

TECNOLOGIA

Argomento: **ALTRE FUNZIONI DI INTERNET**

- A.** Studiare sul Libro dal capitolo “*La rete Internet*” da pag. 461 a pag. 464 (Chat, Forum, Blog, Wiki, Condivisione delle proprie creazioni, I Social Network, Posta Elettronica, Messaggi istantanei, Telefono e Video telefono).
- B.** **Svolgere e completare l’esercizio** Unità 5 n°10 di pag. 467 del Libro.
- C.** Leggere le pagine allegate a seguire, fare una ricerca sui Social e fare un **TEMA:**

“I Social. Evidenzia aspetti positivi e aspetti negativi. Analizza il concetto di condivisione (foto, messaggi, video) sui Social e mettilo a confronto con il concetto di condivisione reale, fisico con le persone, soprattutto tenendo presente questo particolare momento in cui siamo costretti al distanziamento sociale.”

(Non un breve e scarno pensiero, ma una riflessione seria. Immaginate sia il Tema d’esame)

Inviare entro Mercoledì 1 Aprile a: ruggeri.tecnologia@gmail.com

Buon lavoro!

Sappiamo usare consapevolmente lo smartphone?

Quasi tutti possediamo e usiamo regolarmente uno smartphone. Lo smartphone è un "cellulare intelligente", quasi un piccolo computer con il quale ci si può connettere a Internet e si può accedere a moltissimi servizi: si possono inviare e-mail, cercare informazioni sui siti web, pagare elettronicamente, giocare, scambiare messaggi, fare video, registrare audio e tante altre cose ancora. Questi dispositivi sono molto utili perché integrano le funzionalità di diversi strumenti tecnologici e si possono portare sempre in tasca. Ma **accedere a Internet e navigare sul web sono operazioni che richiedono consapevolezza e attenzione.** Condividere con leggerezza foto e pensieri online, su un social network o su un blog può creare situazioni sgradevoli o addirittura pericolose perché ogni cosa che mettiamo sul web o spediamo online, esce dal nostro controllo.

Quali pericoli puoi incontrare quando usi lo smartphone e accedi a Internet? Qual è il comportamento corretto?



un po' di definizioni

chat: applicazione che permette di comunicare con uno o più utenti attraverso la rete Internet in tempo reale.

social network: è un sito Internet nel quale gli utenti possono incontrarsi virtualmente e scambiarsi informazioni, pubblicare testi, video e immagini, chiacchiere utilizzando chat. Facebook e Instagram sono i social network più conosciuti.

blog: è un sito Internet particolare nel quale l'autore, definito blogger, pubblica regolarmente degli articoli (post) che il più delle volte gli utenti possono commentare. Spesso i post contengono immagini e video.

wiki: è un sito di scrittura collaborativa, all'interno del quale gli utenti registrati possono contribuire alla stesura dei contenuti. Ogni modifica portata dagli utenti viene registrata ed è quindi possibile, in ogni momento, risalire all'autore ed eventualmente ripristinare lo stato originale delle pagine.

postare: pubblicare testi, immagini e video in social network o blog.

RICORDA: per navigare sicuro non dimenticare di...

- installare e mantenere aggiornato nel tuo dispositivo un **antivirus**, cioè un software che lo protegga dai *malware*, quei programmi realizzati con lo scopo di creare un danno alla macchina che li esegue o all'utente.
- utilizzare sempre una **password** diversa per ogni sito in cui ti registri; componila in modo che non contenga informazioni facilmente riconducibili a te (data di nascita, nome del fratellino ecc.)
- fare attenzione alle pagine che visiti, perché potresti capitare su siti creati per danneggiare il tuo dispositivo o rubarti informazioni personali. Controlla la presenza del "**lucchetto**" (sulla barra degli indirizzi) prima di inserire password e dati che ti riguardano: è un simbolo che garantisce la sicurezza della pagina che stai visitando; chiudi subito le pagine segnalate come sospette.
- consultare con prudenza le e-mail, controllare il mittente ed **evitare di aprire allegati o link** in essa contenuti, se provengono da soggetti che non conosci. Corri il rischio di "infettare" il dispositivo con un malware o di cadere in una frode informatica con lo scopo di rubarti informazioni riservate come password o codici di carte di pagamento (*phishing*).
- utilizzare un **nickname**, cioè un soprannome, quando comunichi con qualcuno all'interno di una chat o di un forum, per proteggere la tua privacy.

DIFENDI LA TUA SOCIAL PRIVACY



1 Internet e la diffusione online delle informazioni pongono seri problemi di *privacy* e minacciano il diritto alla **riservatezza della propria vita privata** e dei propri dati personali. Ogni volta che intervieni con un post su un social network, chiacchieri su una chat, o pubblichi una fotografia che ti riguarda, metti una parte della tua vita privata sul web, a disposizione di tutti. Una volta nel cyberspazio, infatti, i tuoi dati non sono più sotto il tuo controllo.



2 Non è una buona idea rendere noti il tuo indirizzo, il numero di telefono, la mail, l'età, la scuola o altri luoghi che frequenti, perché qualche *criminale informatico* potrebbe approfittarne per scopi illegali.



3 Non è consigliabile neppure pubblicare foto scattate in situazioni strane, che giudichi divertenti: fra qualche anno queste stesse foto potrebbero metterti in imbarazzo. Ricorda: anche online hai una **reputazione che tutti vedono** e che devi **difendere**, pubblicando solo contenuti che non ti mettano in difficoltà.

UNA FOTO DI TROPPO....



4 Con il termine inglese *sexting* (*sex + texting*) si fa riferimento alla diffusione di video, foto o testi a **contenuto sessuale esplicito** nei social network, nelle chat o nei messaggi.



5 Presta particolare attenzione a ciò che pubblichi attraverso lo smartphone: quando condividi foto "sexy" o in pose provocanti, anche solo con un amico fidato, non puoi essere certo che non finiranno online e che non saranno diffuse dall'altra persona a tua insaputa, oppure che non saranno scaricate da criminali informatici e usate illegalmente con finalità disoneste.



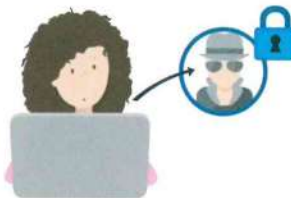
6 Se fossi tu a ricevere materiali di questo tipo, è importante che tu non contribuisca alla loro diffusione, anche se ti sembra uno scherzo divertente. **Cancellali**. Rivolgiti sempre a un adulto di fiducia (un genitore, un insegnante...) se la situazione ti mette a disagio.

CONOSCI VERAMENTE CHI C'È DALL'ALTRA PARTE?



7 Evita contatti online con chi non conosci realmente nella vita. Ci sono malintenzionati in rete che potrebbero entrare in contatto con te attraverso le chat e i giochi online, i social network, i messaggi. Si chiamano **adescatori**: fingendosi persone diverse da quelle

che in realtà sono (per esempio un tuo coetaneo, un ragazzo che ha i tuoi stessi interessi ecc.), cercano di conquistare la tua amicizia e spingerti a incontrarli o a fare quello che ti chiedono: non accettare mai un invito di chi hai "conosciuto" solo in rete.



8 Se qualcuno che hai conosciuto così ha comportamenti che ti sembrano sospetti, se certe richieste, conversazioni o immagini ti sembrano strane o sconvenienti, rivolgiti subito ai tuoi genitori o a un adulto di fiducia: salva le conversazioni o le immagini che ti sono state inviate, e mostrale loro con fiducia, **bloccando il profilo** di queste persone.