Scambi intergenerazionali per la cybersecurity

NONNO CLICCA QUI!

promosso da moige proteggiamo i nostri figli

in collaborazione con

con il patrocinio di

con il contributo di Fondo Beneficenza Intesa Sanpaolo

Ciao a tutti,
ci presentiamo.
Siamo Matilde, Matteo e Gaia,
tre fratelli ma soprattutto nipoti
di quattro fantastici nonni.

Nonna Franca: abile giocatrice di burraco, Maestra in pensione, paziente custode delle nostre lacrime durante lo svolgimento dei compiti.

Nonno Antonio: il nostro Schumacher, sempre pronto ad accompagnarci ad ogni nuova attività sportiva e ad accogliere i nostri segreti nella sua macchina rossa fiammante.

Nonna Pina: donna protettiva, cuoca eccezionale, abbiamo sempre pensato che la canzone dello Zecchino d'oro fosse un inno alle sue tagliatelle.

Nonno Luigi: Medico attento e premuroso, con i pazienti e con noi nipoti. Ad ogni influenza raccomanda riposo e una maratona di film della Disney.

Così diversi tra loro, i nonni hanno una cosa in comune: non riescono a comprendere i pericoli che si nascondono dietro all'utilizzo dei Social Network e della rete Internet in generale.

Dato che su questo argomento siamo dei veri esperti, abbiamo deciso di aiutare i nostri (e altrui) nonni a non incorrere nei pericoli della Rete.

Cominciamo!

Matilde (19 anni), da sempre appassionata a codici e lucchetti per proteggere i fiumi di parole riportati nei suoi diari segreti, è oggi un'abile creatrice di password e conoscitrice della mente dei criminali informatici:

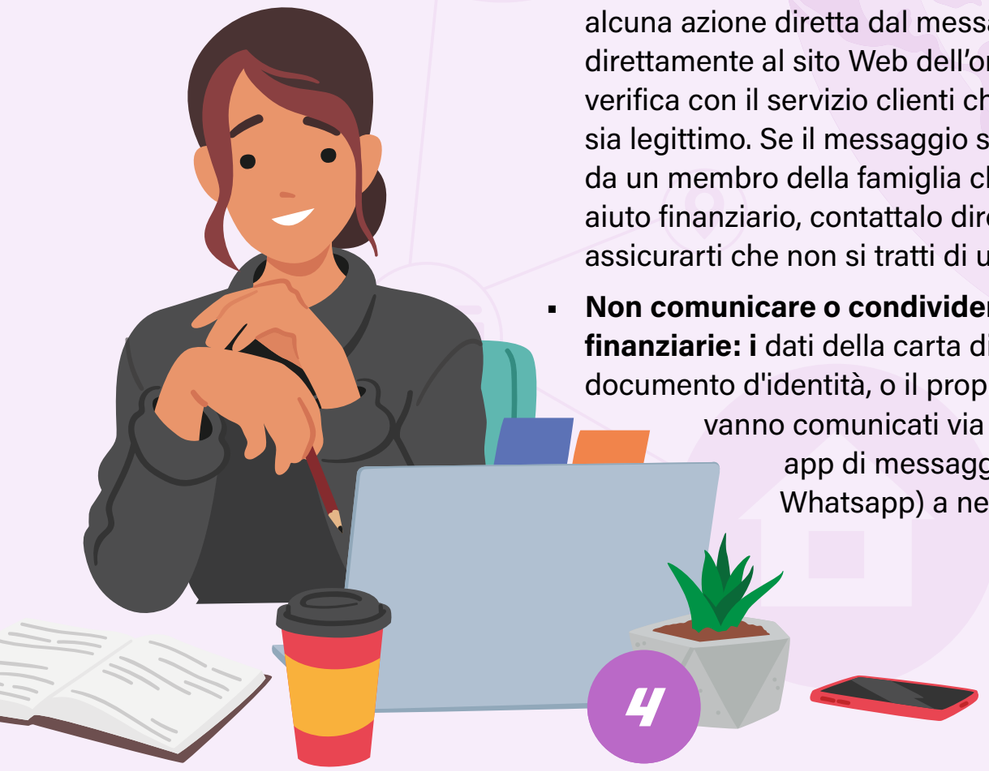
Caro nonno, cara nonna, il segreto per battere i criminali informatici? Semplice, è pensare come loro. Guarda i tuoi comportamenti online e i tuoi dati dal loro punto di vista, valuta cosa potrebbe renderti un obiettivo ideale, ad esempio il tuo fondo pensione. Cosa puoi fare per proteggerti? Ecco una serie di consigli.

- **Usa password complesse e univoche.** Spesso non comprendiamo appieno l'importanza della password, che è la chiave che protegge la nostra identità (e i nostri soldi!) in rete. Molte persone usano la stessa password o sue varianti in tutti i propri account (profilo digitale costituito da due elementi: un Nome Utente/Username e una Password/Parola chiave). Questo significa che, se un criminale informatico scopre una sola password, più dati personali sono improvvisamente a rischio. Pertanto, diversifica i tuoi codici di accesso per evitare che, se una password viene compromessa, i criminali possano ottenere l'accesso a tutti i tuoi account in una sola volta.
- **Attiva l'autenticazione a più fattori.** L'autenticazione a più fattori fornisce un ulteriore livello di sicurezza in quanto richiede più forme di verifica, come la scansione di un dito o il riconoscimento facciale. Questo riduce il rischio che criminali informatici possano assumere con successo la tua identità.
- **Se non puoi attivare l'autenticazione multifattoriale, usa una passphrase:** Se una password "mette un lucchetto" sul tuo conto, una passphrase equivale a un completo impianto di vigilanza! Le passphrase sono versioni più potenti e più sicure delle password. Le passphrase usano quattro o più parole a caso come password. Ciò le rende difficili da indovinare per i criminali informatici ma facili per te da ricordare.

Quando crei una passphrase, devi farla:

- Lunga. Cerca di crearla con una lunghezza di almeno 14 caratteri. Quattro o più parole a caso da ricordare sarebbero ideali. Ad esempio, “rosso cane pane marmellata”.
- Imprevedibile. Le frasi possono formare delle ottime passphrase ma sono facili da indovinare. Un insieme di quattro o più parole scelte a caso rendono la passphrase più potente.

Attenzione: se stai pensando di inserire i nomi dei tuoi nipoti, non è una buona idea!



- **Ignora le e-mail, i messaggi di testo e le telefonate sospette.** Non aprire messaggi sospetti o non pertinenti perché possono causare un’infezione al tuo telefono o computer. Presta particolare attenzione ai messaggi che contengono numerosi errori di ortografia. Le aziende, gli istituti finanziari, le banche controllano sempre la loro corrispondenza. Le e-mail di phishing (e-mail malevola scritta appositamente con lo scopo di spingere la vittima a cadere in una trappola. Spesso l’intento è portare gli utenti a rivelare informazioni bancarie, credenziali di accesso o altri dati sensibili), gli SMS e le chiamate spesso spingono i destinatari ad agire rapidamente ma tu mantieni la calma e valuta attentamente se il contenuto del messaggio sembra sospetto.
- **Vai direttamente alla fonte.** Se ricevi un’e-mail che sembra provenire da un’azienda o anche da un membro della famiglia nella quale ti viene chiesto il numero della tua tessera sanitaria, la tua password o del denaro, fermati e rifletti. Non fare clic su nulla e non intraprendere alcuna azione diretta dal messaggio. Invece, vai direttamente al sito Web dell’organizzazione e verifica con il servizio clienti che il messaggio sia legittimo. Se il messaggio sembra provenire da un membro della famiglia che chiede un aiuto finanziario, contattalo direttamente per assicurarti che non si tratti di un truffatore.
- **Non comunicare o condividere informazioni finanziarie: i** dati della carta di credito o del documento d'identità, o il proprio IBAN non vanno comunicati via e-mail, SMS o app di messaggistica (ad es. Whatsapp) a nessuno.

Per sfruttare al massimo le infinite possibilità che Internet mette a disposizione, è necessario seguire alcuni consigli base di sicurezza:

- **Compra e installa dei programmi di sicurezza informatica.** Gli antivirus permettono di navigare online in piena sicurezza. Minacce come virus o trojan vengono rilevate da questi programmi e rese innocue.
- **Installa regolarmente gli aggiornamenti.** Gli aggiornamenti servono a correggere le falle di sicurezza. Quando il tuo computer o un programma richiede di essere aggiornato, dovresti eseguire l’aggiornamento il prima possibile.
- **Naviga su siti web criptati.** Per riconoscere un sito web criptato basta verificare che l’indirizzo Internet inizi con "https". Se l’indirizzo web contiene solo "http", gli hacker possono intercettare i tuoi dati più facilmente. È importate prestare attenzione a questo dettaglio, soprattutto se desideri fare degli acquisti online. (possibilmente inserire una grafica che indichi dove si trova l’indirizzo https)

- **Se vuoi fare un acquisto online, verifica sempre le recensioni del sito e-commerce.** Prima di completare un ordine di acquisto su un sito, è bene verificare le recensioni di altri acquirenti che hanno utilizzato in precedenza quel servizio. Scrivi nel motore di ricerca (ad es. Google) “esperienze nome shop” o “nome shop affidabile”: se le esperienze sono per la maggior parte negative, evita allora di acquistare su quel sito. Le recensioni false si possono riconoscere da una formulazione eccessivamente positiva e che suona quasi promozionale, oppure, dal fatto che su un sito sono state scritte numerose recensioni positive per un prodotto in un lasso di tempo molto breve.
- **Non utilizzare le reti pubbliche.** Centri commerciali, bar e ristoranti spesso mettono a disposizione una connessione Internet gratuita. Queste reti, tuttavia, di solito non sono criptate e quindi i truffatori possono facilmente rubare i tuoi dati.
- **Rimani anonimo.** Quando navighi su Internet, fornisci soltanto le informazioni che sono assolutamente necessarie. Se hai l’impressione che un sito web non sia affidabile, non inserire nessun dato personale.

- **Non scaricare file e allegati da fonti sconosciute.** I file scaricati possono contenere virus. Scarica dunque solo file provenienti da fonti certe e fidate.
- **Proteggi la tua rete domestica.**
  - È sempre meglio far installare il router Wi-Fi da un professionista. In genere, quando si acquista un router, viene inviata anche una password. Per motivi di sicurezza, è sempre consigliabile sostituirla con una nuova password scelta da te. In questo modo puoi assicurarti che nessuno abbia accesso alla tua rete domestica senza il tuo permesso.
  - La password deve essere lunga almeno 10 caratteri e contenere una combinazione di lettere maiuscole e minuscole, numeri e caratteri speciali come !?/%
  - Non utilizzare sempre la stessa password. Trova una password diversa per ciascun account.
  - Non comunicare la password a nessuno. Se ti viene richiesto di fornire la password via e-mail o durante una telefonata, non soddisfare mai tali richieste.

Matteo (17 anni), fin da piccolo il più amato tra i suoi amici, definito dai suoi nonni "il socializzatore", è oggi maestro assoluto nell'utilizzo dei Social Network e sogna un futuro come Social Media Manager:

Eccomi nonna, nonno, ma lo sai che grazie ai social network è possibile connettersi e comunicare virtualmente con molte persone contemporaneamente? I social network si possono definire come delle "comunità virtuali", dove le persone possono incontrarsi e stringere amicizia. Su queste piattaforme è possibile condividere contenuti come testi, foto e video. A seconda delle impostazioni, questi contenuti vengono visti e condivisi in tutto il mondo o soltanto dai tuoi amici. Gli utenti hanno di solito la possibilità di commentare o aggiungere una reazione a ciò che si pubblica.
La maggior parte dei social network permette inoltre di scambiare messaggi privati con gli altri utenti.

Per essere certi di poter navigare e comunicare con gli amici in sicurezza anche su queste piattaforme, è necessario prendere gli opportuni accorgimenti:

- **Prestare attenzione ai propri dati**
  Sui social network gli utenti hanno la possibilità di presentarsi e costruire la propria identità. Tuttavia, è bene riflettere attentamente su quali informazioni personali si desidera rivelare.
- **Riconoscere i profili fake (o falsi)**
  Accetta solo richieste di amicizia da persone che conosci. A volte, purtroppo, hacker e truffatori creano dei profili falsi per poter rubare i vostri dati. Quando accetti una richiesta di amicizia, controlla sempre attentamente il profilo e cerca eventuali incongruenze.
- **Cambiare le impostazioni della privacy**
  Imposta il tuo account sui social media in modo che solo gli amici e i follower (cioè, le persone che ti seguono) possano vedere i contenuti che pubblichi e inviarti messaggi.
- **Controlla attentamente i messaggi e i post**
  Fai sempre molta attenzione sui social network e non fidarti di ogni messaggio o post che vedi. Molti utenti, infatti, pubblicano delle notizie false (le cosiddette "fake news").

Gli anziani possono più facilmente cadere vittima delle truffe "a bassa tecnologia" che non richiedono grosse competenze tecniche da parte dei truffatori.

Un esempio sono le truffe telefoniche: i criminali possono prendere informazioni in rete, ad esempio sui social media, sulla famiglia della persona anziana presa di mira. Possono scoprire che un nipote lavora all'estero, trovarne nome e cognome e altre informazioni preziose (il nome della moglie, o della fidanzata) e poi chiamare la vittima convincendola a inviare del denaro per aiutare il nipote, finito in guai economici o con la giustizia. Pubblicare sui social media informazioni personali (la data di nascita, il nome del proprio animale domestico, la via di casa) equivale a fornire a potenziali truffatori le informazioni che stanno cercando.

Un'altra variante di questo tipo di truffa è il contatto da parte di un "vecchio compagno di scuola". A quanti sarà capitato di iscriversi su Facebook al gruppo degli alunni della scuola frequentata alle elementari, alla ricerca di persone di cui si sono perse le tracce. Purtroppo, però, non si può avere la certezza che gli appartenenti al gruppo siano tutti in buona fede e che al loro interno non si nasconda qualche truffatore.

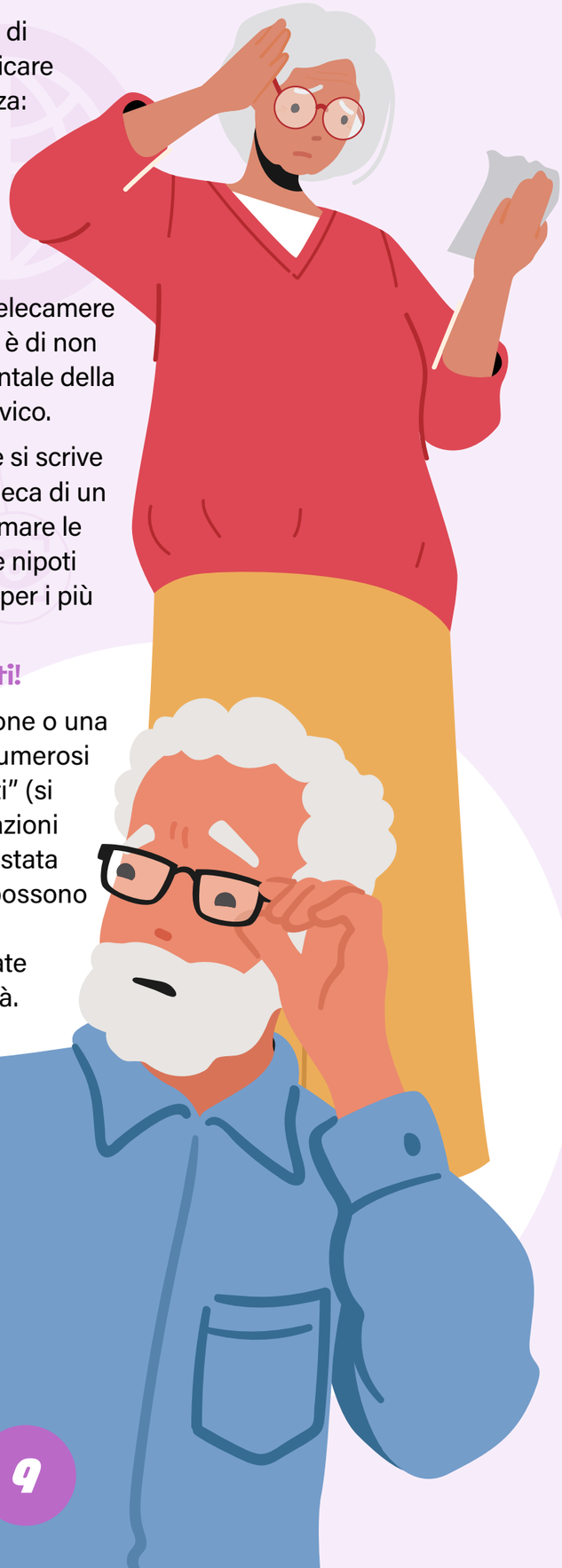
Siate diffidenti nei confronti degli sconosciuti che si spacciano al telefono per parenti o conoscenti. Non fornire alcun tipo di informazione riguardante la vostra situazione familiare o economica, nemmeno tramite internet. Se ricevi richieste di denaro per telefono, consultati con i familiari o persone di tua fiducia. Non affidare mai a sconosciuti denaro contante od oggetti di valore. Se nutri dei sospetti sulla persona che ti ha telefonato, informa subito i tuoi cari e insieme capirete se sporgere denuncia.

Per evitare spiacevoli sorprese, gli esperti di sicurezza online consigliano di non pubblicare foto sui social media mentre si è in vacanza: criminali e ladri non aspettano altro e hanno tutto il tempo per studiare come farvi una bella visita. Utilizzando Google Maps un ladro può riuscire a scoprire l'indirizzo esatto della vostra abitazione e vedere se c'è un allarme o un sistema di telecamere ad aspettarlo. Un altro utile accorgimento è di non condividere foto che mostrino la parte frontale della propria casa o il cancello con il numero civico.

É importante poi stare attenti a quello che si scrive quando si commenta qualcosa sulla bacheca di un amico o di un famigliare: evitiamo di informare le altre persone su possibili vacanze di figli e nipoti o di una loro assenza prolungata da casa per i più svariati motivi.

Prestiamo attenzione ai metadati!

Qualsiasi foto scattata con uno smartphone o una macchina fotografica digitale contiene numerosi dati incorporati nel file stesso. I "metadati" (si chiamano così) forniscono molte informazioni come la posizione, la data e l'ora in cui è stata scattata la foto. Questi tre semplici dati possono essere pericolosi se cadono nelle mani sbagliate, perché possono essere utilizzate da criminali per il classico furto di identità.



Cos'è una fake news?

Il termine fake news in italiano viene tradotto letteralmente come false notizie, ma può essere anche riconducibile ad una bufala o ad una pseudo notizia solitamente con l'intento di manipolare e ingannare l'utente.

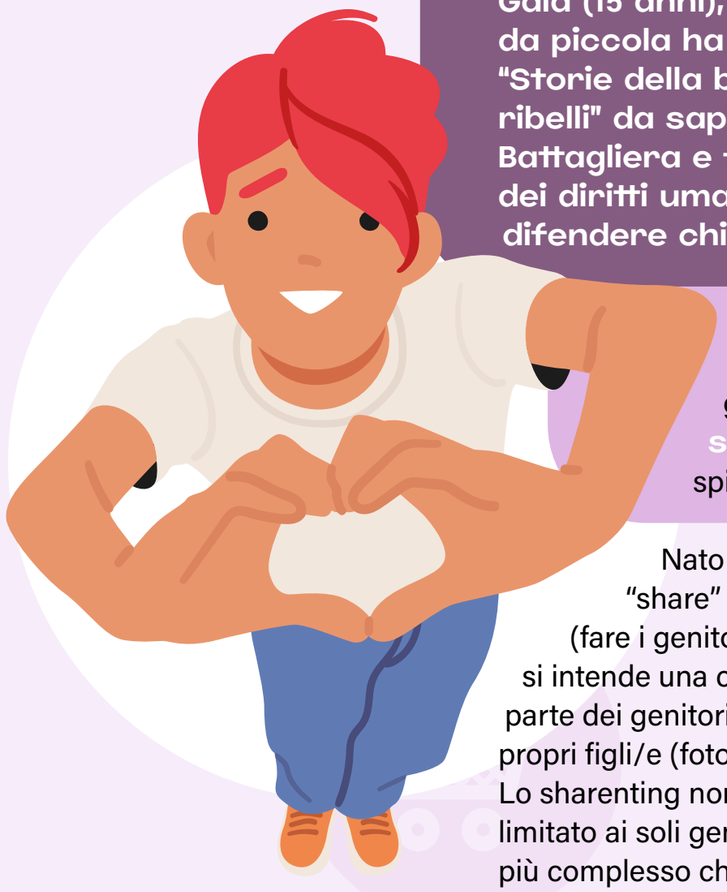
Proprio per questo le fake news assumono diverse forme passando per una varietà quasi infinita di argomenti ed andando a toccare moltissimi campi soprattutto in ambito scientifico e politico.

Come riconoscere una fake news

Vediamo ora alcune linee guida per facilitare il riconoscimento delle false notizie, ma soprattutto per allenare il nostro senso critico, che risulterà l'arma più potente a nostra disposizione per la lotta alla disinformazione.

Possiamo suddividere questi consigli in 8 punti:

1. **Leggere e capire il contenuto:** Non fermarti al titolo dell'articolo, aprilo e leggilo con attenzione. Le informazioni sono scritte in modo corretto? Presentano molti errori di ortografia? La data è corretta? Solitamente una corretta informazione cerca di riportare le notizie in modo neutro, dividendo fatti da opinioni.
2. **Controllare l'organo di stampa:** Lo conosci? L'URL sembra strano? Cerca tutte le informazioni possibili su chi lo finanzia e su chi sono. In più verifica le fonti anche da altre parti.
3. **Controllare l'autore:** É presente il nome dell'autore? É una persona reale? Usa uno pseudonimo? Cerca informazioni online sull'affidabilità del giornalista e sulla sua esperienza lavorativa.
4. **Controllare le fonti:** Le fonti sono presenti? I link sono funzionanti? Fai sempre una verifica in cerca delle fonti da dove l'articolo trae le informazioni. Solitamente se le fonti non sono presenti è probabile che le informazioni siano false.
5. **Pensa prima di condividere:** Prima di condividere rifletti ul contenuto, è una notizia ufficiale? É una notizia satirica? Cerca di capirne il contesto prima di diffondere qualcosa.
6. **Fatti delle domande:** Una cosa molto importante è quella di mettere sempre in discussione ciò che si legge (soprattutto sul web). Ogni tanto si trovano articoli che sono fin troppo belli per essere veri, ma saranno davvero così? Cerca di rimanere vigile e consulta molteplici fonti per tenerti aggiornato.



Gaia (15 anni), divoratrice di libri, da piccola ha letto così tante volte "Storie della buonanotte per bambine ribelli" da saperlo quasi a memoria. Battagliera e fervente conoscitrice dei diritti umani, lotta per poter difendere chi non ha voce.

Caro nonno, un tema che affronta spesso con nonni e genitori è il fenomeno dello **sharenting**, oggi vorrei spiegarti di che si tratta:

Nato dalla fusione delle parole "share" (condividere) e "parenting" (fare i genitori), con il termine "sharenting" si intende una condivisione online costante da parte dei genitori di contenuti che riguardano i propri figli/e (foto, video, ecografie).
Lo sharenting non è più un fenomeno isolato e limitato ai soli genitori, è diventato qualcosa di più complesso che ha colpito un'altra categoria di adulti: i nonni. La variante grandsharenting vede protagonisti i nonni nella veste di inconsapevoli "sharer" (utenti che condividono) di preziose informazioni che fanno la gioia di criminali, sempre pronti a escogitare nuove truffe.

Nella sua Relazione annuale del 2021, il Garante della privacy ha sottolineato come in presenza di sharenting si possa agevolare il fenomeno del cyberbullismo. Quando un contenuto compare su uno schermo può essere catturato e riutilizzato a propria insaputa da chiunque, anche per scopi impropri o per attività illecite. Prima della condivisione di una foto o di un video che ritrae un minore, l'Autorità invita a porsi la semplice domanda: "Mio/a nipote in futuro potrebbe non essere contento/a di ritrovare questa immagine a disposizione di tutti o non essere d'accordo con l'immagine di sé stessi che si potrebbe andare a costruire pubblicando quel contenuto?".
Lo stesso Garante ha poi fornito agli adulti una serie di accorgimenti da tenere bene in mente ogni volta che si pubblica un'immagine che riguarda i minori. Tra le accortezze troviamo:

- **il rendere irriconoscibile il viso del minore**, provvedendo a coprirlo con un adesivo.
- **limitare, quanto più possibile, le impostazioni di visibilità delle proprie immagini sui social network.** Si potrà scegliere, ad esempio, di mostrarle solo ai propri amici più stretti e ai familiari, impedendo così che quel contenuto inizi a circolare oltre il dovuto. Si tratta, naturalmente, soltanto di una limitazione che, infatti, potrebbe non condurre al risultato sperato. Pensiamo, ad esempio, al caso in cui un amico o un familiare decida di scaricare quella stessa immagine del minore e farla circolare in autonomia, sui propri profili social, magari privi delle restrizioni sperate;
- **fare una netta distinzione tra le immagini private – che devono rimanere tali – e quelle pubbliche.** L'immagine di un bambino in una foto di gruppo avrà sicuramente una pericolosità minore rispetto a quella che lo vede ritratto da solo, magari mentre svolge delle attività che sarebbe meglio lasciare private.

È tutto chiaro?
Se avete dei dubbi,
chiedete ai vostri familiari,
sapranno darvi una mano.

Oggi ribaltiamo la situazione,
siamo noi nipoti a dirvi:

FATE ATTENZIONE!

promosso da

moige

proteggiamo i nostri figli

in collaborazione con

con il patrocinio di

anci

con il contributo di

Fondo Beneficenza

INTESA SANPAOLO