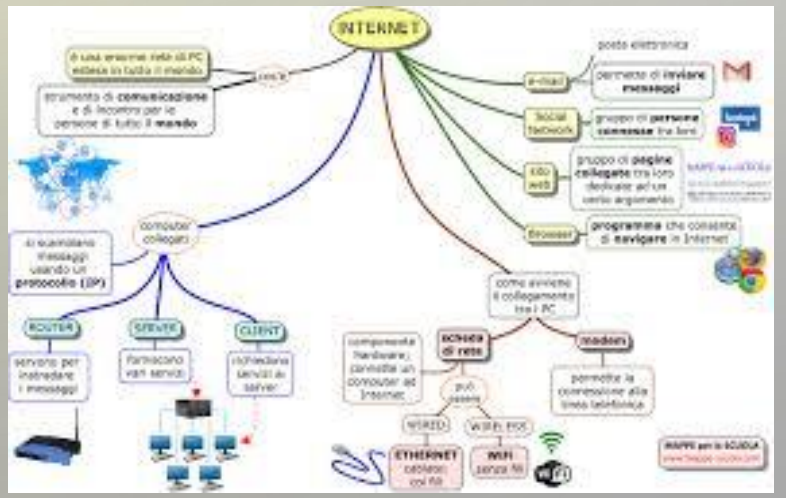
INTERNET E MINORI, ISTRUZIONI PER L'USO

Suggerimenti e spunti per genitori diversamente tecnologici

INDICE DEGLI SPUNTI TRATTATI

- Alcune regolette per l'utilizzo del Web
- Quali sono i dispositivi per navigare
- Quali programmi permettono di navigare (browser)
- Modalità d'uso degli strumenti di navigazione (strade possibili)
- Limitare il Computer , Browser e You Tube (Profili/Controllo Parentale e impostazioni di sicurezza)
- Limitare app tramite app sui dispositivi mobili (smartphone, tablet etc.)
- Internet : qualche precauzione da adottare
- I rischi nell'uso dei Social Network e di Internet
- Conclusioni



REGOLE E SUGGERIMENTI PER L'UTILIZZO DEL WEB

- “Negare l'utilizzo di internet non significa evitarne i rischi connessi

- “ Invece di negare bisogna informare/si e mettere i giovani in guardia cercando di effettuare:

- Un controllo diretto/indiretto (verifica cronologia) del loro comportamento nell'uso di internet e social

Adottare delle regole (orari e limiti) e strategie che definiscano le modalità di uso dei dispositivi

- Ricordare ai minori di non comunicare con estranei online (chat o social)
- Evitare di fornire identità reali e dati personali a utenti virtuali (usare nickname o nomi di fantasia)

I DISPOSITIVI POTENZIALMENTE “PERICOLOSI”

- Computer desktop e laptop (Windows, Mac, Linux etc.) - gestibili (profili)
- Cellulare/Smartphone/Tablet – non facilmente gestibili (no profili)
- SmartTV e Console (PlayStation, Xbox, Wii etc) – poco pericolosi
- Altri dispositivi (smartwatch etc.)

I PROGRAMMI PIU’ COMUNEMENTE USATI PER NAVIGARE

- Navigatori - Browser (Internet Explorer soppiantato da Spartan, Mozilla, Safari, Opera, Chrome etc.)
- Qualsiasi app su Play Store (Androidsamsung o altri) o su App Store (Ios – Iphone/Ipad)
- Posta elettronica – Microsoft Outlook, Mozilla Thunderbird, Opera (include mail), PostBox
- I social network (facebook, twitter, Instagram, Tik Tok, etc.)
- Messaggistica via Chat (whatsapp, snapchat, viber, Telegram, etc.)
- Altri programmi che comunicano via internet

MODALITA' D'USO DEGLI STRUMENTI PER NAVIGARE : POSSIBILI STRADE

Nel caso si tratti di un Computer:

Le strade che si potrebbero adottare per mettere in sicurezza potrebbero essere le seguenti:

- ❑ Bloccare tutto – pc, smartphone etc.
- ❑ Limitare/Bloccare tutti i contenuti "non desiderati" - Controlli Parentali automatizzati
- ❑ Attivare solo i contenuti "desiderati" – bisogna configurare i browser
- ❑ Vigilare continuamente sulle attività dei minori (più incisiva ma richiede notevole sforzo)

Nel caso si tratti di Smartphone o Tablet:

Per questi dispositivi è difficile attuare delle politiche di gestione per farlo si necessità di installare delle app apposite come ad esempio su Android Family Link (https://families.google.com/intl/it/familylink/)
o su IOS è possibile andare su Restrizioni contenuti e privacy in Tempo di utilizzo, si può bloccare o limitare determinate app e funzioni sul dispositivo del proprio figlio (https://support.apple.com/it-it/HT201304)

!!!!! Attenzione a come possono bypassare le restrizioni su smartphone

LIMITARE IL PC : USO DI DIVERSI PROFILI

Come limitare le funzionalità del computer

Creazione di account utente diversi sui diversi sistemi operativi (Windows 10, Windows 8, Mac)

- ❑ account amministratore che può fare tutto
- ❑ account utente con limitazioni per i minori L' utente con limitazioni non può installare nuovo hardware o software, evitando di installare giochi, lettori multimediali e programmi di chat (scaricati da internet) senza il vostro intervento.

Sui computer è possibile poi impostate i cosiddetti Parental Control – Controlli Parentali in Mac e Controllo Genitori in Windows vediamo dove...

Per Windows 10 : Controllo genitori in Windows 10 e 8.1

Il **programma Family Safety è integrato in Windows 10** e combina le opzioni di Windows 7 con i controlli su internet. Per attivare il controllo genitori basta andare nelle impostazioni di Windows 10, in **Account > Famiglia e altri utenti** e creare nuovi utenti che un certo account utente appartiene ad un bambino per attivare la gestione online dell'account e tutti i filtri.

Dal **sito di Family safety** si potranno leggere tutte le statistiche sull'uso del computer, sui siti più visitati, la quantità di tempo in cui è stato usato e cosi via. Si potranno poi configurare le restrizioni e i divieti attivando o disattivando varie opzioni scritte in modo chiaro in italiano: programmi utilizzabili, tempo permesso di stare su internet, filtro di siti web e avvisi su siti sconosciuti per decidere se sono permessi o vietati.

https://account.microsoft.com/family/about

Per Windows 10 o MAC : K9 Web Protection è uno dei programmi migliori gratuiti per **bloccare siti sul pc o limitare il tempo di navigazione su Facebook, Youtube o altri**

LIMITARE IL PC : ATTIVARE I CONTROLLI PARENTALI

I filtri famiglia sono programmi che permettono di bloccare l'accesso ai siti Web inadatti ai minori (siti pornografici o con scene di violenza). –

Cosa permettono di fare:

- ❑ definire profili in base all'età e alle fasce orarie (decidere quando autorizzare i minori a navigare)
- ❑ possibilità di sbloccare singoli programmi di posta elettronica o di messaggistica istantanea o giochi

Indicati per:

- ❑ soprattutto per i bambini più piccoli, poiché sono facili da aggirare per gli adolescenti pratici d'informatica

Non servono per:

- ❑ proteggere i bambini e i giovani da contenuti inappropriati diffusi attraverso i media sociali, i blog, le messaggerie istantanee e le chat.

LIMITARE L'USO DEI BROWSER

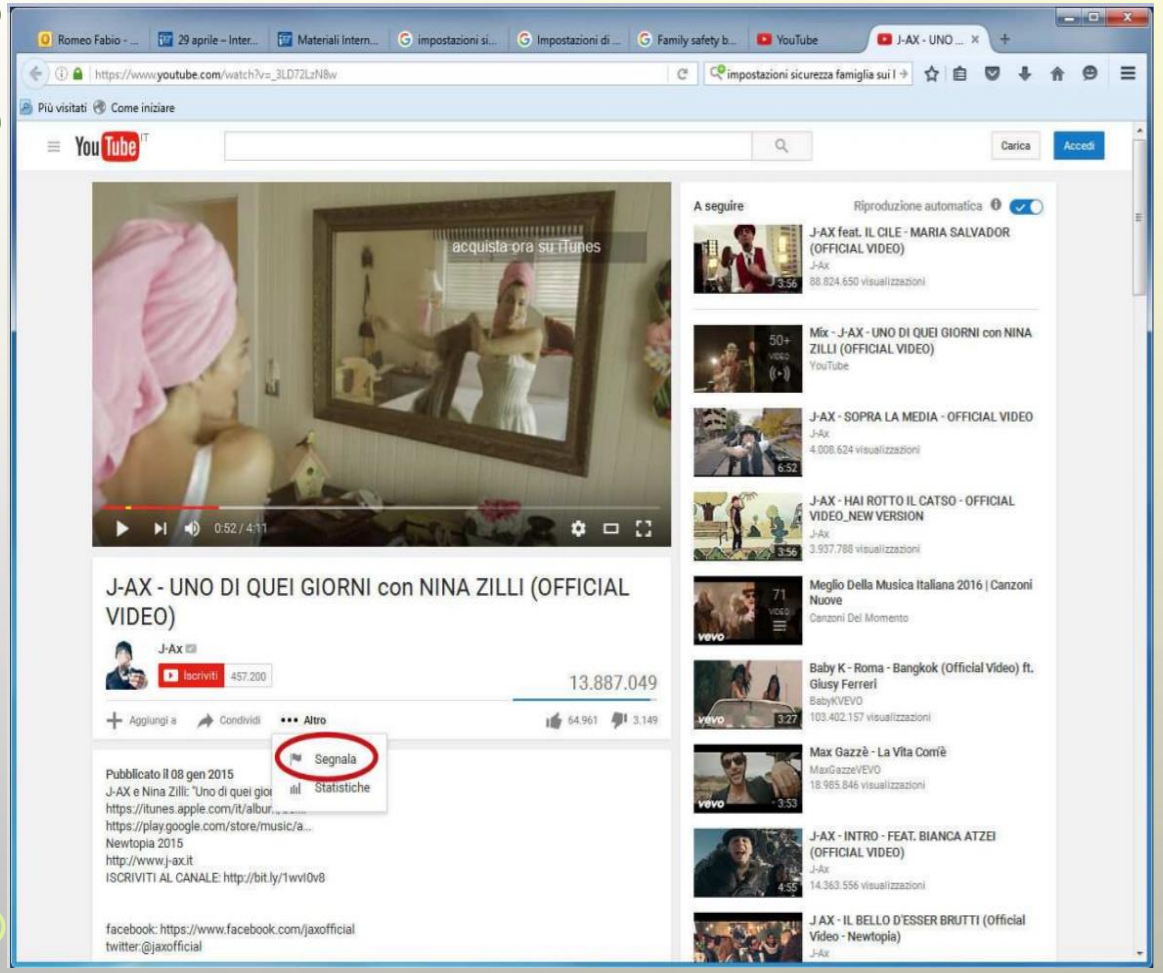
- ❑ Disattivare la tracciabilità - cookies
- ❑ Attivare la navigazione anonima se necessario (su siti particolari)
- ❑ Prestare attenzione quando i siti richiedono informazioni personali
- ❑ Impostare i siti Web aperti (ad. Esempio Disney.com)
- ❑ Impostare i siti Web non ammessi

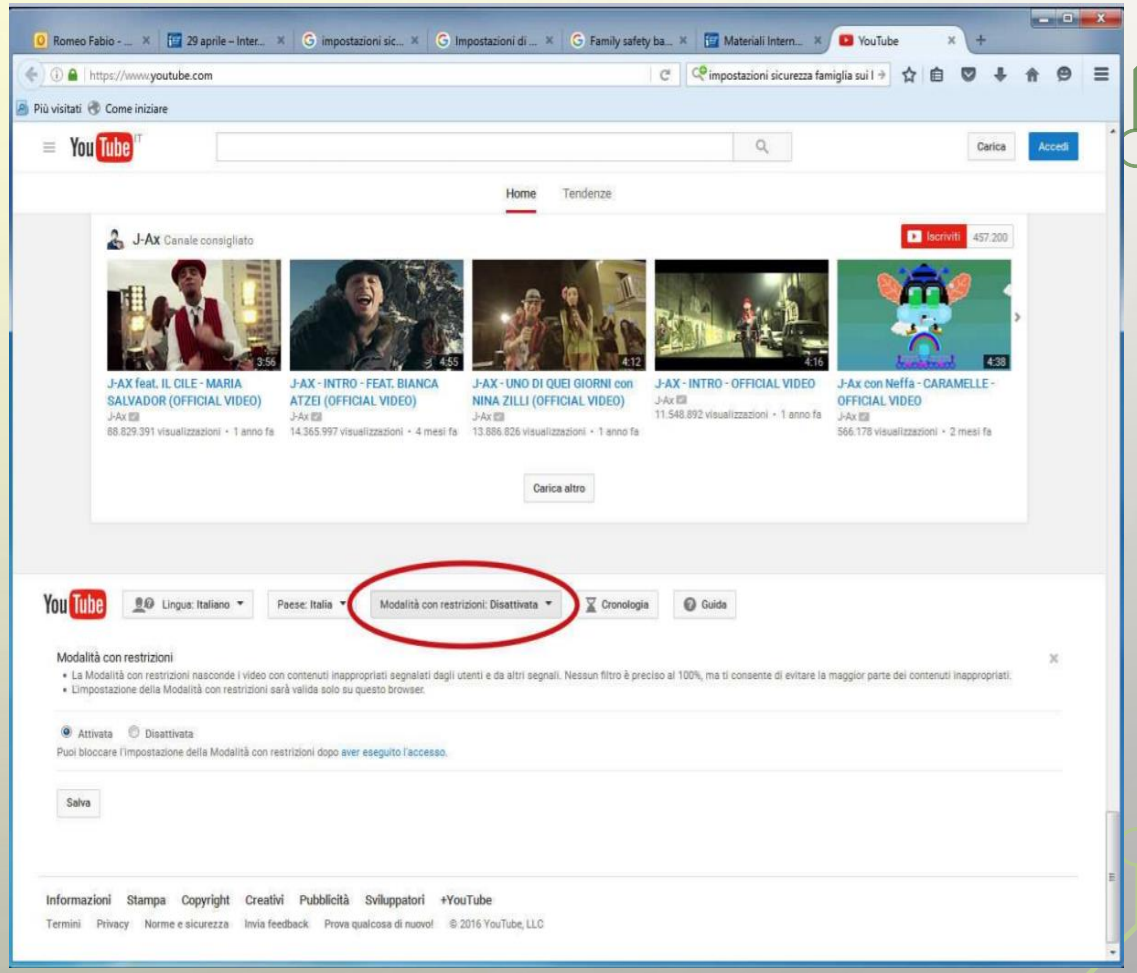
Nota Bene: le impostazioni funzionano solo sul browser che è stato configurato!!!

PC browser

Mobile browser

LIMITARE YOUTUBE DA CONTENUTI INAPPROPRIATI





INTERNET : QUALCHE PRECAUZIONE DA ADOTTARE

Utilizzare i firewall

I firewall sono degli strumenti, sia di tipo hardware che software, che permettono di vigilare sullo scambio di dati che intercorre tra il nostro pc o la nostra rete locale ed il mondo esterno.
Essi sono programmabili con una serie di regole così da inibire, ad esempio, il traffico di dati proveniente dall'esterno e diretto verso alcune porte del nostro pc solitamente utilizzate per porre in essere intrusioni telematiche.
Permettono inoltre la visualizzazione sul monitor dei tentativi di intrusione verificatisi, comprensive dell'indirizzo telematico utilizzato dall'autore di questi. In Rete possono essere facilmente reperiti numerosi software di tipo “firewall” gratuitamente.

Utilizzare un software di tipo antivirus e aggiornarlo regolarmente

Il virus informatico non é altro che un programma che ha la capacità di auto-replicarsi e, una volta scrittosi sui dischi, di effettuare una serie di operazioni sul pc ospitante più o meno dannose che vanno dalla visualizzazione sul video di un messaggio fino alla cifratura del contenuto del disco fisso rendendolo così illeggibile.
Considerato che ogni giorno vengono creati nuovi virus e che, con lo sviluppo della rete Internet, questi si diffondono con eccezionale rapidità, risulta fondamentale, non solo installare sul proprio pc un buon antivirus ma anche aggiornarlo frequentemente.
Infatti, un software antivirus, se non aggiornato con regolarità, ci potrebbe far correre rischi maggiori rispetto al non averlo affatto poiché ci potrebbe far sentire sicuri fino a trascurare le più elementari norme di sicurezza informatica.

Non aprire gli allegati ai messaggi di posta elettronica se non dopo averli esaminati con un antivirus.
Il principale veicolo di diffusione dei virus è la posta elettronica. Per essere più precisi dovremmo dire i messaggi allegati ai messaggi di posta elettronica.
Infatti, un virus può trasmettersi unicamente tramite file eseguibili (programmi con estensione exe,com,drv e dll) o contenenti una parte di codice che viene eseguita.(Es. documenti in formato word che contengono macro).
Non é quindi possibile infettare il nostro computer leggendo semplicemente il testo di una e-mail, ma è necessario eseguire il file infetto che potremmo trovare allegato alle e-mail che riceviamo.
Va inoltre precisato che l'aprire un file allegato ad un messaggio di posta elettronica, solo se si conosce il mittente non é di per se sufficiente a metterci al riparo dal contagio poiché alcuni tipi di virus prelevano dal pc infettato gli indirizzi di posta elettronica registrati nel client di posta elettronica ed inviano a questi una mail a nostro nome contenente in allegato il virus.
I destinatari di tali messaggi potrebbero aprirli (allegato compreso) senza utilizzare alcuna precauzione, forti della sicurezza che gli deriva dal conoscere il mittente.
E' il modo con cui il virus " Melissa" ha contagiato milioni di computer!
D'altro canto non possiamo neanche cestinare tutti gli allegati che riceviamo presumendo che siano infetti!
Vale quindi sicuramente la pena di perdere qualche secondo per salvare l'allegato in un supporto di memoria, per poi analizzarlo con un antivirus.
Va infine segnalato che vi sono alcuni programmi che, una volta eseguiti sul vostro pc, ne permettono il controllo da una postazione remota. Anche questi possono essere contenuti nei file allegati ai messaggi di posta elettronica e possono essere segnalati da un buon antivirus.
•Non eseguire programmi prima di averli analizzati con un antivirus
Abbiamo visto che cos'è un virus e come si trasmette. Ciò vale, ovviamente, non solo per gli allegati dei messaggi di posta elettronica ma anche per tutti quei file eseguibili contenuti nei floppy disk o nei cd rom. É quindi opportuno, in ogni caso, analizzare tali file con un antivirus prima di eseguirli.

Effettuare copie di backup

Gli antivirus riducono drasticamente i rischi di contagio ma bisogna anche tener presente che se un antivirus riconosce un virus è perché precedentemente c'è stata qualche vittima. Ciò significa che si potrebbe anche verificare il caso che il nostro antivirus, poiché non aggiornato o poiché deve analizzare un virus nuovissimo, non riconosca quel file come uno contenente un virus.
In questo caso potremmo, a seguito del contagio, anche perdere i dati contenuti sul nostro disco fisso. In tale sventurato caso sarà di vitale importanza avere effettuato, nei giorni precedenti il disastroso evento, una copia di back up dei nostri dati.

Non fornire nelle chat i propri dati personali

Non cedere alla tentazione durante le conversazioni virtuali (chat) di fornire ad ignoti utenti i propri dati personali.
Questo per un duplice motivo:

- Non possiamo sapere chi c'è dall'altra parte della tastiera.
- I nostri dati potrebbero essere utilizzati come punto di partenza per ricavare le nostre password.

Sceglier una password sicura e non comunicarla a nessuno

Per creare una password sicura bisogna seguire i seguenti accorgimenti:

- La password deve essere della lunghezza massima permessa dal sistema ed almeno di sei caratteri. Infatti, i programmi utilizzati per forzare le password richiedono, per riuscire nell'opera, un tempo direttamente proporzionale alla lunghezza delle password da violare.
- La password non deve essere un termine di senso compiuto contenuto in un dizionario poiché esistono dei programmi che, supportati dalla potenza di calcolo degli elaboratori, provano tutte le parole contenute in un dizionario.
- É preferibile che la password non contenga esclusivamente lettere minuscole o maiuscole ma che le contenga entrambe possibilmente unitamente a simboli alfanumerici come, ad esempio, asterischi e trattini. In questo modo, i programmi di forzatura delle password dovranno provare tutte le combinazioni di caratteri possibili richiedendo così, nel caso venga adottata una password lunga, molto tempo per trovarla.
- La password non deve essere in alcun modo collegata alla vita privata del titolare ed a ciò che lo circonda. Non deve quindi essere costituita dalla targa della sua auto, dalla sua squadra del cuore, dal suo nome, dalla sua data di nascita etc. Questo perché i primi tentativi fatti da chi vorrà indovinare la password saranno legati alla vita privata del titolare della stessa.
- La password non deve essere scritta da nessuna parte. A cosa serve scegliere una password inattaccabile se viene scritta su un post-it che viene lasciato attaccato al monitor o sul tappetino del mouse? Per creare una password che possa essere ricordata facilmente si può utilizzare la così detta "frase password" composta dalla prima lettera di ogni parola che compone una frase. Per esempio, dalla frase “Nel Mezzo Del Cammin Di Nostra Vita” si ricava la password NMDCDNV la quale, per risultare più difficile da indovinare, sarà composta sia da lettere maiuscole che da lettere minuscole: nmdcDNV.
- É preferibile utilizzare una password diversa per ogni applicazione. Infatti, nel caso in cui fosse scoperta i danni derivati sarebbero minori.
- La password di default, assegnata dai sistemi la prima volta che vengono utilizzati, deve essere sostituita subito.
- La password deve essere cambiata periodicamente.
- Non comunicare a nessuno la propria password! Se vi è la necessità di comunicarla a qualcuno per qualsiasi motivo, bisogna cambiarla non appena possibile.

Utilizzare, per le comunicazioni riservate, software di cifratura

Quando si inviano dati riservati é opportuno affidarsi ad un software di cifratura che permetta di crittare i messaggi da noi trasmessi.
Questo perché, se anche il messaggio venisse intercettato, senza la chiave utilizzata per crittare il documento si avrebbero solo una serie di caratteri privi di alcun senso compiuto. Vi sono numerosi programmi che offrono questo tipo di protezione, prelevabili dalla rete Internet, disponibili gratuitamente. Le considerazioni ed i consigli elencati in questo articolo sono sicuramente basici eppure se ognuno di noi si attenesse a queste elementari “misure di sicurezza” nell’utilizzo e nell’interazione con la rete Internet assisteremmo ad una drastica riduzione dei crimini informatici e soprattutto dei danni da essi arrecati.

I RISCHI DEI SOCIAL NETWORK : DAL PHISHING AL CYBERBULLISMO, I CONSIGLI PER DIFENDERSI

Internet è **un mondo virtuale ma con pericoli reali**, sebbene le azioni vengano percepite come impersonali e non arrecanti danni a sé o agli altri. In particolare, è bene conoscere **i rischi legati ai social network**, per capire come evitarli: phishing, sextortion, cyberbullismo, Revenge Porn, sono fenomeni puniti dalla legge, a proposito dei quali è necessario informare gli utenti, soprattutto i più giovani.

Ogni anno, il numero di italiani che trascorrono del tempo online è in costante crescita. Si è stimato che gli italiani in media navigano ogni giorno circa 6 ore da diversi dispositivi. Mentre è di circa 35 milioni il numero di italiani attivi sui social network, di cui circa 31 milioni ne fa uso da un device mobile, la media giornaliera del tempo che una persona passa sui social network è di circa 1 ora e 51 minuti.

Stando alle statistiche di Digital 2019, gli utenti attivi in Italia su ciascuna piattaforma risultano essere:

- 31 milioni su Facebook;
- 19 milioni su Instagram;
- 12 milioni su LinkedIn;
- 2,50 milioni su Snapchat;
- 2,35 milioni su Twitter.

Per quanto riguarda i minori da un'indagine svolta da Save The Children è emerso che è sempre più precoce l'età in cui si accede ad Internet.

La percentuale di bambini dai 6 ai 10 anni che si connette ad Internet è del 54%, percentuale che arriva al 94% nella fascia di età tra i 15 ed i 17 anni.

I RISCHI DEI SOCIAL NETWORK

Ciò che si scrive e le immagini che si pubblicano sui social network hanno quasi sempre un impatto a breve ed a lungo termine sulla vita reale . Ogni volta che si inseriscono i nostri dati personali su un sito, su un social network se ne perde il controllo, spesso si concede automaticamente al fornitore del servizio **la licenza di utilizzare il materiale** che si inserisce foto, chat, opinioni.

Ogni volta che si utilizza una carta di credito/debito, che si inserisce una password per accedere a determinati servizi, che si utilizza una carta fedeltà o una tessera di sconto messa a disposizione dalle grandi catene commerciali, che si fa un acquisto online o una ricerca tramite un qualsiasi browser, si compie inevitabilmente una piccola cessione di sovranità.

Stessa cosa avviene quando si installano sul nostro smartphone o sul nostro tablet delle app, i programmi di queste applicazioni a volte possono **richiedere l'accesso alla nostra rubrica**, alle nostre foto o contenuti multimediali che nulla hanno a che vedere con la funzionalità della APP stessa.

Inoltre, ciò che si inserisce può essere copiato e registrato dagli altri utenti del social e non sempre per fini leciti.

Tutto ciò che si scrive e posta, poi, contribuisce a rivelare a terzi chi siamo, cosa facciamo, le nostre abitudini, le nostre condizioni di salute, il nostro tenore di vita, i nostri interessi, le nostre opinioni politiche, religiose, il nostro orientamento sessuale: insomma, tutte informazioni che consentono di creare un nostro profilo che servirà alle aziende commerciali per un marketing più mirato (basta cliccare un "mi piace" su una pagina di un social o su un commento per essere analizzati e etichettati).

Nell'uso di Internet e dei social network vi sono rischi ben più gravi, dal punto di vista delle conseguenze che possono causare ad esempio:

- **furto di identità**
- **diffusione illecita di immagini;**
- **pedopornografia, sextortion, sexting e grooming;**
- **cyberbullismo;**

FURTO D'IDENTITA': L'attività attraverso la quale si può procedere al furto dell'identità digitale è il **phishing**.
Con tale attività, un soggetto cerca di appropriarsi di informazioni quali: numeri di carte di credito, informazioni relative ad account, password o altre informazioni di natura personale, convincendo l'utente a fornirle mediante falsi pretesti, come ad esempio l'invio di posta che sembra provenire da siti web noti o fidati come il sito della propria banca o della società di emissione della carta di credito.
Il phishing è il cyber attacco più utilizzato perché è quello più economico e più efficace, basta che l'utente "si fidi" ed inserisca i dati

SEXTORTION ; designa un metodo di estorsione per mezzo di immagini o filmati che mostrano la vittima mentre compie atti di natura sessuale (ad es. masturbazione) e/o nuda

SEXTING : l'invio, la ricezione e la condivisione di testi, video ed immagini sessualmente esplicite . L'invio di foto che ritraggono minorenni in pose esplicite configura il reato di pedopornografia. Almeno il 35,9% dei ragazzi conosce una persona che abbia fatto sexting. Le conseguenze possono essere gravi: diminuzione dell'autostima, insorgenza di episodi depressivi, paura, frustrazione, problemi scolastici, ecc.

GROOMING : si tratta di una manipolazione psicologica utilizzata da adulti potenziali abusanti che attraverso i social network e le chat cercano di mettersi in contatto con i minori, stabilire un rapporto emozionale con lo scopo di realizzare un'attività sessualizzata.
Dall'indagine svolta da Save The Children è emerso che le ragazze condividono maggiormente rispetto ai ragazzi foto o video personali sui profili e fatto grave è che non si rendono conto della pericolosità di inviare e/o ricevere messaggi con riferimenti sessuali, lo ritengono un comportamento diffuso tra gli amici e pertanto privo di pericolosità.
Inoltre, è emerso che molte ragazze si sono iscritte in modo autonomo su Instagram o WhatsApp, all'insaputa dei genitori ed alcune falsificando l'età ove necessario.

CYBERBULLISMO : fenomeno in cui le nuove tecnologie vengono utilizzate per intimorire, molestare, mettere in imbarazzo e far sentire a disagio alcune persone, ritenute le più deboli. Vi è inoltre un rischio maggiore per i più giovani rispetto agli adolescenti, circa il 7% dei bambini tra 11 e 13 anni è risultato vittima di prepotenze tramite cellulare o Internet una o più volte al mese, mentre la quota scende al 5,2% tra i ragazzi da 14 a 17 anni.

GAMBLING : il gioco d'azzardo per i più giovani, spesso promosso nei social media (Facebook o Youtube). Da ricordare che la partecipazione di un minore a giochi online con vincite in denaro è ovviamente vietata dalla legge.

CONCLUSIONI

- Le limitazioni sono possibili
- Per effettuarle è necessario un certo sforzo (uso di software, lingua inglese etc.)
- Importante è valutare e decidere quale sia la strada da perseguire
- Talvolta invece di preoccuparci troppo potremo anche farci guidare o insegnare dai minori questi nuovi strumenti

GRAZIE !

Luca Mastromauro