1. INTRODUZIONE

A chi ci rivolgiamo. Come usare questa guida.

Questa breve guida è rivolta a **genitori, insegnanti** e **pediatri** di ragazzi dai 9 ai 14 anni.

Abbiamo voluto creare uno **strumento rapido** e **agevole** per aiutare chi ha, ogni giorno, rapporti con i **nativi digitali**.

Le nuove tecnologie offrono innumerevoli opportunità di apprendimento e di socializzazione, ma possono anche nascondere insidie, che devono essere conosciute e affrontate, senza demonizzazioni.

È importante che i ragazzi siano sostenuti e indirizzati a un rapporto sano, positivo ed equilibrato verso la rete.

L'**argomento è complesso** e richiede una grande sensibilità e attenzione. Per questo vi invitiamo a leggere con cura e a **riflettere sui contenuti che sono presentati prima di condividerli con i ragazzi.**

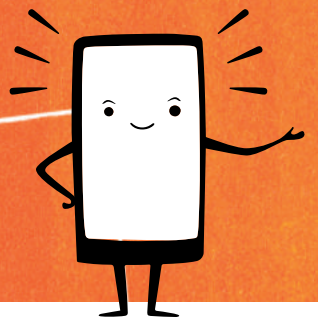
Fra i molti consigli che troverete, ci sentiamo di anticiparne due: **ascolto** e **dialogo** con i ragazzi sono la base per comprendere quello che essi cercano in rete, perché la rete è parte della loro vita quotidiana, e non un mondo a parte.

La guida nasce da una collaborazione fra la **Società Italiana di Pediatria**, la **Polizia postale**, **Google**, **A.N.C.I.** e **UniCredit Foundation**.

Buon lavoro a tutti.

2. CONOSCERE LA RETE

Tanti vantaggi per i nostri ragazzi.

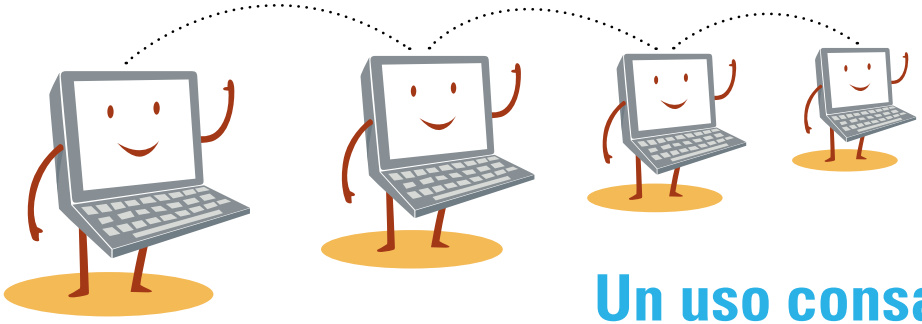


I nostri ragazzi sono spesso più competenti in ambito digitale rispetto a noi: per loro le nuove tecnologie digitali sono infatti un **luogo familiare** con cui hanno imparato a relazionarsi fin da piccoli.

Come ogni tecnologia creata dall'uomo, la rete può avere effetti benefici di grande importanza, ma al tempo stesso può anche comportare rischi che è bene conoscere. Come spesso succede quello che può essere sbagliato è l'uso del mezzo, non il mezzo in sé.
Per questo è importante incoraggiare i ragazzi verso un utilizzo responsabile di Internet e dei dispositivi in generale.

Le **opportunità** che le nuove tecnologie digitali offrono ai ragazzi sono molteplici:

- sviluppare le abilità di **ricerca** e di **valutazione** critica delle informazioni,
- potenziare il senso di competenza e di autoefficacia,
- incrementare le abilità relazionali,
- entrare in contatto con interlocutori di tutto il mondo, sradicando pregiudizi e luoghi comuni.



Un uso consapevole della rete

Apprendimento

I media digitali sollecitano la capacità del nostro cervello nel processare le informazioni, producendo una maggiore funzionalità dell'attenzione e della memoria. Tuttavia vi è il rischio che questa rapidità possa poi essere causa di maggiore superficialità nell'elaborare le informazioni e possa aumentare il rischio di perdere la concentrazione e di avere una capacità ridotta di tollerare le frustrazioni.

Socializzazione

Le nuove tecnologie di rete possono comportare una sovrapposizione tra "sfera pubblica" e "sfera privata": nei ragazzi la costruzione di una rete sociale ampia è un elemento prioritario, tanto che a volte può andare a scapito della riservatezza della propria vita privata, spesso esibita, con ripercussioni che vanno al di là della loro sfera di controllo. I nativi digitali costruiscono la propria identità anche tramite i nuovi media e spesso integrano la realtà dei rapporti in presenza con quella online. Questo fatto, se da un lato accresce la possibilità di contatti, dall'altro può comportare pericoli di adescamento.

Identità

L'uso della rete può servire ai ragazzi per uscire dalla timidezza e dall'isolamento, così come per stabilire relazioni senza temere, ad esempio, pregiudizi legati al loro stile o aspetto fisico. Per coloro che si sentono isolati e depressi, Internet e smartphone possono fornire un aiuto per migliorare l'umore, sentirsi più autonomi e indipendenti, essere accettati dai coetanei e aumentare l'autostima. A fronte di questi effetti positivi la rete può essere utilizzata per discriminare, isolare e umiliare coloro che sono ritenuti diversi da noi.

3. NAVIGARE SICURI

I rischi principali e come evitarli.

Per spiegare ai ragazzi quali siano le buone **regole di comportamento** in rete si può partire da un semplice esercizio: immaginarsi fuori dal contesto della rete e iniziare a porsi con loro precise domande. Ad esempio: ti comporteresti allo stesso modo se sapessi che il tuo insegnante potrebbe leggere quello che hai inserito online? Prima di caricare/postare la "**foto ridicola"** di un tuo amico/a ti sei chiesto se a te farebbe piacere trovarti in quella stessa situazione? Hai mai pensato cosa succederebbe se un estraneo iniziasse a far circolare **notizie false** su di te? Domande di questo genere aiutano ad affrontare, ma soprattutto a gestire le relazioni umane, sia quelle autentiche, fatte di strette di mani, sorrisi e scambi di opinioni sia quelle virtuali fatte di **conversazioni in chat** e **commenti digitali**.

I RISCHI PRINCIPALI

1 **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.

2 **Cybermolestie**
Comportamenti indesiderati e molestie attuate tramite Internet e i social network.

3 **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.

4 **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.

5 **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.

6 **Adescamento, violenze sessuali online, sexting, sextortion**
I minori in questo caso sono sottoposti attraverso la rete ad 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.

7 **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).

8

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.

9

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.

10

Revenge porn

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

11

Challenges

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

È importante educare i ragazzi a una navigazione consapevole. Troverete qui una serie di consigli facilmente applicabili con i ragazzi: basta **trovare un po' di tempo**, essere capaci di ascoltare e parlare argomentando e non imponendo.

Insegnate che cosa sono le loro tracce digitali online

Insieme ai vostri figli svolgete, per esempio, una ricerca online su un cantante che amano e parlate dei risultati che trovate. Vi consigliamo di controllare i risultati prima di farlo con loro. Spiegate quindi che chiunque può avere molte informazioni sulle persone in rete e che queste tracce digitali online restano nel tempo.

Aiutateli a dare il giusto peso a ciò che vedono online

Spiegate loro che ciò che viene condiviso online dagli amici rappresenta solo un aspetto della realtà, di solito i momenti migliori. Ricordate loro che tutti trascorrono dei momenti noiosi, tristi o imbarazzanti che non condividono. È importante aiutare i ragazzi a capire che le persone e le situazioni online non sono sempre quello che sembrano.

Definite chiare regole familiari su che cosa condividere

Chiarite ai ragazzi che cosa è opportuno condividere online e cosa non è opportuno condividere, ad esempio foto o informazioni private, e quali sono le implicazioni e/o i rischi. Provate a scattare qualche foto insieme e parlate di come si mette in pratica una condivisione responsabile. Ad esempio, invitateli a fermarsi per qualche secondo e a ragionare sulle possibili conseguenze prima di condividere immagini, non solo di sé, ma anche di altri. Ricordate loro di parlare sempre con voi se hanno dubbi. Invitateli a evitare un'eccessiva condivisione di contenuti. Chiarite loro qual è il comportamento corretto da tenere online: trattare gli altri come si vorrebbe essere trattati ed esprimere online solo ciò che si direbbe apertamente a qualcuno sono ottimi punti di partenza.

Spiegate cos'è il furto d'identità

Spiegate loro perché qualcuno potrebbe volere impossessarsi delle loro password o dei dati privati. Chiarite loro i rischi collegati al fatto che chiunque potrebbe utilizzare il loro account e usarlo al loro posto.

Aiutateli a individuare i tentativi di phishing e le truffe

I ragazzi possono non rendersi conto che alcune persone vogliono indurli a farsi consegnare le loro informazioni personali. Evidenziate loro l'importanza di confrontarsi con voi se ricevono un messaggio, un link o una email da uno sconosciuto con una richiesta di informazioni sull'account oppure con un allegato strano. Spiegate loro che certe truffe ingegnose sembrano provenire da un amico mentre provengono da soggetti diversi. Se un messaggio sembra strano, chiedete loro di controllarlo insieme. Dite loro di prestare attenzione ai seguenti tipi di email:

- Richieste urgenti di denaro.
- Persone che sostengono di essere bloccate in un altro paese.
- Persone che dicono che è stato rubato loro il telefono e non possono quindi essere chiamate.

Cercate insieme indizi sulla sicurezza

Visitate un sito web insieme e cercate simboli di sicurezza. A fianco dell'URL appare un lucchetto oppure l'URL inizia con https, che indica che è sicuro? L'URL e il nome del sito corrispondono? Fate notare i simboli che devono cercare quando visitano un sito e che ne garantiscono la sicurezza

Ragionate insieme sull'importanza della privacy

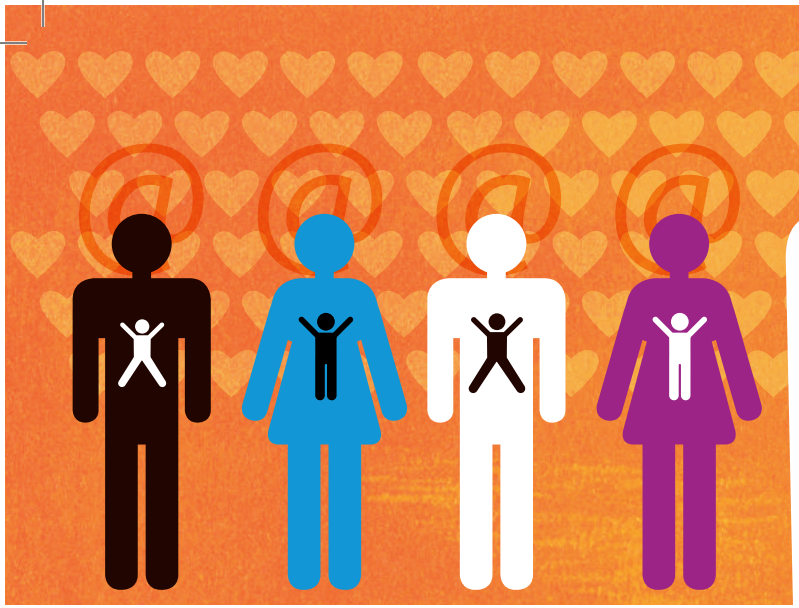
Parlate delle informazioni che dovrebbero mantenere private, ad esempio l'indirizzo di casa, le password o il nome della scuola che frequentano. Invitateli a rivolgersi a voi se uno sconosciuto chiede loro informazioni di questo tipo.

Favorite un uso positivo della rete

Internet è un potente amplificatore che può essere usato per diffondere positività e negatività. Aiutateli a fare la cosa giusta applicando il concetto "tratta gli altri come vorresti essere trattato" alle loro azioni online. Questo crea un impatto positivo sugli altri e scoraggia il bullismo.

Create un dialogo sul bullismo online

Parlate insieme di come le persone sfruttano



gli strumenti online per ferire intenzionalmente gli altri. Chiedete se loro o i loro amici hanno subito episodi di cattiveria sul web. Alcune domande utili possono essere: in che forma è avvenuta l'offesa o l'abuso?
Come si è dispiegata? Pensavi di avere il potere di fermarla, magari parlando con un adulto?

Parlate del significato che si nasconde dietro le parole e promuovete la positività

Parlate del "tono di voce" e ricordate loro che è facile fraintendere ciò che qualcuno intende dire online. Invitateli a partire dal presupposto che gli altri abbiano buone intenzioni e a confrontarsi con i diretti interessati se non sono certi di quello che qualcuno voleva dire. Parlate della sensazione piacevole che si prova all'inviare e ricevere messaggi positivi online. Prendete in considerazione la possibilità di utilizzare insieme una delle app che utilizzate nell'inviare un complimento o un messaggio positivo.

Invitate i ragazzi a parlare con voi

Una lezione valida per tutto il mondo digitale: quando i giovani si imbattono in qualcosa di dubbioso o che ritengono potenzialmente pericoloso, dovrebbero sentirsi a proprio agio nel rivolgersi a un adulto fidato. È bene favorire questo tipo di comportamento incoraggiando una comunicazione aperta in famiglia e a scuola.

Parlate delle loro attività online

Trascorrete del tempo a discutere del modo in cui la tecnologia è utilizzata dai ragazzi. Mostrate interesse per le app o i siti più utilizzati da loro e chiedete di farveli conoscere. Scoprite in che modo le usano e che cosa piace loro.

Impostate dei limiti variabili nel tempo

Impostate delle regole sui loro account, ad esempio per i filtri sui contenuti e per i limiti di tempo. Informateli che queste restrizioni possono cambiare man mano che crescono. Le impostazioni dovrebbero evolversi nel tempo.
Non affermate:
"È così, punto e basta".

Incoraggiate il tempo di qualità trascorso online

Invitateli a utilizzare giochi e app che insegnino loro a essere creativi, a risolvere i problemi, a imparare le lingue.

4. CRESCERE SANI

Conoscere i rischi e le patologie legate alla rete.

Questi sono i **principali rischi**, che è bene conoscere per aiutare i ragazzi a correggersi per condurre una vita sana ed equilibrata.

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.

Una buona relazione genitore-adolescente contribuisce a prevenire il rischio di dipendenza diminuendo il livello di ansia sociale spesso diffuso tra i ragazzi. 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.

SONNO

L'uso dello smartphone 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 causa conseguenze negative nella vita dei ragazzi come stanchezza, depressione, disturbi ossessivo-compulsivi, abuso di sostanze, risultati scolastici scadenti.

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. Ad 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. Anche qui l'esempio dei genitori è fondamentale per i figli.

APPRENDIMENTO

Secondo evidenze scientifiche, l'uso eccessivo di smartphone, 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.

VISTA

L'esposizione a tablet e smartphone può interferire con la vista. L'uso continuo dello smartphone può causare il disturbo di secchezza oculare. Il ragazzo può avvertire una sensazione di corpo estraneo nell'occhio e/o bruciore oculare, sintomatologia del tutto simile a quella dell'occhio secco. Per di più gli smartphone sono utilizzati a una distanza ravvicinata a causa del loro piccolo schermo, inducendo quindi 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 si verifica quando appare una forma di diplopia che coinvolge dapprima solo la visione lontana e poi anche quella ravvicinata.

MUSCOLI

L'uso eccessivo dello smartphone 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 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.

5. GESTIRE LA PRIVACY

Come tutelare i dati personali.

La privacy è un diritto fondamentale e come tale deve essere fatto comprendere e insegnato ai nostri ragazzi.

Nello specifico 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 196 /2003 e dal Regolamento Generale sulla Protezione dei dati (GPDR).

Ma cosa intendiamo con la parola **"dati personali"**? Essi sono tutte le informazioni che identificano una persona in maniera diretta, come ad 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 ad 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 aggiornato (art. 2 quinquies) 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. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale".

Leggete quindi le informative dei siti e delle app che usano i vostri ragazzi: considerate anche

che il Codice della privacy prevede che, nel caso in cui il minore dia il consenso direttamente, tutte le informative e comunicazioni devono utilizzare un linguaggio semplice e chiaro, facilmente comprensibile dal minore stesso.

Siate consapevoli che la responsabilità di gestione delle attività in rete dei vostri figli minorenni potrebbe essere vostra: l'articolo 2048 del Codice Civile prevede infatti espressamente che padre e madre, congiuntamente tra loro, rispondono dei danni cagionati dal figlio salvo che provino di non aver potuto impedire il fatto.

Il primo passo per tutelare la privacy è dare importanza alla sicurezza dei **propri dati personali**. Ecco alcuni semplici consigli che vi invitiamo a condividere con i ragazzi.

Create password difficili da decifrare

Insegnate loro come trasformare una frase facile da ricordare in una password efficace.

Utilizzate almeno otto lettere maiuscole e minuscole e sostituitene alcune con simboli e numeri. Ad esempio, "Mia sorella più piccola si chiama Anna" diventa **mS+psCan**.
Aiutali a capire quando una password è inefficace: ad esempio, può essere facile da indovinare se contiene l'indirizzo, la data di nascita, 123456 oppure la parola "password".

Insegnate buone norme di gestione delle password

Insegnate loro a pensarci due volte prima di inserire la password da qualche parte, così come a ricontrollare di trovarsi sull'app o sul sito corretto. Nel dubbio, prima di inserire qualcosa, invitateli a rivolgersi ai genitori. Inoltre, suggerite loro di usare password diverse per app e siti diversi. Possono avere una password principale a cui aggiungere qualche lettera per ciascuna app.

Imparate a difendervi 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.

Mantenete aggiornato il software

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

Non installate app potenzialmente dannose sul telefono

Scaricate sempre le app per dispositivi mobili da una fonte attendibile. Per proteggere i dati:

- Controllate le app ed eliminate quelle inutilizzate.
- Andate alle impostazioni del vostro store e attivate gli aggiornamenti automatici.
- Concedete l'accesso ai dati sensibili come posizione e fotografie solo alle app che ritenete attendibili.

Utilizzate il blocco schermo

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

Bloccate il telefono in caso di smarrimento

Se perdete il telefono o vi viene rubato, bloccatelo immediatamente. Se utilizzate Google potete 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.

Prestate attenzione alle richieste di informazioni personali

Non rispondete a email, 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 ritenete attendibile, ad esempio quello della banca, non fate mai clic sul link e non inviate mai un messaggio di risposta.

È opportuno visitare direttamente il sito web o l'app e accedere all'account. Ricordate: i siti e i servizi affidabili non mandano mai messaggi che richiedono di inviare password o informazioni finanziarie via email.

Fate attenzione alle frodi via email, ai finti premi e ai regali

I messaggi provenienti da sconosciuti sono sempre sospetti, specialmente se sono "troppo belli per essere veri", ad 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 fate mai clic sui link sospetti e non inserite mai le informazioni personali in moduli e sondaggi insoliti.

Controllate con attenzione i file prima di scaricarli

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

Usate reti sicure

Prestate attenzione quando usate 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 vostra attività su Internet, ad esempio i siti web visitati e le informazioni digitate. Anche a casa, proteggete la privacy e la sicurezza dell'attività di navigazione assicurandovi che la rete Wi-Fi sia criptata e impostando una password efficace.

Verificate la sicurezza delle connessioni prima di inserire dati sensibili

Quando navigate in rete, in particolare se intendete inserire dati sensibili come una password o il numero di una carta di credito, assicuratevi che la connessione ai siti che visitate 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.

6. UNA CASSETTA DEGLI ATTREZZI PER I GENITORI

I campanelli d'allarme e le regole per vivere bene in rete.

Alcuni campanelli d'allarme possono aiutarvi a riconoscere il rischio di dipendenza da smartphone negli adolescenti.

1. Sintomi da astinenza quando il dispositivo è inaccessibile

2. Disturbi muscolo-scheletrici in particolare a collo e a schiena

3. Disturbi visivi

4. Modifiche nel ciclo del sonno

5 Aumento di peso

6 Relazioni online che sostituiscono i rapporti dal vivo

7 Mancanza di interessi nelle attività della vita quotidiana e incapacità di parlare di cose diverse da quelle che si vedono in Internet

2 4 3

8 Scarsi risultati scolastici

9 Controllo compulsivo delle informazioni online

10 Scarsa igiene personale

In conclusione, questi sono i **comportamenti virtuosi** che è bene mettere in atto per trasformare la rete in un grande potenziale per il futuro dei nostri ragazzi.

1

Parla con i ragazzi
È importante favorire una comunicazione aperta tra genitore e adolescente, spiegando ai ragazzi cosa vuol dire un utilizzo positivo e intelligente dei media digitali, prestando attenzione ai contenuti che vengono pubblicati e letti e ricordando loro che è indispensabile proteggere la privacy online per tutelare se stessi e la propria famiglia.

2

Comprendi, impara e controlla
Il genitore dovrebbe monitorare il tempo che il proprio figlio spende su tablet, smartphone e pc, imparando per primo le tecnologie a disposizione per poterle comprendere per quanto è possibile, giocando insieme a lui e condividendo alcune applicazioni sui media device.

3

Stabilisci limiti e regole chiare
Occorre stabilire alcune regole, come evitare l'uso dei media device durante i pasti, i compiti e le riunioni familiari. Considerare i media come un'opportunità per tutta la famiglia per vedere insieme film o condividere contenuti social o messaggi in chat e video.

4

Dai il buon esempio
Come genitore l'esempio è fondamentale, per questo mamme e papà dovrebbero limitare per primi l'utilizzo di smartphone; è importante inoltre che i genitori scelgano sempre contenuti appropriati e linguaggi adeguati sui social network.

5

Fai rete
È indispensabile la collaborazione tra genitori, pediatri, operatori sanitari, insegnanti, forze dell'ordine e operatori digitali per tutelare e sostenere i ragazzi attraverso campagne di informazione che forniscano una maggiore consapevolezza degli aspetti positivi, ma anche dei rischi che presenta l'uso eccessivo dei media digitali.