Sicurezza Online per giovani Ninja

CoderDojo

Internet è uno strumento straordinario e un ottimo modo per imparare e trovare attività da fare, giochi per divertirsi o anche solo video di simpatici animali da guardare! Tuttavia, ci sono alcune cose che dovresti fare per proteggerti da chiunque online voglia turbarti, ferirti o rubarti informazioni.

Se stai già facendo tutte queste cose, puoi aiutare i tuoi compagni Ninja a mettere in sicurezza anche loro!

PASSWORD

È consigliato avere buone password, che puoi ricordare, e tenerle segrete e al sicuro.

La tua password è come la chiave di una cassaforte o di una casa: è molto più facile entrare con essa che senza di essa!

La maggior parte dei siti stabilisce alcune regole per la durata di una password, per la quantità di lettere e numeri che deve contenere, ecc. ma esistono alcune buone regole generali da seguire:

1. Le password più lunghe sono più sicure. Scegli le password con 10 o più caratteri. Evita di usare il tuo nome utente o il nome del sito web.
2. È meglio usare una determinata password per pochi account, in questo modo se qualcuno la dovesse scoprire, avrà l'accesso limitato solo a quei pochi account.
3. La password per il tuo indirizzo e-mail principale non dovrebbe mai essere utilizzata altrove. Infatti, se qualcuno riuscisse ad accedere, potrebbe reimpostare tutte le altre password!

Puoi utilizzare un gestore di password, come **LastPass**, che ti permetterà di salvare password molto lunghe e sicure. Hai solo bisogno di ricordare la tua password per il gestore di password stesso!

Puoi, inoltre, utilizzare l'**autenticazione a due fattori** su siti Web importanti, se è prevista, così da impedirne l'accesso a meno che non vengano in possesso anche del tuo telefono.

http://kata.coderdojo.com/images/8/89/Online_Safety_Ninjas_Checklist.pdf

Verifica la chechlist sulla Sicurezza Online http://dojo.soy/safe

CONDIVISIONE & SOCIAL MEDIA

Dovresti stare attento a condividere online informazioni, video o immagini che potrebbero essere utilizzati per trovarti, ferirti, metterti in imbarazzo o turbarti, ora o in futuro. Quindi, prima di condividere, fai alcune considerazioni:

- Queste informazioni possono essere utilizzate per trovare me o la mia scuola?
- Sto condividendo con qualcuno che non conosco e non ho mai incontrato di persona?
- Stanno usando un nuovo account che non mi hanno mai menzionato prima?
- Ciò che sto condividendo potrebbe essere usato, ora o in futuro, per mettere in imbarazzo me o qualcun altro o fare del male a me o ad altri?

Se la risposta a una di queste domande è "sì", allora probabilmente non dovresti condividerla!

Su qualsiasi sito Web, dovresti assicurarti di aver configurato correttamente le tue impostazioni sulla privacy e controllarle regolarmente! Un genitore/tutor può aiutarti a farlo.

VIRUS E MALWARE

Il tuo computer può essere stato infettato da un pericoloso software visitando siti Web infetti o scaricando file infetti come giochi, video, ecc.
Dovresti proteggerti sia facendo attenzione ai siti che visiti in Internet, sia installando un programma antivirus (**Avast** è una valida soluzione gratuita) che funzioni in ogni momento!

FAI LA TUA PARTE

Tu hai un ruolo importante da svolgere per rendere Internet un posto più attraente e più sicuro, per tutti! Non insultare o maltrattare le persone, non è bello. Sii educato, positivo e coinvolgente con tutti.

Infine, ricorda: se sei turbato o preoccupato per qualcosa che è accaduto online o che hai visto o che hai fatto, o qualcuno ti ha riferito o altro, puoi *sempre* parlarne con un adulto di cui ti fidi. Ti aiuterà!