2023

Progetto finanziato dalla Presidenza del Consiglio dei Ministri - Dip. Pari opportunità

Progetto finanziato dalla Regione Calabria - L.R. 20/2007

Centro Antiviolenza
"Centro Aiuto Donna"
FONDAZIONE CITTÀ SOLIDALE ONLUS

Fondazione Città Solidale onlus
www.fondazionecittasolidale.it

Progetto:

TI ASCOLTO, TI SOSTENGO

Il Progetto "Ti Ascolto, Ti Sostengo" nasce dall'esigenza di sviluppare la rete di sostegno per le donne vittime di violenza e i loro figli, attraverso il rafforzamento dei servizi territoriali, del Centro Antiviolenza "Centro Aiuto Donna" e dei servizi di assistenza, prevenzione e contrasto, favorendo un percorso di fuoriuscita dalla condizione di disagio.

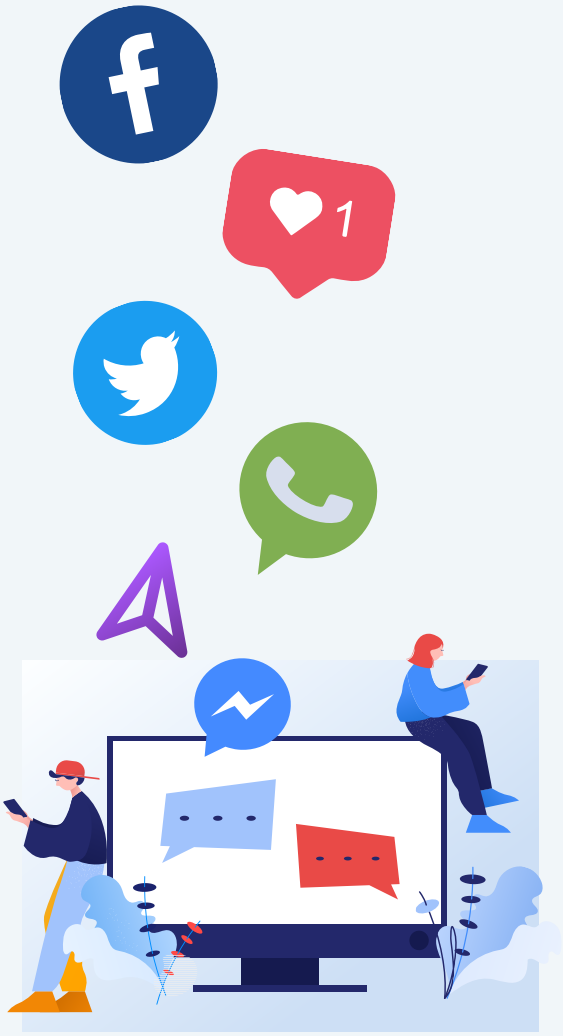
Indice

Introduzione

I **social network** sono diventati una parte integrante della vita quotidiana di milioni di persone in tutto il mondo. Tuttavia, con l'aumento dell'uso dei social network, anche i **rischi associati** ad essi sono aumentati. La diffusione di **notizie false**, la **violazione della privacy** e il **cyberbullismo** sono solo alcune delle minacce che possono essere incontrate sui social network.

Per questo motivo, è importante conoscere le linee guida per difendersi sui social network e proteggere se stessi e la propria reputazione online. In questo opuscolo, troverete **consigli utili** per navigare in modo sicuro e responsabile sui social network.

Mettere KO uno stalker su
FB, GOOGLE, TWITTER, MESSENGER, WHATSAPP



Il reato di stalking

Il reato di stalking (dall'inglese to stalk, letteralmente "fare la posta") è entrato a far parte dell'**ordinamento penale italiano mediante il d.l. n. 11/2009 (convertito dalla l. n. 38/2009) che ha introdotto all'art. 612-bis c.p., il reato di "atti persecutori",** il quale punisce chiunque "con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita".

Il reato di stalking indica un **insieme di comportamenti molestie ripetuti** quali appostamenti continui nei pressi del domicilio o degli ambienti comunemente frequentati dalla vittima, inseguimenti, telefonate oscene o molestie sul web che implicano ingerenze nella sua vita privata alla ricerca di un contatto personale. Il temine stalker, infatti, significa "colui che insegue furtivamente la sua preda".
La maggior parte degli stalker sono individui che conosci, con cui hai avuto una relazione romantica o amichevole in passato e che non accetta la fine di tale storia.

In altri casi si può parlare di **stalker ossessionati** da un'idea amorosa; in questo caso si tratta di persone che non hai mai incontrato (o semplici conoscenti con cui non hai un vero e proprio rapporto), ma che si convincono che tra voi ci sia una relazione. Le persone che perseguitano le celebrità rientrano in questa categoria. Altri ancora sono affetti da **fantasie psicotiche**, persone che trasformano le attenzioni in vere e proprie minacce che, se non dessero i frutti "sperati" potrebbero generare nello stalker, una vera e propria violenza.

Di recente la norma è stata modificata; infatti non è più possibile mettere in atto una "condotta riparatoria" e il conseguente risarcimento in denaro per estinguere il reato. **Lo stalking è un reato perseguibile penalmente e l'eventuale iter risarcitorio può essere avviato costituendosi parte civile nel processo penale o in un separato processo civile.**
Inoltre, la legge stabilisce che le vittime di alcuni reati, tra i quali rientra lo stalking, possano richiedere il gratuito patrocinio anche se superano il reddito stabilito come base massima per potervi accedere. La vittima potrà costituirsi parte civile senza pagare alcun contributo e senza dover corrispondere alcun compenso all'avvocato (le spese saranno sostenute dallo Stato).

Come comprendere se è stalking?

Un comportamento si può definire stalking se altera le nostre **abitudini di vita**, se viviamo in un costante stato di **ansia e paura**, se gli atti persecutori si ripetono per almeno quattro settimane e determinano **effetti negativi** perduranti nella vittima.

Di seguito indichiamo alcuni elementi dello stalker che contribuiscono ad individuare tale comportamento:

1. **Aggressioni verbali**
   anche in presenza di testimoni o continui apprezzamenti indesiderati

2. **Continue telefonate**
   sgradite, sia nelle ore diurne che notturne

3. **Inseguimenti o appostamenti**
   in macchina o lo stalker ci aspetta nei luoghi che frequentiamo

4. **Continue pubblicazioni**
   di post o video sul web in cui la vittima è destinataria delle attenzioni dello stalker

5. **Continui sms**
   o messaggi su whatsapp, su messenger

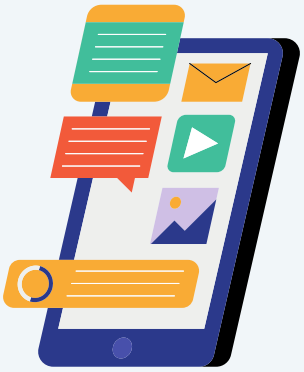
6. **Minacce dirette**
   a noi o alle persone con le quali siano in relazione: amici, parenti, colleghi

7. **Danneggiamento dei beni**
   della vittima in concomitanza con gli elementi di cui sopra: auto rigata, gomma bucata, ecc

8. **Diffusione di notizie diffamatorie**
   sul tuo conto, sul posto di lavoro, con gli amici, con i genitori che ricevono messaggi che mettono in cattiva luce).

Questi sono solo alcuni degli atteggiamenti più comuni dello stalker.
Nelle prossime pagine spiegheremo come difendervi da uno stalker in ambito informatico e come raccogliere le prove per fare una denuncia.

Come difendersi da uno stalker



Se i punti elencati nel paragrafo precedente corrispondono alla vostra situazione occorre valutare il pericolo in modo serio e rivolgersi immediatamente alle forze dell'ordine soprattutto se si tratta di un pericolo immediato.

Se lo stalking avviene online in una forma che non si può considerare un pericolo imminente per la nostra incolumità bisogna seguire i seguenti step:

- Mettere in **sicurezza** i dati online ed iniziare a raccogliere le prove
- Per avere un elevato grado di sicurezza, bisogna non rivelare mai il proprio indirizzo di casa, la città natale; se lo hai fatto, **cancellalo**
- Inizia a tenere un diario su cui riportare l situazioni che potrebbero tornare utili in caso di denuncia
- Dire in modo deciso e senza tentennamenti, allo stalker, che una relazione è finita o comunque non potrà mai avere inizio (minacciando anche eventuale denuncia se ciò non si dovesse verificare
- Nel caso dello stalking telefonico non cambiare numero di telefono né il telefono stesso, anche se questa potrebbe essere la reazione più immediata per fuggire dalla paura e dalle minacce. Infatti, così facendo perdiamo l'opportunità di **documentare le prove dello stalking**. Tramite l'analisi forense del dispositivo, si potrà conferire valore legale all'atto di stalking. Quindi conserva il telefono con cura, registrando le telefonate (ci sono delle app specifiche che lo consentono) e gli sms, senza mai rispondere allo stalker. Si può anche prendere un nuovo telefono ma mantenendo comunque attivo quello su cui si viene contattati dallo stalker
- Nel caso di stalking sui social, NON ELIMINARE I POST ma conservali e richiedi una copia autentica per conferirle valore legale (ci sono dei dispositivi e delle organizzazioni in grado di fare ciò
- Per evitare che lo stalker contatti i nostri amici bisogna limitare la visibilità delle amicizie sui social affinchè non siano visibili agli sconosciuti
- Nel caso di stalking con biglietti e testi per email conservali nel dispositivo affinchè possano essere documentate successivamente con valore legale
- Nel caso di appostamenti dello stalker sotto casa o al lavoro scattare delle foto con il telefono e lasciarle nel dispositivo affinché possano essere documentate successivamente con valore legale
- Nel caso di apprezzamenti verbali, registriamoli con il telefono e lasciamo il file audio nel dispositivo affinchè possano essere documentate successivamente con valore legale
- In linea di massima occorre quindi documentare ogni cosa, in modo da avere delle prove valide da presentare alle autorità.

La PROCEDURA DI AMMONIMENTO, più rapida di una denuncia!

QUANDO AVETE RACCOLTO LE PROVE FATE SUBITO LA PROCEDURA DI AMMONIMENTO, CHE È PIÙ RAPIDA DI UNA DENUNCIA!

Sappiate che allo scopo di prevenire la consumazione del reato di atti persecutori, l'art. 8 della l. n. 38/2009 ha previsto anche che la persona offesa possa ricorrere alternativamente, prima di proporre eventuale querela, ad una "procedura di ammonimento", che mira a far desistere lo stalker dalle attività persecutorie attraverso un invito allo stesso rivolto, attraverso le autorità di pubblica sicurezza. Avanzate dunque la richiesta al questore di ammonimento (**avvertimento verbale**) nei confronti dell'autore delle condotte persecutorie. Il **vantaggio** dell'ammonimento è che laddove il soggetto non ottemperi all'invito formulato dall'autorità e insista nel perpetrare le proprie condotte persecutorie, avrà un notevole **AUMENTO DELLA PENA** procedibile poi d'ufficio.

Un esempio del modulo di ammonimento

AL QUESTORE DELLA PROVINCIA DI _____
La sottoscritta_____, nata il _ _ / _ _ /_____ a_____, residente a_____in _____tel._____e-mail _____
non avendo ancora sporto querela per i fatti di seguito narrati

_____
_____
_____
_____
_____

CHIEDE

che la S.V. proceda alla completa identificazione ed all'ammonimento nei confronti del/della Sig./Sig.ra_____,il/la quale, con le proprie reiterate condotte di stalking qui allegate, ha costretto la sottoscritta a modificare radicalmente le proprie consuete abitudini di vita, ingenerando il fondato timore per l'incolumità personale e causando, per tali motivi, un perdurante e grave stato di ansia e di paura. La sottoscritta, si riserva inoltre la facoltà di sporgere querela nei confronti del/della Sig./Sig.ra_____, nei previsti termini di legge.
Luogo e data _____
La Richiedente_____(si allega la documentazione informatica)

NOTA: Per quanto concerne la decorrenza del termine per la proposizione della querela, il termine non scadrà prima di sei mesi dopo l'ultimo della serie di atti che integrano la condotta.

In questa fase occorre continuare a raccogliere delle prove ma al contempo essere maggiormente attenti alla propria sicurezza.

Lo stalker potrebbe diventare più maniacale.

Evitare ogni situazione di pericolo, come spostarsi in luoghi solitari soprattutto di notte.

Ogni atto di stalking deve essere documentabile. Attendere 20/30 giorni dall'ammonimento e se le molestie continuano documentarle nuovamente al questore affinché il delitto di stalking sia perseguito d'ufficio.

Se lo stalker si presenta davanti a casa, non farsi vedere e chiamare subito i carabinieri informandoli della procedura di ammonimento in atto.

Se lo stalker viene fermato dai carabinieri in questa circostanza sarà perseguito d'ufficio.

A questo punto siamo giunti alla fase nella quale attiveremo tutte le procedure possibili per fare muro contro lo stalker:

- **Cambiamo il telefono ed il numero di cellulare** (ATTENZIONE: il telefono nel quale abbiamo ricevuto le molestie non va gettato ma conservato con cura come prova richiedibile dal giudice. Meglio prendere un nuovo telefono per non inquinare le prove e sovrascrivere i dati);
- **Mettiamo in massima sicurezza** i nostri social network tramite le apposite guide che si trovano su internet;
- **Segnaliamo lo stalking ricevuto a tutte le figure che possono "aiutarci".** Se sei una studentessa, ad esempio, avvisa le autorità universitarie, come ad esempio un professore, il preside di facoltà. Se lavori in una società fallo sapere al tuo datore di lavoro.

Uno screenshot non ha valore legale

Molte persone credono che per **copiare una pagina web** sia sufficiente fare una stampa della pagina o di un commento sui social per acquisire una prova con valore legale, da allegare, ad esempio, ad una denuncia. Procedere in questo modo, al contrario, **non ha alcun valore legale** poiché non è possibile garantire l'origine del documento e la controparte può disconoscerne la validità sulla base del principio di cui all'art. 2712 cod. civ.

1. Diffamazione su Facebook

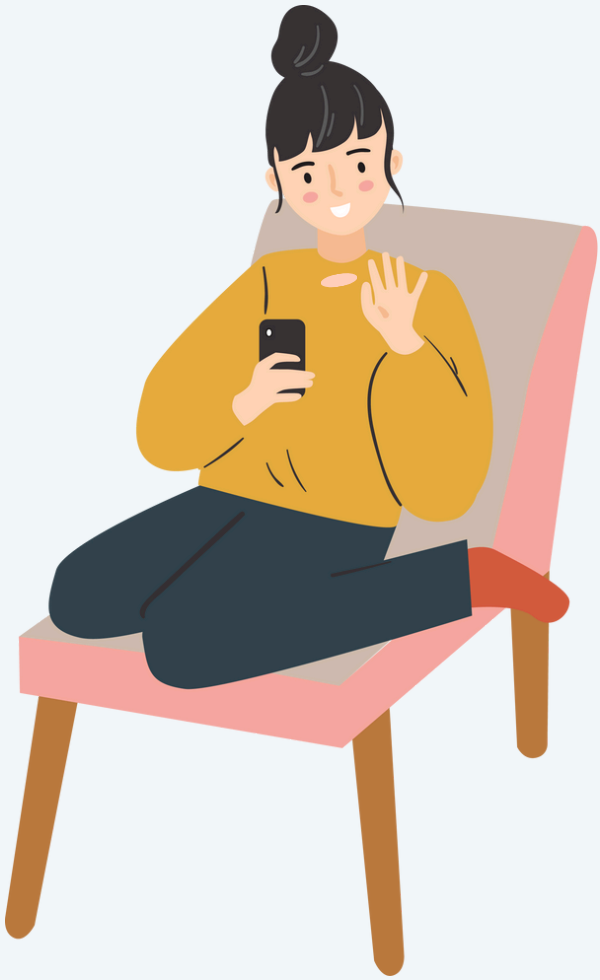
Nel caso ad esempio di una diffamazione su Facebook, senza i requisiti necessari che vi offre una copia autentica, il CTU (consulente tecnico di ufficio) incaricato dal giudice di accertare la titolarità dell'account Facebook autore della diffamazione, dal quale sono stati diramati in rete i messaggi a contenuto diffamatorio, nonché di verificare l'integrità/autenticità delle copie di pagine Facebook da voi stampate, allegate alla denuncia, evidenzierebbe che le copie stampate di pagine internet, allegate alla querela sporta dalla parte offesa, non offrono da sole garanzie certe, né sull'autenticità e integrità dei messaggi, né sulla loro data, né sulla loro provenienza da un eventuale sito effettivamente intestato all'imputato o assegnatogli ad utilizzo con account registrato e ciò in considerazione del fatto che qualsiasi copia cartacea che riproduca una pagina Facebook, se recuperata senza il rispetto delle procedure standard che ne garantiscono la corretta acquisizione, potrebbe come afferma la Corte di Cassazione - essendo una copia non ufficiale - anche costituire, il risultato di operazioni dì adattamento o rielaborazione di pagine effettivamente esistenti, ma di contenuto differente.

2. La pagina web

La pagina web può essere senza dubbio ricompresa nella definizione di documento informatico quale "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti", contenuta nell'art. 1 lett. p) del D. Lgs 82/2005 - Codice dell'Amministrazione Digitale (in sigla CAD) e, come tale, può essere duplicata in formato digitale. Ciò che appare sullo schermo del nostro computer quando accediamo ad un sito internet non è altro che la replica, scaricata nella memoria di lavoro del nostro PC, delle informazioni presenti sul sito che stiamo visitando. Si tratta, pertanto, della «rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti» o, in altri termini, di un documento informatico.

La pagina web (così come i messaggi di posta elettronica non muniti di firma elettronica o i messaggi di testo SMS) è dunque un documento che può essere introdotto nel giudizio come prova, con valore probatorio, anche se non sottoscritto.

3. Ma come si fa a copiare una pagina web?



La Corte di Cassazione, con la sentenza n. 2912/04,ha chiarito che, ai fini probatori, non basta tuttavia produrre la mera stampa della pagina web (salvare la pagina html o dinamica), bensì è necessario depositarne copia autenticata da soggetti abilitati come notai, avvocati e consulenti tecnici forensi con firma digitale e marcatura temporale.

Più recentemente sempre la stessa corte ha affermato che va escluso che costituisca documento utile ai fini probatori una copia di "pagina web" su supporto cartaceo che non risulti essere stata raccolta con garanzia di rispondenza all'originale e di riferibilità a un ben individuato momento (Cassazione Sezione Lavoro n. 2912del 18 febbraio 2004, Pres. Mattone, Rel. Spanò).

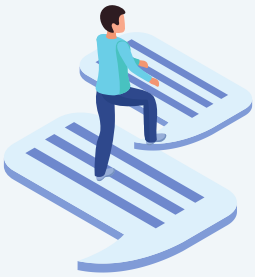
La mancanza di sottoscrizione elettronica, infatti, rende instabile sia la validazione dei dati, che potrebbero essere modificati in ogni tempo, che la provenienza del documento che li contiene, caratteristiche entrambe che, con diversi gradi di certezza, vengono invece attestate dalla apposizione di una firma elettronica con marcatura temporale.

PER QUALI SCOPI VIENE UTILIZZATA UNA COPIA AUTENTICA ?

A scopo puramente esemplificativo la copia autentica di una pagina web o copia conforme con valore legale di una pagina web viene solitamente utilizzata per:

- Diffamazione, calunnia, stalking e minacce su internet come documento per la cristallizzazione delle prove da presentare nella denuncia
- Raccolta informazioni presenti su pagine web e social network
- Uso illecito di marchi e concorrenza sleale
- Violazione del diritto d'autore

SENTIRSI SICURI ONLINE



Nel web si nascondono **numerosi pericoli**: i principali sono sicuramente il rischio di truffa e quello di violazione della privacy, ma ne esistono tanti altri che spesso non si considerano. Per questo motivo occorre innanzitutto informarsi bene sulle insidie della rete, poi bisogna prendere le dovute precauzioni e adottare dei comportamenti per un uso corretto e responsabile di internet.
Vediamo insieme quali sono i rischi e poi le **strategie da adottare** per proteggersi quando si naviga in rete.
Secondo le statistiche della Polizia, ormai un crimine su cinque viene commesso online. Si tratta, quindi, di veri e propri reati penali che è utile conoscere per non diventarne vittime.

Ecco quali sono i principali rischi che si corrono navigando online:

Phishing

Si tratta di un sistema che approfitta della vulnerabilità del tuo dispositivo per installare **virus nascosti al fine di rubarti dati sensibili**, come ad esempio PIN e altri dati personali. Il virus si installa aprendo mail dannose - spesso camuffate da comunicazioni provenienti da istituti bancari o simili - oppure cliccando su banner pubblicitari ingannevoli o siti pericolosi.

Truffe

Sempre cliccando su banner pubblicitari ingannevoli capita spesso anche di imbattersi in **siti che richiedono dati personali** all'utente per riscuotere un premio. Si tratta ovviamente di una truffa, reato di cui si può essere vittime anche su siti di e-commerce oppure anche attraverso annunci di privati. Succede spesso, ad esempio, nel settore dei viaggi, dove vengono venduti finti pacchetti vacanze o affittate case che non esistono.

Furti d'identità

Sono frequenti sui social network, dove alcune persone si impossessano dell'identità di qualcuno allo scopo di **diffamarlo, denigrarlo o distribuire password o numeri di telefono**. A volte le vittime sono personaggi pubblici la cui identità viene rubata per cercare di metterli in cattiva luce compiendo atti illeciti, come la pubblicazione di post compromettenti o ingiuriosi, screditando così il loro nome, oppure per ottenerne dei benefici.

Utenti pericolosi

Navigando in rete, utilizzando i social network e soprattutto le chat, ci si può imbattere in persone con cattive intenzioni come **hacker, pedofili, maniaci o individui che fingono di essere qualcun altro** con lo scopo di danneggiare in qualche modo la vittima di turno.

Da non sottovalutare, in questo senso, è anche il pericolo di essere diffamati o di diventare **vittime del cyberbullismo**, fenomeno che interessa soprattutto i giovani: sui social network si può rischiare, infatti, che vengano pubblicate foto o video per ridicolizzarci e denigrarci, oppure può capitare che qualcuno, magari nascosto dietro a un nickname falso, ci insulti o riveli pubblicamente fatti o dati che ci riguardano, violando così la nostra privacy.

5 STRATEGIE PER DIFENDERSI SUL WEB

Abbiamo analizzato quali sono i principali pericoli del web. Vediamo adesso 5 strategie da adottare per difendersi da queste **minacce** e prevenire ogni possibile **rischio**.

Installare un antivirus

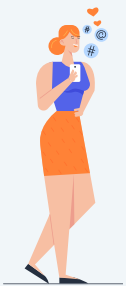
Per proteggersi da **phishing** e **software malevoli** il primo passo è quello di **installare sul proprio computer un antivirus valido e sempre aggiornato**. È opportuno, poi, navigare sempre in **modalità protetta**, disabilitando tutti quegli accessori del browser, come ad esempio i java script, che di solito vengono usati proprio per carpire informazioni e dati sensibili. Altri importanti accorgimenti da seguire sono: **non aprire mai email provenienti da mittenti sconosciuti e comunque non cliccare mai sui link contenuti al loro interno**.
Non fidatevi delle mail nelle quali compare il nome della vostra banca: in genere in questi messaggi viene chiesto di inserire i propri dati o i propri codici bancari per un problema riguardante il sistema di internet banking o per un aggiornamento dei vostri dati. Si tratta, appunto, di tentativi di phishing: **le banche non inviano mai questo tipo di comunicazioni ai clienti via email**, quindi non bisogna mai cliccare su link sospetti o fornire i propri dati.

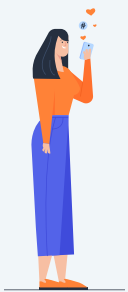
Non fidarsi in chat

Quando si conosce una persona in una chat, ma anche attraverso applicazioni di messaggistica istantanea come Skype, WhatsApp e Messenger, bisogna fare **attenzione a confidare cose personali, a rivelare i propri dati e anche a inviare proprie foto**. Dall'altra parte dello schermo potrebbe nascondersi un truffatore o un malintenzionato che potrebbe utilizzare ciò che gli dite o inviate per scopi illeciti, incluso il diffondere le vostre foto in rete senza la vostra **autorizzazione**.

Attenzione a cosa si scarica

Quando si effettua il download di un programma o un file dal web bisogna stare sempre in guardia in quanto potrebbe trattarsi di **virus**, uno **spyware** o di un altro software malevolo. Inoltre, ogni volta che si condivide o si scarica qualcosa in rete bisogna considerare il problema del **copyright**: il materiale in questione, infatti, potrebbe appartenere a qualcuno che potrebbe rivendicarlo e chiederne i diritti.





Non condividere informazioni personali sui social network

Spesso, per rubare l'identità di qualcuno il ladro si serve proprio delle informazioni che la persona in questione ha già condiviso sui social. Più dati personali si pubblicano e più è alto il rischio di subire un furto d'identità. Bisogna dunque **evitare di inserire data di nascita, indirizzo, luogo di lavoro o scuola frequentata**. Inoltre, quando si pubblicano le proprie foto bisogna considerare che poi resteranno in rete e sarà molto difficile eliminarle o controllarle, e chiunque potrà scaricarle e usarle per creare un nuovo profilo fingendo di essere la persona della foto. Queste avvertenze valgono anche per i minori, che andrebbero controllati costantemente per evitare che forniscano dati personali a sconosciuti.

Sottoscrivere una polizza di tutela legale cyber

Stipulare **un'assicurazione** che copra le eventuali spese legali per difendersi dai reati commessi o subiti sul web è un ottimo metodo per tutelare sé stessi e la propria famiglia e per poter così navigare in rete con una protezione in più.

DIFENDERSI DALLA TRUFFE SENTIMENTALI SUL WEB

Quelle sentimentali (o **romance scam**) sono le più subdole fra le truffe online. Non colpiscono solo il portafoglio, ma anche il cuore. Una lettrice ci ha raccontato la sua esperienza e noi abbiamo indagato: ecco come difendersi. Sono molte le donne che restano vittima di truffe online ad opera di esperti che le raggirano fingendosi innamorati.[1]

Decine di casi ogni anno

Un caso isolato? Affatto. Sono decine e decine le storie come questa. Tutte in qualche modo simili: personaggi che si fingono uomini colti e affascinanti contattano le donne su Facebook, inventandosi magari fantomatiche origini francesi o inglesi. Le corteggiano e quando capiscono che sono completamente cotte fingono di aver avuto un inconveniente in qualche Stato africano e di aver bisogno di soldi. Per convincerle che è tutto vero, invia loro foto o fotocopie di documenti trafugati su altri profili di persone ignare o raggirate a loro volte. Per questo è importante anche non mandare mai documenti o dati personali. I truffatori utilizzano persino dei software per truccare le video-conversazioni su Skype. Le donne sono convinte di vedere realmente il loro uomo e invece è solo l'ennesimo inganno.

Le donne più colpite

L'FBI, in un report del 2011, ha stimato circa 10.000 casi negli Stati Uniti. Ha calcolato anche l'età delle vittime: il 35% ha fra i 50 e il 60 anni, il 33% fra i 40 e i 50, il 14% più di 60 anni e il 17% la fascia 20-30. La generazione più colpita riguarda dunque le donne fra i 40 e i 60 anni. Le inchieste della magistratura e della polizia postale hanno dimostrato l'esistenza di vere e proprie organizzazioni criminali dedite a questo tipo di truffe.

[1] Donna Moderna numero del 05/10/2016 di Fabio Brinchi Giusti "Truffe online, come difendersi da quelle sentimentali" -https://www.donnamoderna.com/news/societa/truffe-online-sentimentali-come-difendersi

Le associazioni e i gruppi di auto-aiuto

Ma il reale numero di vittime del romance scam (il nome inglese che indica le truffe sentimentali) è molto più alto. Tante vittime si vergognano e non denunciano. Si sentono ingenue, stupide e temono di essere giudicate e criticate dagli altri. Qualcuna invece trova il coraggio di uscire allo scoperto, come Jolanda Bonino, che oggi ha fondato un'associazione per aiutare le vittime delle truffe sentimentali. Jolanda ha inviato migliaia di euro ad un presunto ingegnere francese che diceva di lavorare in Costa d'Avorio. "Ci sono caduta anche io che mi credevo assai furba." –racconta– "Il fatto è che alcune volte si è in uno stato di fragilità emotiva oppure di ignoranza informatica dove è possibile tutto. E così questi personaggi incantano donne e uomini in carenza affettiva per trarne vantaggi economici. La piaga della solitudine miete molte più vittime di quanto non si pensi e non c'è da escludere che molte arrivino a gesti estremi come è accaduto in Francia e in Belgio." Altre donne hanno costituito, sempre sui social-network, gruppi di auto-aiuto dove si confrontano, si parlano, cercano in qualche modo di ricostruire la loro autostima distrutta o di aiutare altre donne a sfuggire e a riconoscere le truffe.

I trucchi per riconoscere la truffa

Il Centro Antiviolenza "Marie Anne Erize" di Roma, invece, ha realizzato e diffuso un vademecum ricco di consigli e trucchi per stanare i truffatori dell'amore. Prima operazione da fare è controllare il profilo che ci chiede l'amicizia o che ci ha scritto in chat. "Fanno già suonare un primo campanello d'allarme" –spiegano gli esperti del Centro– "il numero esiguo di amicizie e l'assenza di notizie precise e specifiche sui dati personali, nonché la scarsità di aggiornamenti sul profilo Facebook." Attenzione anche alla foto; cliccando col tasto destro del mouse sull'immagine è possibile cercarla su Google e scoprire se è stata copiata da Internet. Il Centro Antiviolenza "Marie Anne Erize" di Roma, invece, ha realizzato e diffuso un vademecum ricco di consigli e trucchi per stanare i truffatori dell'amore.

Prima operazione da fare è controllare il profilo che ci chiede l'amicizia o che ci ha scritto in chat. "Fanno già suonare un primo campanello d'allarme" –spiegano gli esperti del Centro– "il numero esiguo di amicizie e l'assenza di notizie precise e specifiche sui dati personali, nonché la scarsità di aggiornamenti sul profilo Facebook." Attenzione anche alla foto; cliccando col tasto destro del mouse sull'immagine è possibile cercarla su Google e scoprire se è stata copiata da Internet.

L'identikit del truffatore

"I truffatori" -proseguono gli esperti- "poi, tendono sempre a presentarsi con profili standard: uomini di mezza età, bianchi, europei, professionisti di successo (ingegneri, architetti e consulenti sono le professioni più gettonate), spesso vedovi e con bambini." Raccontano di una vita sentimentale triste e di essere alla ricerca di una partner seria e affidabile. "Il truffatore diventerà una presenza costante" –avvertono gli esperti del Centro– "vi scriverà mattina e sera, diventerà una consolazione alle fatiche e tristezze quotidiane. Il truffatore farà sentire le donne speciali e amate e la cosa può andare avanti anche per mesi". Un lavoro lento e psicologico per rendere la vittima dipendente dal truffatore. Anche qui un buon consiglio è quello di osservare con attenzione i messaggi che vengono ricevuti: spesso si tratta di frasi fatte, messaggi generici e poco precisi. Non fermarsi all'apparenza ma porre domande precise e dettagliate. Spesso lo scammer non saprà cosa rispondere e lo farà in modo vago. Fare attenzione anche al numero di telefono che vi darà: spesso iniziano con il prefisso +4470; in questo caso si tratta sicuramente di falsi numeri.

Mai dare soldi

"Il punto fondamentale" –proseguono– "è la richiesta di denaro. Diffidate sempre di chi chiede soldi via Internet e non date mai neppure un euro a chi non conoscete personalmente." I truffatori useranno tutte le tecniche possibili per convincere donne generose e sole ad aiutarli. Una volta ricevuto il denaro o ne chiederanno altro con nuove scuse o troncheranno il rapporto. Il risultato è quasi sempre lo stesso. Chi ha sostenuto una relazione virtuale con un truffatore si sentirà distrutto per molto tempo. Non tanto per il denaro quanto per le energie investite in questo rapporto e per il fatto di aver perso la testa prima ancora di aver incontrato fisicamente l'eventuale futuro/a partner. Segue a questa prima fase, una depressione profonda. E di qui la mancata denuncia del raggiro subito non soltanto alle forze dell'ordine ma anche a terapeuti. Anzitutto denunciare alla polizia di essere stati vittima di un raggiro: in taluni casi i truffatori sono stati arrestati! In secondo luogo, investigare con l'aiuto di un terapeuta, la ragione per la quale si è stati raggirati senza porre attenzione. In terzo luogo, collaborare con i siti che raccolgono le testimonianze dei truffati. È fondamentale arricchire banche dati pubbliche on-line con testimonianze e dati. Ciò fa comprendere come anche tante altre persone siano state vittima del raggiro. Non si è soli. E soprattutto, non ci si può colpevolizzare per aver cercato l'amore, anche se con modalità un pochino superficiali."

Cos'è il REVENGE PORN

Cosa succede quando foto intime vengono messe online, spesso come vendetta personale, senza il consenso delle dirette interessate?

Breve indagine su un fenomeno complesso le cui vittime sono perlopiù donne, tra nuove forme di **ricatti sessuali e gravi carenze legislative**.

Che cosa si intende quando si parla di revenge porn e perché è un fenomeno che ci riguarda tutti?

Il significato letterale è semplice: si tratta della **diffusione non autorizzata** di immagini intime di persone coinvolte in atti sessuali, a volte riprese a loro insaputa. A diffondere quelle immagini spesso sono gli ex o persone nella cerchia di amici e familiari, mentre i luoghi di diffusione deputati sono le chat e i gruppi su Facebook e WhatsApp, sia chiusi che aperti, ma anche specifici siti e forum specializzati nella ricondivisione di materiale di questo tipo.

Un meccanismo difficilissimo da spezzare

In Italia ne abbiamo parlato molto spesso, anche recentemente, basti pensare al caso di un gruppo di 63 studentesse di un liceo di Modena che avevano l'abitudine di scambiarsi foto, anche erotiche, su WhatsApp. Quei file, intercettati da un compagno di scuola e da lui diffusi senza il consenso delle ragazze coinvolte, sono finiti in rete e ora potrebbero trovarsi potenzialmente nel telefono o nel computer di chiunque in Italia e nel mondo. Così funziona internet, dove stoppare la circolazione di immagini contro la volontà del soggetto è un'operazione quasi impossibile. **Le foto e i video vengono infatti regolarmente scaricati e ricaricati da altri utenti che non hanno nessun contatto "reale" con quelli di partenza, creando così un circolo vizioso difficilissimo da spezzare.**

Il caso di Tiziana Cantone

In Italia, il caso più conosciuto legato alla diffusione non autorizzata di immagini intime è quello di **Tiziana Cantone**, trentunenne originaria di Mugnano di Napoli che si è **suicidata il 13 settembre 2016.**

All'incirca un anno prima, **alcuni video che la ritraevano mentre faceva sesso** erano diventati virali, impendendole di condurre, da quel momento in poi, una vita normale.

Non del tutto consapevole del meccanismo che abbiamo descritto prima, Cantone acconsente inizialmente a una prima diffusione dei video, d'altronde si tratta di un gioco erotico tra lei, il fidanzato di allora, Sergio Di Palo, e alcuni uomini vicini alla coppia, ma quando i filmati si diffondono a cascata da WhatsApp a Facebook, da Google ai siti di quotidiani, anche autorevoli, che la descrivono come il nuovo "fenomeno del web".

Eppure Cantone ha utilizzato sin da subito tutti gli strumenti legali a sua disposizione per fermare la diffusione di quei video, ma l**a giustizia italiana non è al passo con la velocità delle immagini virali su Internet.**

I provvedimenti d'urgenza da lei richiesti non arriveranno in tempo per restituirle il suo – sacrosanto – **diritto all'oblio**.

Se da una parte la mancanza di misure di sicurezza tecnologiche per contrastare il problema evidenzia l'incapacità da parte dei gestori di social network e servizi di chat di affrontare la questione, dall'altra è altrettanto evidente il buco legislativo su queste tematiche.

IL VOYEURISMO NELL'ERA DI INTERNET

Se si pensa che contenuti di questo tipo si trovino solo negli angoli più nascosti della rete, ci si sbaglia di grosso. I casi di revenge porn e di voyeurismo sono infatti **all'ordine del giorno** tanto che oggi si assiste ad una vera e propria "normalizzazione" di questi fenomeni. Di foto "rubate" alle dirette interessate, e **il femminile non sembri casuale**, perché sono principalmente le donne a essere vittime di questo tipo di ricatti, sono pieni i **gruppi ristretti** su Facebook e WhatsApp, così come esistono spazi dedicati alla raccolta di immagini di questo tipo in forum e altre piattaforme di discussione molto frequentate.

UN ERRORE LINGUISTICO

Nel caso del Revenge Porn c'è un problema linguistico di partenza, che molto probabilmente ha a che fare con la difficoltà di stabilirne i limiti legali. Lo stesso termine con cui questa odiosa pratica è conosciuta, quello di Revenge Porn, appunto, è un'espressione imprecisa utilizzata per indicare **un atto di violenza grave**, una nomenclatura vaga che riduce la violazione di privacy di un individuo a una categoria di gusto paragonabile a quelle che si possono trovare navigando sui siti pornografici. Non è così ed è bene specificarlo. **Qualunque genere di pornografia implica soggetti consenzienti, professionisti o meno che siano e la necessità di trovare nomi più corretti non è una piccolezza.** È fondamentale per cambiare l'approccio di fronte a una tipologia di crimine dalle radici antiche, ma che ha trovato nuovi modi per ledere le sue vittime.

UNA NUOVA DEFINIZIONE: COSA SIGNIFICA NCII

In un recente annuncio reso pubblico da Facebook viene proposta una soluzione paradossale: che gli utenti condividano le proprie foto di nudo attraverso Messenger, in modo che il social network possa imparare a riconoscere i file ed evitarne così la diffusione non volontaria. In quello stesso annuncio, però, c'è un elemento interessante: l'introduzione del termine **NCII, acronimo che sta per non-consensual intimate imagery, letteralmente immagini intime non consensuali**, decisamente più adatto per descrivere il fenomeno di cui si parla. Riformulare la definizione di revenge porn in NCII permette infatti di includere nello stesso insieme anche il voyeurismo e gli spy shot – un sottogenere di voyeurismo che consiste nel pubblicare foto scattate di nascosto in bagni, camerini e simili –, che sono poi categorie diverse di abusi che però funzionano sistematicamente allo stesso modo.

COME E DOVE AVVIENE LA CONDIVISIONE

Nel caso di NCII ottenute da chat o videochat, la maggior parte delle vittime viene adescata nelle chat di incontri o nei social network tradizionali come Facebook. La fonte di fotografie "spy" invece è solitamente interna a gruppi che condividono le immagini e si sfidano a rubare scatti sempre più scabrosi. **È impossibile controllare la diffusione di questi gruppi**, presenti come chat di gruppo su WhatsApp e Messenger ma anche come veri e propri gruppi su Facebook o forum dedicati, **molti si presentano come forum di erotica per poi nascondere tra le proprie "stanze" una dedicata al voyeurismo e ad altre forme di foto intime rubate.**
Ci sono utenti che si specializzano, partendo da una singola foto, nel raccogliere, attraverso lavori maniacali di ricerca immagini inversa, archivi interi della stessa persona, il più delle volte inconsapevole dell'utilizzo che viene fatto delle immagini che la ritraggono. Altri si producono in vere e proprie recensioni sugli strumenti migliori per spiare i vicini o da installare in bagni pubblici. E ovviamente ci sono quelli che le foto le scattano in prima persona, e le condividono.

COSA DICE LA LEGGE

Tutelare le vittime di questo tipo di molestie è molto difficile, perché spesso sono consenzienti nel momento dello scatto o delle riprese, ma non al momento della diffusione. E questa è una differenza fondamentale, che spesso dà il via alla cosiddetta sextortion, il ricatto in cambio della non diffusione di scatti.
Secondo il codice penale (articoli 610 e 615 bis) **il voyeur può incorrere in due reati:**

- **la "violenza privata"**
- **la "interferenza illecita nella vita privata".**

Se non si tratta di immagini rubate in casa o in un luogo di proprietà ma dal web o da luoghi diversi da questo contesto, la vittima potrà fare ben poco. È il caso delle riprese rubate nei bagni pubblici, nelle palestre, nei camerini. I reati di questo tipo in Italia non sono puniti direttamente. **Chi diffonde foto sensibili sul web verrà processato a seconda dei casi per diffamazione, violazione della privacy, stalking, tentativo di estorsione, trattamento illecito dei dati.**
Il reato è disciplinato meglio in paesi come Germania, Regno Unito, Australia, Israele e in 34 Stati degli USA.

SCREENSHOT E VIDEO QUASI INCANCELLABILI

Cancellare quegli screenshot è spesso più facile a dirsi che a farsi - ormai tutti gli smartphone offrono servizi di backup delle foto via internet, anche gratuiti, come Apple e Google Photos, e spesso è possibile recuperare foto e screenshot da altri dispositivi loggandosi nell'account del proprio telefono. Per cui, anche nel caso si conosca la persona che ha rubato la foto è quasi impossibile assicurarsi che non sia in grado di ottenerne una copia in un secondo momento. Video intimi, anche live, hanno lo stesso problema: registrare lo schermo di un telefono oggi è facilissimo e molti di questi strumenti non causano segnalazioni all'utente dall'altro lato della conversazione.

COME PROTEGGERE I PROPRI DATI

Bisogna ricordare, infine, che tutti i servizi che mediano le nostre comunicazioni – sia i big come Facebook o quelli relativamente più piccoli come le app di incontri – fanno raccolta dati, e i loro livelli di sicurezza sono estremamente variabili. Tutti dovrebbero dotarsi di strumenti per proteggere almeno parte dei propri dati, conoscere bene licenza dei servizi che usano, e gestire le impostazioni della privacy del proprio telefono

COSA FARE SE QUALCUNO PUBBLICA LE TUE FOTO

La prima reazione è di rivolgersi alle **autorità**. Carabinieri e Polizia di Stato hanno apposite sezioni dedicate all'investigazione di questo tipo di violazione della privacy e per quanto, come nel triste caso di Tiziana Cantone, la legislazione in materia sia ancora in larga parte carente e/o lenta, **rimane fondamentale denunciare** chi diffonde foto private senza il consenso del diretto interessato. **È importante anche rilevare l'assenza di una vera e propria rete istituzionale che si occupi dell'argomento sia dal punto di vista dell'educazione – che è educazione sessuale e tecnologica allo stesso tempo – che da quello del supporto psicologico delle vittime.**

UN PROBLEMA IN ATTESA DI SOLUZIONE

Parte del problema deve essere affrontato anche dalle **aziende che gestiscono i servizi web**, sebbene la responsabilità centrale resti nelle mani dello Stato. È facile pensare che il problema delle immagini intime su Internet non ci riguardi, magari perché ci fidiamo del nostro partner, eppure da un sondaggio svolto da due università australiane è emerso un dato che dovrebbe farci riflettere: **una persona su cinque sa che proprie immagini intime sono state ricondivise su internet senza il proprio consenso.** Come a dire che ci stiamo abituando al problema invece di provare a risolverlo.

SEXTORTION

l'ultima trappola del web

Il termine "sextortion" è un neologismo che nasce dalla crasi tra le parole "**sexual**" ed "**extortion**" con cui si identifica un particolare illecito che si sta largamente diffondendo tramite i vari social network e siti di incontri presenti sul web.

La condotta incriminata si scandisce, come da copione, in tre fasi:

1. Una persona particolarmente avvenente aggancia la sua vittima in chat **fingendosi molto interessata** e disposta ad intrattenere una relazione con uno sconosciuto, giustificando tale interesse con le motivazioni più disparate, come la voglia di riscattarsi da una delusione amorosa, fare un dispetto al proprio ex o una particolare voglia di trasgressione
2. Una volta che è stata carpita la fiducia del malcapitato, viene lanciata la proposta di spogliarsi davanti alla webcam o **scambiarsi foto "hot"**
3. Se la vittima acconsente, viene subito ricattata con la **minaccia di diffondere tali immagini** qualora non venga pagata una consistente somma di denaro.

Il reato che viene integrato in questo modo è evidentemente quello di "estorsione", severamente punito dall'articolo 629 del nostro codice penale con una pena compresa tra cinque e venti anni di reclusione.

Nel caso in cui la vittima decida di non sottostare al ricatto, il reato sussisterà comunque, anche se nella forma del cosiddetto "**tentativo**", sanzionato con una pena diminuita da un terzo a due terzi.

Gravitano intorno al concetto di "sextortion" anche quelle varianti del reato in cui viene richiesto alla vittima di inviare, al posto di una somma di denaro, **altre immagini dal contenuto erotico** oppure di **compiere gesti di autoerotismo davanti alla webcam**.

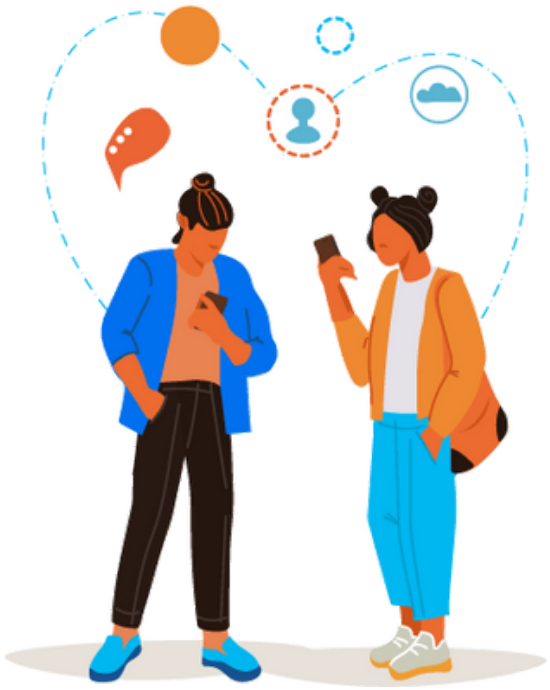
Occorre specificare che, **nel primo caso**, verrà integrato il reato di **"violenza privata"**, che consiste nell'obbligare una persona, dietro minaccia o violenza, a fare o non fare qualcosa, mentre **nel caso della costrizione** alla masturbazione, si versa nell'ipotesi, decisamente più grave, di **"violenza sessuale"**.

Per i nostri lettori che dovessero dubitare dell'esistenza del reato di violenza sessuale in assenza di un contatto fisico, si segnala che secondo il più recente orientamento della Corte di Cassazione sussiste questo reato quando "pur in mancanza di contatto fisico tra imputato e persona offesa, la condotta tenuta denoti il requisito soggettivo dell'intenzione di raggiungere l'appagamento dei propri istinti sessuali e quello oggettivo della idoneità a violare la libertà di autodeterminazione della vittima nella sfera sessuale".

VIOLENZA E SOCIAL NETWORK

Quando la rete si scatena contro... le donne

Nell'era del web, la violenza come è noto corre anche in rete e le donne sono le principali vittime del **"discorso d'odio" online**, come dimostrato dal fenomeno degli haters scatenati in gruppi chiusi di Facebook, dove spesso si registrano **insulti sessisti e volgari** o da altri continui esempi.



Nel maggio del 2016, è stata istituita alla Camera dei deputati la **Commissione sull'intolleranza, la xenofobia, il razzismo e i fenomeni di odio**, intitolata alla memoria della parlamentare inglese **Jo Cox**, uccisa prima di un comizio elettorale per le sue posizioni a favore della permanenza del Regno Unito nell'Unione europea.

La relazione finale redatta dalla Commissione Jo Cox si è concentrata anche sul tema della **violenza di genere** e ha messo in evidenza come questo tipo di violenza abbia una **matrice culturale fortissima**, che nasce innanzitutto dalla convinzione di "debolezza e inferiorità" femminile.

Nel documento conclusivo si legge:

> **"Le manifestazioni di odio nei confronti delle donne si esprimono nella forma del disprezzo, della degradazione e spersonalizzazione, per lo più con connotati sessuali"**

Mappe dell'Intolleranza
Progetto curato da VOX

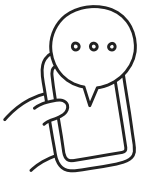
Il progetto delle "Mappe dell'Intolleranza" curato dall'Osservatorio Italiano sui Diritti "Vox", attraverso Twitter, è riuscito a geolocalizzare le zone dove razzismo, odio verso le donne, omofobia e discriminazione verso le persone diversamente abili, sono maggiormente diffusi.

Uno dei social più attivi nel condividere l'odio verso le donne è Twitter, con oltre 1 miliardo di tweet sessisti rilevati (su un campione di oltre 2 miliardi complessivi).

Secondo la **ricerca sulla misoginia** condotta da Vox, i tweet contro le donne sono i più numerosi. Si twitta l'odio in tutta Italia: Milano, insieme a Roma, sono le città più intolleranti (rispettivamente con 8.134 e 8.361 tweet contro le donne).

La diffusione dei social media sembra alimentare anche un bisogno di **visibilità sociale**: postare o condividere immagini e contenuti, anche personali e intimi, cercare consensi (like) e via dicendo. Questi comportamenti costituiscono esempi di un **«esibizionismo mediatico»** che spinge adulti e minori a atteggiamenti disinvolti, disinibiti, spesso incuranti degli effetti reali delle condotte online.

Secondo un'indagine dell'Osservatorio Nazionale Adolescenza del 2016, su un campione di oltre 7.000 adolescenti italiani il 4% dichiara di aver inviato - attraverso Instagram o Facebook - foto e video di se stesso in atteggiamenti sessuali attraverso i canali social e il 10%, tra cui anche ragazzi non ancora adolescenti, ha scattato selfie intimi. **In questo contesto, è facile immaginare che si possa cadere in trappole come grooming, sexting e revenge porn.**



Diamo una definizione
Cos'è il Grooming?

«**Il grooming**, ad esempio, si verifica quando **gli adulti**, per mezzo delle tecnologie di comunicazione e di informazione, **propongono intenzionalmente ai minori**, con condotte insidiose, ingannatorie o minacciose, volte a carpirne la fiducia, degli **incontri con lo scopo di commettere atti sessuali o a carattere pornografico**.

La pratica del **sexting**, sempre più diffusa anche tra i minori e con risvolti giurisprudenziali contrastanti, consiste nell'invio di immagini connotate sessualmente con il mezzo del cellulare o via Internet. La pubblicazione di foto o video intimi e pedopornografici sul web, posta in essere generalmente dopo la fine di una relazione sentimentale o affettiva, a scopo di **vendetta** (revenge porn), vede colpite soprattutto ragazze per mano dei loro ex partner.

Per tutelarli il **legislatore ha previsto strumenti penali repressivi**, all'interno del codice penale, potenziati anche da riforme recenti, che vanno a rafforzare le strategie di protezione di natura preventiva ed educativa».

L'obiettivo da raggiungere è quello di rendere la rete e i social network un luogo aggregativo e di confronto positivo.

In questo scenario, **il ruolo dell'informazione** tra cui giornali, telegiornali, programmi d'informazione tramite stampa, tv e web continua a rimanere CENTRALE nell'influenzare la percezione di un problema e nel creare o meno distorsioni nell'immaginario collettivo. **È opportuno, ad esempio, evitare di riferirsi alle donne come "soggetti deboli" o vittime predestinate.**

Mettere in sicurezza i social

I social network sono diventati **parte integrante** della nostra vita quotidiana, ma purtroppo possono anche rappresentare un rischio per la nostra sicurezza.

È importante **sentirsi sicuri sui social** e conoscere le **precauzioni** da prendere per proteggere la propria **privacy** e le proprie **informazioni personali**.

In questo paragrafo, esploreremo alcune delle strategie più efficaci per garantire la propria sicurezza sui social network.

Mettere in sicurezza Facebook

ASPETTI DI SICUREZZA NELLA CREAZIONE DI UN ACCOUNT

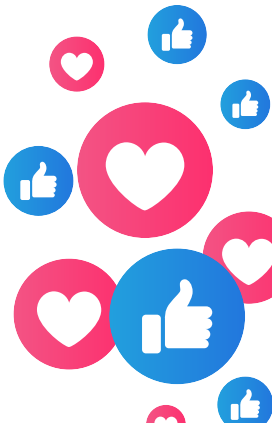
Nella creazione di un account Facebook occorre prestare attenzione a questi aspetti:

- **utilizzare un nome utente reale** (utilizzare un nome utente falso va contro il regolamento di fb);
- **registrarsi con una email funzionante e sicura** (non utilizzare email temporanee poiché non si potrebbe avere più accesso qualora facebook dovesse inviarci un messaggio per questioni di sicurezza nelle quali siamo informati che il nostro account è stato violato)
- **inserire una password sicura** (password poco sicure sono quelle inferiori agli 8 caratteri, non alfanumeriche. Una buona password dovrebbe essere composta da numeri e lettere, meglio se minuscole e maiuscole insieme);
- **associare il numero di cellulare al proprio account e attivare la verifica in due passaggi**: https://www.facebook.com/settings?tab=security&section=approvals&view
- **configurare una buona domanda e risposta di sicurezza** https://www.facebook.com/update_security_info.php visto che può essere utilizzato come metodo per ottenere accesso all'account.

ASPETTI DI SICUREZZA DOPO LA CREAZIONE DI UN ACCOUNT

Una volta creato l'account facebook per metterlo in massima sicurezza come consigliato dal Facebook security center https://www.facebook.com/help/security/security_features procedere come segue:

- come prima cosa se stiamo verificando le nostre impostazioni di sicurezza facebook per un account già creato nel passato, è bene disconnettere i dispositivi non utilizzati. Alla pagina https://www.facebook.com/settings?tab=security nella sezione "DOVE HAI EFFETTUATO L'ACCESSO", fare click su dispositivi da cui hai effettuato l'accesso poi individuare la sessione che desideriamo terminare e cliccare su Termina attività.
- impostare la sicurezza per venir avvisati degli accessi all'account facebook tramite questa pagina https://www.facebook.com/settings?tab=security nella sezione "CONFIGURAZIONE DI UN'ULTERIORE SICUREZZA" impostare a "SI" la domanda Ricevi avvisi sugli accessi non riconosciuti.
- scegliere l'autenticazione a due fattori, sempre allo stesso link: https://www.facebook.com/settings?tab=security nella sezione "Configurazione di un'ulteriore sicurezza" per accedere con un codice dal tuo cellulare e una password.
- scegliere gli amici da contattare se non riusciamo ad accedere all'account, sempre allo stesso link https://www.facebook.com/settings?tab=security nella sezione "Configurazione di un'ulteriore sicurezza" alla voce "Scegli da 3 a 5 amici da contattare se non riesci più ad accedere al tuo account", in modo che i tuoi contatti fidati possano inviare un codice e un URL da Facebook per consentirti di accedere di nuovo.
- controllare regolarmente tutte le applicazioni che vengono aggiunte al nostro account facebook tramite questo link https://www.facebook.com/settings?tab=applications, rimuovendo le applicazioni non riconosciute.
- bloccare gli utenti e messaggi che ci disturbano: https://www.facebook.com/settings?tab=blocking
- Sempre al link https://www.facebook.com/settings?tab=security&section=public_key&view è possibile stabilire una chiave pubblica per crittografare i messaggi email di notifica che ti invia facebook.
- decidere cosa deve essere fatto del tuo account se rimane inattivo o in caso di incidente e decesso https://www.facebook.com/help/1568013990080948?helpref=faq_content
- sempre nel setting alla voce DIARIO E AGGIUNTA DI TAG https://www.facebook.com/settings?tab=timeline impostare come segue : Chi può scrivere nel tuo diario : Solo io ; --> Chi può vedere cosa pubblicano gli altri sul tuo diario ? : Solo Io ; Chi può vedere i post in cui ti hanno taggato nel tuo diario? : Solo Io ; --> Quando ti taggano in un post, quali persone vuoi aggiungere al pubblico del post se non possono già vederlo? : Solo Io; --> Vuoi controllare i post in cui ti taggano prima che il post sia visualizzato sul tuo diario?: Si; --> Vuoi controllare i tag che le persone aggiungono ai tuoi post prima che i tag siano visualizzati su Facebook? Si



ASPETTI RELATIVI ALLA PRIVACY

Le impostazioni relative alla Privacy vanno configurate a questa pagina https://www.facebook.com/settings?tab=privacy nella quale è possibile decidere:

- Chi può vedere i nostri post e la nostra lista di amici. Il massimo livello di sicurezza è "SOLOIO" che significa che i vostri amici non saranno più visibili agli altri. Un buon livello di sicurezza se hai pochi amici è selezionare "AMICI", mentre se ne hai molti allora seleziona "AMICI SPECIFICI". Logicamente queste scelte vengono compiute qualora vi siano delle valide ragioni come ad esempio se siete stati vittima di una sex extorsion e dovete proteggere il vostro account.
- Come controllare tutti i post in cui sei taggato, opzione che deve mostrare "USAIL REGISTRO ATTIVITA"
- Come restringere il pubblico per i vecchi post sul tuo diario se sarà impostato su "SOLO VECCHI POST" (opzione che va confermata con un click)
- Chi può contattarmi. Il massimo livello di sicurezza è "AMICI DI AMICI"
- Chi può cercarmi. Per la ricerca tramite indirizzo email il massimo livello di sicurezza è "AMICI", stessa cosa per il numero di telefono e la scelta per il reinderizzamento del profilo va impostata su "NO", per impedire che i motori di ricerca reindirizzino al nostro profilo.
- Cosa accade alle persone che ci seguono. Unico punto non gestito dal link sopra indicato sono le impostazioni relative alle persone che ci seguono accessibili qui:: https://www.facebook.com/settings?tab=followers e per i massimi livelli di sicurezza accertarsi che l'opzione rechi la scritta "AMICI"

ASPETTI DI SICUREZZA PER VERIFICARE CHE UN MESSAGGIO DI SICUREZZA PROVENGA REALMENTE DA FACEBOOK

Avete ricevuto un avviso di sicurezza da Facebook e non sapete se è reale?
Bene, andate a questo indirizzo e controllare gli ultimi messaggi che facebook vi ha inviato con sicurezza:
https://www.facebook.com/settings?tab=security&section=recent_emails&view.

ASPETTI DI SICUREZZA PER VERIFICARE I CONTENUTI CHE HAI CONDIVISO SU FACEBOOK

È possibile ottenere una copia dei contenuti che hai condiviso su facebook tramite questo link "SCARICA UNA COPIA DEI TUOI DATI FACEBOOK" che si trova al terminedella pagina https://www.facebook.com/settings?tab=account

Mettere in sicurezza
GOOGLE PLUS O GOOGLE +

ASPETTI DI SICUREZZA NELLA CREAZIONE DI UN ACCOUNT

Nella creazione di un account Google occorre prestare attenzione a questi aspetti:

- Utilizzare un **nome utente reale** (utilizzare un nome utente falso va contro il regolamento di Google)
- Registrarsi con una **email funzionante e sicura** (non utilizzare email temporanee poiché non si potrebbe avere più accesso qualora Google dovesse inviarci un messaggio per questioni di sicurezza nelle quali siamo informati che il nostro account è stato violato)
- Inserire una **password sicura** (password poco sicure sono quelle inferiori agli 8 caratteri, non alfanumeriche. Una buona password dovrebbe essere composta da numeri e lettere, meglio se minuscole e maiuscole insieme)
- Attivare la **verifica in due passaggi**: https://myaccount.google.com/signinoptions/two-step- verification
- Configurare le opzioni di recupero:

per email di recupero https://myaccount.google.com/signinoptions/rescueemail
per telefono di recupero https://myaccount.google.com/signinoptions/rescuephone

ASPETTI DI SICUREZZA DOPO LA CREAZIONEDELL'ACCOUNT

Una volta creato l'account Google per metterlo in massima sicurezza come consigliato dal GOOGLE security center https://myaccount.google.com/security procedere come segue:

- Come prima effettuare un controllo sicurezza automatico, premendo su INIZIA alla voce Controllo di Sicurezza mostrata a questa pagina https://myaccount.google.com

- Scegliere l'autenticazione a due fattori https://myaccount.google.com/signinoptions/two-step-verification per accedere con un codice dal tuo cellulare e una password.

- Modificare la visibilità delle nostre informazioni https://aboutme.google.com/. Fare attenzione al fatto che vi siano dei Lucchetti accanto alle informazioni che non vogliamo siano pubbliche

- Gestire le impostazioni di Google plus o Google + https://plus.google.com/settings per ottenere il massimo livello di sicurezza. Se abbiamo bisogno di non essere raggiunti da nessuno per proteggere il nostro account, come nel caso di una **sex estorsion** allora impostare alla voce "CHI PUO' INVIRTI NOTIFICHE?" selezionare l'opzione "SOLO TU", stessa cosa per "CHI PUO' COMMENTARE I TUOI POST PUBBLICI" e "CHI PUO' VEDERE LE TUE ATTIVITA'. Nella sezione successiva FOTO E VIDEO nulla deve essere abilitato. Nella sezione PROFILO disabilitare nuovamente ogni voce

- Controllare regolarmente il registro attività dei like https://plus.google.com/apps/activities il fatto che non siano attive condivisioni della posizione https://myaccount.google.com/locationsharing tutte le applicazioni che vengono aggiunte al nostro account tramite questo link https://myaccount.google.com/security#connectedapps rimuovendo le applicazioni non riconosciute qui https://myaccount.google.com/permissions

- Bloccare un utente non gradito https://support.google.com/plus/answer/6320399 e verificare che sia presente nella lista degli utenti bloccati https://plus.google.com/apps/activities/blocked_users e https://myaccount.google.com/blocklist

- Decidere cosa deve essere fatto del tuo account se rimane inattivo o in caso di incidente e decesso https://myaccount.google.com/inactive

ASPETTI DI SICUREZZA DOPO LA CREAZIONE DELL'ACCOUNT

Una volta creato l'account Google per metterlo in massima sicurezza come consigliato dal GOOGLE security center https://myaccount.google.com/security procedere come segue:

- Come prima effettuare un controllo sicurezza automatico, premendo su INIZIA alla voce Controllo di Sicurezza mostrata a questa pagina https://myaccount.google.com

- Scegliere l'autenticazione a due fattori https://myaccount.google.com/signinoptions/two-step-verification per accedere con un codice dal tuo cellulare e una password.

- Modificare la visibilità delle nostre informazioni https://aboutme.google.com/. Fare attenzione al fatto che vi siano dei Lucchetti accanto alle informazioni che non vogliamo siano pubbliche

- Gestire le impostazioni di Google plus o Google + https://plus.google.com/settings per ottenere il massimo livello di sicurezza. Se abbiamo bisogno di non essere raggiunti da nessuno per proteggere il nostro account, come nel caso di una **sex estorsion** allora impostare alla voce "CHI PUO' INVIRTI NOTIFICHE?" selezionare l'opzione "SOLO TU", stessa cosa per "CHI PUO' COMMENTARE I TUOI POST PUBBLICI" e "CHI PUO' VEDERE LE TUE ATTIVITA'. Nella sezione successiva FOTO E VIDEO nulla deve essere abilitato. Nella sezione PROFILO disabilitare nuovamente ogni voce

- Controllare regolarmente il registro attività dei like https://plus.google.com/apps/activities il fatto che non siano attive condivisioni della posizione https://myaccount.google.com/locationsharing tutte le applicazioni che vengono aggiunte al nostro account tramite questo link https://myaccount.google.com/security#connectedapps rimuovendo le applicazioni non riconosciute qui https://myaccount.google.com/permissions

- Bloccare un utente non gradito https://support.google.com/plus/answer/6320399 e verificare che sia presente nella lista degli utenti bloccati https://plus.google.com/apps/activities/blocked_users e https://myaccount.google.com/blocklist

- Decidere cosa deve essere fatto del tuo account se rimane inattivo o in caso di incidente e decesso https://myaccount.google.com/inactive

ASPETTI DI SICUREZZA DOPO LA CREAZIONEDELL'ACCOUNT

Le impostazioni relative alla Privacy vanno configurate a questa pagina https://plus.google.com/settings nella quale è possibile cancellare la cronologia delle ricerche e gestire le attività su google https://myaccount.google.com/privacy#accounthistory

ASPETTI DI SICUREZZA PER VERIFICARE CHE UN MESSAGGIO DI SICUREZZA PROVENGA REALMENTE DA GOOGLE

Avete ricevuto un avviso di sicurezza da Google e non sapete se è reale?
Bene, andate a questo indirizzo e controllare eventuali avvisi di sicurezza: https://myaccount.google.com/security#activity

ASPETTI DI SICUREZZA PER VERIFICARE I CONTENUTI CHE HAI CONDIVISO SU GOOGLE

È possibile ottenere una copia dei contenuti che hai condiviso su Google tramite questo link https://takeout.google.com/settings/takeout?pli=1

Mettere in sicurezza skype

ASPETTI DI SICUREZZA SKYPE

Entrare nel proprio account skype tramite web https://secure.skype.com/portal/overview e controllare:

- Nella sezione RECAPITI la presenza di un numero di telefono nel profilo https://secure.skype.com/portal/profile
- Nella sezione IMPOSTAZIONI DEL PROFILO se non si desidera essere più individuati dagli utenti deselezionare "individuabilità". In questo modo non potrete più essere trovati ed aggiunti su skype
- Per bloccare un contatto In Skype, nella scheda Contatti, fai clic con il pulsante destro del mouse sul contatto che desideri bloccare e seleziona Blocca questo utente.... mentre per segnalare un contatto fastidioso a Skype, seleziona Riporta un abuso. Approfondimenti qui

Mettere in sicurezza Instagram

ASPETTI DI SICUREZZA NELLA CREAZIONE DI UN ACCOUNT INSTAGRAM

Nella creazione di un account Instagram occorre prestare attenzione a queste impostazioni:

- Nella gestione delle impostazioni account alla pagina https://www.instagram.com/accounts/edit/ selezionare "PRIVATE ACCOUNT" per garantirvi che solo le persone che voi approverete potranno vedere il vostro profilo
- Nella sezione AUTHORIZED APPLICATIONS a questa pagina https://www.instagram.com/accounts/manage_access/ controllare che non vi siano applicazioni non desiderate che possano gestire il vostro account. inoltre verificare se il vostro account Instagram risulta collegato a Facebook https://www.facebook.com/help/instagram/176235449218188?helpref=hc_fnav
- Nella gestione delle notifiche a pagina https://www.instagram.com/emails/settings/ assicurarsi che siano selezionate tutte le voci
- Abilitiamo l'autenticazione a due fattori come mostrato in questa guida https://www.facebook.com/help/instagram/566810106808145
- Verifichiamo chi abbiamo bloccato su Instagram o segnaliamo un molestatore https://help.instagram.com/426700567389543?helpref=faq_content

Mettere in sicurezza Pinterest

ASPETTI DI SICUREZZA NELLA CREAZIONE DI UN ACCOUNT PINTEREST

Sicurezza dell'account pinterest
https://help.pinterest.com/it/articles/account-security-and-hacked-accounts
Autenticazione a due fattori pinterest
https://help.pinterest.com/it/articles/two-factor- authentication
Modifica impostazioni account pinterest
https://help.pinterest.com/it/articles/edit- your-setting
Proteggere l'account pinteest
https://help.pinterest.com/it/articles/protecting-your- account

Mettere in sicurezza LINKEDin

ASPETTI DI SICUREZZA NELLA CREAZIONE DI UN ACCOUNT LINKEDIN

Nella creazione di un account linkedin occorre presare attenzione a queste impostazioni:

- Controlliamo i dati presenti nel nostro profilo pubblico https://www.linkedin.com/public- profile/settings
- Nella gestione delle impostazioni account alla pagina https://www.linkedin.com/psettings/ aggiungiamo un numero di telefono
- Controlliamo con regolarità dove viene eseguito l'accesso al nostro profilo https://www.linkedin.com/psettings/sessions
- Decidiamo se vogliamo che gli altri vedano che abbiamo visitato il loro profilo https://www.linkedin.com/psettings/profile-visibility
- Verifichiamo i servizi consentiti che abbiamo autorizzato https://www.linkedin.com/psettings/permitted-services
- Scegliamo chi può seguirci su linkedin https://www.linkedin.com/psettings/allow-follow
- Controlliamo gli utenti bloccati su linkedin https://www.linkedin.com/psettings/member- blocking
- Decidiamo chi può trovare il nostro profilo tramite email https://www.linkedin.com/psettings/visibility/email
- Decidiamo chi può trovare il nostro profilo tramite telefono https://www.linkedin.com/psettings/visibility/phone

ASPETTI DI SICUREZZA PER VERIFICARE I CONTENUTI CHE HAI CONDIVISO SU LINKEDIN
E' possibile ottenere una copia dei contenuti che hai condiviso su linkedin tramite questo link https://www.linkedin.com/psettings/member-data

Mettere in sicurezza TRIPADVISOR

ASPETTI DI SICUREZZA TRIPADVISOR

Modifica del profilo e controllo se facebook è collegato al profilo di tripadvisor https://www.tripadvisor.it/Settings-a_ame.true oppure google+ https://www.tripadvisor.it/Settings-cpf
Informazioni sull'account tripadvisor https://www.tripadvisor.it/Settings-cp Informazioni per la privacy tripadvisor https://www.tripadvisor.it/Settings-cs

Mettere in sicurezza SPOTIFY

ASPETTI DI SICUREZZA SPOTIFY

Proteggi il tuo account spotify
https://support.spotify.com/it/account_payment_help/privacy/protect- your-spotify-account/
Cosa fare per email sospette inviate da spotify
https://support.spotify.com/it/account_payment_help/privacy/suspicious-email/
Revoca gli accessi ad app esterne https://www.spotify.com/account/apps/

Mettere in sicurezza TWITTER

ASPETTI DI SICUREZZA TWITTER

Nella creazione di un account twitter occorre presare attenzione a queste impostazioni:

- Nella gestione del profilo https://twitter.com/settings/account controllare di aver eseguito la verifica dell'accesso nella sezione SICUREZZA e di aver selezionato la casella "Richiedi informazioni personali per reimpostare la password"
- Nella sezione delle notifiche https://twitter.com/settings/notifications controllare di aver selezionato tutti gli aggiornamenti nella sezione AGGIORNAMENTI DA TWITTER
- Controllare gli account silenziati https://twitter.com/settings/muted_following e quelli bloccati https://twitter.com/settings/blocked
- Verificare le applicazioni autorizzate ad accedere all'account https://twitter.com/settings/applications
- Esaminare i dati personali che twitter ha di noi https://twitter.com/settings/your_twitter_data
- Riferirsi alla guida di twitter per la gestione della privacy https://help.twitter.com/it/safety-and- security#ads-and-data-privacy

ASPETTI DI SICUREZZA PER VERIFICARE I CONTENUTI CHE HAI CONDIVISO SU TWITTER
E' possibile ottenere una copia dei contenuti che hai condiviso su twitter tramite questo link https://twitter.com/settings/account nella sezione ARCHIVIO TWITTER

Biblioteca

Consigli su alcune letture sull'utilizzo dei social network.

Cybersecurity, digital forensics e data protection. Responsabilità delle organizzazioni, le prove digitali e il fattore umano

Vivendo nella società digitale non possiamo esimerci dal conoscere i benefici e i rischi connessi alla rete. Da una parte, si rende necessario conoscere i nostri diritti e le libertà fondamentali, anche per evitare i rischi inerenti alla diffusione dei nostri dati personali. La crescita vertiginosa di crimini informatici, compiuti anche sfruttando le vulnerabilità del fattore umano, apre ad importanti interrogativi in termini di responsabilità e di tutela, che trovano una puntuale risposta in questo volume. Dall'altra parte, il testo affronta le diverse tematiche con la consapevolezza che, di fronte ad uno scenario digitale in continua evoluzione, sono necessarie competenze multidisciplinari, da quelle tecniche e legali a quelle psicologiche e sociali. Occorre pertanto accrescere tutte quelle conoscenze utili a identificare e contrastare efficacemente i rischi inerenti la cybersecurity in ambito pubblico e privato. Tale obiettivo può essere raggiunto

Sociologia dei new media

Questo libro adotta una prospettiva che mette in relazione la novità dei new media con i rapporti di debito e credito che essi continuano a intrattenere con la cultura di massa e con i media tradizionali. L'obiettivo è di descrivere l'insieme delle trasformazioni introdotte dai new media e riguardanti sia l'agire collettivo (il modo in cui organizzazioni e istituzioni incorporano le nuove tecnologie e vi si adattano), sia l'agire individuale (attraverso il mutare delle relazioni tra persone reso possibile dai nuovi media o anche dal connubio essere umano-macchina che si fa sempre più stringente e interconnesso). Al lettore vengono presentati i temi centrali per comprendere tutto ciò: gli autori affrontano il digital divide e la dimensione politica, la costruzione dell'identità e la gestione della socialità, e propongono infine un'utile parte metodologica su come è possibile fare ricerca sociale nel mondo digitale. Il testo è accompagnato da una ricca strumentazione didattica orientata allo studente e volta a stimolarne la curiosità e l'interesse critico.

La società dell'incertezza

Nel nostro mondo postmoderno non c'è posto per la stabilità e la durata, l'apparenza prevale sulla sostanza, il tempo si frammenta in episodi, la salute diventa fitness, la massima espressione di libertà è lo zapping. Dalle macerie del vecchio ordine politico bipolare sembra emergere solo un nuovo disordine globale. Le figure emblematiche che abitano questo traballante universo sono il giocatore (in borsa o alla lotteria) e il turista, lo sradicato e il "collezionista di sensazioni". Ma forse, più di ogni altro, lo straniero. Per impedire che l'individuo diventi presto straniero anche a se stesso, è giunto forse il momento di guardare a nuove strategie di vita.

La solitudine del cittadino globale

Alle glorie della nuova era globale si contrappone la solitudine dell'uomo comune: la socialità è incerta, confusa, sfocata. Si scarica in esplosioni sporadiche e spettacolari per poi ripiegarsi esaurita su se stessa. Per porre un freno a questo processo occorre ritrovare lo spazio in cui pubblico e privato si connettono: l'antica agorà, in cui la libertà individuale può diventare impegno collettivo. Postfazione di Alessandro Dal Lago

Non aver paura di chiedere aiuto.

Meriti di vivere una vita libera dalla violenza.

Fondazione Città Solidale onlus

Centro Antiviolenza
"Centro Aiuto Donna"
FONDAZIONE CITTÀ SOLIDALE ONLUS