

CYBER ACADEMY

Trend Micro ti dà il benvenuto nella sua Cyber Academy, il posto giusto per imparare quello che ti occorre per utilizzare Internet in modo sicuro e divertente.

GUIDA ALLA CONVERSAZIONE: IMPOSTAZIONI DI SICUREZZA

Domande e risposte utili per supportarti nella conversazione con i bambini

1. Dove si trovano le 'impostazioni' di una app o di un dispositivo?

Cerca l'immagine di una ruota dentata, tre lineette o magari tre puntini. Possono chiamarsi impostazioni per la privacy, impostazioni di sicurezza o protezione, o controlli parentali. Quando usi una nuova app o un nuovo dispositivo per la prima volta, è importante che la relativa configurazione venga fatta con l'aiuto di un adulto.

2. App e dispositivi possono sapere dove ti trovi. Cosa puoi fare per impedirlo?

Disattiva 'Servizi di localizzazione'. È una voce che puoi trovare tra le impostazioni.

3. Quali app hanno bisogno di usare la 'localizzazione' del tuo dispositivo?

Pochissime app hanno bisogno di sapere dove ti trovi, ma alcune sono inutili se non si abilitano i 'servizi di localizzazione', come per esempio le mappe o le app per il meteo o quelle per il fitness. I social network richiedono la localizzazione, ma le relative app funzionano perfettamente anche senza.

4. Quali app hanno bisogno di usare il microfono e la fotocamera del tuo dispositivo?

I social network e le app per video chat usano il microfono e la fotocamera del tuo dispositivo perché tu possa parlare, ascoltare e vedere i tuoi amici online. Le console per videogiochi usano il microfono del dispositivo perché tu possa contemporaneamente chattare e giocare online con gli altri. Molte app tuttavia non hanno bisogno del microfono o della fotocamera. La prossima volta che una app ti chiede il permesso di utilizzarli, rifletti attentamente e chiedi aiuto a un adulto se non ne sei sicuro.

5. A cosa serve la Autenticazione a 2 Fattori (2FA)?

È una tecnica per accertarsi che la persona che prova a entrare nel tuo account sia proprio tu. Se attivi 2FA ti verranno richiesti due codici: solitamente la tua password PIÙ un codice speciale, che riceverai in genere via SMS o email. Questo rende il tuo account ultrasicuro.

6. Online, le persone mentono su chi sono veramente. Cosa fare per proteggerti in questi casi?
Configura il tuo account come 'privato' nelle impostazioni delle app. In questo modo solo le persone che conosci e di cui ti fidi nel mondo reale potranno contattarti o vedere quello che pubblichi.

7. Le persone possono commentare quello che condividi online. Come puoi proteggerti dai commenti e conservare il controllo della situazione?
Con l'aiuto di un adulto puoi decidere chi può commentare quel che pubblichi. Puoi anche decidere che nessuno possa commentare alcunché. Ricordati che le impostazioni di sicurezza esistono per proteggerti e tenerti al sicuro. È importante che un adulto ti aiuti a configurarle. Soprattutto, ricorda di riflettere bene prima di condividere qualcosa online.

8. Quali sono le 5 cose che puoi fare con le impostazioni di sicurezza per proteggerti online?

- Rifletti attentamente prima di consentire a una app di utilizzare il microfono, la fotocamera, la localizzazione o i contatti.
- Disattiva 'Servizi di localizzazione', non tutte le app devono sapere dove sei per poter funzionare.
- Usa SEMPRE le impostazioni per la privacy.
- Attiva la funzione 2FA in tutte le app (specialmente nei giochi!).
- Conserva il controllo: configura le impostazioni di protezione su ogni app e dispositivo con l'aiuto di un adulto.