

Sicurezza dello Smartphone

Protezione dei dati personali





Perché Proteggere i Dati?

Frodi Finanziarie

Accesso non autorizzato a conti bancari e carte di credito

Furto di Identità

Uso improprio delle informazioni personali per scopi illegali

Violazione Privacy

Accesso a foto, messaggi e documenti privati

Password Sicure

Il primo passo verso la sicurezza digitale



Caratteristiche Password Robusta

1 Lunghezza e Complessità

Almeno 12 caratteri con lettere maiuscole, minuscole, numeri e simboli

2 Unicità per Servizio

Password diversa per ogni account e applicazione

3 Non Prevedibile

Evitare date di nascita, nomi o sequenze ovvie

Metodo della Frase

Trasforma una frase in password

"Il mio gatto ha 3 anni e ama giocare!"

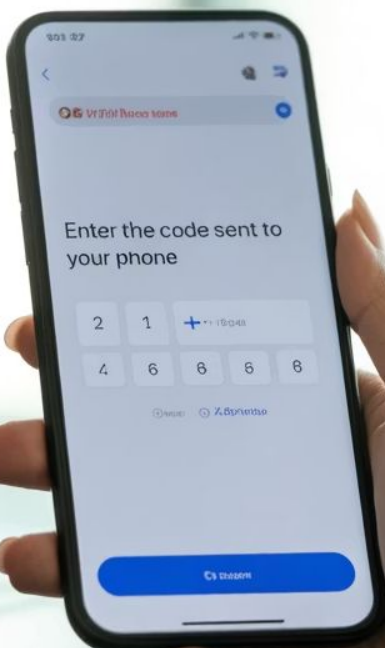
Diventa:

ImGh3AeAg!

Sicura ma facile da ricordare



Autenticazione a Due Fattori



01

Inserisci Password

Il primo livello di sicurezza tradizionale

02

Codice Temporaneo

SMS, app authenticator o notifica push

03

Accesso Garantito

Doppia verifica = massima protezione

Blocco Biometrico



Impronta Digitale

Caratteristica unica e impossibile da replicare per accesso rapido



Riconoscimento Facciale

Tecnologia avanzata che analizza i tratti del viso



Gestione Credenziali

Password Manager

Strumento per organizzare e generare password uniche automaticamente

Non Riutilizzare

Ogni servizio deve avere credenziali completamente diverse

Aggiornamento Regolare

Cambiare periodicamente le password più importanti

Le Quattro Regole d'Oro



Password Forti

Lunghe, complesse e uniche



Autenticazione a due fattori

Doppio livello di sicurezza



Blocchi Biometrici

Impronta e riconoscimento facciale



Consapevolezza

Uso responsabile delle credenziali

Smartphone Sicuro = Vita Digitale Protetta

Con questi accorgimenti, la tua sicurezza digitale sarà molto più solida

