Guida a un uso intelligente di Internet

1. La Dichiarazione dei diritti in Internet

Internet ha contribuito in maniera decisiva a ridefinire lo spazio pubblico e privato, a strutturare i rapporti tra le persone e a cancellare confini. Ha costruito modalità nuove di produzione e fruizione della conoscenza. Ha ampliato le possibilità di intervento diretto delle persone nella sfera pubblica. Ha modificato l'organizzazione del lavoro. Ha consentito lo sviluppo di una società più aperta e libera. Internet va dunque considerato come una **risorsa** globale, ma soltanto **se usata correttamente** e in modo intelligente.

La *Dichiarazione dei diritti in Internet* (2015) richiama alcuni aspetti da osservare con attenzione.

Ogni persona ha uguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.

L'uso consapevole di Internet è fondamentale garanzia per lo sviluppo di uguali possibilità di crescita individuale e collettiva, la prevenzione delle discriminazioni e dei comportamenti a rischio e di quelli lesivi delle libertà altrui.

Ogni persona può accedere alla rete e comunicare

usando strumenti anche di natura tecnica che proteggano l'anonimato ed evitino la raccolta di dati personali, in particolare per esercitare le libertà civili e politiche senza subire discriminazioni o censure.

La sicurezza in rete deve essere garantita come interesse pubblico, attraverso l'integrità delle infrastrutture e la loro tutela da attacchi, e come interesse delle singole persone.

Non sono ammesse limitazioni della libertà di manifestazione del pensiero.

Deve però essere garantita la tutela della dignità delle persone da abusi connessi a comportamenti quali l'incitamento all'odio, alla discriminazione e alla violenza.

2. 11 regole per usare Internet

1. Usa Internet in modo intelligente

La tecnologia in generale, e Internet in particolare, sono strumenti che semplificano la vita.
Ma sono questi strumenti che devono essere al nostro servizio e non viceversa: dobbiamo evitare di diventare loro schiavi restando collegati alla rete tutto il giorno.
Per chi studia o lavora, Internet è uno strumento molto utile, come molte applicazioni per smartphone.
Tuttavia, stiamo acquisendo cattive abitudini durante il loro utilizzo.
Passiamo la maggior parte della giornata guardando uno schermo, quello del computer, di un cellulare o del televisore.
E a quanto pare non ce ne rendiamo conto.
Durante l'attività scolastica non si può perdere tempo: quando inizi a cercare informazioni su un argomento, spesso prevale la tentazione di guardare l'e-mail, le reti sociali, un video o di mettersi a giocare online.
Tutto ciò porta solo a **stressarsi** perché non siamo in grado di assimilare tante informazioni che crediamo essere utili ma che, nella maggior parte dei casi, non lo sono affatto.
Quindi è davvero importante essere consapevoli di quanto tempo passiamo perdendo tempo in Internet.

2. Fermati a ciò che è importante

Ci sono cose importanti su cui soffermarsi, per esempio trovare informazioni e approfondimenti su un argomento di interrogazione o di esame.
Devi quindi utilizzare Internet per questa attività, una volta letto e compreso l'argomento di studio.
Per questo tipo di attività devi stabilire il tempo opportuno (mezz'ora, un'ora), magari al termine della giornata: se alla fine ti ritrovi a navigare nei social network, almeno non avrai perso le ore precedenti.

3. Fermati e pensa a fine giornata

Alla fine della giornata fatti le seguenti domande.

- Quanto tempo ho usato Internet per fare ricerche scolastiche?
- Quanto tempo ho guardato i social network, siti Web o blog?
- Ho ricavato qualcosa di importante da questi ultimi?

Forse hai letto l'articolo di un blog che ti ha fatto riflettere o insegnato una nuova tecnica di studio. Questo va bene, purché tu sia arrivato direttamente a quest'articolo dopo averlo cercato perché ne avevi bisogno, e non perché, dopo aver visualizzato 50 pagine, sei arrivato lì per caso.
Da tutti i blog a cui sei iscritto, da tutti i siti Web che visiti, ottieni qualcosa di importante?
Forse è opportuno fare una selezione tra i blog che segui abitualmente.
Lo stesso vale per gli account Instagram, altri siti Web e applicazioni mobili che sai che ti distrarranno e non comportano altro che perdita di tempo.

4. Studia lontano dallo smartphone

Cambia il modo in cui ti relazioni a Internet e cambierà il modo in cui studi. Così come perdi tempo, puoi giocare a tuo favore usando la tecnologia e la forza di volontà.
Le cattive abitudini nell'uso della rete sono ormai così profondamente radicate in noi che non è facile fare un uso consapevole e intelligente di Internet.
Per evitare qualsiasi tipo di distrazione, dovresti studiare senza essere connesso a Internet e con il cellulare lontano da te.

5. Fai una navigazione consapevole

Pianifica ogni giorno il tempo da dedicare alle ricerche in Internet, anche nel fine settimana e, per lo più a fine della giornata di studio.
Cerca di essere il più possibile concreto e conciso nelle ricerche, senza divagare.
Va bene seguire un link se pensi di poter trovare informazioni utili ma, prima di fare clic, fermati e pensa se davvero pensi che sia utile.
Se ogni volta che segui un link ti poni questa domanda, sicuramente potrai risparmiare grandi quantità di tempo.

6. Dimentica le chat

Tenere aperta la messaggistica istantanea mentre studi (o ascoltare il suono di avviso dei messaggi al massimo volume) è uno dei peggiori errori che puoi fare.
Disinstalla tutte le applicazioni (inutili) che puoi: quelle di cui proprio non puoi fare a meno, lasciale chiuse o silenziale.
Ogni volta che si verifica un'interruzione nello stu-

dio, il cervello impiega molto tempo a tornare a concentrarsi.
Con ogni conversazione in chat perdi molti minuti e molto probabilmente non ti ha portato grandi benefici.

7. Si può esistere anche senza social network

La maggior parte degli studenti sono nativi digitali e quindi oggi ti sembra di essere emarginato se non sei sempre attivo in diversi social (e ce ne sono molti).
Pensa seriamente al motivo per cui usi ogni social network e quali vantaggi effettivi ciò ti porta.
Potresti far parte di un gruppo di studenti che fornisce informazioni utili o invece appartenere a un gruppo in cui le informazioni fornite sono confuse e poco attendibili.
Cerca di capire se è davvero utile o meno appartenere a determinati gruppi, e se davvero vale la pena di perdere molto tempo leggendo tutte le discussioni.
Hai bisogno di essere in tutti quei social? Li usi tutti?
Sicuramente non li usi tutti, ma ricevi migliaia di notifiche ogni giorno da tutte le tue reti.
Sei cosciente del tipo di conversazioni che segui in rete?
Se li usi tutti i giorni, e se sono anche vari, il tempo che userai è molto. Devi sottrarlo allo studio o al riposo. Ne vale la pena?

8. L'informazione eccessiva porta alla disinformazione

Oltre a vari tipi di notizie, più o meno vere, che trovi su Facebook, Twitter o su qualsiasi social network, ci sono anche le notizie che puoi trovare sui media digitali e nei blog.
In questo caso c'è il serio rischio di perdere molto tempo, passando da un link all'altro, anche solo per confrontare le notizie.
Se sei veramente interessato ad alcuni blog, dedica un tempo specifico ogni giorno, o una volta alla settimana, per leggerli e stabilisci un tempo massimo di lettura. Quando hai intenzione di iscriverti a un nuovo blog, chiediti quanto tempo sarai in grado di dedicare alla lettura e se è davvero rilevante per i tuoi studi o interessi.
Leggi l'articolo, ma non perderti nelle migliaia di commenti a riguardo: spesso si perde più tempo di quello speso per la lettura dell'articolo.
Inoltre, nella maggior parte dei casi, certi interventi violenti e negativi ti metteranno solo di cattivo umore.

9. Navigare non è sinonimo di riposare

Il riposo è particolarmente importante per gli studenti, ma non è certo riposante stare tutto il giorno incollato a uno schermo. Prenditi momenti di riposo, oltre che fisico, anche per gli occhi.
Esci all'aria aperta, fai sport, incontra i tuoi amici, trascorri del tempo con la tua famiglia.
Le pause devono essere reali: dimenticati del cellulare, del computer e della TV per alcuni minuti, almeno ogni due ore.

10. La costanza vale l'ingegno

Anche lo studente più brillante può avere dei cali nel rendimento scolastico se perde troppo tempo in rete. Diventa quindi importante porsi delle regole precise, quando ti rendi conto che perdere troppo tempo in Internet può pregiudicare l'andamento scolastico. Non aspettare che siano i docenti o i tuoi genitori a porti delle limitazioni: ciò rischia di creare solo incomprensioni e conflitti all'interno della tua famiglia e in ambito scolastico.

11. Sii sempre rispettoso della netiquette

Esiste un insieme di regole denominato *netiquette* che si potrebbe tradurre in "galateo (*etiquette*) della rete (*net*)".
Entrando in Internet si accede a una massa enorme di dati messi a disposizione, spesso gratuitamente, da altri utenti. Bisogna portare rispetto verso quanti, spesso in maniera volontaria, hanno prestato e prestano opera per consentire a tutti di accedere a dati e informazioni che altrimenti sarebbero patrimonio di pochi o che difficilmente si potrebbero reperire, se non in biblioteche specialistiche. Dobbiamo quindi seguire le regole richieste dai siti (registrazioni, privacy, copyright, ecc.) e interloquire con altri utenti usando un linguaggio corretto e rispettoso.

3. I pericoli della rete

Navigando in Internet e utilizzando i social ci esponiamo spesso, in maniera più o meno consapevole, a una serie di rischi.
La Polizia Postale ne elenca una notevole quantità: vediamo quelli più eclatanti.

Adescamento, violenze sessuali online, sexting, sextortion

I minori in questo caso sono sottoposti attraverso la rete a episodi di violenza a sfondo sessuale, che si traducono spesso nell'uso di un linguaggio spinto fino a arrivare all'adescamento dei minori da parte di soggetti adulti. In questo caso spesso vengono condivise immagini e video a sfondo pedopornografico.

Body shaming

Commenti, video offensivi, denigrazioni che hanno come argomento il corpo del soggetto che si vuole colpire. Si mettono in evidenza in maniera denigratoria difetti fisici, abbigliamento e abitudini dell'alimentazione.

Challenges

Sono sfide, spesso pericolose, che nascono in rete e che i ragazzi provano a emulare.

Cyberbullismo

Attacco virtuale per intimorire, molestare, mettere in imbarazzo o semplicemente far sentire a disagio altre persone. Pettegolezzi, immagini o video imbarazzanti, costruzione di falsi profili social sono solo alcune delle modalità con cui possono essere realizzati gli attacchi online con finalità di cyberbullismo.

Cyberstalking

Comportamenti persecutori commessi mediante l'utilizzo del Web. L'utilizzo della rete comporta infatti l'immissione online di numerosi dati personali che possono essere facilmente reperiti e utilizzati dallo stalker.

Dipendenza dal gioco online

Oggi è possibile giocare nella solitudine della propria stanza, 24 ore su 24, a volte con estranei conosciuti solo in rete. Questa pratica può creare pratiche compulsive e dipendenza.

Phishing

È un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi una persona o un ente affidabile in una comunicazione digitale.

Revenge porn

La condivisione pubblica di immagini o video intimi tramite Internet senza il consenso dei protagonisti degli stessi.

Risse virtuali

Sono una delle massime espressioni della violenza in rete. Possono avvenire tra coetanei per "bullizzare" un solo soggetto, oppure possono essere innescate da parte di adulti, magari sotto una falsa identità, per minare la psicologia di un ragazzo e attirarlo, indifeso, tra le proprie mani.

Uso incontrollato dei dati personali

In questo caso i dati dei minori possono essere usati per la creazione di un alter ego digitale (*Impersonation*), per una sostituzione di persona (*Masquerade*) oppure si può utilizzare un'identità fittizia per conquistare la fiducia di un minore e poi aggirarlo (*Trickery*).

4. Alcune patologie legate alla rete

Numerose sono le possibili malattie legate all'uso prolungato e incontrollato di Internet e dei dispositivi digitali in genere. Il Ministero della Salute segnala alcune tra le più insidiose.

Apprendimento

Secondo evidenze scientifiche, l'uso eccessivo di Internet, a meno che non sia finalizzato a ricerche inerenti allo studio, può determinare un approccio superficiale all'approfondimento, una minore concentrazione e una maggiore tendenza alla distrazione, con conseguenti scarsi risultati scolastici.

Dipendenza

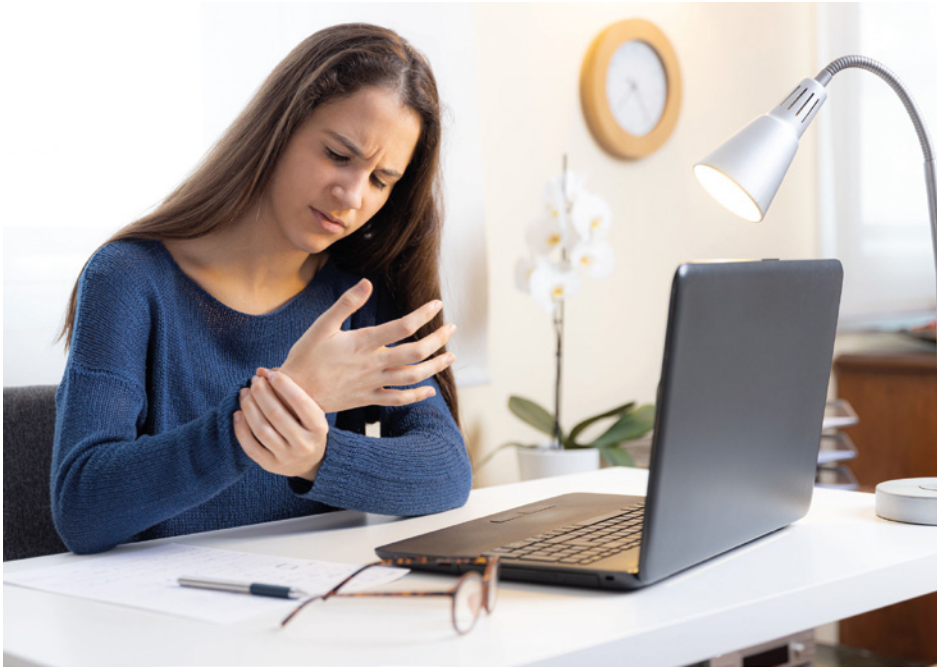
Il rischio di dipendenza è favorito dal facile accesso agli smartphone. Alcune caratteristiche della dipendenza sono: sbalzi d'umore, isolamento, perdita del controllo, ansia, astenia, difficoltà a staccarsi dallo smartphone e irritabilità dopo un periodo di astinenza.
Internet spesso rappresenta un rifugio soprattutto per i **soggetti più timidi** e con difficoltà a instaurare relazioni con i coetanei: evidenze scientifiche hanno confermato che la dipendenza dagli smartphone può essere causata soprattutto da **noia** e **solitudine**.
In generale, secondo alcuni studi, le ragazze sono le più esposte; il rischio per loro è tre volte maggiore rispetto ai ragazzi perché trascorrono più tempo sui media digitali, soprattutto alla ricerca di maggiori relazioni sociali. I **genitori** svolgono un ruolo cruciale nella prevenzione di questo tipo di dipendenze fornendo sostegno ed educazione affettiva.
Quando l'isolamento diventa patologico si parla di un fenomeno chiamato **Hikikomori**, che in Italia coinvolge circa **120 mila adolescenti** che trascorrono su Internet oltre **12 ore al giorno**, mostrando sintomi importanti di patologie psichiatriche.

Disattenzione

Un'iperattività concentrata sugli smartphone è associata a una maggiore distrazione cognitiva e disattenzione che occasionalmente mette in pericolo la stessa vita degli utenti.
Per esempio, gli Stati Uniti hanno registrato nel 2018 un aumento del 5% degli incidenti mortali che coinvolgono gli adolescenti: tra le cause, un utilizzo improprio dello smartphone da parte dei ragazzi distratti ad ascoltare musica, giocare o rispondere ai messaggi mentre camminavano o attraversavano la strada.

Muscoli

L'uso eccessivo del computer, e dello smartphone in particolare, può provocare dolori articolari e muscolari. Alcuni studi internazionali hanno evidenziato che il 70% degli adolescenti manifesta dolore al collo, il 65% alla spalla e nel 46% dei casi dolore al polso e alle dita. I disturbi muscolo-scheletrici legati agli smartphone possono essere influenzati da molti fattori, tra cui la dimensione degli schermi, il numero di messaggi di testo inviati e le ore al giorno trascorse al computer e sugli smartphone. Alcuni ricercatori hanno scoperto che l'invio di messaggi di testo è uno dei fattori che contribuisce maggiormente allo stress della colonna vertebrale cervicale e del collo negli utenti iperconnessi, ovvero quelli che trascorrono più di 5 ore al giorno in rete.



Sonno

L'uso dello smartphone e di Internet prima di dormire ha un impatto negativo sul ritmo circadiano del sonno perché causa eccitazione e difficoltà ad addormentarsi: studi recenti dimostrano che l'uso dei media digitali prima di dormire può ridurre la durata totale del sonno di ben 6 ore e mezzo durante la settimana scolastica. Un utilizzo di 5 o più ore al giorno può causare risvegli notturni e difficoltà ad addormentarsi rispetto a chi li utilizza solo un'ora al giorno.
Recenti ricerche confermano che il sonno è fondamentale per il funzionamento mentale e fisico del nostro organismo e che quando è insufficiente o non adeguato è correlato all'insorgenza di malattie cardiovascolari, disfunzioni metaboliche e diabete.
Inoltre, una scarsa qualità del sonno è correlata con l'insorgenza di conseguenze negative come stanchezza, depressione, disturbi ossessivo-compulsivi, abuso di sostanze, risultati scolastici scadenti.

Vista

L'esposizione a tablet e smartphone può interferire con la vista. L'uso continuo dello smartphone può causare il disturbo di secchezza oculare. Puoi avvertire una sensazione di corpo estraneo nell'occhio e/o bruciore oculare, sintomatologia del tutto simile a quella dell'occhio secco.
Per di più se usi lo smartphone a una distanza ravvicinata a causa del piccolo schermo, aumentano fatica oculare, abbagliamento e irritazione. L'eccessivo uso degli smartphone a breve distanza può influenzare lo sviluppo di una condizione chiamata "esotropia acquisita concomitante", cioè una tipologia di strabismo che coinvolge dapprima solo la visione lontana e poi anche quella ravvicinata.

5. Come gestire la privacy

La privacy è un diritto fondamentale: in relazione a Internet la **privacy** è il diritto di poter controllare i propri dati personali (nome, cognome, indirizzo ecc.) ed essere consapevoli di poterli condividere liberamente con persone, enti e associazioni affidabili, che diventano a loro volta titolari del trattamento delle informazioni rilasciate.
Questo diritto è espressamente tutelato dalla legge sul *Diritto alla Privacy* n.196 /2003 e dal *Regolamento Generale sulla Protezione dei Dati* (GPDR).
Ma quali sono i "**dati personali**"?
Essi sono tutte le informazioni che identificano una persona in maniera diretta, come per esempio nome e cognome, o indiretta, come il numero di cellulare. Esistono poi ulteriori informazioni più specifiche che possono fornire dati idonei a rivelare aspetti delicati della vita privata di ogni singolo individuo, come per esempio la razza, il credo religioso, l'orientamento politico, lo stato di salute e perfino la vita sessuale, i cosiddetti "**dati sensibili**".

Per i dati sensibili esistono doveri particolari per i titolari del trattamento, specificatamente indicati dalla legge. Bisogna dunque prestare sempre attenzione **ogni qualvolta effettuiamo un'iscrizione online** (**e offline**) acconsentendo alle condizioni e alle normative sulla privacy.
Se iscrivendoci a un social network concediamo necessariamente ai gestori della piattaforma di usufruire dei nostri dati, utilizzando i meccanismi di protezione della privacy si riusciranno a proteggere gli stessi dati da persone estranee (gli altri utenti del social network).
Il Codice Privacy prevede che "*il minore che ha compiuto 14 anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione*".
Leggete quindi con attenzione le informative dei siti e delle app che usate e verificate che tutte le informative e le comunicazioni utilizzino un linguaggio semplice e chiaro, facilmente comprensibile.

Alcune indicazioni per proteggere la privacy

Il primo passo per tutelare la privacy è dare importanza alla sicurezza dei **propri dati personali**.
Per farlo basta seguire alcuni semplici consigli.

1. Creare password difficili da decifrare

Per una password efficace utilizzate almeno otto lettere maiuscole e minuscole e sostituitene alcune con simboli e numeri.
Per esempio, *"Mia sorella più piccola si chiama Anna"* diventa **mS+psCan**.
Una password è inefficace quando può essere troppo facile da indovinare, per esempio se contiene l'indirizzo, la data di nascita, 123456 oppure la parola *"password"*.

2. Utilizzare buone norme di gestione delle password

Pensa due volte prima di inserire la password da qualche parte, e ricontrolla sempre di essere sull'app o sul sito corretto. Nel dubbio, prima di inserire qualcosa, rivolgetevi a chi è più esperto di voi. Inoltre, conviene usare password diverse per app e siti diversi. Possiamo avere una password principale, alla quale aggiungere qualche lettera per ciascuna app.

3. Difendersi dagli hacker con la verifica in due passaggi

La verifica in due passaggi aiuta a proteggere l'account da chiunque non debba avere accesso, richiedendo un secondo fattore di sicurezza oltre al nome utente e alla password per accedere.
Per una maggiore protezione contro il **phishing**, molti operatori online rendono disponibili servizi gratuiti o token di sicurezza fisici da inserire nella porta USB del computer o da collegare al dispositivo mobile tramite NFC (*Near Field Communication*) o Bluetooth.

4. Mantenere aggiornato il software

Per proteggere i device dalle vulnerabilità di sicurezza, usa sempre un software aggiornato per il browser web, il sistema operativo, i plug-in e gli editor di documenti. Quando ricevi una notifica per aggiornare il software, fallo il prima possibile.
Controlla regolarmente il software utilizzato per assicurarti di avere sempre installata l'ultima versione disponibile. Alcuni servizi si aggiornano automaticamente.

5. Evitare app potenzialmente dannose

Scarica sempre software per PC e app per dispositivi mobili da una fonte attendibile. Per proteggere i dati:

- controlla le app ed elimina quelle inutilizzate;
- vai alle impostazioni dello store e attiva gli aggiornamenti automatici;
- concedi l'accesso ai dati sensibili come posizione e fotografie solo alle app che ritieni attendibili.

6. Utilizzare il blocco schermo

Quando non utilizzi il computer, il laptop, il tablet o il telefono, blocca lo schermo per impedire ad altri di entrare nel dispositivo.
Per una maggiore sicurezza, imposta il blocco automatico del dispositivo quando va in sospensione.

7. Bloccare il telefono in caso di smarrimento

Se perdi il telefono o ti viene rubato, bloccalo immediatamente. Se utilizzi Google puoi visitare la pagina Account Google e selezionare *"Trova il tuo telefono"* per proteggere i dati con pochi e brevi passaggi. Sia per Android che per iOS, è possibile individuare a distanza il telefono e bloccarlo, in modo che nessun altro possa utilizzarlo e accedere alle informazioni personali.

8. Prestare attenzione alle richieste di informazioni personali

Non rispondete a e-mail, messaggi immediati o finestre pop-up di dubbia provenienza che richiedono l'inserimento di informazioni personali quali password, conti bancari, numeri di carta di credito o la data del compleanno. Anche se il messaggio proviene da un sito che ritieni attendibile, per esempio quello della banca, non fare mai clic sul link e non inviare mai un messaggio di risposta.
È opportuno visitare direttamente il sito Web o l'app e accedere all'account.
Ricorda: i siti e i servizi affidabili non mandano mai messaggi che richiedono di inviare password o informazioni finanziarie via e-mail.

9. Fare attenzione alle frodi via e-mail, ai finti premi e ai regali

I messaggi provenienti da sconosciuti sono sempre sospetti, specialmente se sono "troppo belli per essere veri", per esempio se comunicano la vincita di un premio, se offrono regali per il completamento di un sondaggio o se promuovono modi rapidi per guadagnare denaro.
Non fare mai clic sui link sospetti e non inserire mai le informazioni personali in moduli e sondaggi insoliti.

10. Controllare con attenzione i file prima di scaricarli

Alcuni attacchi di phishing più sofisticati possono avvenire tramite documenti e PDF allegati infetti.
Se trovi un allegato sospetto, puoi per esempio utilizzare Chrome o Google Drive per aprirlo e ridurre il rischio di infettare il dispositivo.

11. Usare reti sicure

Presta attenzione quando usi reti Wi-Fi pubbliche o gratuite, incluse quelle che richiedono una password. Queste reti potrebbero non essere criptate, quindi chiunque nelle vicinanze può monitorare la tua attività su Internet, per esempio i siti Web visitati e le informazioni digitate.
Anche a casa, proteggi la privacy e la sicurezza dell'attività di navigazione assicurandoti che la rete Wi-Fi sia criptata e impostando una password efficace.

12. Verificare la sicurezza delle connessioni prima di inserire dati sensibili

Quando navighi in rete, in particolare se intendi inserire dati sensibili come una password o il numero di una carta di credito, assicurati che la connessione ai siti che visiti sia sicura.
Se l'URL è sicuro, nel campo dell'URL del browser viene mostrata un'icona grigia a forma di lucchetto chiuso. ***https*** consente di mantenere sicura la navigazione sul Web collegando in tutta sicurezza il browser o l'app ai siti Web che visitate.

In conclusione...

Se sapessi che il vicino di casa o un tuo professore potrebbero leggere quello che hai inserito online, scriveresti le stesse cose e nella stessa forma?
Sei sicuro che le foto e le informazioni che pubblichi ti piaceranno anche tra qualche anno?
Prima di caricare/postare la "foto ridicola" di un amico, ti sei chiesto se a te farebbe piacere trovarti nella stessa situazione?
I membri dei gruppi ai quali sei iscritto possono leggere le tue informazioni personali?
Sei sicuro che mostreresti "quella" foto anche al tuo nuovo ragazzo/a?

6. Il dizionario della rete

ALIAS / FAKE

Falsa identità assunta su Internet (per esempio su siti di social network). L'utente può scegliere un nome di fantasia, uno pseudonimo, o appropriarsi dei dati di una persona realmente esistente.
A volte il termine fake viene utilizzato per segnalare una notizia falsa (fake news).

BANNARE / BANDIRE

L'atto che l'amministratore di un sito o di un servizio online (chat, social network, gruppo di discussione effettua per vietare l'accesso a un certo utente. In genere si viene bannati/cancellati quando non si rispettano le regole di comportamento definite all'interno del sito.

CARICARE / UPLODARE / UPLOADARE

Inserire un documento di qualunque tipo (audio, video, testo, immagine) online, anche sulla bacheca del proprio profilo di social network.

CHATTARE

Sistema di messaggistica testuale istantanea. Termine mutuato dalla parola inglese "chat", letteralmente, "chiacchierata". Il dialogo online può essere limitato a due persone, o coinvolgere un gruppo più ampio di utenti.

CONDIVIDERE

Permettere ad altri utenti, amici/sconosciuti, di accedere al materiale (testi, audio, video, immagini) che sono presenti sul nostro computer o che abbiamo caricato online.

CONDIZIONI D'USO / USER AGREEMENT / TERMS OF USE

Le regole contrattuali che vengono accettate dall'utente quando accede a un servizio. È sempre bene stamparsele e leggerle con attenzione quando si decide di accettarle. Possono essere modificate in corso d'opera dall'azienda.

CYBERBULLISMO

Indica atti di molestia/bullismo posti in essere utilizzando strumenti elettronici.
Spesso è realizzato caricando video o foto offensive su Internet, oppure violando l'identità digitale di una persona su un sito di social network.
Si tratta di un fenomeno sempre più diffuso tra i minorenni.

IDENTITÀ / PROFILO / ACCOUNT

Insieme dei dati personali e dei contenuti caricati su un sito Internet o, più specificamente, su un social network. Può indicare anche solo il nome-utente che viene utilizzato per identificarsi e per accedere a un servizio online (posta elettronica, servizio di social network, chat, blog, ecc.).

LOGGARE / AUTENTICARSI

Accedere a un sito o servizio online, facendosi identificare con il proprio nome-utente (login, user name) e password (parola chiave).

NICKNAME

Pseudonimo.

POKARE / MANDARE UN POKE

È l'equivalente digitale di uno squillo telefonico fatto a un amico per attirarne l'attenzione. In origine, su Facebook, con un "poke" (cenno di richiamo) si chiedeva a uno sconosciuto il permesso di accedere temporaneamente al suo profilo per decidere se inserirlo nella propria rete di amici.

POSTARE

Pubblicare un messaggio (post), non necessariamente di solo testo, all'interno di un newsgroup, di un forum, di una qualunque bacheca online.

PRIVACY POLICY / TUTELA DELLA PRIVACY / INFORMATIVA

Pagina esplicativa predisposta dal gestore del servizio (a volte un semplice estratto delle Condizioni d'uso del sito) contenente informazioni su come saranno utilizzati i dati personali inseriti dall'utente sul sito di social network, su chi potrà usare tali dati e quali possibilità si hanno di opporsi al trattamento.

SCARICARE /DOWNLODARE / DOWNLOADARE

Salvare sul proprio computer o su una memoria esterna (dischetto, chiave USB, hard disk esterno, ecc.) documenti presenti su Internet.
Per esempio, le fotografie o i video trovati su siti quali Facebook o su YouTube.

SERVER

Generalmente, si tratta di un computer connesso alla rete utilizzato per offrire un servizio (per esempio per la gestione di un motore di ricerca o di un sito di social network). Sono denominati "client" i computer (come quello di casa) che gli utenti utilizzano per collegarsi al server e ottenere il servizio.

TAG

Marcatore, "etichetta virtuale", parola chiave associata a un contenuto digitale (immagine, articolo, video).

TAGGARE

Attribuire una "etichetta virtuale" (tag) a un file o a una parte di file (testo, audio, video, immagine). Più spesso, sui social network, si dice che "sei stato taggato" quando qualcuno ha attribuito il tuo nome/cognome a un volto presente in una foto messa online. Di conseguenza, se qualcuno cerca il tuo nome, appare la foto indicata.