Sicurezza informatica personale in azienda

Il tuo laptop è sbloccato sulla scrivania. La stessa password protegge la tua email aziendale e Netflix. L'ultimo aggiornamento lo hai rimandato per la terza settimana.

Non sei il solo. Ma questo ti rende vulnerabile.

BITAGORÀ PMI ITALIANE

Gruppo BitAgorà Smart Network

La sicurezza informatica non è solo un problema del reparto IT

Ogni dipendente è un punto di accesso ai dati aziendali. Un account compromesso, un disco non cifrato, una password riutilizzata: bastano pochi minuti per causare danni che richiedono settimane di recupero.

Account compromesso

Accesso immediato a email, documenti e sistemi interni aziendali.

Disco non cifrato

Un laptop rubato espone tutti i dati in pochi minuti, senza ostacoli.

Password riutilizzata

Una sola violazione su un servizio secondario compromette tutto il resto.

Autenticazione a due fattori

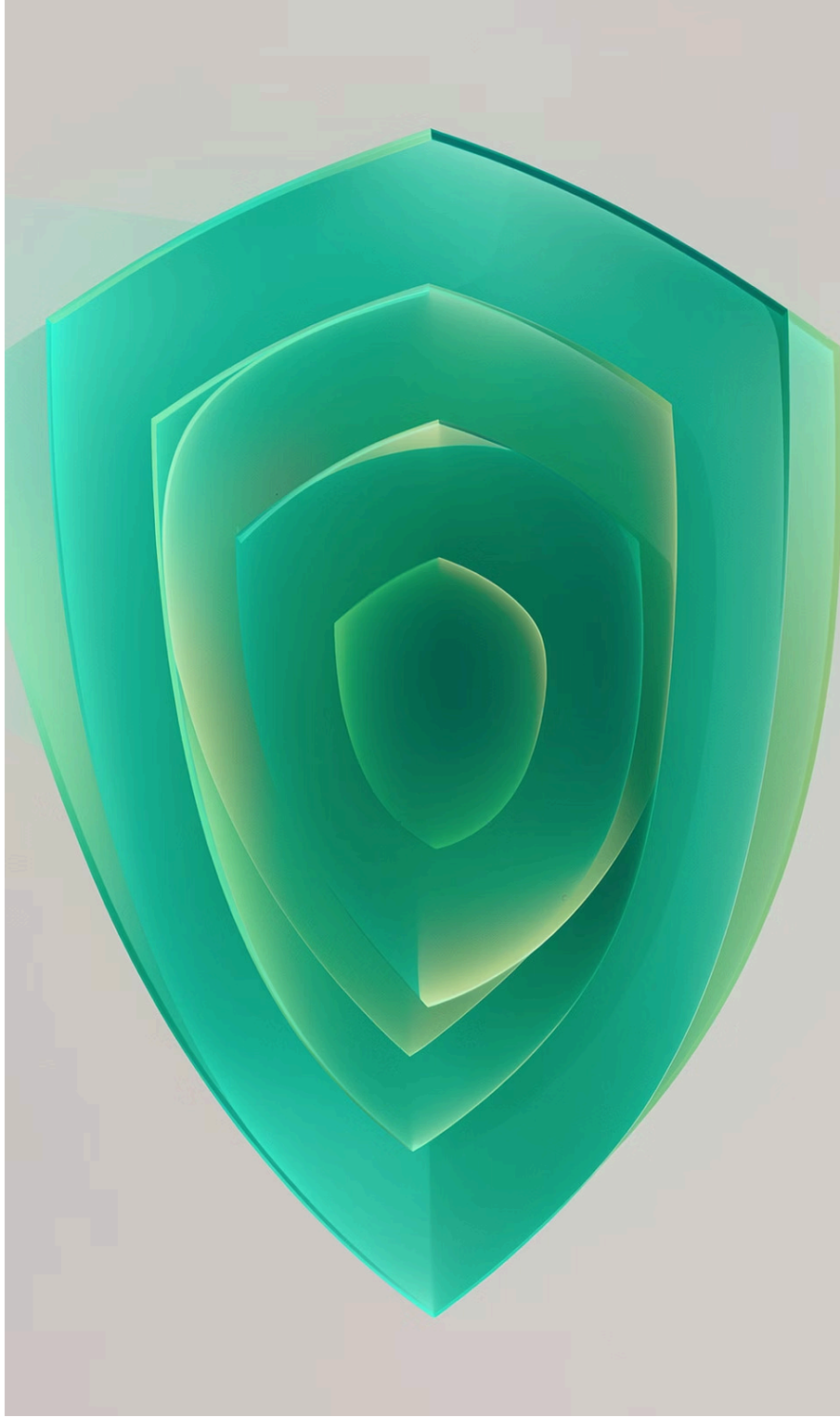
Attivala su tutto ciò che conta. La password da sola non basta: se qualcuno la ottiene, ha accesso immediato. La 2FA aggiunge un secondo livello di verifica che blocca l'accesso anche quando le credenziali sono state rubate.

Come attivarla

- Usa un'app di autenticazione come Microsoft Authenticator o Google Authenticator
- Evita gli SMS: sono intercettabili e meno sicuri delle app dedicate
- Per gli account critici, valuta una chiave hardware fisica come YubiKey

Una chiave hardware fisica (YubiKey) costa meno di 50 euro ed è il metodo di autenticazione più robusto disponibile oggi.

Inizia dagli account più importanti: email aziendale, gestionale, accessi cloud e strumenti di collaborazione.



Gruppo BitAgorà Smart Network

Cifra il disco del tuo laptop

Se il tuo laptop venisse rubato, i dati sarebbero leggibili in pochi minuti senza cifratura. Non è uno scenario remoto: i furti di dispositivi aziendali sono tra gli incidenti più frequenti nelle PMI.

Windows: BitLocker

Incluso in Windows Pro ed Enterprise. Attivazione in circa 5 minuti dalle impostazioni di sistema. Nessun costo aggiuntivo.

Mac: FileVault

Disponibile nelle impostazioni Privacy e sicurezza. Attivazione semplice, impatto sulle prestazioni impercettibile.

Verifica subito

In molte aziende i laptop vengono consegnati senza cifratura attiva. Controlla oggi stesso che sia abilitata sul tuo dispositivo.

Usa un password manager

Una password robusta è lunga, casuale e diversa per ogni account. Nessun essere umano riesce a ricordarne decine. Il risultato pratico: si finisce per usare varianti della stessa password ovunque, rendendo ogni account vulnerabile nel momento in cui uno solo viene violato.

Un password manager genera e memorizza password complesse per ogni servizio. Tu ricordi solo una password principale, lui gestisce tutto il resto.

Bitwarden

Open source, gratuito per uso personale, verificabile pubblicamente.

1Password

Interfaccia curata, ottima integrazione con browser e dispositivi mobili.

Keeper

Soluzione enterprise con funzionalità avanzate per team e aziende.

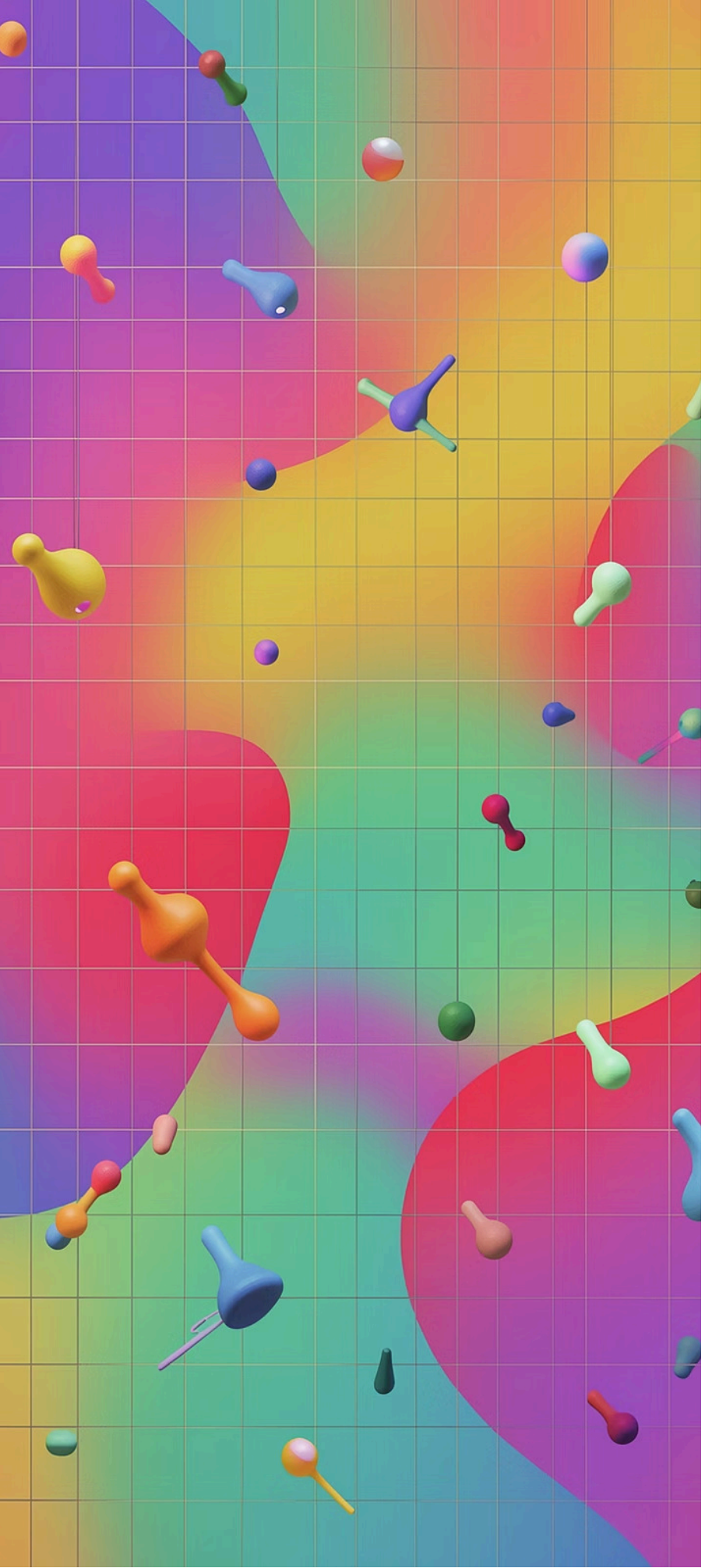
VPN: quando usarla

La VPN cifra il traffico tra il tuo dispositivo e internet, rendendo illeggibili i dati in transito anche su reti non sicure. Non sostituisce la 2FA né la cifratura del disco: aggiunge un livello utile in contesti specifici.

Quando attivarla

- Lavori da una rete pubblica: bar, hotel, aeroporto, coworking
- Accedi a risorse interne aziendali da remoto
- Sei fuori ufficio e la tua azienda ha una VPN aziendale

> ⚠ Se la tua azienda ha una VPN aziendale, usala sempre quando sei fuori ufficio. Non aspettare che qualcosa vada storto.



I permessi delle app sul telefono

Il telefono usato per il lavoro ha accesso a email, documenti e contatti aziendali. Molte app installate nel tempo hanno ottenuto permessi che non servono alla loro funzione principale.

01

Disinstalla le app inutilizzate

Ogni app installata è una potenziale superficie di attacco. Se non la usi da mesi, rimuovila.

02

Controlla i permessi attivi

Microfono, fotocamera, posizione, contatti: verifica quali app hanno accesso a questi dati sensibili.

03

Revoca i permessi non giustificati

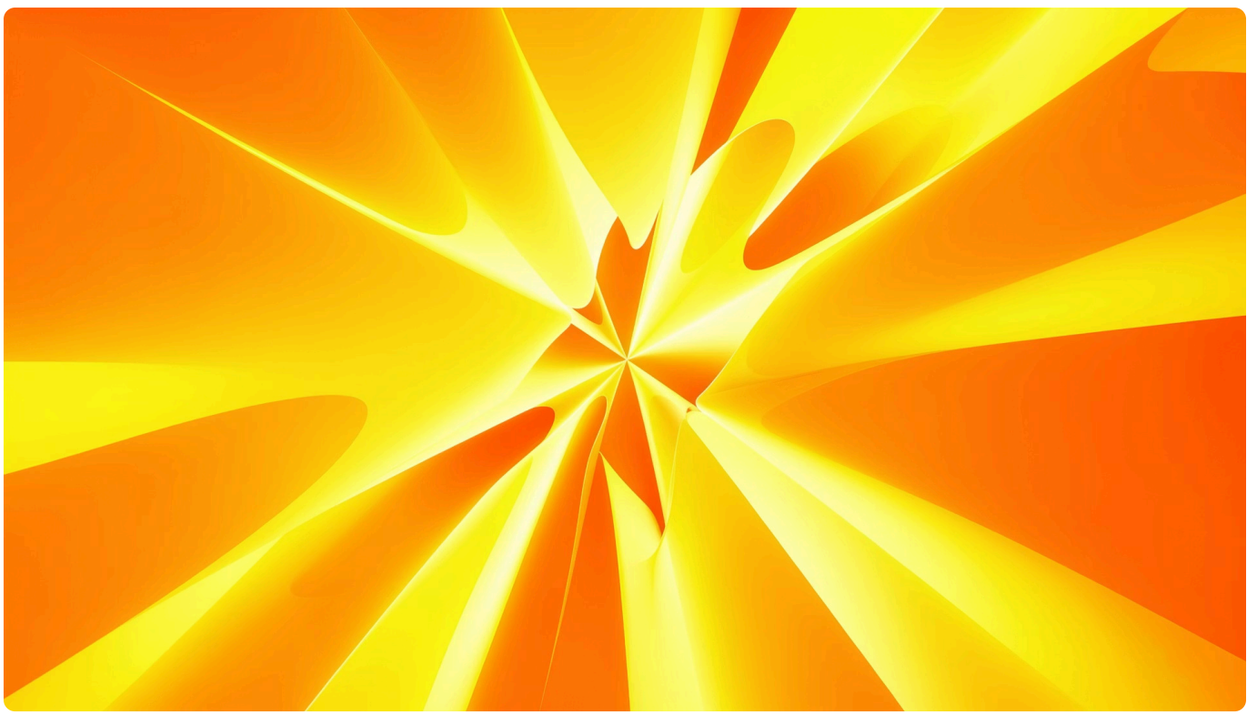
Se un'app non ha bisogno di un permesso per funzionare, revocalo. Il rischio non vale la comodità.

04

Dove trovare le impostazioni

iPhone: Impostazioni, Privacy e sicurezza. Android: Impostazioni, App, Autorizzazioni. Dedica 10 minuti oggi.

Aggiornamenti: smettila di rimandare



La maggior parte degli attacchi sfrutta vulnerabilità note, per cui esiste già una patch. Il tempo medio tra la pubblicazione di una vulnerabilità e il suo sfruttamento è spesso inferiore a 24 ore.

Ogni aggiornamento rimandato è una finestra aperta. Non aspettare il momento comodo: configura gli aggiornamenti automatici oggi.

Come organizzarsi

- Configura gli aggiornamenti automatici su tutti i dispositivi
- Programma gli aggiornamenti fuori orario lavorativo se necessario
- Includi sistema operativo, browser, app e firmware del router

Questa singola abitudine riduce la superficie di attacco più di qualsiasi altro strumento.

La checklist in sintesi

Sei abitudini. Un pomeriggio per implementarle tutte.

1	**Autenticazione a due fattori** Attiva su tutti gli account critici: email, gestionale, cloud, strumenti di collaborazione.
2	**Cifratura del disco** BitLocker su Windows o FileVault su Mac, attivo sul laptop aziendale.
3	**Password manager** Per tutte le credenziali, con password uniche e complesse per ogni servizio.
4	**VPN** Su reti pubbliche e per tutti gli accessi remoti alle risorse aziendali.
5	**Permessi app rivisti** Disinstallate le app inutilizzate, revocati i permessi non necessari.
6	**Aggiornamenti automatici** Attivi su tutti i dispositivi: sistema operativo, browser e applicazioni.

Quanto tempo richiede davvero?

Implementare tutte e sei le abitudini richiede un investimento iniziale di tempo. Poi diventano routine.

5min

Cifratura disco

Attivare BitLocker o FileVault richiede meno di cinque minuti.

10min

Permessi app

Una revisione completa dei permessi sul telefono in un quarto d'ora.

24h

Finestra di rischio

Il tempo medio tra pubblicazione di una vulnerabilità e primo sfruttamento.

50€

Chiave hardware

Il costo di una YubiKey, il metodo di autenticazione più robusto disponibile.

Il punto

La sicurezza informatica non è una responsabilità solo del reparto IT. È una responsabilità condivisa: ogni anello debole espone l'intera azienda.

Queste sei abitudini non richiedono competenze tecniche avanzate. Richiedono tempo, la prima volta, e poi diventano routine.

> Il team di BitAgorà aiuta le PMI a costruire percorsi di sicurezza informatica concreti e sostenibili.

Per i dipendenti

Sei abitudini pratiche che proteggono te e l'azienda, senza competenze tecniche avanzate.

Per i manager

Un framework condivisibile con il team, implementabile in autonomia nel giro di un pomeriggio.

Per le PMI

Percorsi di sicurezza informatica su misura con BitAgorà. Scopri di più su bitagora.it