



GUIDA PRATICA

Autenticazione a due fattori

Un secondo controllo rende molto piu difficile l'accesso anche se la password viene rubata.

1 Cos'e l'MFA?

L'autenticazione a piu fattori richiede due o piu prove per accedere: per esempio una password e un codice temporaneo, una notifica su app o un dispositivo fisico.

2 Tipi di secondo fattore



App OTP

Codici temporanei generati da un'app di autenticazione.



Notifica

Conferma dell'accesso tramite app sul telefono.



SMS

Codice inviato via SMS; meglio di niente, ma meno robusto.



Chiave fisica

Dispositivo USB/NFC usato come prova di possesso.



Biometria

Impronta o volto usati sul dispositivo.



Codici recupero

Codici di emergenza da conservare in luogo sicuro.

3 Perche usarla

- 1 Protegge anche se la password e rubata.
- 2 Riduce l'efficacia del phishing.
- 3 Aumenta la sicurezza dell'email.
- 4 E utile per banca, cloud e social.

4 Attenzione

- 1 Non approvare richieste inattese.
- 2 Non comunicare codici OTP.
- 3 Conserva i codici di recupero.
- 4 Aggiorna il numero o il dispositivo associato.



REGOLA D'ORO

Una password puo essere rubata; un secondo fattore aggiunge un'altra barriera.



GUIDA PRATICA

MFA: configurazione sicura

Come usarla senza rischiare di restare bloccati fuori dai propri account.

1 Impostazione consigliata

- 1 Attiva l'MFA sugli account più importanti.
- 2 Preferisci app di autenticazione o chiavi fisiche quando disponibili.
- 3 Salva i codici di recupero in un luogo separato.
- 4 Aggiungi un metodo di recupero affidabile.
- 5 Controlla periodicamente i dispositivi autorizzati.

2 Quando compare una richiesta

- 1 Verifica di aver avviato tu l'accesso.
- 2 Controlla luogo e dispositivo.
- 3 Rifiuta richieste inattese.
- 4 Cambia password se le richieste continuano.

3 Cosa non fare

- 1 Non inviare screenshot dei codici.
- 2 Non comunicare OTP al telefono.
- 3 Non approvare per 'far sparire' la notifica.
- 4 Non ignorare richieste ripetute.

4 MFA fatigue

Un attaccante può inviare molte richieste di approvazione sperando che la vittima ne accetti una per errore. Rifiuta sempre gli accessi che non riconosci.



CONSIGLIO FINALE

Se non hai iniziato tu l'accesso, non approvare la richiesta.