Cyberscudo

MODULO
CS

Inquestomodulo

Cari lettori,

Questa guida vuole essere uno *strumento* pratico e facilmente consultabile per conoscere le caratteristiche dei principali luoghi quotidianamente vissuti on line siano essi social network, app, videogiochi o piattaforme di video condivisione e riflettere assieme su come rendere l'esperienza *positiva, piacevole e formativa*.

Ci rivolgiamo dunque a voi **ragazzi** perché possiate *sperimentare* il reale e il virtuale della *vita on life* con *coraggio, curiosità e rispetto* per voi stessi e per il prossimo, prendendo coscienza anche delle *norme* che regolano le interazioni sul web e dei *rischi* cui potrebbe esporvi una navigazione poco attenta e consapevole.

Ci rivolgiamo a voi **genitori**, perché possiate continuare a essere il primo modello di riferimento per i vostri figli *accompagnandoli* nell'ambiente digitale restando informati anche sugli *strumenti di protezione* on line oggi disponibili per garantire una navigazione più sicura. Troverete inoltre indicazioni utili per rinnovare insieme quel patto educativo così prezioso nel momento in cui un nuovo device entra in famiglia.

E infine a voi **educatori** e **insegnanti** che quotidianamente siete chiamati a rispondere alle *sfide* dettate dalle nuove tendenze oltre che dalla ancora incerta situazione pandemica che ha obbligato tutti noi a rivedere le modalità di fare attività e lezioni in *presenza e a distanza,* promuovendo una partecipazione funzionale e rispettosa da parte dei ragazzi coinvolti.

In ogni sezione della guida troverete *analisi di contesti, indicazioni pratiche* e *suggerimenti* finalizzati a comprendere come vivere l'ambiente digitale e le risorse in esso contenute, in modo attento e responsabile perché ricordiamo: "*internet non è uno strumento, ma un luogo che dobbiamo imparare ad abitare*".

Dott. Ivano Zoppi
Segretario Genearle di Fondazione Carolina

Introduzione al modulo

Intr

Il Modulo “Cyberscudo” è dedicato al cyberbullismo, conclude l’insieme dei testi relativi alle competenze e alle conoscenze necessarie all’utilizzo consapevole dei dispositivi digitali. Questo Modulo copre gli argomenti relativi al comportamento da tenere in rete e a cosa fare se ci si imbatte in comportamenti online non corretti, quando non decisamente abusivi.

Proseguendo nella lettura, ci si renderà subito conto che la struttura di questa parte è leggermente diversa da quella utilizzata per le due parti precedenti, che sono state organizzate secondo l’ordine delle competenze elencate nei syllabi delle rispettive certificazioni ICDL Information Literacy e ICDL IT-Security.

Il motivo è che si è deciso di impostare il contenuto in modo da partire dall’analisi delle app e delle piattaforme disponibili online e passare solo successivamente all’analisi e comprensione del fenomeno “cyberbullismo”.

Per quanto l’organizzazione del testo non segua quindi passo passo la struttura del syllabus della certificazione Cyberscudo di AICA, tutti gli argomenti della certificazione sono coperti e il volume (Modulo) può essere utilizzato per la preparazione all’esame.

In aggiunta al materiale del testo cartaceo, sono inoltre state previste delle pagine online contenenti degli approfondimenti a diversi argomenti. L’accesso alle pagine può avvenire digitando nel browser l’indirizzo: **www.edizionimanna.com/cyberscudo**).

Sempre online e disponibile come pdf gratuito il volume “Minori Online”,(www.pepita.it/pepita-informa/pepita-informa-pubblicazioni/) prodotto da Pepita e Fondazione Carolina, indirizzato ai genitori e agli educatori, che si pone come naturale affiancamento a questo, dedicato ai ragazzi.

Comprendere il fenomeno e contestualizzarlo

1.1.1 Distinguere tra bullismo e altre manifestazioni **CS-15**

Comprendere e contestualizzare il fenomeno del cyberbullismo

2.1.1 Distinguere tra cyberbullismo e altre manifestazioni **CS-21, CS-28**

Le manifestazioni di cyberbullismo

2.2.1 Conoscere le peculiarità del Flaming **CS-22**

2.2.2 Conoscere le peculiarità dell'Harassment **CS-23**

2.2.3 Conoscere le peculiarità del Cyberstalking **CS-23**

2.2.4 Conoscere le peculiarità dell'incitamento all'odio in rete **CS-22**

2.2.5 Conoscere le peculiarità del Cyberbashing **CS-22**

Altre manifestazioni di disagio in rete

2.3.1 Conoscere le caratteristiche del fenomeno dell'Hikikomori **CS-19**

2.3.2 Conoscere le caratteristiche del fenomeno del Vamping **CS-18**

2.3.3 Conoscerei il fenomeno delle Challenge Autolesive **CS-20**

2.3.4 Conoscere il fenomeno del selfie Estremi **CS-22**

2.3.5 Conoscere le forme di dipendenza da internet **CS-16, CS-17, CS-18, CS-19, CS-20**

Comprendere e contestualizzare il fenomeno del sexting

3.1.1 Conoscere le peculiarità del Sexting **CS-24**

3.1.2 Conoscere le caratteristiche peculiari del cyberbullismo sessuale **CS-16, CS-17, CS-25**

3.1.3 Conoscere le peculiarità della Sextortion **CS-25**

La legge L.71/2017 per la prevenzione ed il contrasto del fenomeno del cyberbullismo

4.1.1. Conoscere l'esistenza della Legge per la prevenzione ed il contrasto del fenomeno del cyberbullismo **CS-21, CS-28**

4.1.2 Conoscere da che età un minore può chiedere l'oscuramento del contenuto offensivo sul web da parte del gestore **CS-29**

4.1.3 Le tutele previste per i minori dalla L. 71 /2017 in caso di offesa sul web **CS-29**

4.1.5 Comprendere come deve attivarsi il Garante per la Privacy deve per tutelare la reputazione di minori **CS-29**

4.1.6 Comprendere le modalità dell'ammonimento del cyberbullo presso il Questore **CS-30**

Concetto di Responsabilità legato ai reati a mezzo internet

4.2.1 Conoscere l'età a partire dalla quale un minore è imputabile **CS-26**

4.2.2 Comprendere le responsabilità di cui rispondono i genitori in caso di episodi di cyberbullismo **CS-26**

Reati a mezzo internet

4.3.1 Conoscere il reato di diffamazione a mezzo internet **CS-27**

4.3.2 Conoscere il reato di sostituzione di persona **CS-27**

4.3.3 Conoscere il reato di trattamento illecito dei dati personali **CS-27**

4.3.4 Comprendere il reato di diffusione di materiale pedopornografico **CS-27**

Conoscere le nuove norme in materia di Privacy e protezione dei dati personali introdotte dal GDPR

5.1.1 Comprendere le caratteristiche del GDPR **CS-33**

6.1 Concetti di sicurezza

6.1.1 Comprendere come proteggere i propri dati di accesso **CS-34**

6.1.2 Comprendere i motivi per proteggere le informazioni personali su internet **CS-35**

6.1.3 Comprendere che tutto ciò che viene messo su internet resta per sempre **CS-35**

Comportamento da tenere nelle conversazioni on line

6.2.1 Comprendere l'importanza di rispettare le regole di buon comportamento nelle comunicazioni on line **CS-36**

Conoscere il funzionamento dei principali social network

7.1.1 Comprendere i motivi per riflettere sul tipo di immagine che si associa al proprio profilo su Social Network **CS-37**

7.1.2 Comprendere i motivi per modificare le impostazioni alla geolocalizzazione **CS-37**

7.1.3 Comprendere come leggere il contratto al momento dell'iscrizione ad un social network **CS-36**

Sezione 0

Introduzione. I luoghi online

Il Regolamento Privacy del 25/05/2018, meglio noto come GDPR, è un regolamento dell'Unione Europea in materia di trattamento dei dati personali e di privacy e tra le varie novità introdotte vi è l'indicazione dei 16 anni come età minima per accedere a social network o app di messaggistica istantanea.

Le caratteristiche di alcune app e social network vengono riassunte qui di seguito. Maggiori informazioni sono riportate online, sul sito **www.edizionimanna.com/cyberscudo**

Nel recepire il nuovo regolamento Privacy in Italia, il Garante ha richiesto che:

- il consenso al trattamento dei propri dati personali possa essere espresso al compimento dei 14 anni;
- l'età minima per iscriversi in autonomia a un social network o utilizzare app di messaggistica istantanea, sia 14 anni.

Di fatto ogni app di videochiamate, di messaggistica istantanea e social network ha mantenuto una propria politica circa l'età minima consentita per l'utilizzo dei propri servizi.

0.1 APP DI VIDEOCHIAMATE

Zoom | www.zoom.us/

Zoom è una delle app di videochiamata maggiormente utilizzate in ambito scolastico e professionale, che permette la partecipazione di un massimo di 100 utenti contemporaneamente, tutti visibili. Funziona da cellulare, tablet e PC. L'età minima per il suo utilizzo è 16 anni.

Google Meet | www.meet.google.com

Google Meet è un'app per riunioni video che consente di inviare messaggi scritti e condividere lo schermo. È progettata per le aziende ma può essere utilizzata anche in ambito personale e scolastico. La versione gratuita consente la partecipazione di un massimo di 100 utenti contemporaneamente. L'età minima per il suo utilizzo è 13 anni.

Google Duo | www.duo.google.com/about/

Google Duo è un'app per videochiamate di gruppo che permette di collegare fino a 8 persone. L'età minima per poter disporre di un account Google in Italia, in accordo con quanto previsto dal Garante della Privacy, è di 14 anni.

Skype | www.skype.com/it/

Conosciuta come app per videochiamate e molto popolare fino a qualche anno fa, Skype può mettere in contatto fino a 50 persone contemporaneamente, consente di registrare le chiamate e di abilitare i sottotitoli in tempo reale. L'età minima per il suo utilizzo è 13 anni.

Google Hangouts | www.hangouts.google.com/

Google Hangouts è una piattaforma gratuita di messaggistica che consente di inviare ai propri contatti messaggi di testo, audio e video, in chat privata o di gruppo. È necessario un numero di cellulare per registrarsi sul telefono e un account Gmail per registrarsi sul proprio PC. Il numero di partecipanti ad una videochiamata o ad una conversazione varia a seconda della tipologia di "pacchetto" utilizzato.

L'età minima per poter disporre di un account Google in Italia, in accordo con quanto previsto dal Garante della Privacy, è di 14 anni.

0.2 APP DI MESSAGGISTICA ISTANTANEA

WhatsApp | www.whatsapp.com

WhatsApp è una app per cellulare, utilizzabile anche da PC, che necessita della connessione Internet per inviare messaggi, video, foto, file e fare telefonate o videotelefonate. Oltre all'immagine profilo è possibile inserire uno "stato" che permette di condividere aggiornamenti con testo, foto, video e GIF, visibili per 24 ore.

L'app presenta la notifica di lettura in modo che si possa sapere se il messaggio sia stato ricevuto o sia stato letto.

L'età minima per il suo utilizzo è 16 anni, ma viene utilizzata anche dai più piccoli inizialmente per i gruppi scolastici o sportivi. In effetti per i giovani è luogo online di scambio di messaggi ed immagini anche molto intimi, con relativa pericolosità in termini di atti di danno all'immagine, quali ad esempio il *sexting* (invio di messaggi sessuali espliciti).

Telegram | www.telegram.org

Telegram è un'app di messaggistica istantanea simile a WhatsApp che permette l'invio di messaggi, foto, video, file anche di grandi dimensioni (fino a 1,5 Gb), con la differenza che questi vengono salvati su cloud, permettendo l'accesso anche da PC o tablet senza avere con sé il proprio telefono. L'età minima per il suo utilizzo è 16 anni.

0.3 PIATTAFORME DI CONDIVISIONE VIDEO

YouTube | www.youtube.com

YouTube è una piattaforma in cui vengono caricati video musicali, documentari, film, cartoni, tutorial e recentemente anche le *stories*, o storie, che restano visibili per 7 giorni. L'età minima per poter disporre di un account YouTube è 13 anni.

Dailymotion | www.dailymotion.com/it

Dailymotion è una piattaforma di condivisione video e la seconda più famosa ed utilizzata al mondo dopo YouTube, da cui non si differenzia molto. Gli utenti, una volta registrati, possono caricare video di massimo 60 minuti e che non superino i 2Gb – principale differenza con YouTube. L'età minima per il suo utilizzo è 18 anni.

Twitch | www.twitch.tv

Twitch è una piattaforma di diretta streaming, lanciata ed utilizzata specialmente per i videogiochi e i loro giocatori. Tramite il sito, infatti, è possibile creare e caricare dirette di sessioni di gioco e tornei di e-Sport. I servizi di Twitch sono vietati sotto i 13 anni e tra i 13 e i 18 anni è necessario avere il consenso dei genitori.

Vimeo | www.vimeo.com

Vimeo è una piattaforma di condivisione video la cui caratteristica è che possono essere caricati solo video interamente prodotti dall'utente. Su Vimeo infatti non è possibile caricare pezzi di film o di programmi tv per questioni di diritti d'autore e per favorire la creatività di giovani artisti e film maker. L'età minima per il suo utilizzo è 16 anni, oppure è l'età minima consentita dal proprio paese per l'accesso ai social network, che in Italia è 14 anni.

0.4 SOCIAL NETWORK

Instagram | www.instagram.com

Instagram è un'app gratuita e un *social network*, o rete sociale, fotografico che permette di scattare foto/video e di condividerle come *post* o come *stories*. Il caricamento delle foto sfrutta gli *hashtag* (etichette/aggregatori tematici che servono a facilitare la ricerca di contenuti specifici) che permettono di inserire il contenuto in diverse categorie, così che possa essere ritrovato anche dagli altri utenti attraverso la parola chiave usata.

L'età minima per poter disporre di un account è di 13 anni. Instagram ha creato una serie di strumenti per la tutela dell'utente da commenti spiacevoli o contenuti dannosi.

Tik Tok | www.tiktok.com/it

Tik Tok è un social network che consente di caricare video brevi di massimo 15 secondi e rappresenta un luogo di creatività e di libera espressione per i più giovani.

Nei termini di servizio l'età minima indicata per aprire un account è di 13 anni, anche se l'app indica 12 anni.

Snapchat | www.snapchat.com/it-it/

Snapchat è un social network accessibile solo da cellulare che permette di inviare foto (*snap*) e video ai propri contatti, con la particolarità che i contenuti si autodistruggono dopo averne preso visione. Le *stories*, invece, restano visibili per 24 ore e, trascorso questo tempo, si eliminano.

L'età minima per poter disporre di un account è 13 anni.

Ask.fm | www.ask.fm

Ask è un social network che si basa sullo scambio di domande e risposte da parte degli utenti allo scopo di conoscersi meglio sfruttando l'anonimato. Il lato negativo di tale aspetto è che diventa facilmente luogo utilizzato per domande scomode, insulti, pettegolezzi. Le domande non possono superare i 300 caratteri e le risposte date sono poi visibili sul profilo ed accessibili a tutti. È stato criticato per essere luogo di cyberbullismo e istigazione al suicidio. Come la maggior parte delle app, anche Ask.fm ha un servizio di segnalazione in caso di contenuti negativi/violenti. L'età minima per avere un profilo è di 13 anni.

Facebook | www.facebook.com

Facebook è il social network in cui si possono condividere foto, video, eventi, pensieri, messaggi. La sua idea primaria era di tenere in contatto le persone, ma negli anni ha sviluppato molti contenuti extra diventando una piattaforma che permette di fare moltissime altre cose (vendere o acquistare prodotti, creare gruppi aggregativi...). Di fatto, ad oggi, è sempre meno vissuto dai teenager che privilegiano Instagram.

L'età minima per poter disporre di un profilo è di 13 anni, ma Facebook ha creato appositamente Messenger Kids per tutelare i minori.

Reddit | www.redditinc.com

Reddit è un forum di discussione o notizie sociali, in inglese, utilizzato però anche in Italia. Gli utenti possono condividere i loro *post* e valutare quelli già esistenti determinandone la visibilità. I contenuti presenti variano dall'istruzione alle serie tv al gioco, passando per i film e l'intrattenimento. La piattaforma non è utilizzata da un pubblico giovanissimo sia a causa della lingua, sia perché meno immediata e più "complessa" rispetto ad altre. L'età minima per poter accedere a Reddit è 13 anni.

ThisCrush | www.thiscrush.com

In ThisCrush gli utenti condividono il collegamento del proprio profilo in altri social network popolari, invitando i loro amici a scrivere un commento e a fare domande. Il destinatario non può rispondere direttamente da ThisCrush ai messaggi ricevuti, ma deve rispondere da un altro social network (solitamente Instagram). L'età minima per poter aprire un profilo su ThisCrush è 16 anni.

Tellonym | www.tellonym.me

Tellonym funziona praticamente nello stesso modo di ThisCrush, con la differenza che, se si accetta di rispondere, automaticamente appare sul proprio profilo ed è visibile a tutti.

Nei termini di servizio è scritto che accettandoli si dichiara di avere più di 17 anni.

Kik | www.kik.com

Kik è un'app di messaggistica istantanea per cellulare, simile ad iMessage di iPhone, e permette l'invio di testi, foto e video a singoli utenti o a gruppi. L'età minima per poter utilizzare Kik è 13 anni

Zepeto | www.zepeto.me

Zepeto è un'app che permette di creare un *avatar* a partire dal proprio selfie e di personalizzarlo acquistando i vari accessori. Condivide tutte le informazioni personali (compreso il numero di telefono) con alcune società per fini commerciali.

Nei termini di servizio l'età minima indicata per aprire un account è 13 anni, ma l'app indica 12 anni.

0.5 APP DI INCONTRI

Tra le diverse tipologie di app, esistono anche le app di incontri, che consentono ai propri utenti di creare il proprio profilo e indicare in modo più o meno generale i propri gusti e le proprie preferenze.

Queste informazioni vengono quindi utilizzate per mettere in contatto i diversi utenti.

Esempi di queste app sono **Tinder** e **Omegle**, entrambe utilizzabili ufficialmente solo a partire dai 18 anni.

0.6 VIDEOGIOCHI

Per i videogiochi è stata definita una classificazione ad hoc, denominata PEGI (Pan European Game Information), presente sulle confezioni dei videogiochi, che fornisce un'indicazione sull'adeguatezza del contenuto del gioco in base all'età. Maggiori informazioni sono riportate online, sul sito **www.edizionimanna.com/cyberscudo**

Minecraft | www.minecraft.net/it-it/

Minecraft è un gioco che permette di costruire e creare un mondo virtuale usando i mattoni. Altre attività includono l'uso della funzione multigiocatore per esplorare i mondi creati da altri utenti per chattare e giocare con loro. Secondo la classificazione PEGI, Minecraft è adatto per giocatori a partire da 7 anni.

Fortnite | www.epicgames.com/fortnite/it/home

Fortnite è un popolare gioco d'azione di sopravvivenza che include contenuti violenti. È possibile parlare con altri giocatori usando la chat pubblica, privata e vocale. L'età minima consentita per giocare a Fortnite è 12 anni.

Pokémon GO | www.pokemon.com/it/

Pokémon GO è un gioco per cellulare gratuito in cui gli utenti trovano e catturano creature Pokémon da aggiungere alla propria collezione. Il gioco è progettato per essere giocato all'esterno, con i giocatori che trovano Pokémon in luoghi diversi. I minori di 13 anni necessitano dell'autorizzazione dei genitori per scaricare il gioco.

Clash of Clans | www.clashofclans.com/it/

Clash of Clans è un gioco di combattimento in cui i giocatori costruiscono i propri eserciti (clan) e combattono contro altri eserciti di tutto il mondo. È possibile unirsi con altri o combattere da soli. È anche presente una funzione di chat tramite cui è possibile parlare con altri giocatori. Secondo la classificazione PEGI, Clash of Clans è adatto per giocatori a partire da 13 anni.

Clash Royale | www.clashroyale.com/it/

Clash Royale è un gioco di combattimento in cui i giocatori possono costruire le proprie comunità di battaglia. È anche presente una funzione di chat tramite cui è possibile parlare con altri giocatori. Secondo la classificazione PEGI, Clash of Clans è adatto per giocatori a partire da 13 anni.

Brawl Stars | www.brawlstarsitalia.com

Brawl Stars è un videogioco d'azione. I giocatori combattono tra loro in un'arena tramite personaggi chiamati *brawler*, ognuno con abilità diverse. Sono presenti diverse modalità di gioco, che vanno dal collezionare il maggior numero di gemme con la propria squadra, alla modalità sopravvivenza in stile "battle royale". Secondo la classificazione PEGI, Brawl Stars è adatto per giocatori a partire da 7 anni.

GTA Grand Theft Auto | www.rockstargames.com/grandtheftauto/

Grand Theft Auto, comunemente abbreviato in GTA, è un gioco in cui il giocatore esplora una città immaginaria nei panni del personaggio centrale e si rende complice di conflitti con criminali e gang rivali, portando a compimento le missioni che gli vengono assegnate. Questo gioco contiene temi per adulti, tra cui violenza, sesso e uso di droghe ed è vietato ai minori di 18 anni.

League of Legend | euw.leagueoflegends.com/it-it/

League of Legend, abbreviato con la sigla LoL, è il videogioco online più giocato al mondo, con 100 milioni di giocatori ogni mese.

In una mappa chiusa, due squadre, arroccate nelle proprie basi, che contano diversi edifici e il quartier generale, hanno l'obiettivo di distruggere il quartier generale avversario e preservare il proprio. Secondo la classificazione PEGI, League of Legend è adatto per giocatori a partire da 12 anni.

Among Us | www.innersloth.com/gameAmongUs.php

Among Us è un gioco ambientato su un'astronave giocato con altri 4-10 giocatori. I giocatori possono scegliere di partecipare a una partita con persone che non conoscono o creare il proprio gioco privato con gli amici. Il gioco seleziona casualmente uno dei giocatori come "impostore" che gli altri giocatori devono sconfiggere per vincere la partita. Secondo la classificazione PEGI, Among Us è adatto per giocatori a partire da 7 anni.

Roblox | www.roblox.com

Roblox è una piattaforma online dove chiunque può creare e condividere i propri giochi o giocare a giochi realizzati da altri utenti. Alcuni giochi sono gratis, mentre altri devono essere pagati con "Robux", la valuta online che i giocatori usano per acquistare giochi e oggetti come vestiti o accessori.

Secondo la classificazione PEGI, Roblox è adatto per giocatori a partire da 7 anni.

0.7 DIDATTICA A DISTANZA E TUTELA DELLA PRIVACY

Nell'intento di fornire a scuole, atenei, studenti e famiglie **indicazioni utili** a un utilizzo consapevole e positivo delle nuove tecnologie a fini didattici, il 26 marzo 2020 il Garante per la privacy ha condiviso le implicazioni più importanti dell'attività formativa a distanza sul diritto alla protezione dei dati personali.

Le indicazioni per l'uso fornite dal Garante per la Protezione dei Dati Personali e dal MIUR sono le seguenti. Nessun bisogno di consenso

Le scuole che utilizzano sistemi di didattica a distanza non devono richiedere il consenso al trattamento dei dati di docenti, studenti, genitori, poiché *il trattamento è riconducibile alle funzioni istituzionalmente assegnate alle scuole*, ma le stesse sono tenute a rendere un'informativa sull'uso di nuove piattaforme tecnologiche.

Non è necessaria la valutazione d'impatto

Non c'è bisogno della valutazione d'impatto perché il trattamento dei dati da parte delle scuole non è così massivo da comportare elevati rischi per gli interessati.

Nel caso si ritenga necessario ricorrere a piattaforme che erogano servizi più complessi non rivolti esclusivamente alla didattica, si dovranno *attivare i soli servizi strettamente necessari alla formazione, configurandoli in modo da minimizzare i dati personali da trattare* (evitando, ad esempio, geolocalizzazione e login sociali).

Svolgimento delle lezioni online

La *registrazione* delle video-lezioni da parte dello studente è consentita, *ma solo per finalità di studio personali* e compatibilmente con le specifiche disposizioni scolastiche al riguardo. Per ogni altro utilizzo o eventuale diffusione di immagini e/o videoregistrazioni delle videolezioni è necessario prima *informare* le persone coinvolte nella registrazione (professori, studenti…) e *ottenere il loro consenso*. Nel caso di minori, va ottenuto il consenso dei genitori o di coloro che esercitano la responsabilità genitoriale.

Si avrà invece un *illecito civile* consistente nella *violazione della privacy* nel caso in cui le foto e/o i video delle lezioni online vengano divulgati, manipolati o diffusi senza il consenso delle persone ivi ritratte.

Liceità, correttezza e trasparenza del trattamento dei dati

Al fine di garantire la trasparenza e la correttezza del trattamento, le istituzioni scolastiche devono *assicurare la trasparenza del trattamento informando gli interessati (studenti, genitori e docenti)*, con un linguaggio comprensibile anche ai minori, in ordine, in particolare, alle caratteristiche essenziali del trattamento, che deve peraltro limitarsi all'esecuzione dell'attività didattica a distanza, nel rispetto della riservatezza e della dignità degli interessati.

Maggiori informazioni relative alla sicurezza della didattica a distanza e i link alle fonti sono riportate online, sul sito **www.edizionimanna.com/cyberscudo**

Il bullismo

Sezione 1

1.1 COMPRENDERE IL FENOMENO E CONTESTUALIZZARLO

1.1.1
Distinguere tra bullismo e altre manifestazioni

Cercando sul dizionario il termine "bullismo", si ottengono delle definizioni che in qualche modo si potrebbero interpretare come "positive", perché si riferiscono a comportamenti spacconi e spavaldi. Invece si deve sempre tenere conto che il bullismo è un comportamento **violento**, **premeditato** e **ripetitivo**, che viene diretto contro persone percepite come deboli e incapaci di difendersi a causa di una differenza di status sociale o di potere: le **vittime**. In generale il bullismo non riguarda un'interazione tra due persone, ma coinvolge un gruppo di persone che si coalizzano contro uno o più individui.

Ambienti tipici in cui si manifesta il bullismo sono sia le scuole, che tutti quei contesti sociali frequentati dai giovani. Gli attori coinvolti negli episodi di bullismo, oltre alle **vittime** e al **bullo**, sono anche i **sostenitori**, cioè chi sostiene l'aggressione del bullo ad esempio incitandolo durante l'atto, e gli **spettatori**, che invece si tengono in disparte durante l'aggressione e non prendono posizione.

Esistono diversi tipi di aggressione che si possono configurare come bullismo. Ad esempio si possono avere aggressioni di tipo **fisico**, **verbale**, **relazionale**, **sessuale**, **cyberbullismo**.

Si parla di bullismo **fisico** quando il bullo aggredisce fisicamente la vittima, mediante calci, pugni, spinte, oppure aggredendo le proprietà della vittima, ad esempio danneggiandole o rubandole.

Si parla di bullismo **verbale** quando la vittima viene insultata, derisa e umiliata in pubblico.

Si parla di bullismo **relazionale** quando le azioni del bullo provocano un isolamento sociale della vittima, che viene estraniata dal proprio gruppo di amici.

Si parla di bullismo **sessuale** sia quando il bullo mette in atto delle molestie sessuali nei confronti della vittima, sia quando gli atti di bullismo verbale sono associati a insulti di tipo omofobo o transfobico, cioè quando gli insulti riguardano la sfera sessuale e di genere della vittima.

Si parla infine di **cyberbullismo** quando gli atti di bullismo vengono attuati mediante le nuove tecnologie, quali ad esempio email, chat, blog e reti sociali.

Sezione 2

I rischi che si possono incontrare Online

I ragazzi accedono sempre più precocemente ad Internet: dati recenti dicono che il 20% dei minori riceve il primo cellulare prima degli 11 anni ed è un dato certamente in crescita.

Ad oggi i luoghi virtuali più vissuti dai minori di 11 anni sono le live chat, la messaggistica, le piattaforme musicali, le piattaforme di condivisione video e i videogiochi.

I rischi a cui sono esposti bambini e ragazzi quando navigano online possono andare dall'incontro con adulti malintenzionati, a sfide folli che possono sfociare nell'autolesionismo e arrivare all'estremo, alla dipendenza dalla propria presenza su internet e ai "like" ricevuti dagli "amici". Si dovrebbe sempre ricordare che il proprio valore non si misura con la quantità di approvazione ricevuta sui social network, e che la vita reale è un'altra cosa rispetto a quella virtuale della rete.

2.1 GROOMING

3.1.2
Conoscere le caratteristiche peculiari del cyberbullismo sessuale

Con **grooming**, o **adescamento**, si intende il rischio di essere contattati da adulti malintenzionati che modificano la loro identità per fare richieste sessuali. Anche se normalmente si tratta di un rischio che i ragazzi riescono a percepire, in misura crescente all'aumentare dell'età e dell'esperienza di uso della rete, è anche possibile che si riesca a individuare la situazione per tempo e si forniscano informazioni personali all'adescatore, quali ad esempio la scuola frequentata o l'indirizzo di casa. Un ulteriore rischio è che si ceda alla richiesta dell'adescatore di non farne parola con nessuno e si pensi quindi di trovarsi completamente isolati e senza possibilità di chiedere aiuto. Questo non è vero: non appena ci si rende conto di trovarsi in una situazione di pericolo, è sempre importante parlarne con qualcuno e chiedere aiuto.

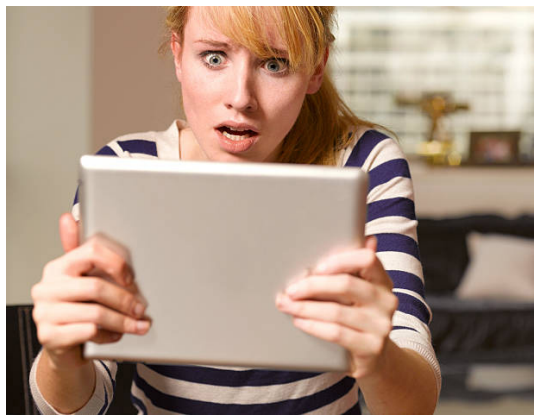
2.2 GAMING

2.3.5
Conoscere le forme di dipendenza da internet

Dati del 2019 dicono che tra gli 8 e gli 11 anni quasi 1 ragazzo su 2, più maschi che femmine, usa il cellulare principalmente per giocare online. Molti di loro, 1 su 4, giocano per circa 2 ore al giorno. Crescendo, le ore dedicate al gioco aumentano a 3.

Pur non essendo di per sé dannoso, il gioco porta con sé alcuni rischi:

- esposizione a contenuti potenzialmente dannosi e violenti;
- approcci indesiderati in caso di videogioco online;
- uso eccessivo e abuso;
- *phishing*, violazione della privacy;
- disinteresse verso lo studio e le relazioni personali;
- stress, disturbi del sonno, ansia;
- miopia per la continua messa a fuoco statica;
- obesità per mancanza di movimento fisico;
- virus nel dispositivo.



Altra problematica è il rischio delle "microtransazioni". I video giocatori sono, infatti, spesso spinti all'acquisto di monete virtuali usate nei giochi per potenziare i personaggi e le prestazioni.

2.3 CONTENUTI LESIVI, PORNOGRAFIA E PEDOPORNOGRAFIA

3.1.2
Conoscere le caratteristiche peculiari del cyberbullismo sessuale

Nel corso della navigazione ci si può imbattere in contenuti inappropriati, violenti, pornografici, potenzialmente anche molto pericolosi per il proprio equilibrio psicologico.

Oggi chiunque può caricare o cercare materiale online facilmente e questo rende il mondo virtuale pericoloso per un viaggiatore giovane e poco esperto.

Non solo social, ma anche app, piattaforme e videogame possono essere luoghi non sicuri se attraversati da soli: si potrebbe infatti incorrere in immagini traumatiche o ambigue per la cui elaborazione spesso non si possiedono gli strumenti necessari.

2.4 DIPENDENZA DA LIKE

2.3.5
Conoscere le forme di dipendenza da internet

Gli adolescenti sono alla perenne ricerca di approvazione da parte degli altri. In particolare all'interno di social network e app di incontri l'effetto positivo di ricevere approvazione sotto forma di *like* è amplificato, e si tende quindi a cercare nuovamente il piacere ottenuto. Tuttavia il rovescio della medaglia è che la riduzione del numero di like può portare alla riduzione graduale della propria sicurezza e autostima.

2.5 INTERNET ADDICTION DISORDER

2.3.5
Conoscere le forme di dipendenza da internet

La **dipendenza da Internet** è stata riconosciuta e inserita nel Manuale Diagnostico e Statistico dei Disturbi Mentali (DSM 5) da alcuni anni. Chi soffre di tale disturbo fa un uso prolungato dello cellulare o del PC ed è restio a separarsene, tanto che lo stare connesso a giocare o chattare diventa un'ossessione e rischia di trasformarsi in dipendenza. Si può parlare di dipendenza quando "*la maggior parte del tempo e delle energie vengono spese nell'utilizzo della Rete, creando in tal modo menomazioni forti e disfunzionali nelle principali e fondamentali aree esistenziali, come quella personale, relazionale, scolastica, familiare, affettiva*".[1]

Essendo un problema riconosciuto, studiato e sempre più diffuso, sono stati creati percorsi appositi di disintossicazione e terapia.

2.6 VAMPING

2.3.2
Conoscere le caratteristiche del fenomeno del Vamping

Il termine **vamping** si riferisce alla pratica di fare un utilizzo intenso di internet, inviando messaggi, frequentando chat e social network, o giocando, durante le ore notturne.

Questo fenomeno provoca una serie di conseguenze che si possono riassumere in:

- mancanza di sonno
- irritabilità, nervosismo, aumento dell'ansia
- scarso rendimento a scuola
- mancanza di attenzione

1 STATE OF MIND - Il giornale delle scienze psicologiche.

2.7 FOMO (FEAR OF MISSING OUT)

Con l'acronimo **FOMO**, o *Fear of Missing Out*, si fa riferimento a una forma di ansia sociale che porta a dover rimanere in contatto costante con gli altri per la paura di essere tagliati fuori e di perdere avvenimenti, informazioni e in generale interazioni online con gli altri membri del proprio gruppo.

2.3.5
Conoscere le forme di dipendenza da internet

2.8 HIKIKOMORI

Il termine **hikikomori** indica una persona che sceglie di isolarsi dalla società e dalle relazioni interpersonali, evitando qualsiasi forma di contatto in presenza ed evitando quindi di avere relazioni significative e/o intimità emotiva e fisica.

2.3.1
Conoscere le caratteristiche del fenomeno dell'Hikikomori

La maggior parte degli hikikomori italiani ha un'età compresa tra i 14 e i 25 anni, con una particolare concentrazione intorno ai 17anni. Circa i 2/3 degli hikikomori sono uomini.

L'isolamento sociale con il quale si definisce l'hikikomori non è causato dall'abuso delle nuove tecnologie, in quanto si tratta di un fenomeno già diffuso in Giappone dagli anni '80, con esordi negli anni '60. Esiste comunque un collegamento: chi si isola in questo modo può trovare un mondo alternativo nel web e creare un rapporto di dipendenza da Internet proprio perché meno invasivo del mondo "reale".

È anche vero, però, che la condizione di grande fragilità psico-emotiva, che spesso caratterizza l'isolamento sociale, aumenta esponenzialmente tutti i rischi connessi all'utilizzo del web, dall'abuso della pornografia, alla depressione legata ai social network, fino alle radicalizzazioni del pensiero (fonte: Hikikomori Italia).

2.9 SELFIE ESTREMI O DAREDEVIL SELFIE

È una moda che ha avuto origine in Russia e Ucraina e che porta i ragazzi a scattarsi una foto in situazioni di rischio per la propria vita. L'idea è quella di una sfida per dimostrare il proprio coraggio agli "amici" e aumentare la propria popolarità, ma non si può dimenticare che il rapporto Eurispes del 2019, che analizza i dati tra ottobre 2011 e novembre 2017, indica che i selfie estremi hanno portato alla morte ben 259 giovani. E ovviamente questo dato è in costante aumento.

2.3.4
Conoscere il fenomeno del selfie estremi

2.10 ISTIGAZIONE AL SUICIDIO, AUTOLESIONISMO, ANORESSIA E BULIMIA

2.3.3
Conoscere il fenomeno delle Challenge Autolesive

Nel percorso di crescita, specialmente nella fase adolescenziale, è normale vivere momenti di insicurezza, sofferenza e disagio. La possibilità di condividere tale malessere in Rete e cercare informazioni a riguardo permette di imbattersi facilmente in blog, chat, forum e siti che promuovono l'assunzione di comportamenti autolesivi, ad esempio spingendo verso l'anoressia o la bulimia, quando non addirittura al suicidio. È invece importante non fermarsi alle indicazioni che vengono date in rete, e parlarne con i propri amici e genitori, ricordando che i veri amici non sono quelli che propongono sfide o spingono verso comportamenti autolesionistici, ma sono quelli che cercando di dare veramente una mano a superare il periodo di crisi.

2.11 GIOCO D'AZZARDO E LUDOPATIA

2.3.5
Conoscere le forme di dipendenza da internet

La tendenza al gioco d'azzardo, sia con le macchine presso i bar sia online è un fenomeno in crescita tra i ragazzi, anche i più giovani.

Online il ragazzo riesce ancora più facilmente a sfuggire alle restrizioni di età e, per la sua maggiore tendenza al bisogno di gratificazione dato dalla vincita, è più esposto al rischio di dipendenza patologica e gioco compulsivo.

Ulteriore pericolo è dato dalle chat di gioco, all'interno delle quali si può essere attirati in chat di appuntamenti o coinvolti in scommesse illegali, giochi a tema erotico ed altre situazioni in cui è facile approfittare dell'ingenuità.

Un altro rischio specifico è la perdita ingente di denaro: perché il ragazzo inserisce nel "conto di gioco o borsellino elettronico" i dati delle carte di pagamento dei genitori senza alcuna tutela di sicurezza nella gestione dei dati forniti, perché l'operatore è illegale e non riconosce le vincite o perché la scommessa si paga con il credito telefonico e questo viene liquidato senza possibilità di riscatto.

2.12 NOMOFOBIA

2.3.5
Conoscere le forme di dipendenza da internet

Con **nomofobia** si intende la paura incontrollata di perdere la connessione con la rete Internet a partire dal telefonino. Questa paura si può trasformare in dipendenza dal telefonino, che viene tenuto costantemente acceso e a portata di mano.

2.13 PHUBBING

Phubbing è l'unione dei termini *phone* (telefono) e *snubbing* (snobbare) e si riferisce all'atto di ignorare o trascurare il proprio interlocutore in un contesto sociale, concentrandosi invece sul proprio cellulare, continuando ad aggiornare e controllare social network, mail e news. Secondo un recente studio condotto da un'equipe di psicologi dell'Università del Kent e pubblicato sulla rivista *Journal of Applied Social Psychology*, il *phubbing* influirebbe negativamente su comunicazione e relazione tra persone.

2.14 CYBERBULLISMO

"*Qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti online aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo*" (Art. 1 - Legge 71/2017).

2.1.1
Distinguere tra cyberbullismo e altre manifestazioni

Il **cyberbullismo** è una forma di aggressione e molestia perpetrata attraverso le nuove tecnologie; inoltre è necessario che negli atti compiuti vi sia intenzionalità, ripetitività e asimmetria di potere. Ogni atto di cyberbullismo è caratterizzato dalla pervasività "in ogni tempo e in ogni luogo" (anywhere/anytime). La maggior parte delle vittime di cyberbullismo ha età compresa tra 11 e 14 anni.

4.1.1
Conoscere l'esistenza della Legge per la prevenzione ed il contrasto del fenomeno del cyberbullismo

Dal confronto tra i dati sul bullismo e quelli del cyberbullismo sembra che quest'ultimo sia riflesso del primo. Se accade nella realtà fisica, può facilmente trovare un corrispettivo in attacchi online e viceversa. Nella maggior parte dei casi, la vittima è il diverso e il debole: per etnia, per religione, per caratteristiche psicofisiche, per genere, per identità di genere, per orientamento sessuale e per particolari realtà familiari. Ciò che rende più dannoso il cyberbullismo è il potenziale anonimato del bullo e l'ampiezza di risonanza che può avere sia in termini quantitativi di spettatori, sia in termini di tempo, vista la difficoltà a cancellare dalla Rete ogni traccia di attacco. Il cyberbullismo porta con sé molte sfumature nel tipo di discriminazione.

Se ci si trova ad essere vittime di cyberbullismo, non ci si deve vergognare o temere che un intervento esterno da parte di genitori, amici o insegnanti possano provocare ulteriori ripercussioni negative da parte del bullo. Per questo è importante parlarne, sempre e comunque.

Tra le principali di manifestazioni di cyberbullismo segnaliamo le seguenti.

2.2.5
Conoscere le peculiarità del Cyberbashing

Il cyberbashing, o *Happy Slapping*, è la forma di cyberbullismo più frequente. Ha inizio nella vita reale, quando la vittima viene aggredita o molestata mentre altri riprendono la scena con lo cellulare, per proseguire su Internet, dove una volta che questi video vengono postati, chiunque è libero di condividerli, commentarli o aggiungere una reazione (ad esempio, *like*).

L'exclusion, o esclusione, significa escludere intenzionalmente un coetaneo da un gruppo online (gli "amici" di un social network), da una chat, da un videogame o da altri ambienti virtuali.

2.2.4
Conoscere le peculiarità dell'incitamento all'odio in rete

Con hate speech, letteralmente "incitamento all'odio", si intende la pubblicazione di contenuti a sfondo razzista o di incitamento all'odio sulle piattaforme digitali.

2.2.1
Conoscere le peculiarità del Flaming

Il flaming, che significa "fiammeggiante", è una battaglia verbale online di messaggi violenti e volgari tra due contendenti che hanno lo stesso potere e che si affrontano ad armi pari. Sono battaglie virtuali che hanno una durata limitata.

Il termine harassment, o "molestia", si riferisce a quei messaggi insultanti e volgari che vengono inviati ripetutamente nel tempo attraverso l'uso del computer e/o del cellulare. A differenza del flaming, qui il comportamento aggressivo è reiterato e non esiste parità di potere tra aggressore e vittima.

2.2.2
Conoscere le peculiarità dell'Harassment

Quando le molestie passano dai messaggi insultanti dell'harassment a minacce vere e proprie, e la vittima inizia a temere per la propria sicurezza, si utilizza la denominazione cyberstalking.

2.2.3
Conoscere le peculiarità del Cyberstalking

Le challenge autolesive sono sfide social in cui si mostra il proprio coraggio online, infliggendosi delle ferite e sopportando il dolore il più a lungo possibile.

Per quanto queste sfide siano un fenomeno pericoloso, è anche vero che spesso sono più raccontate che realizzate, e alcune sono in realtà delle vere e proprie bufale. Il parlarne paradossalmente le rafforza ed aumenta il rischio di emulazione, ma dai giovani di oggi non sono percepite come una tendenza diffusa, e sono ritenute pericolose soprattutto per i più deboli.

2.3.3
Conoscere il fenomeno delle Challenge Autolesive

Sezione 3

Il fenomeno del cyberbullismo sessuale

Quando ci si avvicina al fenomeno del cyberbullismo, ci si rende conto che tra i ragazzi il concetto di cyberbullismo sessuale non è chiaro, e anzi tra di loro c'è la tendenza ad associare al cyberbullismo sessuale episodi di aggressione sessuale come lo stupro. In realtà si tratta di fatti, manifestazioni e azioni che si verificano prima dell'aggressione vera e propria, in cui la vittima viene derisa a partire da suoi elementi fisici, atteggiamenti, modo di vestire o tendenze sessuali.

3.1 IL PROBLEMA DELL'ADESCAMENTO ONLINE

3.1.1 Conoscere le peculiarità del Sexting

Tra le varie tipologie di cyberbullismo si distingue il fenomeno del **sexting** e dell'adescamento online.

Per quanto non si tratti di un fenomeno nuovo, è esploso con la diffusione dei social network e la facilità di scambio di messaggi, foto e video a esplicito contenuto sessuale.

Con sexting, unione tra le parole *sexual* e *texting*, si indica l'invio di immagini e messaggi con esplicito riferimento sessuale attraverso cellulare o PC, con diffusione su app di messaggistica e/o social network. In Italia 2 adolescenti su 5 lo fanno, dai 12 ai 14 anni è più frequente.

La percezione erronea di social e chat come luoghi privati porta i ragazzi ad inviare foto o video con contenuti a sfondo sessuale con leggerezza e senza riflettere sulle conseguenze che tale azione comporta.

Il pericolo del sexting è il non controllo della propria immagine e la perdita della propria intimità. Spesso i giovani, per lo più ragazze, mandano foto molto intime, di cui perdono ovviamente il controllo nel momento stesso dell'invio. Non bisogna infatti dimenticare che il cellulare salva le nostre immagini in spazi virtuali, generalmente molto protetti, ma non di nostra proprietà. Al momento dell'invio il controllo del contenuto è definitivamente perso.

3.2 LE CARATTERISTICHE DEL CYBERBULLISMO SESSUALE

Il **cyberbullismo sessuale** è un termine molto vasto che comprende molestie sessuali, atti di bullismo contro qualcuno in relazione al suo orientamento sessuale, le cose sessuali a cui la vittima è interessata o meno, e il bullismo transfobico.

3.1.2
Conoscere le caratteristiche peculiari del cyberbullismo sessuale

3.3 LA SEXTORTION

Il termine **sextortion** deriva dall'unione dei termini "sex" ed "extortion", e indica l'immissione su internet di messaggi e immagini sessualmente esplicite con finalità estorsive.

Si tratta quindi di un ricatto sessuale che utilizza i dispositivi informatici per costringere le vittime sia a sottoporsi a pratiche sessuali, sia a pagare somme di denaro per evitare la diffusione di testi, immagini o video compromettenti.

3.1.3
Conoscere le peculiarità della Sextortion

Sezione 4

Conoscere la normativa italiana e le leggi che tutelano la vita Online

Il fenomeno del cyberbullismo in Italia è diventato oggetto di una legge per la sua prevenzione e contrasto nel 2017, quando la legge 71 è entrata in vigore il 18 giugno 2017. Questa legge si pone l'obiettivo di contrastare il fenomeno del cyberbullismo in tutte le sue manifestazioni, mediante azioni a carattere preventivo e con strategie di attenzione ed educazione dei minori coinvolti.

Il testo completo della legge 71 del 18 giugno 2017 è stato pubblicato sulla Gazzetta Ufficiale e si trova alla pagina www.gazzettaufficiale.it/eli/id/2017/06/3/17G00085/sg.

4.1 L'IMPUTABILITÀ DEL MINORE

4.2.1 Conoscere l'età a partire dalla quale un minore è imputabile

Il minore di anni 14 non è mai imputabile penalmente. Il minore tra i 14 e i 18 anni è imputabile se viene dimostrata la sua capacità di intendere e di volere attraverso consulenti professionali.

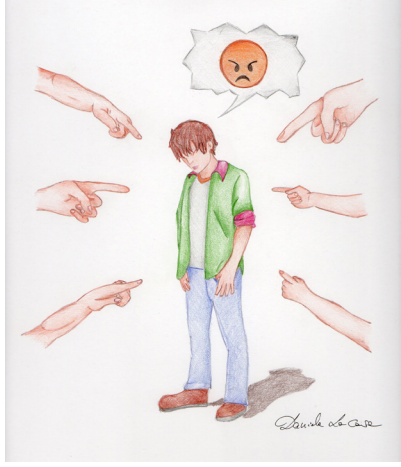
4.2 RESPONSABILITÀ DEI GENITORI: CULPA IN EDUCANDO

4.2.2 Comprendere le responsabilità di cui rispondono i genitori in caso di episodi di cyberbullismo

La responsabilità genitoriale non viene meno neanche quando i figli sono affidati a terzi (scuola e insegnanti). L'affidamento alla sorveglianza di terzi solleva il genitore dalla presunzione di culpa in vigilando, ma non da quella di culpa in educando.

4.3 I REATI A MEZZO INTERNET

Di tutti questi reati un minore risponde direttamente davanti alla legge a partire dai 14 anni se viene dimostrata la sua capacità di intendere e di volere attraverso consulenti professionali.



Diffamazione a mezzo Internet: offendere la reputazione altrui attraverso un "mezzo di pubblicità" sul web (social, chat o qualsiasi sito Internet). Anche la condivisione o i *like* a *post* offensivi possono rappresentare l'integrazione di un reato. Integra il reato anche la pubblicazione di foto imbarazzanti.

4.3.1
Conoscere il reato di diffamazione a mezzo internet

Importante da ricordare:

- il consenso a scattare una fotografia non equivale al consenso a pubblicarla;
- offendere gli insegnanti durante le lezioni online integra il reato di oltraggio a pubblico ufficiale.

Sostituzione di persona: fingere di essere qualcun altro sul web inducendo in errore gli altri, ad esempio creando un falso profilo social (*fake*) o aprendo e utilizzando un account mail sotto falso nome. Può commettere tale reato anche chi chatta sotto falso nome per poter avviare una corrispondenza con soggetti che, altrimenti, non gli avrebbero concesso la loro amicizia e confidenza.

4.3.2
Conoscere il reato di sostituzione di persona

Trattamento illecito dei dati personali: diffondere su Internet dati personali di un'altra persona (pubblicare sue foto o video, condividere il suo numero di telefono o indirizzo mail, taggarla) senza il suo consenso recandole un danno.

4.3.3
Conoscere il reato di trattamento illecito dei dati personali

Detenzione e diffusione di materiale pedopornografico: custodire o condividere foto o video a sfondo sessuale di ragazzi o ragazze minorenni essendo consapevoli della minore età della persona ritratta.

4.3.4
Conoscere il reato di diffusione di materiale pedo-pornografico

Furto d'identità: impossessarsi dei dati personali di un'altra persona senza averne il permesso e a sua insaputa (profili rubati).

Attenzione: il risarcimento dei danni alle vittime di bullismo e cyberbullismo con relativo esborso di soldi spetta ai genitori sempre, fino a prova contraria, fino a che il ragazzo è minorenne

4.4 LEGGE 29 MAGGIO 2017, N. 71. DISPOSIZIONI A TUTELA DEI MINORI PER LA PREVENZIONE ED IL CONTRASTO DEL FENOMENO DEL CYBERBULLISMO

4.1.1
Conoscere l'esistenza della Legge per la prevenzione ed il contrasto del fenomeno del cyberbullismo

La legge dedicata a Carolina Picchio è entrata in vigore il 18 giugno 2017, e la promotrice e prima firmataria è la ex senatrice Elena Ferrara.

FINALITÀ DELLA LEGGE

La legge si pone l'obiettivo di contrastare il fenomeno del cyberbullismo in tutte le sue manifestazioni, con azioni a carattere preventivo e con strategie di attenzione, tutela ed educazione nei confronti dei minori coinvolti, siano essi vittime o responsabili di illeciti.

I PUNTI FONDAMENTALI DELLA LEGGE

1. **Riconoscimento** del termine cyberbullismo
2. **Eliminazione** rapida dei contenuti per i minori (possono agire da soli se hanno compiuto 14 anni)
3. **Identificazione** per ogni istituto scolastico di un referente antibullismo
4. **Introduzione** dell'ammonimento del Questore

RICONOSCIMENTO DEL TERMINE CYBERBULLISMO

2.1.1
Distinguere tra cyberbullismo e altre manifestazioni

Per la prima volta viene introdotta una definizione di cyberbullismo:

«Qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto di identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito dei dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti online aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso o la loro messa in ridicolo» (Art. 1 - Legge 71/2017)

ELIMINAZIONE DEI CONTENUTI PER MINORI ULTRAQUATTORDICENNI

Un minore che abbia compiuto 14 anni e sia vittima di cyberbullismo può chiedere l'oscuramento del contenuto offensivo al gestore del sito anche *senza l'autorizzazione dei propri genitori* (il link per risalire al gestore di un sito è www.whois.domaintools.com). Il titolare del sito dovrà comunicare entro 24 ore dall'istanza di aver assunto l'incarico e provvedere a tale richiesta nelle successive 48 ore. Se la rimozione non avviene o se non è possibile identificare il gestore del sito Internet o del social media, l'interessato potrà rivolgere analoga richiesta al Garante per la protezione dei dati personali, che dovrà intervenire entro le successive 48 ore.

4.1.2
Conoscere da che età un minore può chiedere l'oscuramento del contenuto offensivo sul web da parte del gestore
4.1.3
Le tutele previste per i minori dalla L. 71 /2017 in caso di offesa sul web
4.1.5
Comprendere come deve attivarsi il Garante per la Privacy per tutelare la reputazione di minori

Nello scrivere una segnalazione o un reclamo è necessario:

- rappresentare i fatti;
- indicare eventuali reati;
- indicare l'URL del sito.

Compito del Garante sarà di:

- valutare l'illiceità della condotta;
- rimuovere, oscurare o bloccare il contenuto;
- darne notizia all'interessato.

È possibile scaricare il modulo per segnalare i contenuti dal link:

www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6732688

L'indirizzo a cui inviare la segnalazione è: cyberbullismo@gpdp.it

IMPORTANTE: la segnalazione può essere presentata direttamente da chi ha un'età maggiore di 14 anni o da chi esercita la responsabilità genitoriale sul minore.

IDENTIFICAZIONE PER OGNI ISTITUTO SCOLASTICO DI UN REFERENTE ANTIBULLISMO

Il Referente presente in ogni istituto scolastico:

- deve essere adeguatamente formato;
- viene nominato dall'istituto scolastico nell'ambito della propria autonomia;
- deve coordinare i progetti di prevenzione e contrasto al cyberbullismo anche con la collaborazione delle forze dell'ordine, delle associazioni e dei centri di aggregazione.

Il Referente si interfaccia con:

- le Forze di Polizia;
- i servizi minorili dell'amministrazione della giustizia;
- le associazioni e i centri di aggregazione giovanile sul territorio.

INTRODUZIONE DELL'AMMONIMENTO DEL QUESTORE

4.1.6
Comprendere le modalità dell' ammonimento del cyberbullo presso il Questore

- Fino a quando non è proposta denuncia o querela chiunque (anche l'insegnante) può attivare la procedura di ammonimento.
- Il minore che ha più di 14 anni viene convocato insieme ad almeno un genitore o al tutore.
- Gli effetti dell'ammonimento cessano con la maggiore età.
- L'istruttoria è sommaria. È sufficiente un quadro indiziario che garantisca la verosimiglianza di quanto dichiarato.

4.5 LA NORMATIVA D.P.R. 249/1988 (STATUTO DEGLI STUDENTI)

- Gli insegnanti possono vietare l'uso dei cellulari in classe.
- Gli insegnanti possono chiedere agli studenti di lasciare il telefono negli armadietti.

COSA NON PUÒ FARE IL DOCENTE:

- perquisire lo studente;
- sequestrare il cellulare.

COSA PUÒ FARE IL DOCENTE:

- custodire il cellulare durante l'orario di lezione;
- visionare un video o un messaggio su richiesta dell'interessato (vittima o relativi genitori).

4.6 LEGGE 19 LUGLIO 2019, N. 69 "MODIFICHE AL CODICE PENALE, AL CODICE DI PROCEDURA PENALE E ALTRE DISPOSIZIONI IN MATERIA DI TUTELA DELLE VITTIME DI VIOLENZA DOMESTICA E DI GENERE", DETTA LEGGE CODICE ROSSO

La legge sancisce la punizione di chi realizza e diffonde immagini o video privati, sessualmente espliciti, senza il consenso delle persone rappresentate per danneggiarle a scopo di vendetta o di rivalsa personale, comprendendo anche chi "condivide" le immagini online. Il reato viene punito con la reclusione da 1 a 6 anni e con la multa da euro 5.000 a euro 15.000 e prevede una serie di aggravanti nel caso il reato di pubblicazione illecita sia commesso dal coniuge, anche separato o divorziato o da una persona che è o è stata legata da relazione affettiva alla persona offesa.

Sezione 5

Strumenti di protezione Online

5.1 LINEE GUIDA DI COMPORTAMENTO ONLINE

I diversi siti di social media, quali Instagram, Snapchat, Tik Tok, Facebook, YouTube e così via, danno normalmente indicazioni ai propri utenti, sia in termini di età minima per poter accedere al servizio, sia in termini di comportamento atteso sulle rispettive piattaforme. In particolare, queste informazioni si possono trovare ai seguenti link:

INSTAGRAM
www.help.instagram.com/477434105621119/

SNAPCHAT
www.snap.com/it-IT/terms/

TIK TOK
www.support.tiktok.com/it/privacy-safety/community-policy-it

FACEBOOK
www.facebook.com/policies_center

YOUTUBE
www.support.google.com/youtube/topic/2803176?hl=it&ref_topic=6151248

GOOGLE
www.policies.google.com/terms?hl=it

5.2 PARENTAL CONTROL

Il Parental Control è un sistema che ha lo scopo di proteggere i bambini da contenuti considerati pericolosi o violenti presenti sul Web e nel dispositivo.

Sono diverse le app di Parental Control disponibili sia per Android sia per Apple ed è possibile cercare online quella più adatta alle proprie esigenze. In generale, le principali funzioni riguardano il controllo del bambino attraverso: limite dell'accesso ad alcune app presenti sul dispositivo, impostazione di un timer per limitare l'uso del cellulare, attivazione del blocca acquisti sul Play Store, notifica di quali app vengono maggiormente utilizzate, controllo dei contenuti "in entrata e in uscita" e delle nuove app installate.

5.3 REGOLAMENTO PRIVACY DEL 25/05/2018, MEGLIO NOTO COME GDPR

5.1.1
Comprendere le caratteristiche del GDPR

Il Regolamento Privacy, meglio noto come GDPR, è un regolamento dell'Unione Europea in materia di trattamento dei dati personali e di privacy introdotto nel 2016.

Secondo questo regolamento sulla privacy, così come è stato recepito in Italia:

- il consenso al trattamento dei propri dati personali potrà essere espresso al compimento dei 14 anni;
- viene introdotta l'indicazione di 16 anni come età minima per accedere a social network o ad app di messaggistica istantanea.

Sezione 6

Attività online: sicurezza e norme di comportamento

Ogni giorno milioni di persone si collegano a internet per lavorare, cercare informazioni e notizie, giocare, entrare in contatto con i loro amici attraverso i social network o i programmi di comunicazione istantanea. Internet pervade ormai la nostra vita, permettendoci di entrare in contatto con amici, conoscenti o anche perfetti estranei che si trovano nell'appartamento accanto o in località così geograficamente distanti che servirebbero giorni di viaggio per raggiungerli fisicamente.

A questo utilizzo costruttivo e utile della tecnologia è tuttavia necessario affiancare una serie di norme di buon comportamento e attendersi a regole di sicurezza, così da poter continuare a usufruire in modo tranquillo di questa infrastruttura così variegata e complessa.

6.1 COMPRENDERE COME PROTEGGERE I PROPRI DATI DI ACCESSO

6.1.1 Comprendere come proteggere i propri dati di accesso

Le attività che si svolgono sui diversi social network richiedono agli utenti di identificarsi e di fornire una serie di informazioni personali, come nome e cognome, età, posizione geografica, interessi vari. Tuttavia queste informazioni potrebbero essere utilizzate da eventuali malintenzionati che dovessero entrarne in possesso. Quindi la prima cosa da fare è proteggere i propri dati d'accesso utilizzando delle password sicure e in genere attenendosi a una serie di accorgimenti:

- evitare di usare nella password informazioni personali quali data di nascita, nome e cognome;
- avere almeno 8 caratteri inserendo sequenze di nomi numeri e simboli;
- non usare la stessa password per tutti i siti e per tutti i dispositivi;
- non comunicare a terzi le proprie password;
- scegliere attentamente le app a cui consentire l'accesso ai dati di geo-localizzazione;
- verificare le impostazioni della privacy dei social utilizzati;
- evitare di accettare amicizie da chi non si conosce nella vita reale.

6.2 PERCHÉ PROTEGGERE LE PROPRIE INFORMAZIONI PERSONALI

6.1.2
Comprendere i motivi per proteggere le informazioni personali su internet

È molto importante tenere segrete le proprie password di accesso così come le proprie informazioni personali. Il rischio maggiore che si corre è il furto di identità.

I furti di identità sono molto pericolosi: chi li compie ruba informazioni personali come la data di nascita o il numero di telefono, e le utilizza spesso per scopi illeciti, ad esempio per compiere atti di cyberbullismo su un social network fingendosi la persona a cui sono stati sottratti i dati. In effetti la perdita in sicurezza digitale è oggi l'altra faccia della medaglia della tutela della privacy. La criptazione dei messaggi da parte dei principali fornitori di servizi di messaggistica digitale non permette di controllare facilmente né i contenuti dei messaggi, né l'identità di chi li scrive o di chi posta materiale. Ci si trova quindi esposti al furto di identità digitale, che può essere usato sia per denigrare socialmente la vittima sia, come si è già visto, per essere contattati da parte di adulti sconosciuti che si fingono coetanei.

La poca conoscenza dei propri diritti in tema di privacy, d'altro canto, fa cedere dati personali senza controllo: geolocalizzazione e rischio di stalking, informazioni intime e rischio di ricatti, violazione della privacy per interessi commerciali.

6.3 LA PERMANENZA DEI DATI

6.1.3
Comprendere che tutto ciò che viene messo su internet resta per sempre

Le informazioni e i contenuti che si postano online ogni giorno vanno a costituire la cosiddetta **web reputation**, cioè l'identità digitale che viene associata a una persona che mette in linea foto, video, link ad articoli o pagine web, e che permette agli altri di farsi un'idea positiva o negativa di questa persona.

Anche se si potrebbe pensare che dare un'impressione negativa di sé non sia importante, si deve ricordare che non sono solo gli amici o i conoscenti a poter accedere ai contenuti condivisi in rete, ma anche

insegnanti, datori di lavoro, e in generale persone alle quali in futuro si potrebbe voler fare una buona impressione. Tuttavia ciò che si posta o si condivide su internet rimane indelebilmente in rete, quindi prima di postare o condividere qualcosa è sempre bene chiedersi se davvero si desidera che quei contenuti restino associati per sempre alla propria identità digitale.

6.4 PERCHÉ RISPETTARE NORME DI BUON COMPORTAMENTO ONLINE

6.2.1
Comprendere l'importanza di rispettare le regole di buon comportamento nelle comunicazioni on line

Come nella vita reale, anche nelle attività online è buona norma attenersi a semplici regole di buon comportamento in modo da rendere piacevole la propria esperienza sui social network e in generale su internet. Queste regole di buon comportamento online vengono indicate con il termine *netiquette*, e sono state raccolte nell'arco di decenni di utilizzo della rete.

I punti fondamentali sono i seguenti:

- **Scrivere correttamente**, senza errori ortografici; esistono correttori ortografici che evitano di fare brutte figure e di dare un'immagine sciatta di sé.
- **Evitare di scrivere del testo TUTTO IN MAIUSCOLO**: per convenzione in rete questo equivale a urlare.
- **Presentarsi quando si entra in un nuovo gruppo**: è buona educazione anche nella vita reale quando si incontrano persone nuove.
- **Usare le faccine per chiarire il tono del messaggio**: se chi legge non è un amico stretto, il messaggio potrebbe essere travisato.
- **Non pubblicare informazioni e dati sensibili di altri utenti**.
- **Evitare di andare off topic** in una discussione cambiando argomento.
- **Evitare di usare troppe abbreviazioni**, perché non è detto che tutti gli utenti a cui è diretto il messaggio siano in grado di interpretarle.
- **Evitare di spammare**, inviando costantemente messaggi di promozione relativi al materiale che si condivide.

Social Network e APP per la condivisione di materiale

Sezione 7

Utilizzando quotidianamente internet e i suoi servizi, è abbastanza inevitabile prima o poi decidere di iscriversi a uno dei social network disponibili, anche solo per mantenere i contatti con amici o parenti che vivono lontani. Quando si prende questa decisione, è di fondamentale importanza valutare bene che tipo di informazioni si vogliono condividere con i propri amici e con tutti gli altri utenti della rete.

7.1 TIPO DI IMMAGINE ASSOCIATO AL PROFILO

7.1.1
Comprendere i motivi per riflettere sul tipo di immagine che si associa al proprio profilo su Social Network

Quando si attiva il proprio **profilo** di social media, viene richiesto di associarvi un'immagine, un nome utente e la propria biografia, che normalmente vengono mostrati a tutti.

Tuttavia, proprio la visibilità pubblica di queste informazioni potrebbe portare ad un loro furto da parte di malintenzionati. Per questo motivo è importante scegliere accuratamente la foto o l'immagine da pubblicare (evitare foto di bambini, ad esempio, o immagini altrui).

È anche importante impostare correttamente la privacy del proprio account, in modo che chi desidera seguirlo dovrà inviare una richiesta.

7.2 GEOLOCALIZZAZIONE ATTIVA O NO

7.1.2
Comprendere i motivi per modificare le impostazioni alla geolocalizzazione

La **geolocalizzazione** è una funzionalità particolarmente comoda in determinate situazioni, ad esempio per indicare dove è stata scattata una foto senza doverlo fare necessariamente a mano, magari successivamente cercando di ricordare dove si è stati. Tuttavia la geolocalizzazione permette a chiunque di conoscere la posizione di un altro utente, e così una funzione nata per esigenze reali e positive, ad esempio per poter comunicare a un servizio di emergenza la propria posizione in caso di incidente, può trasformarsi in un "cavallo di Troia" per i malintenzionati, che possono introdursi a casa di una persona dopo averne verificato la posizione e la conseguente assenza da casa.

Per questo motivo è importante sapere come attivare e disattivare la geolocalizzazione sul proprio cellulare, sia esso iOS o Android, e saper decidere quali sono le app che devono necessariamente avere accesso alle informazioni di posizione del telefonino.

7.3 CONDIZIONI DI UTILIZZO

7.1.3
Comprendere come leggere il contratto al momento dell'iscrizione ad un social network

Quando si effettua l'iscrizione ad un social network, è necessario accettare i termini e le condizioni d'uso che vengono proposte. Per evitare di firmare un contratto alla cieca, è buona norma leggere le condizioni generali prima di accettarle, anche perché queste riguardano il modo in cui verranno gestiti i dati e i contenuti del nuovo utente, oltre che la sua privacy.

Il contratto sottoscritto al momento dell'iscrizione ad un social network può essere considerato un contratto di licenza d'uso non esclusiva (ad esempio per finalità di marketing). Normalmente, accettando le condizioni d'uso viene ceduta al social network la licenza d'uso dei contenuti che saranno pubblicati sul proprio profilo.

SITI CONSIGLIATI

www.pepita.it

www.fondazionecarolina.org

www.pepita.it/iocliccopositivo/web

www.swgfl.org.uk/

www.saferInternet.org.uk/

www.nspcc.org.uk/

www.net-aware.org.uk

www.anti-bullyingalliance.org.uk/

www.globalkidsonline.net/

www.betterInternetforkids.eu/

www.saferInternetday.org/

www.e-enfance.org/

www.cyberbullying.org/

www.generazioniconnesse.it

www.lascuolacontinua.it

www.protectyoungeyes.com

ESERCIZI

1. Che differenze ci sono tra il bullismo e uno scherzo?

A. Nessuna se l'atto viene indirizzato a un amico.
B. Nello scherzo l'intento è di ferire la vittima.
C. Il bullismo è un abuso di potere premeditato e ripetititivo.
D. Lo scherzo è un atto di aggressione organizzato da più persone.

2. Cosa si intende per cyberbullismo?

A. Sono atti di prepotenza perpetrati attraverso mezzi elettronici.
B. Sono scherzi di pessimo gusto spediti via mail.
C. Sono tentativi di carpire le password di accesso ai social media.
D. Sono messaggi scambiati tra due adolescenti che litigano via telefonino.

3. Cosa è il Flaming?

A. Un videogame in cui i contendenti combattono con il fuoco.
B. Uno scambio acceso di messaggi.
C. Una battaglia verbale tra due persone.
D. Una battaglia verbale online tra due persone di durata limitata.

4. Quali sono i canali attraverso cui si verifica l'harassment?

A. Di persona in un gruppo di amici.
B. Via mail o telefonate persistenti.
C. Pedinando la vittima.
D. Le chat di un videogame.

5. Quando si parla di cyberstalking?

A. Quando la vittima è una donna.
B. Quando un gruppo di persone invia mail insultanti.
C. Quando la vittima inizia a temere per la propria incolumità.
D. Quando il bullo passa dalle telefonate alle mail.

6. Per quale motivo l'incitamento all'odio si sta diffondendo in rete?

A. Perché tutti hanno internet.
B. Perché si pensa di poter restare anonimi.
C. Perché si può scrivere su internet senza preoccuparsi degli errori.
D. Perché la rete permette di raccogliere tutti gli insulti in un sito solo.

Troverete le soluzioni degli esercizi all'indirizzo: www.edizionimanna.com/soluzioni.htm

7. Quando un gruppo di ragazzi picchia un coetaneo e altri riprendono l'aggressione, si parla di:

A. Cyberbashing.
B. Harassment.
C. Stalking.
D. Hikikomori.

8. Si parla di hikikomori quando:

A. un ragazzo continua a inviare sms a una ragazza.
B. un ragazzo si chiude nella propria camera per molto tempo senza contatti con l'esterno.
C. un gruppo di ragazze assale una ragazza e la veste come un personaggio anime.
D. una ragazza passa tutta la notte a giocare e a chattare in rete.

9. In quali casi si parla di vamping?

A. Quando un ragazzo si traveste da vampiro per giocare online.
B. Quando una ragazza si trucca e si veste elegante per chattare con un ragazzo.
C. Quando un ragazzo resta sveglio abitualmente tutta la notte per giocare e chattare in rete.
D. Quando si ricevono messaggi di minaccia di notte.

10. Quali sono le caratteristiche principali delle challenge autolesive?

A. Dimostrare le proprie conoscenze agli amici.
B. Dimostrare il proprio coraggio provocandosi lesioni dolorose.
C. Dimostrare di essere più forti degli altri.
D. Dimostrare il proprio coraggio mettendosi in ridicolo.

11. Il fenomeno di scattarsi delle foto in situazioni di estremo pericolo viene denominato:

A. selfie estremi.
B. selfie esterni.
C. selfie FOMO.
D. selfie revenge.

Troverete le soluzioni degli esercizi all'indirizzo: www.edizionimanna.com/soluzioni.htm

ESERCIZI

12. Cosa è la "nomofobia"?

A. La paura degli uomini su internet.
B. La paura di restare connessi a internet.
C. La paura di perdere il cellulare.
D. La paura di perdere la connessione a internet.

13. Cosa è il Sexting?

A. La condivisione di foto del proprio corpo su internet.
B. La preparazione di selfie da mandare agli amici.
C. La conservazione di foto intime sul proprio cellulare.
D. L'invio di video intimi al proprio/alla propria partner.

14. Quando il cyberbullismo è di tipo sessuale?

A. Quando si ridicolizza un video porno.
B. Quando si fanno apprezzamenti sull'aspetto di una persona.
C. Quando si ridicolizza una coppia di omosessuali.
D. Quando si inviano messaggi minacciosi a una ragazza.

15. Cosa è la sextortion?

A. È un ricatto attraverso le foto intime della vittima.
B. È un tipo particolare di foto intima.
C. È quando un ragazzo guarda i video porno insieme agli amici.
D. È la rielaborazione grafica di una foto porno.

16. Quando si parla di "revenge porn"?

A. Quando si mostra un film porno a un amico per uno scherzo.
B. Quando si pubblicano su internet foto e video intimi per vendicarsi del proprio/della propria ex.
C. Quando si filma di nascosto un amico mentre guarda un film porno.
D. Quando si scambiano in privato immagini intime con il proprio/la propria partner.

17. A quando risale la legge per il contrasto del cyberbullismo in Italia?

A. È entrata in vigore nel 2017.
B. Entrerà in vigore nel 2022.
C. È in discussione alla Camera.
D. Non è ancora entrata in vigore.

Troverete le soluzioni degli esercizi all'indirizzo: www.edizionimanna.com/soluzioni.htm

18. È possibile per un minore chiedere al gestore l'oscuramento di contenuto offensivo sul web?

A. No, devono farlo i genitori.

B. Sì, a partire da 14 anni.

C. Sì, a partire da 12 anni.

D. Dipende dal gestore.

19. Quali informazioni vanno fornite dal minore al gestore di un sito al momento della segnalazione di un'offesa sul web?

A. I fatti, i reati, l'URL del sito.

B. Il nickname del bullo.

C. Una copia delle pagine contenenti l'offesa.

D. Il nome del proprietario del sito contenente l'offesa.

20. Come va segnalato un illecito al Garante della privacy?

A. Inviando una mail a cyberbullismo@gpdp.it.

B. Telefonando al numero verde del Garante Privacy.

C. Compilando un modulo sul sito contenente l'illecito.

D. Scaricando un modulo e inviandolo a cyberbullismo@gpdp.it.

21. In quali occasioni si deve coinvolgere il Garante della Privacy?

A. Quando il titolare di un sito che pubblica contenuto offensivo non lo oscura entro 48 ore dalla segnalazione.

B. Nello stesso momento in cui si invia una segnalazione al titolare di un sito che pubblica contenuto offensivo.

C. Quando si scopre che un sito pubblica del contenuto offensivo.

D. Solo dopo aver inviato per tre volte la segnalazione al titolare del sito con contenuto offensivo.

22. Per quale motivo il Questore convoca il cyberbullo?

A. Per multarlo.

B. Per ammonirlo.

C. Per arrestarlo.

D. Il cyberbullo non può essere convocato da un Questore.

Troverete le soluzioni degli esercizi all'indirizzo: www.edizionimanna.com/soluzioni.htm

ESERCIZI

23. A partire da quale età un minore può essere imputabile?

A. 12 anni.
B. 15 anni.
C. 17 anni.
D. 14 anni.

24. Quando un atto di cyberbullismo ricade sui genitori del cyberbullo?

A. Sempre.
B. Fino al raggiungimento della maggiore età del cyberbullo.
C. Fino al raggiungimento dei 14 anni del cyberbullo.
D. Fino a quando il cyberbullo vive insieme ai genitori.

25. Cosa si intende per reato di diffamazione?

A. Scrivere messaggi offensivi pubblici rivolti ad altri sulla propria bacheca di social media.
B. Inviare messaggi insultanti via SMS.
C. Ricevere foto intime dal proprio / dalla propria partner.
D. Pubblicare una foto imbarazzante del proprio gatto.

26. Quando si crea un profilo in un social media facendo finta di essere qualcun altro, si commette il reato di:

A. diffamazione.
B. trattamento illecito di dati personali.
C. sostituzione di persona.
D. diffusione di materiale personale.

27. Quando si pubblicano su una chat il numero di telefono e l'indirizzo email di una persona senza aver avuto il suo consenso, si commette il reato di:

A. diffamazione.
B. sostituzione di persona.
C. cyberbullismo.
D. trattamento illecito di dati personali.

28. Quando si commette un reato conservando sul proprio PC delle foto a sfondo sessuale di ragazzi minorenni?

A. Sempre, se si è consapevoli della minore età dei ragazzi nelle foto.
B. Solo se si condividono le foto su internet.
C. Solo se i ragazzi nelle foto hanno meno di 14 anni.
D. Solo se i ragazzi nelle foto hanno meno di 12 anni.

Troverete le soluzioni degli esercizi all'indirizzo: www.edizionimanna.com/soluzioni.htm

29. Secondo il regolamento Privacy, o GDPR, da quale età è possibile accedere ai social network?

A. 18 anni.

B. 15 anni.

C. 13 anni.

D. 16 anni.

30. Come si dovrebbero proteggere i propri dati di accesso a un social network?

A. Usare la stessa password per tutti i social network.

B. Verificare le impostazioni di privacy dei social network utilizzati.

C. Usare una password facile da ricordare, come la propria data di nascita.

D. Scrivere la propria password agli amici per essere sicuri di ricordarla.

31. Per quale motivo è importante proteggere le proprie informazioni su internet?

A. Per non rischiare furti di identità.

B. Per non dover ricordare cosa si è pubblicato.

C. Per evitare che vengano compromesse da un virus.

D. Per evitare che si scopra quando si mente.

32. Come si può evitare di danneggiare la propria web reputation?

A. Evitando di pubblicare contenuti che danno un'impressione negativa.

B. Cancellando contenuti pubblicati che possono risultare insultanti.

C. Modificando il proprio nome nel profilo dei social network frequentati.

D. Pubblicando le proprie idee e interessi solo in chat privata.

33. Postare delle foto pubblicitarie in tutti i gruppi e reti sociali frequentati è considerato corretto?

A. No, secondo la netiquette è considerato spam.

B. Sì, ma solo se si avvisano in anticipo gli altri partecipanti.

C. No, le pubblicità vanno pubblicate solo sui siti predisposti.

D. Sì, non ci sono problemi a pubblicare delle pubblicità.

34. Per quale motivo è importante scegliere correttamente l'immagine associata al proprio profilo?

A. Perché è visibile a tutti.

B. Perché la si può mostrare solo ai propri amici.

C. Perché è bello mostrare come si era da bambini.

D. Non serve sceglierla con attenzione, la vede solo il proprietario del profilo.

Troverete le soluzioni degli esercizi all'indirizzo: www.edizionimanna.com/soluzioni.htm

35. In quale caso è preferibile non avere attiva la geolocalizzazione?

A. Quando si pubblica su un social network, si è in vacanza e a casa non rimane nessuno.

B. Quando si vuole segnalare la propria posizione a un servizio di emergenza.

C. Quando si vogliono condividere foto o video su un social network.

D. Quando si vuole salvare la posizione in cui si scatta una foto.

36. È sempre necessario accettare le condizioni d'uso di un social network prima di iniziare a usarlo?

A. No.

B. Sì.

C. Solo se si è maggiorenni.

D. Solo dopo il primo mese di prova.

ANNOTAZIONI

ANNOTAZIONI