🔒 Google Safety Tips

Letture importanti:

- Our latest scams survey sees changing online security habits
- Sync passkeys securely across your devices
- 6 new ways Google is protecting you from scams
- Our latest fraud and scams advisory

---

1 - Security Checkup

Google offre uno strumento integrato che fa una diagnosi immediata del tuo account. È il punto di partenza migliore.

- **Come fare:** Vai su myaccount.google.com/security-checkup
- **Cosa cercare:** Segui le icone gialle o rosse. Google ti suggerirà azioni immediate (come rimuovere vecchi dispositivi).
- Controlla quali siti e terze parti hanno accesso abilitato tramite il tuo Account Google.
- **Controlla i filtri e l'inoltro** Gli hacker spesso impostano una regola nascosta che inoltra automaticamente una copia delle tue email al loro indirizzo.
    - *Come fare:* Apri Gmail da PC > Impostazioni (ingranaggio) > Visualizza tutte le impostazioni > Scheda **"Inoltro e POP/IMAP"**.
    - *Cosa cercare:* Verifica che non ci siano indirizzi email sconosciuti nel campo "Inoltra una copia della posta in arrivo a...". Se ne trovi uno che non riconosci, disattivalo e rimuovilo immediatamente.

2 - Verifica in due passaggi (2FA)

Avere solo una password, anche se complessa, non è più sufficiente. La "Verifica in due passaggi" richiede che tu confermi l'accesso tramite un secondo passaggio.

- **Perché è importante:** Anche se un hacker ruba la tua password, non potrà entrare senza un secondo passaggio.
- **Come attivarla:**
    - Vai su **Gestisci il tuo Account Google** > **Sicurezza**.
    - Clicca su **Verifica in due passaggi**.
    - Segui le istruzioni.
- **Consiglio Pro:** Evita di usare solo gli SMS (possono essere intercettati). Usa **Google Prompt** (una notifica che appare sul telefono) o un'app come **Google Authenticator**. L'uso di una chiave di sicurezza hardware (come la Titan Security Key) offre un livello di sicurezza aggiuntivo perchè è fisicamente impossibile per un

hacker "clonare" la tua chiave hardware da remoto. Se il tuo business dipende dal tuo account, investi in due chiavi (una primaria e una di backup).

- **Approfondimento**:
  - Protect your business with 2-Step Verification

3 - Opzioni di Recupero

Se dimentichi la password o vieni bloccato, devi avere un modo per rientrare.

- **Email di recupero:** Inserisci un indirizzo email *diverso* da quello di Gmail (es. un vecchio indirizzo Yahoo, Hotmail, o quello del lavoro).
- **Numero di telefono:** Assicurati che il numero sia aggiornato.
- **Codici di Backup (Fondamentali):**
  - Nelle impostazioni della Verifica in due passaggi, cerca **Codici di backup**.
  - Generali e **stampali** o scrivili su un foglio da tenere in un posto sicuro a casa.
  - *A cosa servono:* Se perdi il telefono o ti viene rubato, questi codici sono l'unico modo per entrare subito nel tuo account.
- Recovery Contacts

4 - Dispositivi & App

Spesso il pericolo arriva da vecchi accessi dimenticati.

- **Controlla i tuoi dispositivi:**
  - Vai su **Sicurezza** > **I tuoi dispositivi**.
  - Se vedi un telefono o un PC che non usi più o non riconosci, clicca sui tre puntini e seleziona **Esci**.
- **App di terze parti:**
  - Vai su **Sicurezza** > **Le tue connessioni con app e servizi di terze parti**.
  - Rimuovi l'accesso a vecchi giochi, app di pulizia o servizi che non utilizzi più. Meno app hanno accesso ai tuoi dati, meglio è.

5 - Se hai un canale YouTube

Se hai un canale YouTube, sei un bersaglio più appetibile per gli hacker che vogliono usare il tuo canale per truffe (spesso crypto).

- **Attenzione alle email di collaborazione:** Gli hacker spesso inviano email fingendosi sponsor, allegando file PDF o .exe infetti. Non aprire mai allegati da sconosciuti.
- **Usa un Account del Brand:** Se hai dei collaboratori (editor, grafici), non dare loro la password del tuo account Google principale. Crea un "Account del Brand" e assegna loro il ruolo di "Gestore" o "Editor". Così possono caricare video senza poter eliminare il canale.

- **Attiva la "Navigazione sicura migliorata":** Nelle impostazioni di sicurezza, attiva questa opzione per proteggerti meglio da siti ed estensioni pericolose su Chrome.

6 - La Password

- **Non riciclarla:** La password di Google deve essere *unica*. Non usarla mai per Facebook, Netflix o forum.
- **Lunghezza:** Usa almeno 12-15 caratteri.
- **Usa un Password Manager:** Non cercare di ricordarla a memoria. Usa il gestore password di Google (integrato in Chrome/Android) o app come Bitwarden o 1Password.
- **Check-up:** Periodicamente fare un Password Check-Up per vedere se ci sono password a rischio, troppo ripetitive etc

Utilizza Gmail per aiutarti a identificare le email di phishing

Gmail è progettato per contribuire a proteggere il tuo account mediante l'identificazione automatica delle email di phishing. Fai attenzione agli avvisi relativi alle email e agli allegati potenzialmente dannosi.

Nota: Gmail non ti chiederà mai di fornire informazioni personali, ad esempio la password, via email.

Se ricevi un'email che sembra sospetta, ecco alcuni elementi da controllare:

> Verifica che l'indirizzo email e il nome del mittente corrispondano.
> Controlla se l'email è autenticata.
> Verifica se l'indirizzo email e il nome del mittente corrispondono.
> Su un computer, puoi passare il mouse sopra i link prima di selezionarli. Se l'URL non corrisponde alla descrizione del link, potrebbe reindirizzare a un sito di phishing.
> Controlla le intestazioni del messaggio per accertarti che l'intestazione "Da" non contenga un nome sbagliato.

Non inserire la password dopo aver fatto clic su un link in un messaggio

Se hai eseguito l'accesso a un account, le email di Google non ti chiederanno di inserire la password per questo account.
Se fai clic su un link e ti viene chiesto di inserire la password per Gmail, il tuo Account Google o un altro servizio, non inserirla: vai direttamente al sito web che vuoi utilizzare.
Se ritieni che un'email di sicurezza che sembra provenire da Google sia falsa, vai direttamente alla pagina myaccount.google.com/notifications. In questa pagina puoi controllare le attività recenti di sicurezza del tuo Account Google.

Per PMI, Freelance e chi ha un dominio personalizzato (Google Workspace)

Se usi Gmail per lavoro con un dominio personalizzato (es. @tuaazienda.it), hai accesso a strumenti professionali che puoi configurare per proteggere il tuo account e i tuoi dati.

A. Proteggi la tua identità (SPF, DKIM e DMARC)

- **DKIM (DomainKeys Identified Mail):** Aggiunge una firma digitale invisibile alle tue mail. Conferma che la mail l'hai mandata davvero tu.
- **SPF (Sender Policy Framework):** Dice al mondo quali server sono autorizzati a spedire mail per tuo conto.
- *Consiglio:* Chiedi al tuo gestore del dominio o al supporto IT di verificare che SPF e DKIM siano attivi. Aumenta drasticamente la reputazione del tuo dominio

B. Condivisione Drive Consapevole

Dalla Console di Amministrazione, puoi controllare come i tuoi file vengono condivisi all'esterno.

- **Accesso Offline:** Se i tuoi collaboratori usano computer condivisi, disabilita l'accesso offline ai documenti per evitare che rimangano copie locali su PC non sicuri.
- **Avviso di condivisione esterna:** È utile attivare l'opzione che mostra un avviso ("Stai condividendo con qualcuno esterno all'organizzazione") per prevenire fughe di dati accidentali.

Procedimento per sospetto hackeraggio:

- *Seguire questi step*