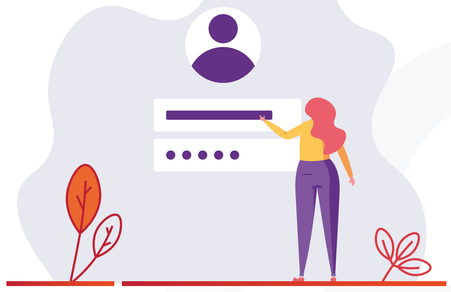
Guida per la sicurezza della tua PEC

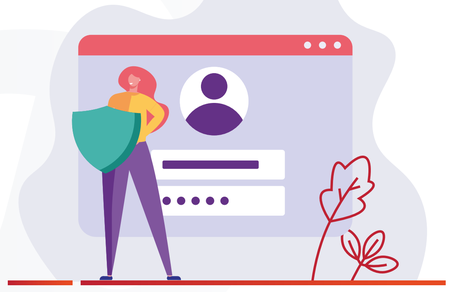
PROTEZIONE ACCOUNT

UTILIZZA UNA PASSWORD UNIVOCA



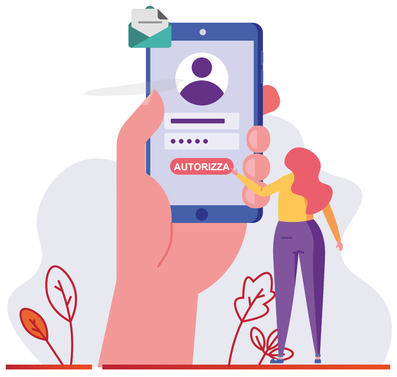
- Ricorri a generatori di password per renderla sicura e robusta
- Utilizza un Password Manager per gestire e conservare le tue password
- Non riutilizzare la stessa password per servizi differenti

PROTEGGI LA TUA PASSWORD



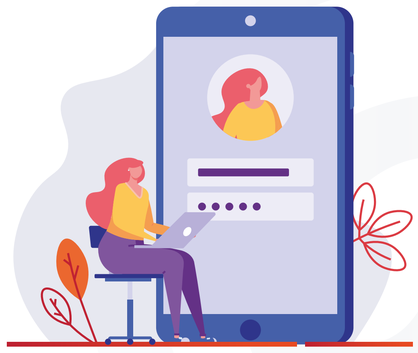
- Reimposta la tua password se pensi che il tuo account sia stato compromesso
- Imposta una scadenza per la password, così da ricordarti di modificarla con regolarità
- Non annotare la tua password su post-it o appunti e non comunicarla a nessuno
- Non conservare la tua password insieme al dispositivo o alla postazione

ATTIVA LA VERIFICA IN 2 PASSAGGI



- Aggiungi una protezione ulteriore all'accesso alla casella oltre a username e password
- Sarai tu ad autorizzare o negare l'accesso o l'esecuzione di operazioni sulla tua casella che ti verranno notificate direttamente sul tuo dispositivo

EMAIL DI RIFERIMENTO



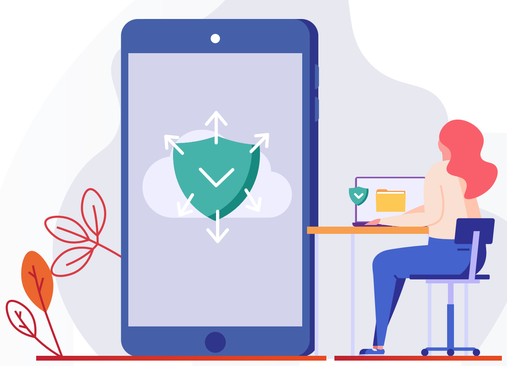
- Utilizza un contatto email principale per l'iscrizione a siti autorevoli e un contatto secondario per l'iscrizione ad altri siti
- Non utilizzare la stessa email di riferimento per tutti i siti

CAMBIA REGOLARMENTE LE PASSWORD

- Cambia le tue password con frequenza, è sempre bene averle aggiornate e robuste
- Imposta una scadenza per le password, così da ricordarti di modificarle con regolarità
- La nuova password deve essere totalmente diversa da quella precedente

PROTEZIONE DISPOSITIVO

TIENI LONTANI I MALWARE



- Utilizza software e antivirus autentici e affidabili e aggiornali frequentemente
- Verifica le notifiche di sicurezza del tuo antivirus
- Utilizza device esterni (chiavette USB o hard disk) affidabili ed esegui sempre una scansione antivirus su questi prima di collegarli
- Non navigare siti web a bassa reputazione o poco affidabili
- Non installare software provenienti da fonti non affidabili

EVITA AZIONI DI PHISHING

- Verifica il mittente delle comunicazioni prima di aprirle o rispondere.
- Verifica la destinazione dei link presenti nelle email posizionandovi sopra il cursore del mouse e non cliccare su quelli che non riconosci come sicuri
- Se hai un sospetto, controlla sulla pagina degli avvisi di Aruba che l'email che hai ricevuto non sia già stata identificata come phishing o fraudolenta
- Non scaricare o aprire file sospetti o inattesi
- Non rispondere a SMS di cui non conosci il mittente o che simulano mittenti autorevoli (come enti o compagnie assicurative)
- Non fornire le tue credenziali su siti e portali che non ritieni siano ufficiali
- Non effettuare pagamenti e non fornire i dati della tua carta di credito se non tramite i canali ufficiali Aruba

PROTEGGI I TUOI DATI

- Attiva la modalità "Aggiornamenti Automatici" sui tuoi dispositivi
- Mantieni sempre un backup affidabile dei tuoi dati e della tua postazione
- Assicurati di effettuare l'accesso ad Internet in modo sicuro e utilizza un servizio VPN se necessario
- Assicurati che il servizio VPN scelto per cifrare le comunicazioni sia autorevole e diffida dalle VPN gratuite
- Assicurati che le applicazioni web nel browser utilizzino una connessione protetta di tipo https
- Elimina o disinstalla applicazioni non più utilizzate, plugin del browser sospetti e software che non beneficiano più del supporto