

GUIDA GRATUITA

Checklist privacy AI per chi lavora con dati di clienti

Cosa non incollare mai così com'è, le impostazioni da controllare e un prompt sicuro pronto da usare

Cosa è successo davvero, a luglio 2026

A luglio 2026 alcune chat Claude condivise tramite link pubblico sono finite indicizzate su Google. Cercando `site:claude.ai/share`, chiunque poteva trovare curriculum con nomi e numeri di telefono veri, chiavi API, note legali riservate. Anthropic ha corretto il problema (mancava un'istruzione tecnica che teneva quelle pagine fuori dai motori di ricerca) nel giro di pochi giorni, ma i link condivisi prima di allora possono essere rimasti copiati su altri siti: cancellare oggi il link originale non cancella le copie già fatte altrove.

Il punto centrale

Il rischio non è l'AI in sé. È cosa finisce in una chat e cosa succede se quella chat viene condivisa con un link.

Cosa non incollare mai così com'è

Tra i dati trovati esposti durante l'incidente di luglio: nomi e numeri di telefono reali, chiavi di accesso a servizi (API key), note legali riservate, dati che sembravano bancari o identificativi. Prima di incollare uno di questi elementi in una chat che potrebbe finire condivisa, sostituiscilo con un segnaposto.

Fai così

- ✓ Sostituisci il nome del cliente con "Cliente A" o un nome di fantasia
- ✓ Togli numeri di telefono, email e indirizzi reali
- ✓ Sostituisci cifre economiche sensibili con un ordine di grandezza ("circa 10.000 euro" invece della cifra esatta di un contratto)
- ✓ Riassumi un documento riservato invece di incollarlo integralmente

Evita

- ✗ Non incollare mai una chiave API, una password o un token di accesso
- ✗ Non incollare contratti, note legali o documenti coperti da riservatezza così come sono
- ✗ Non incollare dati sanitari o identificativi (codice fiscale, documenti) di nessuno
- ✗ Non condividere il link di una chat che contiene uno di questi elementi, nemmeno "solo per un attimo"

Checklist prima di lavorare su un caso di un cliente

- Ho tolto nome e cognome reali del cliente, sostituendoli con un nome generico?
- Ho tolto numeri di telefono, email e indirizzi?
- Ho tolto o arrotondato i dati economici sensibili?
- Ho evitato di incollare contratti o documenti riservati per intero?
- Se ho condiviso un link di questa chat in passato, l'ho ricontrollato di recente?

La domanda da farsi sempre

Prima di incollare qualcosa: questa informazione, se uscisse da qui, mi creerebbe un problema? Se la risposta è sì, anonimizzala prima di scrivere.

Controlla le impostazioni su Claude

DOVE GUARDARE

Vai in Impostazioni, poi Privacy: da lì trovi la sezione che riguarda i contenuti condivisi con un link. Controlla ogni chat o Artifact impostato su "chiunque abbia il link" e valuta se contiene ancora qualcosa di sensibile.

1. Apri Impostazioni, poi Privacy
2. Cerca la sezione dei contenuti o delle chat condivise
3. Rivedi ogni link attivo: contiene nomi, cifre o documenti che non vorresti in giro?
4. Elimina la condivisione dei link che non ti servono più

Un limite onesto

Eliminare un link condiviso ferma nuove visite, ma non cancella le copie che altri siti o utenti potrebbero aver già salvato mentre il link era pubblico. È una precauzione da qui in avanti, non una cancellazione totale del passato.

Un prompt sicuro da usare con i dati dei clienti

PROMPT DA COPIARE

Lavorare su un caso cliente senza incollare dati sensibili

Agisci come consulente di [SETTORE, es. marketing].

Ti do un brief anonimizzato: dove leggi "Cliente A", è il nome reale del cliente, non chiedermelo.

[INCOLLA IL BRIEF ANONIMIZZATO, SENZA NOMI, TELEFONI O CIFRE ESATTE]

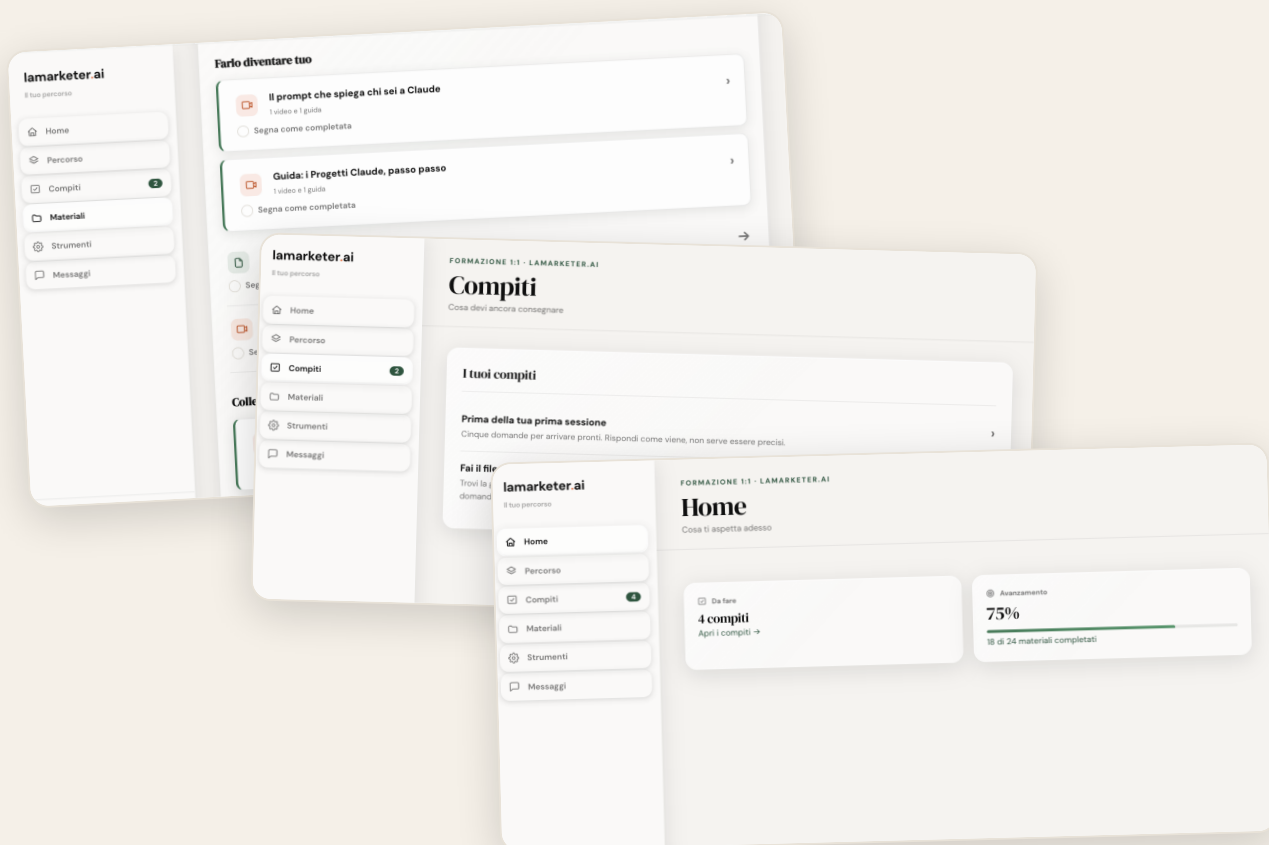
Non dare per scontate informazioni che non ti ho dato. Se ti servono dettagli in più, fammi prima le domande, prima di scrivere qualsiasi risposta.

Compila il brief con dati generici o arrotondati, non con quelli reali del cliente.

Cosa significa lavorare con me

Non sono solo le sessioni live. Chi entra nel percorso accede a una **piattaforma dedicata**, che resta sua anche dopo.

- **Video che spiegano tutto per bene**, non accennato di corsa: ogni argomento ripreso con calma, da riguardare quando serve.
- **Guide scritte apposta** per il percorso, non materiale generico preso altrove.
- **Materiali costruiti su di te**: sulle sessioni che facciamo, sui tuoi obiettivi, sulla tua attività reale.



Materiali, compiti tra una sessione e l'altra, e l'avanzamento reale del percorso.

IL PASSO SUCCESSIVO

Il percorso 1:1.

5 sessioni costruite intorno ai tuoi obiettivi professionali e personali.

5 posti al mese. Prima guardiamo il tuo caso, poi ti dico se posso aiutarti.

Prenota la call gratuita →