L'Autenticazione a Due Fattori (2FA)

La difesa avanzata per proteggere account, dati personali e identità digitale contro gli accessi non autorizzati.

1. Che cos'è la 2FA?

L'**Autenticazione a Due Fattori (Two-Factor Authentication, o 2FA)** è un metodo di sicurezza informatica che richiede all'utente di fornire *due o più prove distinte* di identità prima di concedere l'accesso a un sistema o account.

> **Il principio chiave:** Non basta più conoscere una singola password fissa. Anche in caso di furto della password, l'intruso non potrà entrare senza il secondo fattore di verifica.

2. I Tre Fattori di Autenticazione

La sicurezza informatica si basa tradizionalmente su tre categorie principali di fattori di riconoscimento:

Categoria	Descrizione	Esempi comuni
Conoscenza	Qualcosa che solo l'utente conosce.	Password, PIN, risposta a una domanda segreta
Possesso	Qualcosa che solo l'utente possiede fisicamente.	Smartphone, chiavetta USB di sicurezza, token hardware
Inerenza	Caratteristiche biometriche uniche dell'utente.	Impronta digitale, riconoscimento facciale, scansione iride

3. Come opera la combinazione?

La 2FA autentica l'utente combinando due elementi di categorie differenti (solitamente *Conoscenza* + *Possesso*). Questo rende l'attacco informatico esponenzialmente più complesso per i malintenzionati.

4. Le Tecnologie e Metodi di 2FA più diffusi

Esistono diverse modalità pratiche con cui viene implementato il secondo fattore di autenticazione:

Metodo	Come funziona	Livello di Sicurezza
App Authenticator (TOTP)	Codici temporanei generati offline da app dedicate (es. Google Authenticator, Authy).	Alto
Notifiche Push	Un avviso interattivo appare sul telefono fidato chiedendo di approvare o rifiutare il login.	Alto (attenzione al phishing)
SMS / Email OTP	Invio di un codice numerico monouso tramite messaggio di testo o posta elettronica.	Medio-Basso (vulnerabile a SIM swapping)
Chiavi Hardware (FIDO2)	Dispositivi fisici USB/NFC (es. YubiKey) da collegare o avvicinare al computer o telefono.	Massimo

5. Come si svolge il flusso di accesso

Il processo di login con la 2FA attiva segue una sequenza lineare e protetta:

- **1. Inserimento Credenziali:** L'utente digita nome utente e password sul portale.
- **2. Richiesta Secondo Fattore:** Il sistema verifica la password e richiede la convalida supplementare.
- **3. Convalida e Accesso:** L'utente inserisce il codice OTP o approva la notifica sul proprio dispositivo, sbloccando la sessione.

> **Buone pratiche di configurazione:** Abilita sempre la 2FA su tutti i servizi critici (email, banche, social media, cloud). Preferisci app authenticator o chiavi hardware rispetto agli SMS per una protezione superiore.

6. Considerazioni conclusive

L'adozione dell'Autenticazione a Due Fattori riduce drasticamente il rischio di subire violazioni informatiche personali, rappresentando uno scudo fondamentale nella sicurezza digitale moderna.