

# 5 Suggerimenti per la sicurezza online



Tieni sotto controllo la tua vita digitale seguendo questi semplici consigli:

## 1

### Proteggi le tue informazioni e i tuoi dispositivi



- **Aggiorna i software e le applicazioni su tutti i tuoi dispositivi.**
- **Assicurati che il blocco automatico del dispositivo sia attivo.**

- **Cerca il tuo nome su Google per verificare quali informazioni sono disponibili sul web.**
- **Controlla le impostazioni privacy dei tuoi account social.**



## 2

### Sii discreto online e in pubblico

## 3

### Pensa prima di fare clic o rispondere



- **Fai attenzione quando cerchi di aprire collegamenti o allegati da e-mail sospette.**
- **Se non sei sicuro, chiama o invia una e-mail al mittente utilizzando le informazioni di contatto che hai già a tua disposizione oppure recuperale dai canali pubblici ufficiali.**

- **Utilizza una passphrase (password composta da 3 o più parole): è più facile da ricordare.**
- **Quando possibile, utilizza l'autenticazione a più fattori (MFA) per rendere i tuoi account ancora più sicuri.**



## 4

### Tieni al sicuro le tue password

## 5

### Se hai un sospetto, segnalalo



- **Quando ricevi una chiamata, un messaggio o una e-mail sospetta, segnalalo all'azienda o alla singola persona, per verificare se quanto ricevuto sia legittimo.**
- **Quando contatti l'azienda o l'individuo, utilizza le informazioni che hai già a disposizione oppure recuperale dai canali pubblici ufficiali. Non utilizzare quelle presenti nell'e-mail sospetta.**

Presta sempre attenzione e condividi questi suggerimenti con altre persone in modo che anche loro possano seguire una vita digitale sicura.

Applica questi consigli a tutti i tuoi account!

**Hyundai Capital**



## Phishing

È una particolare tipologia di truffa messa in atto su internet, utilizzando tecniche di ingegneria sociale e si concretizza attraverso l'invio di e-mail ingannevoli.



## Malware

È un tipo di software che influenza o danneggia un dispositivo accendovi senza che l'utente ne sia consapevole.



## Virus

Un virus informatico è un programma utilizzato per causare alterazioni nel funzionamento di un dispositivo senza che l'utente ne sia consapevole.

## MFA

L'autenticazione a più fattori (MFA) è un meccanismo particolarmente sicuro per accedere ai tuoi account. Oltre alla password, si richiedono passaggi di verifica aggiuntivi come ad esempio l'inserimento di un codice di conferma o l'impronta digitale.



## Sicurezza sul Web

HTTPS (HyperTextTransfer Protocol Secure) è un protocollo di comunicazione che protegge i dati degli utenti quando vengono trasmessi dal dispositivo al sito web. Ha un livello di sicurezza maggiore rispetto al protocollo HTTP.



## Copia di backup

Il backup è una copia delle informazioni che viene effettuata su un dispositivo diverso da quello iniziale. L'obiettivo è riuscire a recuperare i dati in caso di perdita degli stessi.

## Ingegneria sociale

Dall'inglese social engineering, nel campo della sicurezza informatica è lo studio del comportamento individuale volto a carpire informazioni riservate e rubare l'identità degli utenti attraverso la manipolazione.



## Passphrase

È una password di 3 o più parole. Il suo utilizzo aumenta la sicurezza perché è più difficile da decifrare rispetto ad una password composta da una singola parola.



## Impostazioni privacy

Tramite le impostazioni privacy puoi controllare quali informazioni condividere e con chi.



## Crittografia

La crittografia di un messaggio consiste nel trasformare il suo contenuto attraverso un algoritmo, in modo che solo gli utenti autorizzati possano accedervi.