

LA CYBER SECURITY INIZIA DALLA SCUOLA



dati personali



Quando navighiamo su internet non ci rendiamo conto della quantità di **dati personali** che condividiamo e di come gli altri possono utilizzarli senza il nostro permesso.

Non condividere mai la tua password, il tuo indirizzo di casa, il numero di telefono e la data del tuo compleanno. Stai attento alle foto e video che pubblichi.

Ricorda: nulla è completamente privato in rete!

applicazioni



Le applicazioni registrano una serie di **informazioni personali**, come i tuoi contatti e la tua posizione permettendo a persone con cattive intenzioni di conoscere il luogo in cui ti trovi mentre le stai usando.

Chiedi il permesso ad un adulto prima di acquistare applicazioni o livelli aggiuntivi di giochi per evitare situazioni indesiderate.

Gioca solo con amici che conosci di persona all'interno di applicazioni e siti adatti alla tua età.

social network

I **Social Network** sono gli strumenti più usati per rimanere in contatto con i tuoi amici, ma nascondono tanti pericoli. È molto semplice, infatti, creare un profilo falso: stai attento perché dietro ad un nickname non puoi sapere chi si nasconde!

Oltre ad incontrare persone con cattive intenzioni, puoi ricevere contenuti non adatti alla tua età, come foto o video che potrebbero metterti a disagio.



pericoli



- Il furto dei tuoi dati
- Il furto della tua identità
- Phishing
- Visione di foto e video non adatti alla tua età
- Le app sanno sempre dove sei con la "posizione" attiva
- Diffusione dei tuoi contenuti personali senza il tuo permesso

lo sapevi che ...

Anche il tuo smartphone contiene informazioni personali, bloccalo sempre ed abbinare cura!



glossario

Phishing: il Phishing è un attacco informatico diffuso tramite email attraverso il quale è possibile rubare informazioni personali, inserendo nell'email un link falso per rubare la password o un file che contiene malware.

Malware: programma che provoca danni a dispositivi informatici (pc, tablet, smartphone).

Parental Control: strumenti che consentono di proteggere i bambini dalle minacce della rete impedendo alcune azioni che possono essere pericolose.

cosa puoi fare per proteggerti in rete?



Blocca sempre il dispositivo quando non lo usi ed imposta password lunghe, complesse e segrete per ogni account.



Imposta il tuo profilo come privato e non condividere informazioni personali con nessuno, usando, se necessario, un nickname.



Accertati di conoscere gli amici con cui interagisci attraverso le chat ed i social network: condividi solo contenuti per i quali ti senti a tuo agio.



Informa un adulto se ricevi richieste o contenuti che ti mettono a disagio o se vedi qualcosa di non adatto alla tua età



Chiedi ai tuoi genitori di impostare il Parental Control sui dispositivi che usi.

