



GUIDA BREVE • RISCHIO • FRODE D'IDENTITÀ

Nuovo cliente, identità falsa? Segnali verificati prima di impegnarsi.

Chi si registra o richiede un contratto inizia dichiarando chi è. Questa guida breve mostra come PaperOffice fornisce indirizzo e-mail, indirizzo IP, dispositivo e documento d'identità come segnali verificabili. Per negozi, piattaforme, locatori e rivenditori che vendono a rate.

IL PUNTO CHIAVE

Ogni controllo restituisce campi su cui la Sua regola può agire: una raccomandazione per l'e-mail, indicatori per VPN e Tor, un ID dispositivo e campi del documento d'identità con la loro posizione di origine. La decisione spetta al Suo team.

01 · IL PROBLEMA

Il nome è giusto. Ma la persona dietro di esso no.

Un nuovo cliente firma online un contratto, e lo smartphone viene consegnato a rate. Nome, indirizzo e indirizzo e-mail sembrano autentici. Solo quando i pagamenti si fermano diventa chiaro: i dati appartengono a qualcun altro, oppure la persona non esiste affatto.

PERCHÉ SUCCEDE

Dati rubati e inventati

I truffatori usano nomi e indirizzi reali provenienti da fughe di dati, oppure li mescolano con dettagli inventati. Sul modulo, entrambi appaiono uguali.

Nascondersi in rete

Indirizzi usa e getta, VPN, Tor e server affittati nascondono chi effettua l'ordine. La stessa persona può aprire molti account con poco sforzo.

Documenti d'identità di fretta

Al banco la copia del documento viene guardata in fretta e digitata. Un errore di battitura o un campo mancante passano facilmente inosservati.

COME SI RICONOSCE

- L'indirizzo e-mail proviene da un servizio usa e getta, oppure il suo dominio non ha un server di posta.
- La registrazione avviene tramite VPN, Tor o un data center invece che con una connessione normale.
- Il paese dell'indirizzo IP non corrisponde all'indirizzo indicato.
- Lo stesso dispositivo compare in più registrazioni con nomi diversi.
- I dati sul modulo e sul documento d'identità non coincidono.

02 · LA SOLUZIONE CON PAPEROFFICE

Dal segnale alla decisione.

PaperOffice fornisce segnali su e-mail, rete, dispositivo e documento, tramite REST API, SDK e nell'app. Ciò che segue dipende dalla Sua regola: far passare, chiedere di nuovo, inviare a verifica o rifiutare.

1

Valutare l'indirizzo e-mail

POST /fakeemail/check verifica domini usa e getta, record MX, SPF e DMARC e restituisce risk_score più la raccomandazione ACCEPT, REVIEW o REJECT.

MODULO: [RILEVAMENTO DI INDIRIZZI EMAIL FALSI](#)

2

Controllare rete e posizione

/ip2location/full restituisce paese, regione e provider, oltre a is_vpn, is_proxy, is_tor e is_datacenter. Il campo type indica l'elenco che ha trovato corrispondenza.

MODULO: [RILEVAMENTO VPN](#)

3

Riconoscere il dispositivo

L'SDK per il browser restituisce un visitor_id per dispositivo. Al login successivo, /fingerprint/verify verifica se si tratta dello stesso dispositivo, e risk.factors indica ogni anomalia.

MODULO: [IMPRONTA DIGITALE DEL DISPOSITIVO](#)

4

Leggere il documento d'identità

Un IDP Agent legge nome, data di nascita, indirizzo, numero del documento e data di scadenza da una foto o una scansione, ciascun valore con la sua posizione nell'originale.

MODULO: [IDP AGENT](#)

5

Decidere

La Sua applicazione combina i campi in una regola, ad esempio: un indirizzo usa e getta o Tor significa verifica da parte di una persona. La decisione spetta al Suo team.

03 · NELL'APP

Chiavi, SDK, agente: come impostarli.

I controlli dei segnali avvengono tramite REST API e SDK, il documento d'identità tramite un IDP Agent nell'app. I nomi corrispondono all'app.

1

Una chiave API per il Suo backend

In **API e Sviluppatore** > **Chiavi API**, usi **Crea nuova chiave** per creare una **Chiave API**. Il Suo backend la usa per controllare e-mail e IP. La chiave può essere copiata lì in qualsiasi momento.

2

Una chiave per l'SDK del browser

In **API e Sviluppatore** > **Chiavi API**, usi **Crea nuova chiave**, scegli il tipo **Chiave Pubblicabile** e inserisca i domini del Suo sito. Il Suo sito carica poi con essa l'SDK per il fingerprint.

3

Creare un IDP Agent per i documenti d'identità

Selezioni una foto di esempio, poi **Azioni** > **Agenti e flussi di lavoro** > **IDP** e **Crea nuovo agente**. Scegli un modello per documenti d'identità oppure descriva i campi con parole proprie.

4

Verificare i valori rispetto all'origine

Nella scheda **Campi dati**, ogni valore compare accanto al frammento del documento d'identità. La vista **IDP Review** mostra tutti i documenti con i campi aperti.

5

Lavorare le attività di verifica

Se manca un campo obbligatorio, viene creata un'attività nella coda di verifica scelta. In **Workflow AI** > **Attività Human In The Loop**, una persona vede il documento d'identità e i campi e completa la verifica.

CONSIGLIO DALLA PRATICA

Valuti più segnali insieme Una VPN da sola ha spesso motivi innocui. Diventa rilevante insieme a un indirizzo usa e getta o a un dispositivo già collegato ad altri account nel Suo sistema. Definisca quando una persona deve verificare.

04 • UN ESEMPIO

Un rivenditore di telefonia. Contratti a rate.



Un rivenditore di telefonia mobile con sei negozi e un negozio online vende smartphone con contratti e piani a rate. In negozio il team copia il documento d'identità e digita i dati; online basta un modulo. Più volte i pagamenti si fermano e i clienti non sono raggiungibili.

PRIMA

- In negozio il documento d'identità viene copiato e i dati vengono digitati nel modulo di contratto campo per campo.
- Online ogni indirizzo e-mail viene accettato, compresi quelli usa e getta.
- Le richieste tramite VPN o data center sembrano uguali a tutte le altre.
- Nessuno nota che un dispositivo ha già inviato più richieste.

CON PAPEROFFICE

- Il modulo online controlla l'indirizzo e-mail e, con REVIEW, la richiesta va a verifica.
- Il controllo IP segnala VPN, Tor e data center, e la richiesta confronta il paese con l'indirizzo.
- Ogni richiesta memorizza il visitor_id, così i dispositivi usati più volte si distinguono.
- In negozio un IDP Agent legge il documento d'identità da una foto, e il team verifica i valori rispetto all'origine.

Esempio a scopo illustrativo: l'azienda e il processo sono inventati. Verifichi con il Suo responsabile della protezione dei dati quali dati del documento d'identità e del dispositivo raccoglie e per quanto tempo li conserva.

05 · CHECKLIST

Dieci punti per l'onboarding dei Suoi clienti.

Verifichi questi punti con vendite, IT e protezione dei dati. Ognuno può essere controllato nella Sua attività.

- ☐ Ogni registrazione verifica l'indirizzo e-mail prima che l'account venga attivato.
- ☐ Il Suo backend invia l'indirizzo IP del cliente all'API nel parametro ip.
- ☐ Il paese dell'indirizzo IP viene confrontato con l'indirizzo indicato.
- ☐ Se un account noto accede da un dispositivo sconosciuto, la Sua applicazione chiede un secondo fattore.
- ☐ Per le richieste di cancellazione è documentato il percorso tramite POST /privacy/forget.
- ☐ Per REVIEW e REJECT è definito cosa succede: chiedere di nuovo, inviare a verifica o rifiutare.
- ☐ VPN, Tor e data center vengono valutati separatamente, con una regola per ciascun caso.
- ☐ Il visitor_id viene memorizzato con ogni account e ogni richiesta.
- ☐ Un IDP Agent legge i documenti d'identità e i campi obbligatori sono definiti.
- ☐ Finalità, base giuridica e periodo di conservazione dei dati del dispositivo sono concordati con la protezione dei dati.

06 · DOMANDE FREQUENTI

Cosa vogliono sapere i team prima di iniziare.

PaperOffice verifica i documenti d'identità in modo biometrico?

PaperOffice funziona senza confronto del volto. Un IDP Agent legge i campi del documento d'identità con la loro posizione di origine, e gli altri controlli forniscono segnali su e-mail, rete e dispositivo. Il Suo team decide se un'identità è confermata.

E le persone che usano una VPN per buoni motivi?

Una VPN è un segnale che la Sua regola valuta. La risposta distingue VPN, proxy, Tor e data center e indica l'elenco corrispondente nel campo type. Gli indirizzi presenti nelle liste di blocco compaiono anche sotto is_vpn.

Come arrivano i controlli nel nostro portale?

Tramite la REST API dal Suo backend, tramite l'SDK fingerprint con una **Chiave Pubblicabile** associata ai Suoi domini, e tramite MCP. Carica i documenti d'identità in un workspace in cui viene eseguito un IDP Agent.

Da dove proviene il punteggio di rischio?

Dal controllo dell'e-mail: risk_score da 0 a 100, risk_level da MINIMAL a CRITICAL e la raccomandazione ACCEPT, REVIEW o REJECT. Il controllo del dispositivo fornisce fattori di rischio propri, ad esempio una VPN o una velocità di viaggio impossibile.

Posso individuare lo stesso dispositivo dietro più account?

Sì, se memorizza il visitor_id con ogni account. Allora lo stesso ID compare su più account. /fingerprint/similar trova dispositivi con caratteristiche simili, /fingerprint/linked i dispositivi della stessa rete.

Come gestisco le richieste di cancellazione?

POST /privacy/forget elimina il profilo del dispositivo, i collegamenti, la cronologia e gli avvisi per un identificativo nella Sua organizzazione. Un contrassegno di blocco impedisce che lo stesso identificativo venga registrato di nuovo.

07 · COME INIZIARE

Verifichi la prossima registrazione con segnali reali.

Crei un account su app.paperoffice.ai, generi una chiave API sotto **API e Sviluppatore > Chiavi API** e verifichi il primo indirizzo con `POST /fakeemail/check`. La fatturazione avviene a consumo; i dettagli sono nella pagina dei prezzi.

Aggiungere il controllo e-mail

Il Suo modulo di registrazione invia l'indirizzo tramite il backend a `/fakeemail/check` e agisce sul campo della raccomandazione.

Aggiungere IP e dispositivo

`/ip2location/full` per rete e posizione, l'SDK fingerprint per il `visitor_id`. Salvi entrambi con la richiesta.

Far leggere i documenti d'identità

Crei un IDP Agent con un modello di documento d'identità e lo lasci eseguire automaticamente dopo l'elaborazione nel workspace per le richieste.

SCHEDE TECNICHE SU QUESTO TEMA

Rilevamento di indirizzi email falsipaperoffice.ai/downloads/paperoffice-ai-datasheet-fake-email-detector.pdf**Rilevamento VPN**paperoffice.ai/downloads/paperoffice-ai-datasheet-anonymity-detector.pdf**API di localizzazione IP**paperoffice.ai/downloads/paperoffice-ai-datasheet-ip-location.pdf**Impronta digitale del dispositivo**paperoffice.ai/downloads/paperoffice-ai-datasheet-device-fingerprint.pdf**IDP Agent**paperoffice.ai/downloads/paperoffice-ai-datasheet-idp-intelligent-document-processing-it.pdf

ALTRI APPROFONDIMENTI SU QUESTO TEMA

Frode d'identitàpaperoffice.ai/it/solutions/rischio/ai-frode-identita-rilevamento-prevenzione

ALTRI APPROFONDIMENTI SU QUESTO TEMA

paperoffice.ai/it/solutions/rischio/ai-frode-identita-rilevamento-prevenzione

PREZZI

paperoffice.ai/en/pricing

CONTATTI

paperoffice.ai/it/contatto