SOCIAL...MENTE

L'utilizzo inesperto dei social media può avere conseguenze emotive, sociali, finanziarie e anche giudiziarie, oltre alla diffusione indesiderata dei propri dati personali. Noi giovani, ragazzi e bambini, siamo più esposti ai pericoli dei social network, ma anche enti, banche o persino le aziende di Internet stesse non sono immuni da rischi.

Circa **2,28 miliardi di persone** (ovvero circa un terzo della popolazione mondiale) usa abitualmente i social network, una tendenza in continua crescita. Facebook è in cima alla classifica tra le piattaforme che ottengono più "clic", per non parlare poi di Whatsapp!

Dove ci sono molte persone, è inevitabile che avvengano ingegnosi furti e raggiri. Nella vita reale sono posti particolarmente popolati ad attirare questo genere di azioni, come vagoni del treno particolarmente pieni, o eventi per strada e attrazioni turistiche. Nel mondo digitale, invece, sono i social network, in cui "lavorano" **hacker, cyber criminali e falsari di dati**.

I giovani spesso sviluppano una **dipendenza da Internet**: in una fase della vita in cui i contatti sociali con i coetanei giocano un ruolo fondamentale per l'autostima e l'identificazione, i *"mi piace"* e le richieste d'amicizia inducono a passare sempre maggior tempo di fronte allo schermo del cellulare, tablet o computer.

Tutto ruota attorno alla sensazione di euforia, che provoca il rilascio di endorfine nel corpo, avvertibile anche solo per un secondo. Nei social network questo avviene quando compare un nuovo messaggio da parte di un "amico" o una nuova notifica relativa a un nostro post. Molti infatti iniziano a provare uno stato di malessere se lo smartphone non è a portata di mano per un periodo di tempo prolungato. La sensazione è quella che ci si stia perdendo qualcosa di importante, mentre la realtà al di fuori dei social media diventa sempre meno attrattiva.

Se alcuni ottengono la propria dose di felicità giornaliera su Internet, altri vivono una profonda umiliazione poiché vittime di **cyber mobbing o stalking**, il corrispettivo digitale di problemi reali. Gli studenti che vengono esclusi e discriminati dagli altri a scuola, soffrono spesso del medesimo trattamento anche in rete. Questo può riguardare minacce di violenza fisica, terribili maldicenze o la pubblicazione di foto personali. Le vittime di *stalking* invece hanno spesso a che fare con **messaggi minacciosi** e con foto pubblicamente visibili. Per questo motivo è importante che i genitori affrontino il discorso dei pericoli dei social media con noi figli, prima che abbiamo la possibilità di creare un account. Importantissime sono le **impostazioni sulla privacy**: meno dati

personali si rendono pubblici, meglio è. Infatti, gli autori di simili reati utilizzano spesso dati riguardanti la scuola, la città di residenza e i programmi per le vacanze, per infastidire, molestare o minacciare le proprie vittime, come risulta da uno studio recente.

Chi naviga in rete, lascia sempre delle tracce. Anche la condivisione di informazioni riguardo a età, musica preferita, marche gradite lasciano una traccia che si traduce in dati forniti.

Nell'informativa sulla privacy di Facebook si dice che esso non possiede solamente i **diritti di tutte le immagini che pubblicate sulla sua piattaforma**, ma anche dei dati di profilo pubblici: una sorta di **dossier digitale**, che può vendere ai propri partner.

Molti utenti non percepiscono questo come un problema, anzi, circa un quarto di essi si rallegra dell'elaborazione dei dati personali per fini pubblicitari, che si traduce in pubblicità personalizzata.

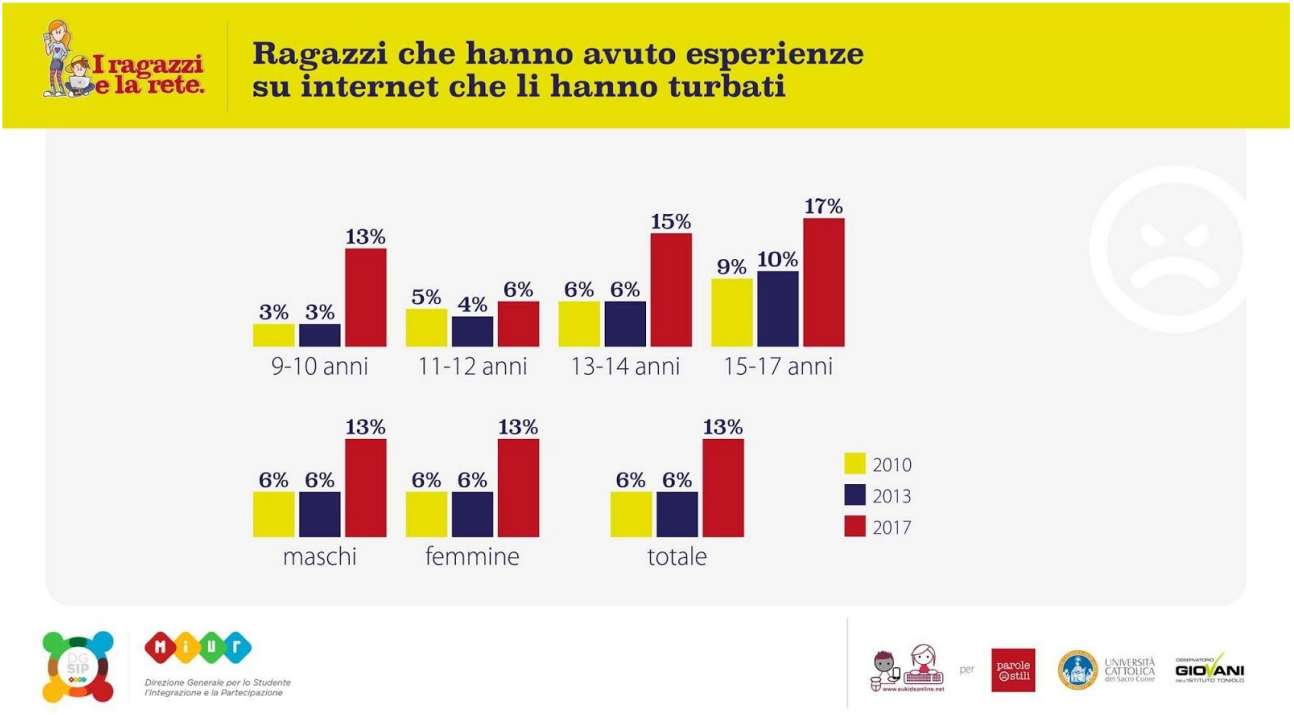
Gli utenti spesso non hanno idea del fatto che il semplice download di un'app garantisce spesso il diritto di tracciare dati di contatto e dettagli relativi alla connessione Internet. Questi dati servono alle aziende, che attraverso la loro vendita possono guadagnare soldi in brevissimo tempo o utilizzarli per rivolgersi agli utenti in maniera mirata con la pubblicità.

Quando i cosiddetti **social engineer** hanno i nostri dati a propria disposizione, il pericolo è maggiore; essi sono infatti i truffatori della nuova era, illudono le proprie vittime e mettono mano ai loro dati o ai loro risparmi. I metodi più utilizzati sono quelli di impadronirsi di una falsa identità così da ottenere la fiducia delle proprie vittime con l'inganno. Spesso si presentano come appartenenti a qualche autorità, ad esempio incaricati della banca o membri delle forze dell'ordine, o si spacciano per amici o parenti, hackerando un profilo e scrivendo ai suoi contatti.

Una variante speciale del social engineering è il **baiting** (letteralmente *adescare*).

Un **esempio**: il truffatore si finge un'azienda del settore dell'Industria Tecnologica che offre una soluzione veloce per problemi ricorrenti di un dato sistema; richiede alla vittima di installare un aggiornamento. Questo si rivela successivamente un virus.

Un altro esempio è quello del **furto d'identità**: i malfattori si servono dei nostri dati personali per fare acquisti o commettere reati.



Il Dipartimento Giustizia Minorile del Ministero ha dedicato agli adolescenti la guida online "**Pensa prima di condividere**"per l'utilizzo consapevole dei social media e la sicurezza online.
La guida ricorda soprattutto che **ciò che si condivide con gli amici può giungere ad altri:** ecco perché è importante riflettere prima di condividere, perché quello che postiamo dice chi siamo.

QUATTRO CONSIGLI

I. Le **password** non si condividono con nessuno, neppure con gli amici più stretti.
II. **Un'immagine** è per sempre: sii molto prudente e rifletti prima di condividerla. La rimozione richiede due secondi, ma chi visualizza l'immagine potrebbe catturarla con uno screenshot. Quindi devi sempre riflettere bene quando condividi.
III. Controlla le tue **impostazioni sulla privacy** per vedere chi può visualizzare i tuoi post e controlla lo strumento di selezione del pubblico ogni volta che pubblichi qualcosa, per assicurarti di condividerlo con il pubblico desiderato.
IV. Non inserire mai come "*pubblico*" il tuo **numero di telefono**, perché potrebbe diventare facilmente accessibile a tutti e quindi anche alle persone con cui non desideri condividerlo.

COME RIMEDIARE A UNA SCELTA SBAGLIATA?

Se qualcuno diffonde le tue foto, video o **contenuti offensivi o diffamatori** (ad esempio, contenuti che non sono veri e danneggiano la tua reputazione) o sono usati per perseguitarti, puoi usare lo strumento di "segnalazione sociale" e puoi anche sporgere denuncia alla polizia.
Ricordati che non sei solo: puoi sempre rivolgerti a i tuoi genitori, a un insegnante o un consulente della scuola come lo psicologo, a un altro adulto di cui ti fidi o a un telefono amico per ricevere consigli e assistenza.

LA MIA IMPRESSIONE?

Secondo me, noi ragazzi di oggi non dovremmo utilizzare Instagram o Facebook per comunicare, ma dovremmo recuperare la gioia e il divertimento attraverso l'incontro reale con gli amici, andare a fare delle passeggiate nei boschi per osservare la flora e la fauna che ci circonda, in compagnia, organizzare della scampagnate in bici o nelle brutte giornate si potrebbe andare a vedere un film a casa di un amico senza creare, però, assembramento poiché non bisogna dimenticare che dobbiamo contrastare la pandemia! Proprio perché essa ci conduce, talvolta, a periodi di isolamento, non dobbiamo cadere nella tentazione dell'utilizzo dei social media, che conducono inevitabilmente ad una solitudine costante e infelice.

G. V.
Classe II°sez.A Riva presso CHIERI