Di seguito **6 consigli pratici**, spunti che è possibile interpretare con lo stile educativo di ciascuno e che possono aiutare genitori e figli ad orientarsi.

1. Presenza e role model

Affianca i più piccoli sin dalle prime navigazioni, capisci i loro interessi, mostra i siti buoni. Sii di esempio a tuo figlio nel rapporto con la tecnologia perché il buon esempio vale off line e vale on line! La rete, in fondo, è l'eco dei nostri comportamenti.

2. Regole e responsabilità

Stabilisci dei limiti all'uso della rete, poiché meno ore = meno rischi. Incoraggia l'uso dei dispositivi di accesso alla rete negli spazi comuni della casa, spiega che ciò che si fa on line lascia tracce e che può essere identificato: la rete è reale!

3. Linguaggio

Insegna a non rispondere alle provocazioni in chat o sui social, a tenersi alla larga dai "troll", a non essere mai offensivo ed a rispettare l'altro come se lo si avesse di fronte.

4. Privacy

Spiega l'importanza di mantenere riservata l'identità in rete: nome, età, indirizzo, etc. non si dicono! Di' di non compilare mai moduli on line senza prima averti consultato. Affianca tuo figlio mentre crea i suoi profili social, scegli con lui la foto e le impostazioni di privacy e, se adolescente, fa' in modo che legga assieme a te tutte le clausole sulla riservatezza dei dati così da comprendere la dimensione del problema.

5. Profili fake

Insegna a tuo figlio che non deve incontrare di persona chi ha conosciuto in rete, che prima di riconoscere on line qualcuno come amico bisogna dubitare e porsi delle domande e che noi possiamo aiutarlo a distinguere ed a ragionare.

6. Difendersi con la tecnologia

Dispositivi mobili, console di gioco, piattaforme di streaming e PC offrono oggi molti strumenti per consentire l'utilizzo sicuro da parte dei minori. A seconda dei casi è possibile per i genitori limitare i contenuti in base all'età, impostare una lista di "app" consentite e dei limiti di tempo su base giornaliera, monitorare la posizione del dispositivo, imporre delle fasce orarie per l'utilizzo e regolare i download. Si tratta di contromisure efficaci che però, via via che i nostri figli cresceranno, saranno inevitabilmente terreno di negoziazione.

Aiutare i nostri figli a stare on line liberando il potenziale delle nuove tecnologie e limitando allo stesso tempo i rischi non è un compito facile, non è lavoro di un giorno e non sempre riesce. Se però noi grandi non impariamo ad essere credibili agli occhi dei giovani quando parliamo di tecnologia, il compito diventa impossibile. Informiamoci perciò, studiamo, sperimentiamo. Facciamo pesare i nostri anni e poi giochiamocela con l'esperienza.

1. Limitare e mantenere a un livello professionale le informazioni personali

Potenziali datori di lavoro o clienti, non hanno bisogno di conoscere la situazione sentimentale o l'indirizzo di un utente. Ciò che è di loro interesse riguarda l'ambito delle competenze e delle esperienze pregresse e come mettersi in contatto con una determinata persona. Non si dovrebbero distribuire ad ogni singolo estraneo online, ovvero milioni di persone, vere e proprie informazioni personali.

2. Continuare ad usare le impostazioni sulla privacy

I distributori, come del resto gli hacker, desiderano conoscere tutto dell'utente: entrambi possono carpire molte informazioni dalla navigazione e dall'uso dei social media. Tuttavia, ognuno può prendersi cura dei propri dati. Come notato da Lifehacker, sia i browser Web sia i sistemi operativi mobili hanno impostazioni per proteggere la privacy online dell'utente. I siti più importanti come Facebook hanno anche a disposizione impostazione per aumentare la privacy. Talvolta, queste ultime sono (deliberatamente) poco evidenti poiché le aziende vogliono che l'utente inserisca le informazioni personali per il loro valore commerciale. Assicurarsi di aver abilitato queste protezioni della privacy e di mantenerle attivate.

3. Navigare in maniera sicura

Nessuno sceglierebbe di camminare in un posto pericoloso: è bene adottare la stesa scelta online. I cybercriminali utilizzano contenuti che non passano inosservati come esca, poiché sanno che le persone vengono attratte da argomenti ambigui e potrebbero abbassare la guardia quando sono alla ricerca di determinati temi. Il demi-monde di Internet è ricco di insidie difficili da individuare e un click poco attento potrebbe mettere a repentaglio i dati personali o infettare con un malware il dispositivo di un utente. Se si resiste alla tentazione, non si dà agli hacker l'opportunità di poter agire.

4. Assicurarsi che la connessione Internet sia sicura

Quando qualcuno è online in uno spazio pubblico, per esempio se si usa una connessione Wi-Fi pubblica, la rivista PCMag ha affermato che in quel momento non vi è un controllo diretto sulla sicurezza della rete stessa. Gli esperti aziendali di cybersecurity si preoccupano a causa degli "endpoint", luoghi in cui una rete privata si connette con il mondo esterno. L'endpoint vulnerabile di ciascuno è rappresentato dalla connessione Internet locale. Assicurarsi che il proprio dispositivo sia sicuro e, in caso di dubbio, aspettare un momento migliore (per esempio finché non è possibile connettersi ad una rete Wi-Fi sicura) prima di fornire informazioni come il numero del proprio conto bancario.

5. Prestare attenzione a ciò che si scarica

Uno degli obiettivi principali dei cybercriminali, è quello di condurre la vittima, col raggiro, a scaricare malware, programmi o app portatori di malware, oppure tentano di rubare informazioni. Questo malware può presentarsi sotto forma di app: dai giochi più scaricati a strumenti che controllano il traffico o le condizioni meteo. Come PCWorld consiglia, è bene non scaricare app che risultano essere ambigue o che provengono da un sito poco affidabile.

6. Scegliere password complesse

Le password sono tra i punti più deboli nell'intera struttura della sicurezza su Internet, ma attualmente non vi sono soluzioni in merito. Il problema delle password è il seguente: gli utenti tendono a scegliere chiavi di accesso semplici per poterle ricordare (come "password" oppure "123456"), semplici da indovinare anche per i cyberladri. Scegliere password complesse, in modo che sia difficile risalirvi anche per i cybercriminali. Il software Password manager può essere utile per la gestione di più password in modo che l'utente non le dimentichi. Una password complessa è una password singolare e di difficile composizione, formata da almeno 15 caratteri, da varie lettere, numeri e caratteri speciali.

7. Fare acquisti online da siti sicuri

Ogni volta che si fanno acquisti online, bisogna fornire informazioni riguardanti la propria carta di credito o il proprio conto bancario, proprio quello che i cybercriminali sono più bramosi di ottenere. Immettere queste informazioni solo in siti che forniscono connessioni sicure e criptate. Come l'università di Boston ha sottolineato, è possibile identificare siti sicuri cercando indirizzi che inizino per *https:* (la S sta per *sicuro*) invece di cercare siti che inizino semplicemente per *http:*.Tali siti protetti potrebbero inoltre essere contraddistinti dall'icona del lucchetto vicino alla barra degli indirizzi.

8. Prestare attenzione a ciò che si posta

Internet non dispone del tasto per l'eliminazione, come ha riscontrato il giovane candidato del New Hampshire: ogni commento o immagine che si posta online può rimanerci per sempre, perché rimuovere l'originale (per esempio da Twitter) non permettere di rimuovere qualunque copia fatta da altri. Non esiste alcun modo per "tornare indietro" e cancellare un commento che non avresti voluto scrivere, o quel selfie imbarazzante fatto ad una festa. Non mettere online ciò che si vorrebbe tenere nascosto alla propria mamma o a un potenziale datore di lavoro.

9. Prestare attenzione a chi si incontra online

Le persone che si incontrano online non sono sempre chi dichiarano di essere, infatti potrebbero persino non essere reali. Come InfoWorld ha riportato, i falsi profili all'intero dei social media rappresentano un modo comune per gli hacker per avvicinarsi ad utenti ignari e derubarli. Bisogna essere tanto cauti e giudiziosi nella vita sociale in rete quanto lo si è in quella personale.

10. Mantenere aggiornato il programma antivirus.

Il software di sicurezza Internet non può proteggere contro ogni minaccia, ma eliminerà e rimuoverà la maggior parte dei malware, perciò bisognerebbe accertarsi che sia aggiornato. Assicurarsi di essere al passo con gli aggiornamenti del sistema operativo e con quelli delle applicazioni che si utilizzano, poiché costituisco un elemento vitale per la sicurezza.

Tenere a mente queste 10 regole di base di sicurezza su Internet e si eviterà di incappare in molte spiacevoli sorprese, in agguato per i disattenti.

Per i genitori:

1. Fa' sì che Internet sia un’attività familiare, ad esempio è buona norma scegliere insieme la lista dei siti da visitare
2. Colloca il computer in stanze comuni, non nella cameretta del bambino
3. Concordate insieme il tempo giornaliero da dedicare alla navigazione
4. Usa dei filtri (dal semplice controllo della cronologia dei siti visitati ai software dedicati al parental control, blacklist, software spia) e verifica periodicamente che funzionino
5. Proteggi il computer con software sempre aggiornati (firewall, antivirus e anti-spam)
6. Custodisci le informazioni personali (prima di inserire dati sensibili controlla che siano presenti i segni di sicurezza della pagina: la scritta https nell’indirizzo e il segno del lucchetto)
7. Mantieni segreta la parola chiave (i ruoli di chi naviga – il ragazzo – e di chi amministra il computer – il genitore – vanno mantenuti distinti)
8. Utilizza password solide (almeno 8 caratteri, con maiuscole e minuscole, lette-re, numeri e simboli), cambiale a seconda dei siti e rinnovale di frequente
9. Non scaricare programmi se non ne conosci la provenienza
10. Insegna ai figli la buona educazione in rete, informali che esiste la netiquette.