



Co-funded by the
Erasmus+ Programme
of the European Union

CYBER 
VIOLENCE

MANUALE

PER GLI EDUCATORI, FORMATORI E INSEGNANTI CHE LAVORANO CON I GIOVANI SULLA CYBERVIOLENCE





Co-funded by the
Erasmus+ Programme
of the European Union

CYBER 
VIOLENCE

Settembre 2018

Questo manuale è disponibile in 5 lingue: inglese, polacco, greco, rumeno e italiano e liberamente accessibile sul sito web del progetto: www.cyberviolence.eu

È possibile essere aggiornati sull'attività del progetto anche seguendo le nostre pagine Facebook, disponibili in 5 lingue.

Il progetto CyberViolence 2016-03-PL01-KA205-035361 è parte del programma Erasmus + dell'Unione europea (Azione 2. Cooperazione per l'innovazione e scambio di buone pratiche, partenariati strategici). Il progetto ha una durata di 24 mesi nel periodo aprile 2017 - marzo 2019.



Indice

Informazioni sul progetto.....	4
Modulo 1: Concetto di cyberviolence	6
Cyberbullismo – una nuova forma di bullismo.....	6
Forme di cyberbullismo.....	9
Programmi anti bullismo per fermare la violenza.....	11
Raccomandazioni:	14
Modulo 2: Cyberbullismo e social media	15
I social media.....	15
Bullismo vs Cyberbullismo: una definizione.....	18
Le forme del cyberbullismo.....	19
Gergo utile da sapere	20
Modulo 3: Identità offline e online, profilazione e tracciamento web:	22
Essere al sicuro sul web.....	22
Identità	22
Aspetti generali sull'identità offline	22
Profilazione.....	24
Tracciamento web.....	25
Cosa viene raccolto attraverso il monitoraggio web e perché?.....	26
Rilevamento della posizione.....	26
Raccomandazioni	27
Raccomandazioni per la privacy dei dati.....	27
Consigli pratici	28
Come proteggere la tua identità online	28
Come ci rintracciano su Internet	30
How to protect ourselves from web tracking	31
Migliori pratiche	31
Modulo 4: Lavorare con i giovani.....	32
Una breve descrizione della gioventù come gruppo sociale.....	32
Regole per lavorare con i giovani.....	32
Motivazione interna	33
Apprendimento cooperativo.....	33
Pianificazione della formazione per i giovani.....	34
Diagnosi	34
La parte iniziale della formazione	35
La parte rilevante della formazione	36
Scopo della formazione e valutazione.....	36
Riferimenti.....	37



Informazioni sul progetto

CyberViolence è un progetto contro la violenza in Internet.

L'Institute of New Technologies Association insieme a tre partner europei ha realizzato il progetto internazionale CyberViolence come parte del programma Erasmus +.

Il problema principale della cyberviolence è la mancanza di conoscenza e consapevolezza del problema del cyberbullismo tra i giovani, gli operatori giovanili, gli insegnanti e i genitori. Per i giovani, il problema è la mancanza di consapevolezza delle minacce online, la mancanza di opportunità e la capacità di rispondere al cyberbullismo. Per i formatori e insegnanti il problema è la mancanza di strumenti e metodologie per lavorare su questo argomento, la mancanza di educazione e di prevenzione. Per i genitori, non c'è consapevolezza del problema e della capacità di riconoscere i primi sintomi del cyberbullismo. Tra i gruppi di riferimento ci sono:

- **Giovani** – il principale gruppo target delle nostre attività. I giovani sono i più vulnerabili ad essere vittime del cyber bullismo poiché sono vulnerabili e inesperti nella vita sociale;
- **Insegnanti, operatori giovanili** – il loro ruolo è educare e prevenire questo fenomeno negativo. Hanno bisogno di nuovi strumenti per sapere come combattere la cyber violence tra gli studenti;
- **I genitori** – quando il loro figlio è vittima del cyberbullismo, dovrebbero essere i primi a riconoscere i sintomi, ma sfortunatamente spesso mancano delle conoscenze di base in questo argomento.

Il progetto ha alcuni obiettivi principali, tra cui:

1. Migliorare la qualità e l'importanza dell'istruzione, attraverso lo sviluppo di approcci nuovi e innovativi (nuovi scenari per workshop, fumetti tematici, concorsi, test di prodotti, attuazione e promozione della diffusione dei risultati);
2. Sviluppare un programma per prevenire il cyberbullismo, sviluppando e fornendo un manuale e altre risorse per gli insegnanti;
3. Aumentare la conoscenza delle minacce online, le conseguenze delle attività online e gli aspetti emotivi del cyberbullismo;
4. Introduzione, sviluppo e promozione di metodi e strumenti innovativi nell'istruzione sostenendo scuole e insegnanti interessati ad aderire al programma;

Promuovere la cooperazione transfrontaliera nell'istruzione e nella prevenzione, poiché tutti i partecipanti al progetto possono imparare gli uni dagli altri.

Il progetto è realizzato da 4 organizzazioni di 4 paesi e ha un carattere transnazionale, poiché Internet non ha confini e la cyberviolence è un problema internazionale che deve essere risolto a livello internazionale:

- Institute of New Technologies Association (Poland) – leader of the project
- Crystal Clear Soft (Greece) – partner,
- DIRECT Association (Romania) – partner,
- CSP – INNOVAZIONE NELLE ICT S.C.A.R.L. (Italy) – partner



Informazioni sul manuale

Questo manuale è un documento importante per tutti gli animatori e gli animatori giovanili, nonché le ONG interessate, i responsabili di attività e i cittadini, che hanno familiarità con i modi e gli obiettivi dell'utilizzo di strumenti pedagogici per fermare la cyber violence, promuovere l'educazione e le competenze non formali e competenze che in questo caso gestiscono la pianificazione degli obiettivi e l'inclusione, l'empatia, la necessità di cooperare, il riconoscimento dei diritti umani, la promozione di differenze e valori universali di tolleranza oltre a risolvere i conflitti attraverso la comunicazione e il controllo dei conflitti. Durante il progetto, i partecipanti adotteranno nuove competenze relative al dialogo sociale e alla cooperazione.

Il numero di manuali sull'apprendimento non formale incentrati sullo stop alla cyber violence è limitato e insufficiente. La mancanza di un adeguato quadro formativo (nell'educazione formale) per gli animatori giovanili porta all'uso inefficiente della capacità dei professionisti che lavorano in questo ambito. Questo manuale colma una delle lacune nel settore giovanile, vale a dire la necessità di metodologie per la formazione di formatori in grado di istruire i giovani lavoratori.

I moduli del manuale sono elaborati in modo tale che gli operatori giovanili, i formatori e gli insegnanti che lavorano con i giovani acquisiscano tutte le conoscenze e le abilità necessarie per prevenire e fermare la cyber violence in modo che i workshop possano essere utilizzati in ulteriori lavori per il benessere delle loro organizzazioni, della comunità locale e oltre.

Speriamo che questo manuale sia utilizzato da giovani lavoratori e giovani leader per diffondere le idee del progetto utilizzando i metodi e il contenuto del manuale. Seguendo le priorità e gli obiettivi del programma Erasmus + e dei partner del progetto, questo manuale sarà uno strumento utile sulla prevenzione della cyber violence, per la partecipazione attiva dei giovani al fine di trovare soluzioni pratiche e sostenibili per fermare il fenomeno della cyber violence.



Modulo 1: Concetto di cyberviolence

Questo modulo offre una panoramica del concetto di Cyber Violence, i tipi di bullismo riferiti all'età, metodi, canali in cui vengono avvicinati, reazioni, esempi teorici di situazioni di cyberbullismo che possono interessare i giovani con la descrizione appropriata sulla modalità per affrontarli.

Verrà presentato uno schema operativo, per affrontare situazioni difficili, soluzioni/rimedi/ risposte, come prevenire, come reagire, come difendersi, il sostegno da parte delle persone più vicine (familiari e amici) e dell'ambiente, approccio sociale, i media, l'opinione pubblica e casi specifici.

Il progetto contribuisce a sensibilizzare l'apprendimento della gioventù come uno strumento importante per l'inclusione sociale. Ci devono essere informazioni più frequenti e adeguate all'età per i giovani in merito ai loro diritti online e alle loro responsabilità nell'uso di internet. Consigliamo anche un kit di strumenti di per istruttori ed educatori per affrontare le situazioni e un approccio educativo per costruire empatia e responsabilità online.

L'apprendimento, condividendo le esperienze e collaborando per sviluppare criteri di qualità comuni, serve a tutte le organizzazioni partecipanti a sostenere le procedure pertinenti nei loro sistemi nazionali.

Cyberbullismo – una nuova forma di bullismo

Il bullismo rovina le vite. Danneggia l'autostima, scoraggia le persone e getta i semi del pregiudizio. Le ultime ricerche hanno rivelato che 1 persona su 2 ha subito episodi di bullismo durante la sua vita. Questa statistica scioccante mostra che c'è ancora molto da fare.

C'è un forte consenso nella comunità accademica sul fatto che il bullismo è una forma di aggressione sociale (Björkqvist, Ekman e Lagerspetz, 1982), ed è caratterizzato da tre criteri principali: l'intento di causare danni; ripetizione del comportamento per un periodo di tempo; uno squilibrio di potere tra le vittime e i bulli (ad es. Olweus, 1993; O'Moore & Minton, 2004; Rigby, 2002). O'Moore e Minton (2004) estendono questa tesi sostenendo che solo un incidente particolarmente grave che contribuisce a un costante senso di intimidazione può costituire un atto di bullismo.

Nel contesto europeo il bullismo avviene in modi sempre più duri, come: scontri di strada, bombings, insulti, molestie, cyberbullismo.

I comportamenti pericolosi e patologici come aggressione e violenza hanno nuovi strumenti e, quindi, hanno nuove forme. Il fenomeno è stato diagnosticato solo diversi anni fa ed è oggi definito "cyber-violenza".

La cyber-violenza è qualsiasi comportamento online che costituisce o causa danni allo stato psicologico, emotivo, finanziario e/o fisico di un individuo o di un gruppo.

La cyber-violenza può essere indirizzata a individui o gruppi, questi ultimi sono obiettivi più caratteristici della cyber violenza rispetto a violenza offline, a causa della facilità con cui un singolo può raccogliere informazioni e contattare un gran numero di persone in Internet. Questo è un altro aspetto della violenza online che può causare effetti diffusi. (*European Network Addressing Cyber violence*)

Negli ultimi 40 anni, i ricercatori hanno studiato il fenomeno, che nel 1970 è stato descritto come "**bullismo**". Dan Olweus è stato uno dei primi ricercatori a realizzare studi scientifici sul bullismo. Definisce il bullismo come segue:

Diciamo che uno studente è vittima di bullismo quando un altro studente o un gruppo di studenti;

- dice cose scortesie o spiacevoli o prende in giro qualcuno o da un soprannome cattivo o fastidioso



- *sta ignorando o escludendo qualcuno dai suoi amici o intenzionalmente non ne include alcuni nelle attività che stanno svolgendo*
- *picchia, prende a calci, spinge e fa il prepotente o minaccia qualcuno*
- *diffonde menzogne o false voci su qualcuno, invia parole sgradevoli o cerca di indurre altri studenti a non gradire qualcuno*

I ricercatori Olweus, Smith, Ortega e Merchan concordano sul fatto che, per definire un comportamento particolare come il bullismo, devono essere applicate almeno tre condizioni: (i) un intento di danneggiare la vittima (ii) una ripetizione del comportamento abusivo rispetto a un certo periodo (iii) uno squilibrio di potere tra la vittima e il bullo/i bulli.

In passato, il bullismo poteva essere limitato in ambito scolastico; ma con la maggior parte dei giovani che ora hanno accesso a smartphone, laptop e tablet, il bullismo e gli abusi possono entrare nelle case dei giovani e accadere in qualsiasi momento, giorno e notte. Abbiamo ascoltato racconti sconvolgenti da parte di bambini e giovani che hanno descritto il cyberbullismo come "ineludibile", e nei casi più estremi ha spinto i giovani sull'orlo del suicidio.

Il cyberbullismo si differenzia dalle forme tradizionali di bullismo in molti modi. Ad esempio Vande Bosch e Van Cleemput (2009) sottolineano che il bilanciamento del potere nel cyberbullismo non dipende dalla forza fisica e può essere basato su abilità tecnologiche più avanzate o sulla capacità di nascondere la propria identità.

Il bullismo, una volta era limitato alla scuola o al vicinato, si è ora spostato nel mondo online. Il bullismo attraverso mezzi elettronici viene definito "**cyberbullismo**". I risultati psicologici ed emotivi del cyberbullismo sono simili a quelli del bullismo nella vita reale. La differenza è che il bullismo nella vita reale spesso finisce quando finisce la scuola. Per il cyberbullismo, non c'è via di fuga.

Negli ultimi anni Internet e le tecnologie dell'informazione e della comunicazione (TIC) hanno avuto un impatto sempre più importante sulla nostra vita quotidiana (Cross et al., 2009). L'uso è ora completamente radicato nella vita quotidiana dei bambini (Livingstone et al., 2011) e la comunicazione elettronica è vista da molti bambini e adolescenti come essenziale per la loro interazione sociale (Kowalski, Limber, & Agatston, 2008).

La connessione tra bullismo e media digitali e social ha creato il fenomeno del cyberbullismo, con effetti nuovi e inaspettati sulle persone. **Il cyberbullismo** è una forma di violenza ripetuta da parte di una o più persone nei confronti di altre persone definite vittime attraverso l'uso del web, utilizzando computer o dispositivi mobili.

Il cyberbullismo permette di nascondere l'identità di un bambino, anche quando il cyberbullismo viene scoperto o segnalato a un adulto. A causa della natura dei media elettronici, i bambini possono configurare account falsi o persino creare un account di parodia del bambino che stanno attaccando. Il cyber bullismo anonimo è un altro dei fatti di cyber bullismo che deriva dalla natura dei media elettronici, come il fatto che il cyber bullismo può verificarsi ovunque.

La tecnologia offre anche ai bulli l'opportunità di molestare la vittima indipendentemente da tempo e luogo. Pertanto il cyber bullismo si verifica al di fuori dei limiti fisici nell'ambiente scolastico o in altri luoghi in cui avviene il bullismo tradizionale. Il bullo o i bulli non devono più trovarsi nello stesso luogo della persona o delle persone che vogliono disturbare.

Il cyberbullismo è cresciuto esponenzialmente come una minaccia alla sicurezza online nell'ultimo decennio. Per citare alcune statistiche, lo studio del Pew Research Center del 2017 sulle molestie online ha rilevato che circa il 40% degli americani ha subito personalmente molestie online, mentre circa il 62% degli americani considera già il cyberbullismo uno dei maggiori problemi nella nostra



società. Lo studio ha anche affermato che quasi un individuo su cinque (18%) delle persone subirà molestie "estreme" come minacce fisiche, stalking e molestie sessuali online. Statisticamente, le molestie alle persone saranno sulle loro opinioni politiche, sul loro aspetto fisico, sulla razza, sul genere e sull'orientamento sessuale.

Mentre le definizioni di cyberbullismo (Hutson, 2016), talvolta chiamate bullismo online, variano da fonte a fonte, la maggior parte delle definizioni consiste in:

- *forme di contatto elettroniche*
- *atto aggressivo*
- *intento*
- *ripetizione*
- *danno all'obiettivo*

La tecnologia, tramite computer o telefoni cellulari, utilizzata per il cyberbullo include:

- *siti web personali*
- *blog*
- *e-mail*
- *sms*
- *siti di social networking*
- *chat room*
- *bacheche online*
- *messaggistica istantanea*
- *fotografie*
- *videogiochi* (Feinberg & Robey, 2009)

Per definizione, si verifica tra i giovani. Quando un adulto è coinvolto, potrebbe incontrare la definizione di "cyber-molestie" o "cyber-stalking", un crimine che può avere conseguenze legali e comportare il carcere.

Il cyberbullismo si verifica "quando qualcuno prende ripetutamente in giro un'altra persona online o attacca ripetutamente un'altra tramite e-mail o messaggi di testo o quando qualcuno pubblica qualcosa di sgradevole online su un'altra persona" (Cyberbullying Research Center, 2016).

Il cyberbullismo è un atto aggressivo, intenzionale, distribuito, da un individuo o da un gruppo, che usa un mezzo elettronico, continuamente e implacabilmente contro qualcuno che non può difendersi facilmente (Smith et al., 2008).

Abbiamo sviluppato questa definizione perché è semplice, concisa e ragionevolmente completa e comprende gli elementi più importanti. Questi elementi includono quanto segue:

- **Volontà:** il comportamento deve essere intenzionale, non accidentale.
- **Ripetizione:** il bullismo riflette uno schema di comportamento, non solo un incidente isolato.
- **Danno:** l'obiettivo deve percepire che il danno è stato inflitto.
- **Computer, telefoni cellulari e altri dispositivi elettronici:** questo, ovviamente, è ciò che differenzia il cyberbullismo dal bullismo tradizionale

Secondo la Commissione europea, il cyberbullismo è la ripetizione di molestie verbali o psicologiche eseguite da un individuo o un gruppo contro altri. Può assumere molte forme: scherno, insulti, minacce, pettegolezzi, "happy slapping", commenti sgradevoli o calunnia. Servizi online interattivi (e-



mail, chat room, messaggistica istantanea) e telefoni cellulari hanno dato ai bulli nuove opportunità e modi in cui possono offendere le loro vittime.

La violenza nel cyberbullismo avviene attraverso messaggi, film e fotografie, intimidendo con scritti attraverso i social media o pubblicati su siti web. Esempi di cyber-violenza includono (ma non sono limitati a) messaggi di testo dannosi o e-mail, frasi spiacevoli inviate via e-mail o pubblicate su social network, condivisione di foto/video/testi intimi senza consenso, bullismo online, molestie, cyberstalking, ricatto, espressioni di razzismo, omofobia e misoginia.

Vandebosch, Van Cleemput, Mortelmans e Walrave (2006) sostengono che non è essenziale che l'aggressività venga ripetuta da parte del bullo per costituire il cyberbullismo. Ad esempio, i contenuti creati o condivisi solo una volta dal cyberbullo possono rimanere online nel tempo, e quindi possono essere visualizzati o condivisi. In tal caso, la ripetizione è caratterizzata dal numero di testimoni rispetto al numero di azioni da parte del cyberbullo.

Inoltre, lo squilibrio di potere nel cyberspazio è un po' meno chiaro che nel mondo reale. Sebbene nei casi di bullismo tradizionale, il potere possa assumere la forma di forza fisica, nel mondo cibernetico il potere può essere costituito dalla capacità di nascondere la propria identità (Vandebosch et al., 2006). È un po' più difficile rimanere anonimi nei casi di bullismo tradizionale.

Ci sono diversi attori coinvolti nel cyberbullismo:

- Bullo/bulli
- Vittima
- Gli osservatori

È importante capire che il ruolo del bullo e della vittima sono correlati e talvolta il ruolo può cambiare, se cambiamo il punto di vista: a volte la vittima può diventare un bullo o un persecutore.

Rey e Ortega (2007) dividono il bullismo tradizionale in cinque forme principali:

1. *fisico*
2. *verbale*
3. *gesti*
4. *esclusione*
5. *ricatto*

Tutti i tipi di bullismo sono collegati a un rischio reale di causare danni psicologici, attività compromessa a scuola e mancanza di relazioni sociali.

Forme di cyberbullismo

Un modo per capire il cyberbullismo è classificarlo secondo media o forma:

- Dai media in cui si verifica l'aggressione, come messaggi di testo, messaggi con disegni, chiamate telefoniche, e-mail, messaggistica istantanea o pagine web
- In linea con il carattere dell'assalto, come flaming, molestie, calunnie, fingendo di essere altri, divulgazione di informazioni private, esclusione, persecuzione e diffamazione.

Queste classificazioni cambieranno con lo sviluppo tecnologico. La seguente panoramica offre una visione più dettagliata dei diversi tipi di cyber-bullismo:

1. *Per tipo di media* (da Smith, 2006)

- SMS: Invio o ricezione di messaggi di testo offensivi tramite telefono cellulare.
- MMS, Snapchat, ecc.: Consente di inviare, inviare o ricevere immagini e/o clip video non piacevoli tramite telefoni cellulari.



- **Telefonate:** Effettuazione o ricezione di telefonate disturbanti, come ad esempio telefonate senza senso o chiamate anonime.
- **E-mail dannose o minacciose** inviate direttamente a una vittima o e-mail con contenuti malevoli su una vittima inviata ad altri.
- **Minacce o abusi** quando si partecipa alla chat: chat room, ad esempio durante i giochi online.
- **Molestie con messaggi immediati** Messaggi: (IM), ad esempio su Facebook, Skype

2. **Dal tipo di comportamento** (Willard, 2007)

- **Flaming:** una breve e intensa discussione che include spesso linguaggio molesto, volgare, insulti e talvolta minacce. "Flaming" può avvenire tramite messaggi di testo o messaggistica istantanea, nei blog, sui siti di social network, nelle chat room, nelle bacheche o tramite giochi per computer online
- **Harassment:** distribuzione ripetuta di messaggi cattivi, meschini e offensivi
- **Slander:** inviare o pubblicare pettegolezzi e notizie su una vittima al fine di danneggiare la sua reputazione o le sue amicizie
- **False identità:** fingere di essere qualcun altro e inviare o pubblicare materiali per creare problemi per la persona che possiede il profilo mirando a danneggiare la sua reputazione o le amicizie
- **Outing:** divulgazione di segreti o informazioni personali e private per umiliare. Un metodo comune è quello di inoltrare un messaggio dalla vittima contenente informazioni personali o intime.
- **Rip:** persuadere qualcuno a rivelare segreti o informazioni umilianti, quindi condividerlo online
- **Exclusion:** esclusione deliberata e feroce di qualcuno da un gruppo o forum online. Per la vittima, l'esclusione dalla partecipazione a attività online con colleghi può causare una sensazione di rifiuto
- **Cyber stalking:** persecuzione, ripetute molestie e calunnie intense, che comprendono minacce e creano una paura significativa
- **Harassment:** uso di Internet o cellulare per attacchi verbali o visivi. I predatori possono inviare commenti nei blog o inviare messaggi di testo da un cellulare. Possono anche scattare foto della vittima o rubare un'immagine da una fonte su Internet e quindi modificare l'immagine in modo umiliante o aggiungere commenti molesti e pubblicarli online in modo che altri possano vederli. Una tendenza speciale ("happy slapping") consiste nel filmare le persone che vengono picchiate e quindi caricare i video online
- **Posing:** una forma di attacco indiretto in cui un bullo pubblica contenuti su Internet utilizzando l'identità della vittima. Questo può accadere se un bullo conosce il nome utente e la password della vittima e può accedere e entrare negli account online della vittima. Quando il bullo finge di essere la vittima, può dire cose brutte agli o sugli amici della vittima. Ciò può indurre gli amici o i compagni a rifiutare la vittima, poiché pensano che sia stata la vittima a dirlo



Programmi anti bullismo per fermare la violenza

Il professor Mc Guckin et al. (2012) ritengono che i bambini e i giovani che hanno un'immagine positiva di sé e che imparano ad agire con fermezza, spesso capiscano meglio come dovrebbero comportarsi in situazioni difficili.

Specialista in psicologia Solfrid Raknes (Norvegia, 2013) ha sviluppato alcuni suggerimenti su come i genitori possono rendere il bambino più forte e migliorare la propria immagine di sé:

- Aiuta il tuo bambino a identificare i suoi sentimenti.
- Insegna a tuo figlio a parlare in modo positivo, incoraggiante e di supporto per se stesso in situazioni difficili.
- Parla delle cose belle che sono successe durante il giorno.
- Facilita buone relazioni ed esperienze positive con gli adulti. Ciò rende più facile per i bambini rivolgersi agli adulti quando ne hanno bisogno.
- Fai in modo che tuo figlio sviluppi amicizie e lasci che portino i loro amici a casa. Le amicizie rendono il tuo bambino più preparato per affrontare le avversità.
- Incoraggia l'indipendenza e proponi ai bambini le attività che possano gestire.
- Insegna a tuo figlio che le avversità sono qualcosa che possiamo usare per diventare più forti. La vita non è solo facile, e non sempre si ottiene ciò che meriti.
- Non puoi impedire a tuo figlio di affrontare esperienze difficili, ma puoi influenzare il modo in cui tuo figlio può gestirle.

I bambini non sempre parlano ai loro genitori del cyberbullismo che avviene tra amici e colleghi. I genitori dovrebbero ascoltare attentamente quando i loro figli parlano delle loro esperienze online e familiarizzare con i vari tipi della comunicazione digitale che i giovani utilizzano (come Facebook, Instagram, Snapchat, ecc.). Se il bambino ha raccontato di un episodio di bullismo, la prima risposta di un genitore potrebbe essere quella di confermare che il bambino ha fatto una buona scelta: - *Grazie per avermelo detto.*

Se i contenuti online sono sconvolgenti e inappropriati e la persona o le persone responsabili sono conosciute, i genitori devono assicurarsi di capire perché il materiale è inaccettabile o offensivo e richiedere di rimuoverlo.

Se il responsabile non è stato identificato, o si rifiuta di rimuovere il materiale, i genitori devono contattare direttamente il sito di social networking per fare un rapporto e richiedere che il contenuto venga rimosso. Il materiale pubblicato potrebbe essere in violazione dei termini e delle condizioni d'uso del fornitore di servizi e può quindi essere rimosso. Alcuni fornitori di servizi non accetteranno reclami presentati da terzi.

In caso di uso illecito di telefoni cellulari, in cui la persona vittima di bullismo riceve chiamate e messaggi malevoli, l'intestatario del conto dovrà contattare direttamente il fornitore. Prima che i genitori contattino un fornitore di servizi web, è importante essere chiari su dove si trova il contenuto, ad esempio scattando una immagine o effettuando uno screenshot del materiale e includendo anche l'indirizzo web.

I genitori dovrebbero rimanere calmi quando un bambino racconta loro di un incidente in cui sono stati vittime di bullismo online. Una risposta calma ed equilibrata aiuta a mantenere aperte le linee di comunicazione con il bambino.

Kowalski (2008) suggerisce inoltre che i genitori e il loro bambino dovrebbero concordare i casi in cui i genitori del bambino informano i genitori della controparte in merito a contenuti negativi e/o contatti online. Fornendo feedback positivi ai bambini, i genitori possono influenzare il



comportamento senza scoraggiare il bambino. Le parole dette con intenzione buona, ma espresse negativamente dagli adulti possono essere percepite in modi che non vengono intesi.

L'autostima deriva dal sentirsi amati, sicuri (Taylor, 2011). I genitori possono aumentare la capacità di recupero dei loro figli contro le conseguenze negative del bullismo costruendo una stima di sé positiva. Possono promuovere la fiducia del loro bambino sviluppando, enfatizzando e riconoscendo i punti di forza del bambino.

Quelle che seguono sono alcune indicazioni che i genitori potrebbero considerare per insegnare ai propri figli a usare Internet in modo sicuro (fonte - <https://www.gov.uk/>)

- Assicurati di utilizzare le impostazioni sulla privacy.
- Rispetta sempre gli altri - fai attenzione a ciò che dici online.
- Fai attenzione a quali foto o video carichi. Una volta che un'immagine è condivisa online, non può essere cancellata.
- Aggiungi solo persone che conosci e di cui ti fidi agli elenchi di amici/follower online. Quando parli con estranei, mantieni le tue informazioni personali al sicuro.
- Tratta la tua password come lo spazzolino da denti - tienilo per te e cambialo regolarmente.
- Blocca il bullo - impara come bloccare o segnalare qualcuno che si comporta male.
- Non reagire o rispondere a e-mail offensive, messaggi di testo o conversazioni online.
- Salva le prove. Conserva sempre una copia delle e-mail offensive, messaggi di testo o una schermata di conversazioni online e inviale a un genitore, un adulto o un insegnante
- Assicurati di dire a un adulto di cui ti fidi, ad esempio un genitore, un insegnante o il coordinatore antibullismo o chiedi aiuto ad uno dei servizi.
- La maggior parte dei servizi di social media e altri siti hanno un pulsante su cui è possibile segnalare il bullismo. Ciò può impedire a un bullo di prendere di mira te e gli altri in futuro. Molti servizi prendono sul serio il bullismo e avvertiranno l'individuo o elimineranno il suo account.
- Mentre sei sul tuo telefono cellulare, assicurati di prestare attenzione anche a ciò che ti circonda.

I genitori possono contattare la scuola, i referenti nell'ambiente giovanile se il bullismo si verifica all'interno di un'attività organizzata, possono contattare la polizia o altre agenzie se lo considerano rilevante in base alla gravità di ciò che è avvenuto.

<p>Cosa possono fare i genitori se il loro bambino è stato vittima di cyber bullismo:</p>	<p>Cosa possono fare i genitori se il loro bambino è coinvolto nel bullismo degli altri:</p>
--	---



<ul style="list-style-type: none">• Ascolta attentamente il tuo bambino• Rimani calmo• Blocca il cyber bullo• Non rispondere• Prove sicure• Scopri cosa c'è di sbagliato• Metti in chiaro che è il bullo ad avere un problema, non la vittima• Crea un'atmosfera di sicurezza• Rafforza l'autostima di tuo figlio• Segnala il problema	<ul style="list-style-type: none">• Definisci una panoramica accurata e obiettiva di ciò che comporta il cyberbullismo in corso• Scopri le ragioni alla base di questo comportamento• Prendi in considerazione la definizione di regole per il bambino al fine di promuovere l'uso responsabile di Internet e dei dispositivi mobili in generale• Prendi in considerazione le misure per seguire in modo appropriato l'uso di Internet e del telefono da parte del bambino• Promuovi e sviluppa la capacità del bambino di empatia e rispetto per gli altri• Costruisci la fiducia e l'autostima di tuo figlio.• Facilitare la "catarsi" dei bambini, lascia che si esprimano e sfoghino le frustrazioni in modo costruttivo
---	--

Anche se il cyberbullismo inizia di solito a scuola e molto spesso coinvolge bambini della stessa classe o della stessa età, gli incidenti di cyberbullismo possono verificarsi al di fuori dei confini scolastici. È molto importante che le scuole investano nell'aumentare la conoscenza e la consapevolezza degli studenti sulle caratteristiche dei nuovi media, su caratteristiche come la loro impronta digitale (Chadwick, 2014).

Il programma Anti-Bullismo Scolastico contiene quattro componenti principali:

1. Una rete di professionisti formati per attuare il programma anti-bullismo nelle scuole partecipanti;
2. Risorse per insegnanti e formazione in servizio organizzate da formatori qualificati;
3. Risorse e informazioni per genitori e altri membri della comunità organizzate da formatori qualificati;
4. I formatori assumono un ruolo di consulenza per la durata del programma nelle scuole partecipanti.

Oltre ai genitori, la scuola dovrebbe informare tutti gli attori rilevanti che possono contribuire a risolvere la situazione, come consulenti psicologici e fornitori di servizi elettronici.

Costruire un ambiente scolastico di sostegno, sensibilizzare sul problema, fornire formazione per insegnanti, studenti, genitori e altro personale scolastico, incorporare il cyber bullismo nel curriculum, pubblicizzare misure antibullismo e assicurare il monitoraggio e la valutazione indispensabili sono tra le varie pratiche che forma un approccio all'intera scuola e quindi contribuisce alla prevenzione dei comportamenti di bullismo.

Attraverso campagne antibullismo, verranno identificati diversi elementi e approcci validi che possono definire una struttura politica ben organizzata, concreta e coerente che potrebbe essere utilizzata nello sviluppo di una politica comune antibullismo dell'UE o nello sviluppo della politica nazionale antibullismo di ogni paese.

In termini di sviluppo di una politica anti-bullismo scolastica, si raccomanda di includere i seguenti elementi:

- Un ethos scolastico positivo con particolare attenzione al rispetto dell'individuo;



- Sensibilizzazione che il bullismo è considerato un comportamento inaccettabile a scuola, tra insegnanti, tra alunni e tra genitori/tutori; supervisione e monitoraggio per contrastare il bullismo in tutte le aree dell'attività scolastica con l'assistenza degli studenti;
- Progettazione di procedure per notificare e segnalare problemi di bullo/vittima come parte integrante del Codice di Comportamento e Disciplina della scuola;
- Fornire assistenza a vittime, bulli e colleghi, compresa la consulenza;
- Inserimento degli enti locali nella lotta al bullismo come forma di comportamento antisociale, poiché è auspicabile coinvolgere la comunità scolastica anche oltre i confini della scuola
- Revisione e valutazione continue dell'efficacia della politica antibullismo scolastico per valutare la prevalenza e i tipi di bullismo all'interno della scuola.

Una delle misure importanti per limitare i comportamenti a rischio è quella di consentire a bambini e giovani di sviluppare competenze digitali. Al fine di essere in grado di guidare i giovani utenti; i genitori e i professionisti devono sviluppare il proprio livello di competenza.

Raccomandazioni:

- Le piattaforme di social media devono essere adeguate all'età, e le aziende dovrebbero avere metodologie per identificare i minori di 13 anni e ottenere il consenso esplicito dei genitori.
- Le società di social media dovrebbero consentire a bambini e giovani di comprendere i loro diritti e responsabilità, incluso il loro comportamento nei confronti degli altri.
- Le società di social media dovrebbero fornire risposte tempestive, efficaci e coerenti al bullismo online.
- Il governo dovrebbe mettere le esperienze dei bambini al centro dello sviluppo della politica di sicurezza di Internet.
- Educatori e genitori dovrebbero insegnare ai bambini e ai giovani come essere sicuri e responsabili online e assicurarsi di sapere come rispondere positivamente ai danni online come il cyber bullismo.

C'è un bisogno vitale di sforzo collaborativo da parte della società, delle scuole, degli insegnanti, dei genitori e dei giovani per determinare le politiche e le pratiche, ed è di particolare importanza che i giovani sentano che le loro voci siano ascoltate in questi argomenti che li riguardano:

- Il cyberbullismo deve essere incluso in un approccio della comunità scolastica all'intero bullismo, che consenta agli studenti di denunciare la vittimizzazione per cercare aiuto sia per loro stessi che per i loro coetanei;
- Sono necessarie per i giovani l'educazione per rimanere al sicuro nel cyberspazio, rispondere efficacemente alle aggressioni e migliorare le abilità sociali online;
- Sia i genitori che gli insegnanti devono assumersi la responsabilità di occuparsi del comportamento abusivo nel cyberspazio e devono offrire sostegno a coloro che sono vittime;
- È importante che gli insegnanti ricevano una formazione sia in pre-servizio che in formazione per lo sviluppo professionale per quanto riguarda le dinamiche di gruppo e la gestione dei conflitti;



Modulo 2: Cyberbullismo e social media

In questo capitolo viene presentata una guida sul fenomeno del cyberbullismo nei social media.

La guida segue il processo mostrato nella figura seguente.

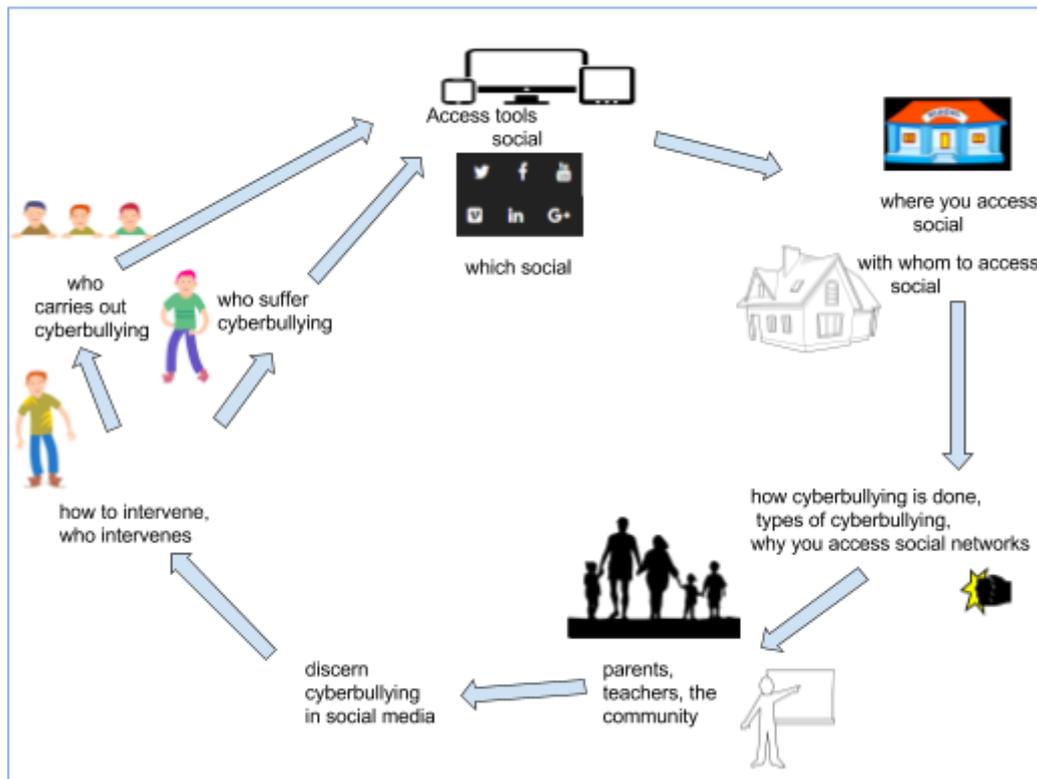


Figura 1 Cyberbullismo il processo dei social media

Il fenomeno del cyberbullismo sui social media è descritto e analizzato nel seguito, considerando:

- la definizione di social media e il cyberbullismo vs bullismo
- gli attori coinvolti nel cyberbullismo nei social media (il bullo, la vittima, gli osservatori/spettatori)
- identificazione del contesto in cui si verificano i fenomeni di cyberbullismo (a scuola, a casa, in gruppo, con gli amici)
- analisi di come avviene il cyberbullismo e i tipi di cyberbullismo
- analisi per riconoscere il cyberbullismo: genitori e insegnanti
- analisi per contrastare il fenomeno e capire come intervenire sul bullo, sulla vittima e su coloro che assistono ai fenomeni del cyberbullismo, delle leggi, della regolamentazione dei social media (Twitter, Facebook, ...) a livello internazionale.

I social media

Social media è un termine generico che si riferisce a tecnologie e pratiche sul web che consentono alle persone di interagire, condividere testo, foto, immagini, contenuti video e audio.



Il professor Andreas Kaplan e Michael Haenlein hanno definito i social media come un gruppo di applicazioni web basate sugli aspetti ideologici e tecnologici del Web 2.0, che consentono la creazione e lo scambio di contenuti generati dagli utenti.

I social media hanno portato un cambiamento radicale nel modo in cui le persone imparano, leggono e condividono informazioni e contenuti. Utilizzando la sociologia e la tecnologia i social media hanno trasformato il monologo (da uno a molti) in un dialogo (da molti a molti) e gli utenti/consumatori nei produttori, parliamo di "prosumer"¹.

Sono diventati molto popolari perché consentono alle persone di utilizzare il Web per stabilire relazioni personali o commerciali. I social media sono anche chiamati contenuti generati dagli utenti (UGC) o media generati dai consumatori (CGM).

L'uso dei social media è molto popolare e il numero di persone che usano questi canali è davvero impressionante, ma ci sono alcune differenze in termini di età e sesso.

Tabella 1 Alcuni dati sui social media²

<p>Facebook è la più grande rete di social media al mondo e ha membri di quasi tutte le generazioni, ma alcuni sono più attratti rispetto ad altri.</p>	<ul style="list-style-type: none"> • Facebook ha 2,01 miliardi di visitatori unici al mese • Gli utenti di Facebook sono per il 53% donne e per il 47% maschi • Il 75% degli utenti di Facebook trascorre oltre 20 minuti su Facebook ogni giorno • L'83% delle donne che usano i social media usa Facebook, contro il 75% degli uomini che usano i social media • Il 63% degli anziani tra i 50 ei 64 anni che usano Internet sono su Facebook, così come il 56% degli anziani online oltre i 65 anni
<p>YouTube è la seconda più grande rete di social media al mondo, ed ha anche la forza di Google.</p>	<ul style="list-style-type: none"> • YouTube ha 1,3 miliardi di visitatori unici al mese • Gli utenti di YouTube sono il 38% di donne e il 62% di uomini • YouTube raggiunge maggiormente le fasce tra i 18-34 e i 35-49 anni rispetto a qualsiasi rete via cavo negli Stati Uniti • L'80% degli utenti di YouTube si trova fuori dagli Stati Uniti
<p>Instagram è diffuso quasi quanto YouTube, ma è la rete di social media in più rapida crescita e questa crescita non mostra segni di arresto.</p>	<ul style="list-style-type: none"> • Instagram ha 700 milioni di visitatori unici al mese • L'80% degli utenti di Instagram proviene da paesi diversi dagli Stati Uniti • Il 59% degli utenti di Internet tra i 18 e i 29 anni è su Instagram, insieme al 33% degli utenti Internet tra i 30 e i 49 anni • Il 17% dei ragazzi afferma che Instagram è il sito di social

¹ <https://en.wikipedia.org/wiki/Prosumer>

² The data are from: How to Find Social Media Audience for Your Business: From Demographics, All the Way to Which Platforms to Use and What to Post <https://revive.social/find-social-media-audience/>



	media più importante (dal 12% nel 2012)
Twitter ha 328 milioni di visitatori unici al mese. È un canale che non può essere ignorato per il business.	<ul style="list-style-type: none"> Il 37% degli utenti di Twitter ha tra i 18 e 29 anni; Il 25% è nella fascia 30-49 69 milioni di utenti di Twitter hanno sede negli Stati Uniti Il 79% degli utenti di Twitter si trova al di fuori degli Stati Uniti
Snapchat è attualmente il secondo social network in più rapida crescita. È il canale più adatto per gli adolescenti.	<ul style="list-style-type: none"> Oltre 300 milioni di utenti attivi su Snapchat ogni mese 173 milioni di persone usano Snapchat ogni giorno Il 71% degli utenti di Snapchat ha meno di 31 anni Il 45% degli utenti di Snapchat ha tra i 18 e i 24 anni
Pinterest è un social in rapida crescita con circa 150 milioni di utenti, è la scelta migliore per le comunicazioni visive, ideale per le attività commerciali connesse alle immagini.	<ul style="list-style-type: none"> L'81% degli utenti di Pinterest sono donne Il 40% dei nuovi iscritti sono uomini; Il 69% sono donne L'età media di un utente Pinterest è 40, ma la maggior parte degli utenti attivi ha meno di 40 anni Il 60% degli utenti di Pinterest proviene dagli Stati Uniti
LinkedIn è il social per le connessioni professionali piuttosto che per le attività sociali.	<ul style="list-style-type: none"> 40 milioni di studenti universitari e neolaureati sono su LinkedIn Il 70% degli utenti di LinkedIn proviene da paesi al di fuori degli Stati Uniti Il 44% degli utenti di LinkedIn guadagna più di \$ 75.000 all'anno Un utente medio trascorre 17 minuti al mese su LinkedIn

Nelle seguenti figure, si possono vedere alcune tendenze nell'uso dei social media.

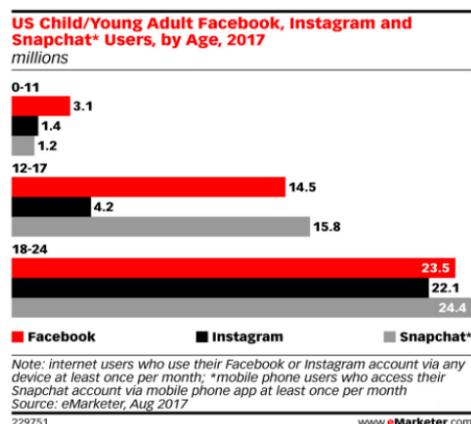
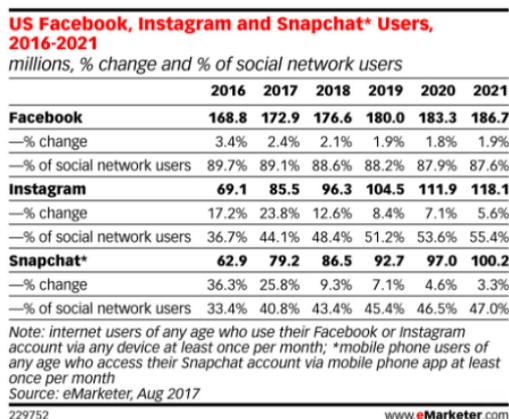


Figura 2 Utenti di Facebook, Instagram e Snapchat - fonte: TechCrunch



Bullismo vs Cyberbullismo: una definizione

Il cyberbullismo è una forma di violenza da parte di una o più persone verso altre persone che sono definite la **vittima** attraverso l'uso del web, utilizzando computer o dispositivi mobili.

Questa violenza avviene attraverso messaggi, film, fotografie, scritti intimidatori attraverso i social media o pubblicati su siti web.

Il bullismo e il cyberbullismo coinvolgono principalmente i giovani, ma anche gli adulti sono coinvolti in questa forma di violenza.

La tabella seguente mostra il confronto tra cyberbullismo e bullismo in un documento del Ministero della Pubblica Istruzione dell'Università italiana di ricerca³.

Tabella 2 Differenze tra bullismo e cyberbullismo

Bullismo	Cyberbullismo
Sono coinvolti solo studenti della classe e/o della scuola;	Possono essere coinvolti bambini e adulti da tutto il mondo;
Solitamente, solo chi ha un carattere forte, capace di imporre il proprio potere, può diventare un bullo;	Chiunque, anche chi è vittima nella vita reale, può diventare un cyberbullo;
I bulli sono studenti, compagni di classe o compagni dell'Istituto, conosciuti dalla vittima;	I cyberbulli possono essere anonimi e sollecitare la partecipazione di altri cosiddetti "amici" anonimi in modo che la persona non sappia realmente con chi sta interagendo;
Le azioni di bullismo sono raccontate agli altri studenti della scuola in cui si sono svolte, sono limitate a un ambiente specifico;	Il materiale utilizzato per le azioni di cyberbullismo può essere diffuso in tutto il mondo;
Il bullismo avviene durante l'orario scolastico o durante il viaggio da scuola a scuola, da scuola a casa;	Le comunicazioni aggressive possono aver luogo 24 ore al giorno;
Le dinamiche del gruppo scolastico o di classe limitano le azioni aggressive;	I cyberbulli hanno ampia libertà di fare online ciò che non potrebbero fare nella vita reale;
Necessità per il bullo di dominare nelle relazioni interpersonali attraverso il contatto diretto con la vittima;	Percezione dell'invisibilità da parte dei cyberbulli attraverso azioni nascoste dietro la tecnologia;

³ <http://www.miur.gov.it/bullismo-e-cyberbullismo>



Reazioni visibili della vittima e visibili nell'atto di bullismo;	Assenza di reazioni visibili da parte della vittima che non consentono ai cyberbulli di vedere gli effetti delle sue azioni;
La tendenza a sottrarsi alle responsabilità prendendo la violenza in modo giocoso.	Scomposizione della personalità: le conseguenze delle tue azioni sono attribuite al "profilo utente" creato.

Le forme del cyberbullismo

Il cyberbullismo può manifestarsi in varie forme, come ad esempio nel gioco multiplayer, che viene spesso chiamato "griefing". Diversi tipi di cyberbullismo sono descritti nella seguente tabella.

Tabella 3 Diversi tipi di cyberbullismo

Flaming	Invio di messaggi violenti e volgari.
Harassment or Stalking	Invio di messaggi ripetuti a un individuo.
Denigration	Diffusione di notizie false.
Identity theft/unauthorized access and Impersonation Masquerading	Furto d'identità. Masquerading è una situazione in cui un bullo crea un'identità falsa per molestare qualcuno in modo anonimo. Oltre a creare un'identità falsa, il bullo può impersonare qualcun altro per inviare messaggi maligni alla vittima.
Tricky Outing	Consiste nell'avere la fiducia della vittima e poi sfruttare e diffondere le informazioni ricevute.
Ostracising/Exclusion	Esclusione intenzionale di una persona da un gruppo.
Happy slapping	Diffusione di materiale online in cui la vittima viene ripresa mentre subisce violenza.
Trolling	Attaccare una persona su importanti questioni personali o familiari.
Roasting	Attaccare una persona fino a quando non si piega, non resiste più agli attacchi.
Creating Websites, Blogs, Polls and More	Sviluppo di siti di denigrazione, blog di denigrazione, di sondaggi per denigrare.



Self-cyberbullying or digital self-harm	Come nel caso di Hannah Smit ⁴ che si è inviata messaggi denigrandosi sul web.
--	---

Gergo utile da sapere

L'uso di slang e gergo è molto comune tra gli adolescenti e aiuta a creare un senso di comunità. Potrebbe essere utile conoscere la lingua utilizzata dagli adolescenti e in particolare alcuni acronimi che possono essere monitorati. Nella tabella seguente, puoi trovare alcuni esempi, ma ovviamente queste cose sono diverse in ogni comunità e possono cambiare molto rapidamente.

PHRASES TO BE AWARE OF

- GNOG: Get naked on camera
- FBOI: A guy who's just looking for sex
- WTPP: Want to trade pictures
- FINSTA: Fake Instagram account
- PAL: Parents are listening
- 1174: Meet at a party

FAM	Refers to someone who is a close friend
LIT/TURNT/TURNT UP	Something that's active or popular, can also refer to being stoned or drunk
SMH	"Shaking my head", meaning "I don't believe it" or "that's so dumb"
KMS/KYS	"kill myself", "kill yourself"
DABBING	Reference to concentrated doses of cannabis; also a dance craze
SNATCHED	On point, very good, or well styled
NETFLIX AND CHILL	Getting together and hooking up
AF	Short for "as f**k", used to mean "extremely"
BASIC	Used to refer to someone viewed as a boring or conforming person
	Emoji used to mean pride or general acceptance of an idea
	Emoji used to refer to the penis
	Emoji used to refer to the butt
	Emoji used to mean "ejaculate", often used in conjunction with the tongue emoji
MOS	Mom over shoulder
9 AND CD9	Parents are nearby
99	Parents are gone
WTPP	"Want to trade pictures?"

Figura 3 Alcuni acronimi utilizzati dagli adolescenti

Un bambino può essere coinvolto nel cyberbullismo in modi diversi. Un bambino può essere vittima di bullismo o essere presente in una situazione di bullismo. Genitori, insegnanti e altri adulti potrebbero non essere a conoscenza di tutte le piattaforme di social media e le app utilizzate da un

4

<https://www.bustle.com/p/what-is-self-cyberbullying-a-dangerous-new-trend-involves-teens-sending-bullying-messages-to-themselves-3072212>



Co-funded by the
Erasmus+ Programme
of the European Union

CYBER 
VIOLENCE

bambino. Più piattaforme digitali utilizzate da un bambino, maggiori opportunità di essere esposto a potenziali fenomeni di cyberbullismo.

Molti segnali da come viene usato il dispositivo dal bambino indicano che si stanno verificando fenomeni di cyber bullismo. Poichè i bambini trascorrono molto tempo sui loro dispositivi: computer, tablet e soprattutto telefoni cellulari, l'aumento o la diminuzione dell'uso potrebbero essere meno evidenti. È importante prestare attenzione quando un bambino mostra improvvisi cambiamenti nel comportamento digitale e sociale.

Insegnanti, amministratori scolastici, genitori e formatori sono in posizioni uniche per utilizzare le loro competenze e ruoli per creare ambienti sicuri con norme sociali positive. Sono anche in condizione in cui potrebbero notare cambiamenti nel comportamento dei ragazzi nelle relazioni di gruppo, come quando un gruppo di bambini focalizza l'attenzione su un bambino. Ci sono cose che possono essere fatte in classe e altre nel gruppo per affrontare o prevenire il cyberbullismo⁵.

⁵ <https://www.stopbullying.gov/cyberbullying/tips-for-teachers/index.html>



Modulo 3: Identità offline e online, profilazione e tracciamento web:

Essere al sicuro sul web

All'inizio degli anni '90, gli utenti di Internet si sentivano protetti da un velo di anonimato, erano in grado di diventare qualsiasi personaggio volessero. Internet è cambiato enormemente negli ultimi 20 anni, in modi che influiscono direttamente sulla nostra identità online e sulla privacy. I servizi online oggi hanno adottato tecnologie che costruiscono profili dei clienti, offrono indicazioni sui prodotti e conservano dati personali anche per molto tempo ed estremamente dettagliati. La condivisione dei dati tra le aziende web influisce anche sulla nostra identità online e sulla privacy. Attraverso la condivisione dei dati, un fornitore di servizi può collegare sottoinsiemi di dati personali a una massa di dati che potremmo pensare fossero definiti per un'altra persona o un altro contesto.

Mentre alcuni utenti di Internet apprezzano la convenienza di tali identità digitali, altri si preoccupano della quantità di informazioni personali memorizzate e di come queste informazioni vengono condivise.

Identità

Questa sezione aiuterà a spiegare le diverse identità e profili che rappresentano le persone online e offline sia da un punto di vista sociale che tecnico. I bambini e i giovani possono utilizzare Internet per una serie di motivi diversi. Uno di questi è esprimersi e sperimentare la loro identità (Turkle, 1995, 1996, 2011). Usando siti di social network come Facebook, giochi di ruolo online come World of Warcraft e social media come Twitter, possono connettersi con altri, interagire con loro, condividere idee, immagini e filmati e impegnarsi in una varietà di versioni di 'digital flea picking'. Sviluppare, esprimere e sperimentare la propria identità è un elemento centrale per passare dall'infanzia alla maturità, e quindi è importante capire come Internet offra e inibisca le capacità dei giovani di impegnarsi nell'auto-esplorazione online.

I dati qui presentati si basano sul lavoro presentato nel libro⁶ del progetto Primelife EU, sulle pubblicazioni⁷ di Roger Clarke e sugli scenari sull'identità di Goffman (Goffman, 1959), che rimane molto importante.

Aspetti generali sull'identità offline

Gli individui interagiscono con gli altri individui e organizzazioni in modalità diverse, tutte collegate a ruoli diversi dell'individuo, Goffman (1959) definisce l'identità come **"il risultato di esibizioni pubblicamente validate, la somma di tutti i ruoli interpretati dall'individuo, piuttosto che una qualità personale"**. A tale riguardo, tutti i diversi ruoli o caratteristiche possono essere visti come **identità parziali**.

Dal punto di vista pratico, **la nostra identità è la somma delle nostre caratteristiche**, tra cui il luogo di nascita e il compleanno, le scuole che abbiamo frequentato, le dimensioni delle scarpe, la lingua, l'etnia, la religione, il genere, la classe sociale, il sesso, la generazione e così via. Alcune di queste caratteristiche non cambiano mai, come il nostro compleanno, e alcune cambiano nel tempo, come la nostra età o il colore dei capelli. In parole semplici la nostra identità è che cosa siamo, chi siamo e cosa facciamo.

⁶ Camenisch, J., S. Fischer-Hübner & K. Rannenber (2011). *Privacy and Identity Management for Life*. Springer Science & Business Media.

⁷ <http://www.rogerclarke.com/DV/DigPersona.html#Prof>



L'identità dell'individuo è costituita da differenti (tipi di) relazioni che implicano diversi tipi di informazioni. Un singolo individuo quindi consiste in diverse caratterizzazioni legate ai diversi contesti in cui opera.

Secondo Goffman (1959) diversi contesti impongono regole diverse sul comportamento e le persone svolgono ruoli diversi (come in un teatro) in diversi contesti. Inoltre presentano diversi volti di se stessi. Quindi, possiamo dire che le persone si presentano in modi diversi nella vita di tutti i giorni.

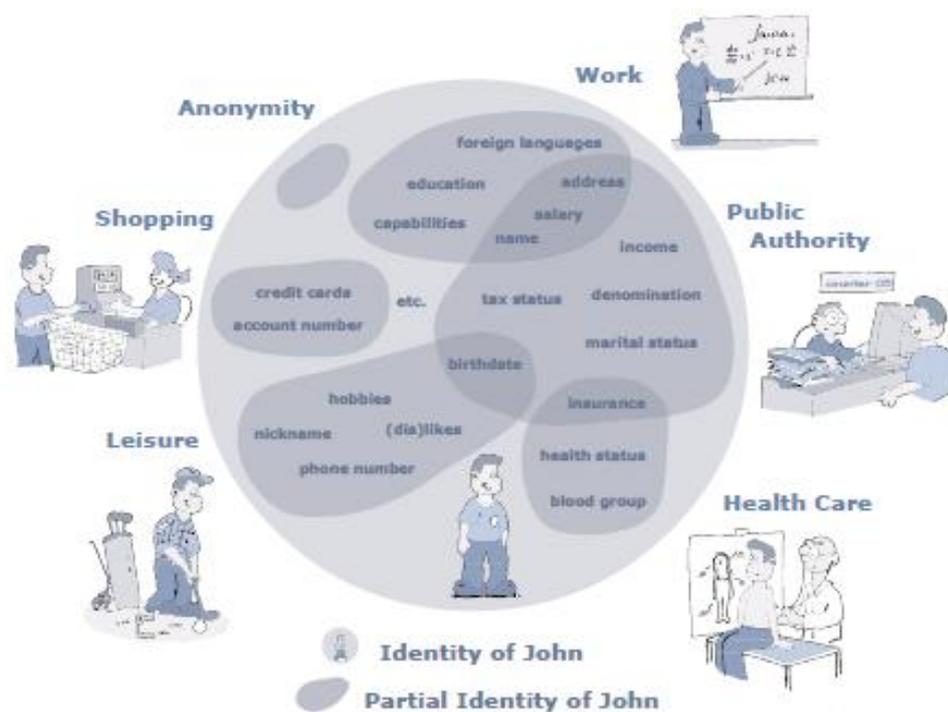


Figura 4 Un'identità composta da più identità diverse [fonte: progetto Primelife D1.3.1].



L'identità online ha valore

La nostra identità ha valore, così come ognuna delle nostre identità parziali online. La nostra identità è preziosa non solo per noi ma anche per gli altri:

1. È un valore per l'individuo, perché la sua identità lo riflette e gli permette di accedere alle risorse che desidera.
2. In secondo luogo, è un valore per il fornitore di servizi che utilizza le caratteristiche dell'identità, ad esempio la banca o un sito di social networking, come Facebook. Sono i detentori delle risorse che vogliamo. La nostra identità è una risorsa aziendale per questi enti.
3. Infine, la nostra identità è utile ai ladri e ad altri utenti per accedere a risorse a cui non hanno diritto. Man mano che il valore delle nostre identità parziali cresce, l'informazione diventa più attraente per i ladri.

Il furto d'identità, in generale, è la perdita di controllo su una o più delle nostre identità parziali.

Poiché qualsiasi identità parziale online può contenere dati privati, è importante gestirli e proteggerli in modo appropriato.

Profilazione

La **profilazione** si riferisce all'uso di "sostanziosi pattern recognition", gli identificatori sopra menzionati, da parte di governi e aziende, che impiegano questa tecnica per prendere informazioni significative da enormi quantità di dati su individui o gruppi di persone, ad esempio a scopo di pubblicità mirata e servizi personalizzati nel caso delle imprese, o di polizia per la prevenzione e individuazione della criminalità, la lotta al terrorismo e nel caso dei governi per sorveglianza. La profilazione ruota attorno all'idea che grandi serie di dati raccolti casualmente su individui e gruppi di persone possano generare interessanti, sorprendenti e significative correlazioni che le macchine, con la loro capacità di calcolo, possono rilevare, mentre con le capacità umane non riusciamo.

Come suggerisce il nome, la profilazione può portare alla creazione di profili estesi, in cui le informazioni su individui o gruppi di individui sono memorizzate, archiviate e utilizzate per gli scopi citati sopra.

I rischi della profilazione

Molti dei rischi in Internet essere ridotti se, in particolare, i giovani preservassero la loro privacy online. Ciò richiede che siano più consapevoli delle conseguenze della divulgazione di informazioni identificative e determinassero quando è opportuno farlo. Sfortunatamente, molti giovani non riconoscono facilmente situazioni in cui divulgare informazioni potrebbe metterli a rischio.

Data la complessità dei dati stessi, assieme alla complessità dei modelli di comportamento umano possono verificarsi di "falsi positivi" nella profilazione (Rubinstein et al., 2008): il software trova correlazioni nei dati che sono ritenute significative, quando in realtà la correlazione è accidentale e casuale.

Inoltre, una delle preoccupazioni più serie che circondano la profilazione è *l'opacità* che la circonda. Spesso non è chiaro agli utenti di Internet quando, dove e per quali scopi vengono profilati. Inoltre, non è chiaro agli utenti in quali casi vengono presentate decisioni che si basano su processi di profilazione, o anche che questo possa succedere.

Questi profili possono quindi essere utilizzati per raggiungere le persone - sia adulti che bambini! - con offerte commerciali, senza che queste persone se ne accorgano, o quali



profili o tracce digitali siano state utilizzate per le raccomandazioni ricevute. Soprattutto nel caso dei bambini è un problema serio.

Molti giochi online per bambini, ad esempio, abbondano di consigli sui prodotti in modo nascosto (o meno) realizzati sulla base delle azioni dei bambini all'interno del gioco o anche al di fuori del gioco, ad esempio quando hanno collegato il loro profilo del gioco al loro profilo su piattaforme di social media come Facebook. Poiché tali raccomandazioni possono essere personalizzate, in base alla profilazione, l'attrazione per acquistare i prodotti offerti può essere molto più grande per questi bambini. Questo può attirare i bambini, a volte fin dai primi anni, in mondi commercializzati in cui l'obiettivo è quello di vendere il maggior numero possibile di prodotti, mentre i bambini stessi non ne sono consapevoli.

Tracciamento web

In questa sezione spiegheremo che cos'è il monitoraggio web e otterremo informazioni migliori sui suoi tipi. Il **Web tracking** è l'attività (e abilità) di un sito web (utilizzando speciali strumenti software) per controllare i visitatori del sito web.

Esistono molti modi in cui le aziende possono utilizzare per tenere traccia del comportamento di navigazione sui siti Web. Questi includono:

Cookies: questi sono piccoli pezzetti di testo che vengono scaricati nel nostro browser mentre navighiamo sul web. Il loro scopo è memorizzare alcune informazioni utili sulla nostra interazione con il sito Web che li imposta. Contrariamente a quanto si crede, i cookie non contengono programmi software, quindi non viene installato nulla su un computer. I cookie generalmente non contengono alcuna informazione che possa identificare una persona. Di solito contengono una stringa di testo o "identificatore univoco". Questo agisce come un'etichetta. Quando un sito web vede la stringa di testo impostata in un cookie, sa che il browser è quello utilizzato precedentemente. I cookie che sembrano causare le maggiori controversie sono utilizzati per la gestione della pubblicità che vediamo su un sito web. Questi cookie possono registrare quando e dove abbiamo visto un annuncio, dove potremmo essere stati quando è successo e se abbiamo cliccato su di esso. Il cookie invierà queste informazioni al proprietario del cookie, che registra questi dati e li utilizza per assicurarsi che non vedremo la stessa pubblicità troppe volte.

Flash cookie: conosciuti anche come "oggetti localmente condivisi". Queste sono informazioni che Adobe Flash potrebbe memorizzare sul nostro computer. Questi sono progettati per salvare dati come le preferenze del volume del video o, forse, i nostri punteggi in un gioco online.

Log del server: quando carichiamo una pagina su un sito Web, stiamo facendo una richiesta al server di quel sito. Questo server registrerà il tipo di richiesta che è stata fatta e memorizzerà informazioni quali: indirizzo IP (che consentirà ai proprietari di siti Web di dedurre la posizione), la data e l'ora in cui il browser ha caricato la pagina, quale pagina è stata caricata e quale sito o pagina il browser era collegato prima che arrivasse a quella pagina (referrer). I registri del server costituiscono la base per l'analisi dei dati Web e possono essere visualizzati solo dai proprietari del sito Web.

Web beacon: si tratta di piccoli oggetti incorporati in una pagina Web, ma non visibili. Possono anche essere conosciuti come "tag", "bug di tracciamento", "pixel tracker" o "pixel gif". Questi sono molto



utili per le aziende che vogliono sapere se i lettori stanno aprendo le e-mail che inviano. Quando il web beacon viene caricato, le aziende possono dire chi ha aperto l'email e quando. Spesso gli inserzionisti incorporano i web beacon nelle loro inserzioni per farsi un'idea di quanto spesso appare un annuncio.

Cosa viene raccolto attraverso il monitoraggio web e perché?

I tracker raccolgono informazioni su quali siti web stiamo visitando, nonché informazioni sui nostri dispositivi.

Un tracker potrebbe essere utilizzato per dare al proprietario del sito informazioni dettagliate sul traffico del suo sito web, ma il resto appartiene a società il cui obiettivo principale è quello di costruire un profilo di chi siamo: quanti anni abbiamo, dove viviamo, cosa leggiamo e ciò che ci interessa. Queste informazioni possono quindi essere confezionate e vendute ad altri: inserzionisti, altre società o governi.

Le aziende che raccolgono i dati e effettuano il monitoraggio non sono correlate al sito web che stiamo visitando. Chiamati "data brokers", tendono ad avere nomi validi per il mercato azionario come DoubleClick, ComScore e cXense (sebbene DoubleClick sia effettivamente di proprietà di Google). La loro intera attività è basata sulla vendita di "dati dei clienti".

Ci sono anche aziende note che effettuano il tracciamento. In alcuni casi in modo anche evidente: il pulsante rosso G+ di Google, ad esempio, è un tracker; il pollice "mi piace" di Facebook è un tracker; e il piccolo uccellino azzurro di Twitter è anche un tracker.

Rilevamento della posizione

Il rilevamento della posizione fornisce un'informazione molto dettagliata di chi siamo, dove andiamo e con chi trascorriamo il tempo. È possibile vedere come viene tracciata la nostra posizione attraverso il nostro telefono, le nostre connessioni wifi, i siti Web che visitiamo, le piattaforme di social media e i provider di posta elettronica che utilizziamo.

I nostri dispositivi - computer, telefoni cellulari e tablet - dicono costantemente agli altri dove siamo. **Il nostro telefono cellulare** in particolare è un dispositivo di tracciamento molto efficace: dove andiamo e registra la nostra posizione per tutto il tempo, anche quando non siamo connessi a Internet.

Le informazioni sulla posizione raccolte nel tempo possono raccontare una storia sorprendentemente completa su chi siamo e come appare la nostra vita. Aggiungiamo indirizzi, tweet, foto e/o i nostri dati telefonici pubblicamente disponibili, e la storia diventa molto dettagliata.

I dati sulla posizione possono anche essere utilizzati per mappare le nostre relazioni con gli altri. Se noi e un'altra persona, o altre persone, siamo nello stesso posto in momenti specifici della giornata, è possibile dedurre quali relazioni abbiamo con queste persone - se, ad esempio, sono collaboratori, amanti, coinquilini o membri della famiglia. Questo tipo di immagine dettagliata può essere utile a tutti i tipi di persone e organizzazioni. Può essere venduto dalle aziende per fare soldi; può anche essere usato per prevedere dove saremo in un determinato punto in futuro.



Se sul nostro telefono sono attivate le informazioni sulla posizione per le immagini, queste informazioni verranno incorporate nell'immagine (ad esempio i metadati dell'immagine includeranno dove abbiamo scattato l'immagine). Quando inviamo o carichiamo queste immagini, possiamo condividere i nostri dati sulla posizione senza pensarci. La maggior parte dei fornitori di social media estrae i dati sulla posizione quando carichiamo l'immagine, ma ci sono ancora molti modi in cui i dati sulla posizione possono essere aggregati dalle immagini che condividiamo.

Raccomandazioni

Raccomandazioni per la privacy dei dati

Le norme UE sulla protezione dei dati, note anche come regolamento generale sulla protezione dei dati (o GDPR) dell'UE, descrivono diverse situazioni in cui un'azienda o un'organizzazione possono raccogliere o riutilizzare le informazioni personali⁸:

1. Quando è consentita l'elaborazione dei dati?

Una società o un'organizzazione è autorizzata a raccogliere o riutilizzare le informazioni personali:

- Quando è presente un contratto - ad esempio un contratto per la fornitura di beni o servizi (ad esempio quando acquisti qualcosa online) o un contratto di lavoro dipendente
- Quando stanno rispettando un obbligo legale - ad esempio, quando l'elaborazione dei dati è un requisito legale, ad esempio quando il datore di lavoro fornisce informazioni sul salario mensile all'autorità di sicurezza sociale, in modo da avere copertura di sicurezza sociale
- Quando l'elaborazione dei dati è negli interessi vitali - per esempio, quando ciò potrebbe proteggere la vita
- Quando si deve completare un compito pubblico - principalmente in relazione ai compiti delle amministrazioni pubbliche come scuole, ospedali e comuni
- Quando vi sono interessi legittimi, ad esempio se la banca utilizza i dati personali per verificare se si è idonei per un conto di risparmio con un tasso di interesse più elevato.

2. Accettazione del trattamento dei dati - consenso

Quando un'azienda o un'organizzazione richiedono il proprio consenso, è necessario intraprendere un'azione chiara in tal senso, ad esempio firmando un modulo di consenso o selezionando sì da un'opzione sì/no chiara su una pagina Web.

Non basta semplicemente opt-out, ad esempio selezionando un box in cui si dice che non si desidera ricevere e-mail di marketing. Devi accettare che i tuoi dati personali vengano archiviati e/o riutilizzati per questo scopo.

Dovresti inoltre ricevere le seguenti informazioni prima di decidere di aderire:

- informazioni sulla società/organizzazione che tratterà i tuoi dati, inclusi i dettagli di contatto e i dettagli del Data Protection Officer (DPO) se ce n'è uno
- il motivo per cui la società/organizzazione utilizzerà i tuoi dati personali
- per quanto tempo intendono conservare i tuoi dati personali

⁸https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm



- i dettagli di qualsiasi altra società o organizzazione che riceverà i tuoi dati personali
- informazioni sui tuoi diritti di protezione dei dati (accesso, correzione, cancellazione, reclamo, ritiro del consenso)

Tutte queste informazioni dovrebbero essere presentate **in modo chiaro e comprensibile**.

3. Regole specifiche per i bambini

Se i figli desiderano utilizzare servizi online, come i social media, scaricare musica o giochi, avranno spesso bisogno dell'approvazione del genitore o tutore legale, in quanto questi servizi utilizzano i dati personali del minore. Il bambino non avrà più bisogno del consenso dei genitori una volta che hanno più di 16 anni (in alcuni paesi dell'UE questo limite di età potrebbe essere basso come 13). I controlli per verificare il consenso dei genitori devono essere efficaci, ad esempio utilizzando un messaggio di verifica inviato all'indirizzo email di un genitore. Vedi il modulo 1 per una legislazione specifica nei paesi dei partner.

4. Accesso ai dati personali

Puoi richiedere l'accesso ai dati personali che un'azienda o un'organizzazione ha e hai il diritto di ottenere una copia dei dati, gratuitamente, in un formato accessibile. Dovrebbero rispondere entro 1 mese e dover fornire una copia dei dati personali e qualsiasi informazione pertinente sul modo in cui i dati sono stati utilizzati o in uso.

5. Eliminazione dei dati personali (il diritto all'oblio)

Se i tuoi dati personali non sono più necessari o vengono utilizzati illegalmente, puoi chiedere che i tuoi dati vengano cancellati. Questo è noto come "il diritto all'oblio".

Queste regole si applicano anche ai motori di ricerca, come Google, in quanto sono considerati anche controller di dati. Puoi chiedere i link alle pagine web incluso il tuo nome possa essere rimosso dai risultati del motore di ricerca, se le informazioni sono imprecise, inadeguate, irrilevanti o eccessive.

Se un'azienda ha reso disponibili online i tuoi dati personali e chiedi che vengano cancellati, l'azienda deve anche informare qualsiasi altro sito web in cui sono stati condivisi, i dati che hai richiesto e i collegamenti da eliminare.

Per proteggere altri diritti, come la libertà di espressione, alcuni dati potrebbero non essere cancellati automaticamente. Ad esempio, affermazioni controverse fatte da altre persone, potrebbero non essere cancellate se per interesse pubblico è meglio tenendoli online.

Consigli pratici

Come proteggere la tua identità online

Anche se non siamo in grado di controllare tutto ciò che è noto su di noi online, ci sono dei passi che possiamo compiere per capire meglio le nostre identità online e avere il potere di condividere ciò che vogliamo, quando vogliamo. Questa sezione ha lo scopo di aiutarci a gestire meglio la nostra identità online⁹.

⁹ More information on the issue can be found at the Internet Society tutorials: <https://www.internetsociety.org/tutorials/manage-our-identity/>



Questi sono alcuni consigli pratici che ci aiutano ad evitare di divulgare informazioni personali sensibili a individui o entità che intendono sfruttarli.

1. **Aggiungere plug-in al browser web:** i plug-in hanno la possibilità di controllare i siti Web e avvisarci di quelli noti che potrebbero essere dannosi.
2. **Proteggere la password.**
 - ❖ **Se una password è facile da indovinare**, allora è facile da rubare. **Selezionare le password che si può facilmente ricordare, ma che non sono facili da indovinare per le altre persone.** Prestare particolare attenzione a scegliere password diverse e difficili da indovinare per ciascuno dei siti Web che sono particolarmente importanti per noi, come i servizi finanziari online.
 - ❖ **Evitare di utilizzare la stessa password** per più siti Web, quindi se un sito Web viene compromesso, le nostre credenziali rubate non possono essere utilizzate su altri siti. Se vogliamo selezionare le password simili per renderle facili da ricordare, prova a personalizzare la password per ciascun sito aggiungendo alcuni caratteri (come il nome del sito). Questo potrebbe non ingannare un attaccante esperto, ma eviterà ad altri di provare la password su altri siti web. Il principio è quello di avere un atteggiamento pratico e proteggersi dagli attacchi più probabili.
 - ✓ **Utilizza l'autenticazione a due fattori:** se la nostra banca o altri importanti fornitori di servizi offrono questo, a meno che la nostra banca non accetti di assumersi tutte le responsabilità nel caso in cui la nostra password sia compromessa. Le reimpostazioni della password hanno lo scopo di aiutarci quando abbiamo perso una password (o sono state bloccate). Ogni sito web ha una modalità leggermente diversa per reimpostare una password. Ecco i passaggi più comuni seguiti per reimpostare le password.
 - ✓ **Durante il ripristino della nostra password**, ci viene chiesto di rispondere ad alcune domande di "sicurezza" personali che abbiamo precedentemente impostato. Potremmo ricevere un'e-mail con un link che consente il reset o una nuova password potrebbe semplicemente essere inviata per e-mail. Per i siti Web che utilizzano domande di sicurezza per convalidare la nostra identità, utilizzare informazioni personali (che lo rendono facile da ricordare) in modi che sono difficili da indovinare. Ad esempio, se la domanda richiede il nome della prima scuola che hai frequentato o il nome della prima strada in cui hai vissuto, rispondi con la seconda scuola che hai frequentato o la seconda strada in cui hai vissuto. In questo modo, anche chi conosce molto su di noi avrà difficoltà a rispondere alle domande. Inoltre, ricorda che non dobbiamo dare risposte "logiche", a patto che abbiano senso per noi e siano importanti per noi. Ad esempio, se la domanda di sicurezza chiede "Qual è il nostro colore preferito", non c'è niente che ci impedisca di dare "tre", o "gli occhi di Monica" come risposta e sarà molto più difficile da indovinare per un aggressore.
3. **Protezione dell'e-mail:** ecco alcuni suggerimenti che possiamo adottare per proteggere la nostra posta elettronica, che aiuta a proteggere la nostra identità online
 - ❖ **Seleziona saggiamente gli indirizzi email**
 - ❖ **Seleziona diversi indirizzi email** per ciascuno dei nostre identità: quando disponiamo di più identità online, come professionisti, personali e accademici, seleziona un indirizzo email diverso per ciascuno. Scegliere con cura l'identità giusta quando qualcuno chiede il nostro indirizzo email può prevenire problemi in seguito. Ad



esempio, la nostra email di lavoro o di scuola potrebbe non essere molto privata se la società o l'istituzione rivendica il diritto di leggere o archiviare la posta elettronica sui propri server.

- ❖ **Utilizzare l'autenticazione a 2 fattori** ovunque sia possibile. Combina diverse tecniche di autenticazione per rendere più difficile per un utente malintenzionato compromettere l'intero processo di autenticazione. Ad esempio, può combinare "qualcosa che conosciamo" (come una password) e "qualcosa che abbiamo" (come un telefono - che significa anche che il processo di autenticazione può fare uso di due metodi di comunicazione separati). Questo tipo di autenticazione a 2 fattori funziona come segue: prima inseriamo la nostra password. Un secondo codice viene quindi inviato al nostro telefono. Solo dopo averlo inserito, abbiamo accesso al nostro account. Per sovvertire il processo di autenticazione, un utente malintenzionato deve ora non solo conoscere la nostra password, ma anche essere in grado di intercettare un messaggio separato, in tempo reale, inviato al nostro telefono.

Il sito Web di Online Trust Alliance all'indirizzo <https://otalliance.org/> contiene un elenco di risorse per aiutarci a conoscere meglio le tecnologie che possono aiutare a proteggere la nostra identità su Internet.

Come ci rintracciano su Internet

Per vedere chi ci sta seguendo possiamo usare:

- ❖ [Lightbeam](#): Lightbeam è un componente aggiuntivo di Firefox che mostra quali terze parti sono presenti quando visitiamo un sito Web. Se poi visitiamo un nuovo sito web, Lightbeam mostrerà non solo quali terze parti sono attive su quel sito, ma quali terze parti hanno visto noi su entrambi i siti; e così via mentre visitiamo altri siti web.

Possiamo installarlo tramite il menu principale di Firefox, oppure andare su [Lightbeam](#) -> **aggiungere a Firefox**

Per avviarlo, fai clic sull'icona Lightbeam nella parte superiore del browser -> naviga su Internet per un po' -> controlla la visualizzazione.

- ❖ [Trackography](#) (progetto tecnologico tattico): i siti Web di notizie sono una grande fonte di informazioni su di noi. Quali riviste leggiamo e quali articoli, possono memorizzare molte informazioni sulle nostre opinioni politiche, interessi generali e persino sulla nostra sessualità o affiliazioni religiose. [Trackography](#) ci permette di vedere chi ci sta seguendo quando leggiamo le notizie online - tra le altre cose, come i paesi in cui i nostri dati attraversano lungo il percorso.

Vai a [Trackography](#) -> *seleziona il nostro paese* -> *seleziona i media che leggiamo* -> guarda quante aziende ci stanno monitorando senza che noi ce ne accorgiamo. Se facciamo clic su una società specifica, possiamo anche saperne di più sulla loro politica sulla privacy.



How to protect ourselves from web tracking

Per avere maggiore controllo sui nostri dati, possiamo prendere le seguenti misure:
Cambia le impostazioni per aumentare la nostra privacy mentre navighiamo su Internet e utilizziamo i social media

- **Firefox:** <https://myshadow.org/how-to-increase-our-privacy-on-firefox>
- **Chrome:** <https://myshadow.org/how-to-increase-our-privacy-on-chrome>
- **Twitter:** <https://myshadow.org/how-to-increase-our-privacy-on-twitter>

Installa componenti aggiuntivi / estensioni per bloccare i tracker

Esistono alcuni tipi di software molto efficaci che possiamo installare per bloccare i tracker, crittografare le connessioni del nostro sito Web o interrompere l'attivazione degli annunci, il che può fare una grande differenza per la nostra privacy. Spesso è una buona idea usare più di uno strumento per affrontare gli stessi problemi di privacy.

Ogni strumento utilizza una tecnica diversa per bloccare i tracker e alcuni potrebbero influire sulla nostra esperienza di navigazione. L'approccio migliore è provarli e trovare il mix che funziona per noi.

- **Privacy Badger:** [Install Privacy Badger from website](#) (Firefox, Chrome)
- **Adblock Plus:** [Install Adblock Plus from website](#) (Firefox, Chrome, Opera, IE, Safari, and others)
- **Disconnect:** [Install from the Disconnect website](#)
- **HTTPS Everywhere:** [Install HTTPS Everywhere from website](#) (Firefox, Chrome, Opera)
- **NoScript:** [Install NoScript from website](#) (Firefox)

Migliori pratiche

- ❖ **SAFER INTERNET CENTRES** hanno sviluppato varie risorse educative volte ad aiutare insegnanti, genitori e formatori, bambini e giovani, a trovare le risorse online in modo sicuro. Si può accedere a queste risorse tramite questa [resource gallery](#).
- ❖ **SAFER INTERNET DAY RESOURCES:** Safer Internet Day (SID) 2018 si è svolto martedì 6 febbraio 2018 con il tema "Creare, connettere e condividere rispetto: una migliore connessione Internet inizia con te". Puoi trovare un elenco delle risorse - da tutta la rete Insafe di Safer Internet Centers - per aiutarti a celebrare il SID nella tua scuola ... e in effetti promuovere un internet più sicuro e migliore per tutto l'anno! Cerca per parola chiave o lingua per trovare risorse per le tue esigenze, o semplicemente sfoglia l'elenco [qui](#).



Modulo 4: Lavorare con i giovani

“Sii te stesso, trova la tua strada. Conosci te stesso prima di cercare di conoscere i bambini. Realizza ciò di cui sei capace (...). Tu sei l'unico bambino che devi incontrare, educare ed educare prima di tutto”

Un tale consiglio è stato dato agli educatori dall'eccezionale insegnante polacco Janusz Korczak. Queste indicazioni possono applicarsi agli educatori che lavorano con i bambini, ma si può anche riferirsi ai formatori, educatori e insegnanti giovanili. Conoscere se stessi, lavorare sulle proprie debolezze e sviluppare i propri punti di forza e, soprattutto, l'autenticità consentirà un lavoro efficace con i giovani.

Il lavoro con i giovani differisce dal lavorare con i bambini o con gli adulti. È collegato al costante confronto con la ribellione adolescenziale, con forti emozioni, ma anche con la capacità di imparare velocemente e ricordare. Se un educatore riesce a conquistare la fiducia dei giovani e li incoraggia a lavorare insieme, può fare molto per se stesso, per i suoi alunni e intere comunità.

Una breve descrizione della gioventù come gruppo sociale.

Per parlare di insegnamento ai giovani, dobbiamo pensare a chi intendiamo quando diciamo i giovani. I ricercatori non sono d'accordo sulla definizione di gioventù e giovinezza, e anche dell'età che potrebbe determinare una persona nella categoria della gioventù. Di norma, la categoria degli adolescenti comprende persone di età compresa tra gli 11 e i 21 anni, sebbene il limite superiore sia spesso spostato anche a 30 anni. Tuttavia, il criterio biologico dell'età non è sufficiente per definire i giovani.

I ricercatori che si occupano di problemi giovanili sottolineano la natura transitoria di questo periodo della vita. Serve l'adozione di determinati ruoli vitali e l'acquisizione di competenze per definirli. Allo stesso tempo, è un periodo molto turbolento in cui un individuo sta lottando con la maturazione biologica e la ricerca di identità. Questo è associato a confusione e ansia. I giovani partecipano con entusiasmo ai gruppi su idee o dottrine, sono inclini all'indottrinamento e alla sperimentazione di diverse ideologie. Cercano anche guide tra gli adulti e respingono le autorità. Il periodo della gioventù è il tempo dei conflitti interni ed esterni. Tentativi di definire se stessi e il mondo intorno a se. I giovani costruiscono la loro visione del mondo, determinano quali standard e valori vogliono che siano guide nelle loro vite. Diventano indipendenti dalla famiglia e acquisiscono abilità sociali. Nonostante molte caratteristiche comuni, i giovani sono una categoria eterogenea. Le differenze nascono dal contesto sociale e culturale in cui i giovani sono inseriti e dalle caratteristiche individuali.

Regole per lavorare con i giovani.

Si possono incontrare diverse difficoltà nel lavorare con i giovani, compresa la resistenza ad essere coinvolti, la mancanza di fiducia. Queste difficoltà possono essere contrastate applicando diversi principi:

- Ascoltare i giovani, trattarli alla pari.
- Includere i giovani in tutte le fasi del lavoro - dalla pianificazione, all'implementazione, alla valutazione.
- Usare un linguaggio che tutti possano capire.



- Organizzare incontri in luoghi dove si incontrano altri giovani conosciuti e amichevoli, ad esempio nei centri culturali.
- Creare un'atmosfera di reciproco rispetto e amicizia e, soprattutto, assicurarsi che tutti si sentano al sicuro.

I giovani sono molto più propensi a impegnarsi in attività che suscitano la loro curiosità, si avvicinano ai loro interessi, incoraggiano l'attività fisica, sono ricche di stimoli colorate, illustrate, dipinte, profumi, suoni/musica. È anche importante definire chiaramente lo scopo per cui i giovani potrebbero essere coinvolti. L'obiettivo deve essere coerente con i bisogni e le capacità dei partecipanti, altrimenti il gruppo non vorrà partecipare.

Motivazione interna

Il lavoro con i giovani dovrebbe essere basato sulla stimolazione della motivazione interna, che è una forza che spinge le persone ad agire nonostante la mancanza di ricompense. Parliamo di motivazione interna quando facciamo qualcosa, perché ci rende felici, ci dà un senso di soddisfazione e ci permette di imparare in ambiti che sono importanti per noi. L'attività intrapresa è di per sé una ricompensa. Questo tipo di motivazione favorisce l'impegno e la creatività, motivo che vale la pena di sviluppare nei giovani.

Fattori che aumentano la motivazione interna:

- **Curiosità** - i giovani sono più desiderosi di imparare ciò che è interessante per loro.
- **Senso di decisione** - i giovani sono più disposti a farsi coinvolgere se hanno l'opportunità di scegliere e avere una reale decisione su ciò che stanno facendo.
- **Riconoscimento** - i complimenti usati con saggezza hanno l'effetto di rafforzare la motivazione interna, ma troppo spesso ha l'effetto opposto.
- **Cooperazione** - i giovani collaborano volentieri tra di loro, si ispirano a vicenda e si incoraggiano ad agire.
- **Competizione** - il desiderio di confrontare i risultati con quelli degli altri può essere fonte di motivazione interna. Tuttavia, se le discrepanze tra i risultati sono molto grandi, la motivazione diminuisce.
- **Sfide** - definire chiaramente l'obiettivo e la capacità di tracciare il livello della propria realizzazione favorisce lo sviluppo della motivazione interna. L'obiettivo dovrebbe essere raggiungibile, ma richiede uno sforzo e, soprattutto, dovrebbe essere coerente con i valori e le aspirazioni di una determinata persona.
- **Piacere** - se un'attività ci dà piacere, non solo la facciamo più volentieri, ma ricordiamo anche di più.

L'elemento più importante dell'apprendimento per i giovani è l'esperienza. I giovani dovrebbero, se possibile, usare le proprie conoscenze e abilità per apprendere nuove cose e acquisire nuove abitudini. Tuttavia, se le conoscenze e le competenze esistenti sono insufficienti, l'insegnante o il formatore dovrebbe agire come un esperto e fornire le conoscenze. Gli studenti, tuttavia, dovrebbero avere l'opportunità di verificarle con un compito pratico.

Apprendimento cooperativo

L'apprendimento basato sulla cooperazione di gruppo in un'atmosfera di reciproco rispetto e amicizia favorisce l'apprendimento, per questo è un metodo efficace. Tuttavia, vale la pena organizzare i



partecipanti in gruppi in modo ponderato. Va ricordato che risultati migliori, sia nello sviluppo dei singoli membri che dell'intero gruppo, viene svolto nei gruppi più diversificati. In modo ottimale, i gruppi dovrebbero essere composti da quattro persone, in modo che durante un determinato compito possano lavorare in coppia, e dopo un po', tornare alla discussione con l'intero gruppo. Se la specificità del compito lo consente, vale la pena chiedere ai partecipanti di assegnare ruoli (ad esempio una persona che prende appunti, una persona responsabile dei materiali, un controllore, ecc.) In modo che nessuno rimanga passivo. Gli esercizi possono anche essere suddivisi in fasi e chiedere ai singoli studenti di guidarne l'implementazione (ad es. Fase I - discussione e brainstorming, fase II - traduzione delle questioni discusse in obiettivi e attività, fase III - presentazione dei risultati).

Pianificazione della formazione per i giovani

Diagnosi

Un elemento molto importante della pianificazione del lavoro con i giovani è il riconoscimento dei loro bisogni di formazione. Se non li conosciamo, non sapremo se il programma, gli strumenti e le tecniche che pianificheremo saranno appropriati ed efficaci.

Al fine di conoscere correttamente i bisogni dei giovani, dovrebbero essere coinvolti ad esempio: scuole, istituzioni locali, governi locali, nonché i giovani stessi. Osservando i bisogni dei giovani da diverse prospettive, avremo una migliore possibilità di riconoscere con precisione i problemi reali.

Non è sufficiente chiedere quale formazione e quanta i giovani vogliono. Bisogna essere curiosi, non fermarsi a una domanda, ma esplorare l'argomento e cercare le cause nascoste dello stato esistente. Il metodo "5 Perché" può essere utilizzato per questo scopo. Il primo elemento di questo metodo è raccogliere quante più informazioni possibili su un dato problema. Esempi di domande attraverso cui possiamo trovare le risposte:

- Qual è la situazione? Cosa sta succedendo?
- Da quando appare così? Qualcosa è cambiato? È mai stato diverso?
- Qual è la scala del problema? Quante persone sono interessate?
- Quali saranno le conseguenze se non cambierà nulla?

Quindi determinare chi può aiutarci a cercare la causa del problema. È possibile utilizzare il metodo di brainstorming per questo scopo. Una volta che sai come si presenta il problema e chi chiederne le cause, puoi procedere allo stadio appropriato del metodo "5 Perché", cioè chiedere "perché?". Per conoscere la vera causa del problema, la domanda "perché" dovrebbe essere richiesta in media 5 volte, ad es.

Problema: i giovani non partecipano alle attività delle istituzioni culturali locali.

1. Perché i giovani non partecipano alle attività delle istituzioni culturali locali?
Perché loro non vogliono.
2. Perché i giovani non sono disposti a partecipare alle attività delle istituzioni culturali locali?
Perché preferiscono trascorrere del tempo a casa davanti a un computer.
3. Perché gli adolescenti preferiscono passare il tempo davanti al computer?
Perché hanno paura di costruire relazioni nel mondo reale.
4. Perché gli adolescenti hanno paura di costruire relazioni nel mondo reale?



Perché valutano poco le loro relazioni sociali.

5. Perché valutano poco le loro relazioni sociali?

Perché raramente hanno l'opportunità di allenare queste abilità..

Nel caso precedente, la soluzione potrebbe essere quella di coinvolgere i giovani in attività che consentano lo sviluppo di abilità interpersonali, inizialmente in piccoli gruppi.

Un principio importante nella diagnosi dei bisogni è quello di evitare una semplice categorizzazione. Nel caso di cui sopra, la prima cosa è la divisione tra giovani attivi e inattivi, ma forse i giovani inattivi in alcune aree sono disposti a prendere l'iniziativa e trovare le soluzioni. Dopo aver fatto più domande, una tale divisione può essere fuorviante.

Quando diagnostichi i bisogni dei giovani, vale la pena utilizzare metodi diagnostici attrattivi e interessanti che richiedano la partecipazione dei soggetti, non solo le risposte alle loro domande. Tali metodi possono essere camminare, mappare l'attività, giocare, fare un workshop. Una diagnosi attraente può essere un incentivo per i giovani a partecipare alle lezioni in seguito.

La diagnosi dovrebbe essere completata con una relazione che dovrebbe essere breve, comprensibile a tutti, attraente e disponibile per gli interessati.

La parte iniziale della formazione

Dopo la diagnosi è necessario eseguire le attività previste e completarle. È necessario formulare gli obiettivi di queste attività. I giovani sono allora più disposti a mettersi in gioco, a conoscersi. Quando si pianifica un'azione, si dovrebbero affrontare i bisogni, nonché le possibilità e le caratteristiche di attuazione in base all'età, al luogo di residenza e agli interessi. Su questa base, determina le classi, il tempo e il luogo, quindi pianifica la costituzione della classe.

La classe o le classi dovrebbero iniziare a conoscersi e creare un'atmosfera di fiducia e amicizia. Questo può essere aiutato da giochi di integrazione e dai cosiddetti rompighiaccio. Si tratta di giochi che consentono ai partecipanti e ai giovani lavoratori di imparare qualcosa su se stessi, superare la timidezza e incoraggiare la cooperazione. Nella parte iniziale della formazione, vale anche la pena di determinare lo scopo delle classi e la loro struttura.

Un elemento importante del corso è definire le regole che tutti i partecipanti e i referenti seguiranno. Può essere utile un contratto concordato e firmato da tutti. Aiuta a evitare varie situazioni imbarazzanti nella formazione. Poiché ai giovani piace decidere autonomamente e influenzare ciò che accade intorno a loro, è meglio abbandonare l'imposizione autoritaria di principi che devono essere rispettati. L'insegnante può incoraggiare i partecipanti a presentare proposte sulla regolamentazione, porre domande di orientamento o organizzare discussioni. Sulle regole stabilite nel contratto, tutti i partecipanti devono essere d'accordo, e per dimostrarlo, vale la pena firmarlo. Il contratto dovrebbe essere appeso in un luogo visibile e dovrebbe rimanere fino alla fine della formazione o di un ciclo di formazione. In situazioni critiche, il formatore può fare riferimento alle regole stabilite. Se durante la formazione risulta che nel contratto manca qualche regola, con il consenso dell'intero gruppo, possono essere aggiunte. Inoltre, è possibile cancellare una qualsiasi delle regole salvate se risulta essere difficile da rispettare e se tutti i partecipanti vorranno cancellarla. Il contratto può essere aggiornato in ogni fase della formazione, a condizione che tutte queste modifiche siano accettate.



La parte rilevante della formazione

Una volta che i partecipanti e il formatore hanno familiarità reciproca, l'obiettivo del corso è chiaro a tutti, quali argomenti saranno discussi e quando ci sono pause e tutti accettano il contratto di formazione, è possibile procedere con la parte rilevante del corso.

Quando si organizza un programma di lezioni, è necessario tenere a mente come i giovani apprendono e fornire loro una varietà di stimoli e attività.



I singoli moduli sono chiaramente separati l'uno dall'altro. Le persone ricordano meglio ciò che è all'inizio e alla fine - i problemi più importanti dovrebbero essere in queste parti. I docenti dovrebbero quindi fare molti "inizi" e "fine" attraverso rotture e riassunti pianificati in modo appropriato di singoli lotti di materiali.

È una buona idea introdurre molte attività nella parte giusta del training, perché l'attività migliora il funzionamento del cervello. Se si utilizza il metodo della lezione, vale la pena di creare piccoli distanziatori ogni 8-10 minuti. Può essere una domanda per i partecipanti, uno scherzo o un breve esercizio.

Scopo della formazione e valutazione

Ogni training o altra forma di corso dovrebbe avere le sue conclusioni e il suo sommario. Serve per organizzare le conoscenze. Alla fine di ogni lezione vale la pena raccogliere le opinioni dei partecipanti sulla loro soddisfazione. Comunque, non fermarsi alle valutazioni soggettive, perché non esplicano se gli obiettivi della formazione sono stati raggiunti. Pertanto, è necessario prendere in considerazione altre forme di valutazione. Il modo più semplice è quello di verificare le conoscenze, ma probabilmente a nessun adolescente piacciono i test. Una soluzione migliore consiste nel verificare se i partecipanti sono in grado di utilizzare le conoscenze acquisite in un compito pratico. È inoltre possibile condurre interviste individuali o di gruppo o invitare i partecipanti al processo educativo a partecipare alle relazioni di sintesi. Le domande della valutazione devono essere presentate sotto forma di relazione scritta.



Riferimenti

- American Library Association. (2002). The Children's Internet Protection Act.
<http://www.ala.org/cipa/>
- Bell, Vicki and Denise de la Rue. n.d, Gender harassment on the Internet.
<http://www.gsu.edu/~lawppw/lawand.papers/harass.html>
- Belsey. (2006). Cyberbullying: An emerging threat to the “always on” generation. Available at
<http://www.cyberbullying.ca>
- Biegel, Stuart. (1996). Constitutional issues in cyberspace: Focus on 'community standards'. *Los Angeles Daily Journal*, February 22, <http://www.gseis.ucla.edu/iclp/feb96.html>
- Cyber-stalking.net. (2002). Statistics. <http://www.cyber-stalking.net/statistics.htm>
- Dixon, S., Craven, E., Hayley, C., Weber, S. (2017). Preventing and eliminating cyberviolence initiative: Needs assessment findings. Atwater Library and Computer Centre. Montreal, QC. Retrieved July 13,
- Egan, Jennifer. (2000) Out in cyberspace. *The New York Times Magazine*, December 10, 2000.
- Finkelhor, David, Kimberly Mitchell, and Janis Wolak. (2000). Online victimization: A report on the nation's youth. <http://www.missingkids.com/download/nc62.pdf>
- Herring, Susan C. 2001. Gender and power in online communication. *Center for Social Informatics Working Papers*. <http://www.slis.indiana.edu/csi/WP/WP01-05B.html>
- Kiesler, Sara, Jane Siegel and Timothy W. McGuire. (1984). Social psychological aspects of computer-mediated communication. *American Psychologist* 39: 1123-1134.
- Magid, Lawrence. (2000). When kids surf, think safety first. *San Jose Mercury News*, June 17.
- McRae, Shannon. (1996). Coming apart at the seams: Sex, text and the virtual body. In L. Cherny and E.R. Weise (eds.), *Wired_women*, 242-263. Seattle: Seal Press.
- Mc Guckin C, Cummins PK, Lewis CA. (2010). Cyberbullying among children in Northern Ireland: Data from the Kids Life and Times surveys. *Psychology, Society, & Education*.
- Mc Guckin, C. (2013). School bullying amongst school pupils in Northern Ireland: How many are involved, what are the health effects, and what are the issues for school management?
- Office for Internet Safety (2008) A Guide to Internet Safety for Children. Available at
<http://www.internetsafety.ie/website/ois/oisweb.nsf/page/286BBF5D3E55C002802574C10036C6CB>
- Office for Internet Safety (2012) Get With It – A guide to cyberbullying. Understanding and identifying cyberbullying to help protect your children. Available at
[http://www.internetsafety.ie/website/ois/oisweb.nsf/page/7C7F45450A4CDC2B80257514004B6B10/\\$file/GWIT_Cyberbullying_Dec12.pdf](http://www.internetsafety.ie/website/ois/oisweb.nsf/page/7C7F45450A4CDC2B80257514004B6B10/$file/GWIT_Cyberbullying_Dec12.pdf)
- Olweus, D. (1993). Oxford: Blackwell.
- Olweus, D. (1999). Sweden, i P.K. Smith mfl. (red.) The nature of school bullying. A cross-national perspective. Routledge: London.
- O' Moore, M. (2010). Dublin: Veritas. Understanding school bullying. A guide for parents and teachers
- O'Moore, M. og Kirkham, C. (2001). Self-esteem and its relationship to bullying behaviour, *Aggressive Behavior*
- O'Moore & P. Stevens (Eds.), *Bullying in Irish education: Perspectives in research and practice*. Cork, Ireland
- O'Moore, M. (2012). Cyber-bullying: the situation in Ireland. *Pastoral Care in Education*.



- Pfaffenberger, Brian. (1997). "If I want it its OK": Usenet and the (outer) limits of free speech. *The Information Society* 12.
- Purdy, N. & Mc Guckin, C. (2011). Disablist bullying: An investigation of student teachers' knowledge and confidence. Armagh, Northern Ireland: The Standing Conference on Teacher Education North and South (SCoTENS).
- Shim, Young Hee. 2002. Remarks at UNESCO Chair Symposium on Women's Rights, Cyber Rights. Seoul, South Korea, May 31, 2002.
- Smith PK, Morita Y, Junger-Tas J, Olweus D, Catalano R, Slee P. (Eds.) (1999). The nature of school bullying: A cross national perspective. London and New York: Routledge.
- Smith PK, Pepler DJ, Rigby K. (Eds.) (2004). Bullying in schools: How successful can interventions be? Cambridge: Cambridge University Press.
- Smith, P. K. & Steffgen, G. (Eds.) (2013). Cyberbullying, technology and coping. Oxfordshire: Psychology Press.
- Spertus, Ellen. (1996). Social and technical means for fighting on-line harassment.
<http://www.mit.edu/people/ellens/Gender/glc>
- Thomas, Karen. (2002). Girls know way around Net, parents. *USA Today*, February 13, 2002.
- Tokunaga, R.S. (2010). Following you home from school. A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behaviour*.
- Vandebosch, H. og Van Cleemput, K. (2009). Cyberbullying among youngsters. Profiles of bullies and victims.
- Vandebosch, H., Van Cleemput, K., Mortelmans, D., & Walrave, M. (2006). Cyberpesten bij jongeren in Vlaanderen. [Cyberbullying amongst youngsters in Flanders]. Brussels: viWTA.
- WHO@ (Working to Halt Online Abuse). (2002). <http://www.haltabuse.org/>

Appendice: risorse sul Web

- WHO@ (Working to Halt Online Abuse) -<http://www.haltabuse.org/>
- EU Kids Online, 2013: www.eukidsonline.net
- WiredPatrol (formerly CyberAngels) - <http://www.wiredpatrol.org/>
- CyberTipline -<http://www.cybertipline.com/>
- SafetyEd International - <http://www.safetyed.org/>
- <http://cyberviolence.atwaterlibrary.ca/wp-content/uploads/2016/08/Atwater-LibraryPreventing-and-Eliminating-Cyberviolence-Initiative-press-draft.pdf>