



GUIDE COURT • RISQUE • FRAUDE À L'IDENTITÉ

Nouveau client, fausse identité ? Des signaux vérifiés avant de vous engager.

Quiconque s'inscrit ou demande un contrat commence par déclarer qui il est. Ce guide court montre comment PaperOffice fournit l'adresse e-mail, l'adresse IP, l'appareil et la pièce d'identité sous forme de signaux que vous pouvez vérifier. Pour les boutiques, les plateformes, les bailleurs et les commerçants qui vendent à paiements échelonnés.

L'ESSENTIEL

Chaque contrôle renvoie des champs sur lesquels votre règle peut agir : une recommandation pour l'e-mail, des indicateurs pour VPN et Tor, un identifiant d'appareil et des champs de pièce d'identité avec leur emplacement source. Votre équipe prend la décision.

01 · LE PROBLÈME

Le nom est le bon. La personne derrière ne l'est pas.

Un nouveau client signe un contrat en ligne, et un smartphone lui est livré avec paiements échelonnés. Le nom, l'adresse et l'e-mail paraissent authentiques. Ce n'est que lorsque les paiements s'arrêtent que l'on comprend : les données appartiennent à quelqu'un d'autre, ou la personne n'existe pas du tout.

POURQUOI CELA ARRIVE

Données volées et inventées

Les fraudeurs utilisent de vrais noms et de vraies adresses issus de fuites de données ou les mêlent à des éléments inventés. Sur le formulaire, les deux se ressemblent.

Se cacher sur le réseau

Adresses jetables, VPN, Tor et serveurs loués dissimulent qui passe la commande. La même personne peut ouvrir de nombreux comptes avec peu d'efforts.

Pièces d'identité en vitesse

Au comptoir, la copie de la pièce d'identité est vite regardée puis saisie. Une faute de frappe ou un champ manquant passent facilement inaperçus.

COMMENT LE REPÉRER

- L'adresse e-mail provient d'un service jetable, ou son domaine n'a pas de serveur de messagerie.
- L'inscription passe par un VPN, Tor ou un centre de données au lieu d'une connexion ordinaire.
- Le pays de l'adresse IP ne correspond pas à l'adresse indiquée.
- Le même appareil apparaît dans plusieurs inscriptions sous des noms différents.
- Les indications du formulaire et celles de la pièce d'identité diffèrent.

02 · LA DÉMARCHE AVEC PAPEROFFICE

Du signal à la décision.

PaperOffice fournit des signaux sur l'e-mail, le réseau, l'appareil et le document, via la REST API, le SDK et dans l'application. La suite dépend de votre règle : laisser passer, redemander, envoyer à l'examen ou refuser.

1

Évaluer l'adresse e-mail

POST /fakeemail/check contrôle les domaines jetables, les enregistrements MX, SPF et DMARC et renvoie risk_score ainsi que la recommandation ACCEPT, REVIEW ou REJECT.

MODULE: DÉTECTION DES FAUX E-MAILS

2

Contrôler le réseau et la localisation

/ip2location/full renvoie le pays, la région et le fournisseur, ainsi que is_vpn, is_proxy, is_tor et is_datacenter. Le champ type indique la liste qui a correspondu.

MODULE: DÉTECTION VPN

3

Reconnaître l'appareil

Le SDK navigateur renvoie un visitor_id par appareil. À la connexion suivante, /fingerprint/verify vérifie s'il s'agit du même appareil, et risk.factors nomme tout élément inhabituel.

MODULE: EMPREINTE D'APPAREIL

4

Lire la pièce d'identité

Un IDP Agent lit le nom, la date de naissance, l'adresse, le numéro du document et la date d'expiration sur une photo ou une numérisation, chaque valeur avec son emplacement dans l'original.

MODULE: IDP AGENT

5

Décider

Votre application combine les champs en une règle, par exemple : une adresse jetable ou Tor entraîne un examen par une personne. Votre équipe prend la décision.

03 · DANS L'APPLICATION

Clés, SDK, agent : comment le configurer.

Les contrôles de signaux passent par la REST API et le SDK, la pièce d'identité par un IDP Agent dans l'application. Les noms correspondent à ceux de l'application.

1

Une clé API pour votre backend

Sous **API et Développeur** > **Clés API**, utilisez **Créer une nouvelle clé** pour créer une **Clé API**. Votre backend s'en sert pour contrôler l'e-mail et l'adresse IP. Vous pouvez copier la clé à tout moment à cet endroit.

2

Une clé pour le SDK navigateur

Sous **API et Développeur** > **Clés API**, utilisez **Créer une nouvelle clé**, choisissez le type **Clé publiable** et saisissez les domaines de votre site. Votre site charge alors le SDK d'empreinte avec cette clé.

3

Créer un IDP Agent pour les pièces d'identité

Sélectionnez un exemple de photo, puis **Actions** > **Agents et workflows** > **IDP** et **Créer un nouvel agent**. Choisissez un modèle pour les pièces d'identité ou décrivez les champs avec vos propres mots.

4

Vérifier les valeurs par rapport à la source

Dans l'onglet **Champs de données**, chaque valeur figure à côté de l'extrait de la pièce d'identité. La vue **IDP Review** affiche tous les documents avec leurs champs ouverts.

5

Traiter les tâches d'examen

Si un champ obligatoire manque, une tâche est créée dans la file d'examen choisie. Sous **Workflow AI** > **Tâches Human In The Loop**, une personne voit la pièce d'identité et les champs, puis termine l'examen.

CONSEIL DE TERRAIN

Pesez plusieurs signaux ensemble Un VPN n'a souvent, à lui seul, aucune raison inquiétante. Il devient significatif combiné à une adresse jetable ou à un appareil déjà lié à d'autres comptes de votre système. Définissez quand une personne doit examiner le dossier.

04 · UN EXEMPLE

Un revendeur de téléphones. Des contrats à paiements échelonnés.



Un revendeur de téléphones mobiles avec six magasins et une boutique en ligne vend des smartphones avec contrats et plans de paiement échelonnés. En magasin, l'équipe recopie la pièce d'identité et saisit les données ; en ligne, un formulaire suffit. Régulièrement, les paiements s'arrêtent et les clients sont injoignables.

AVANT

- En magasin, la pièce d'identité est recopiée et saisie champ par champ dans le formulaire de contrat.
- En ligne, chaque adresse e-mail est acceptée, y compris les adresses jetables.
- Les demandes passant par des VPN ou des centres de données ressemblent à toutes les autres.
- Personne ne remarque qu'un même appareil a déjà déposé plusieurs demandes.

AVEC PAPEROFFICE

- Le formulaire en ligne contrôle l'adresse e-mail, et en cas de REVIEW la demande part à l'examen.
- Le contrôle IP signale VPN, Tor et centre de données, et la demande compare le pays à l'adresse.
- Chaque demande enregistre le visitor_id, de sorte que les appareils utilisés à plusieurs reprises se remarquent.
- En magasin, un IDP Agent lit la pièce d'identité sur une photo, et l'équipe vérifie les valeurs par rapport à la source.

Exemple à titre d'illustration : l'entreprise et le processus sont fictifs. Vérifiez avec votre délégué à la protection des données quelles données de pièce d'identité et d'appareil vous collectez et combien de temps vous les conservez.

05 · LISTE DE CONTRÔLE

Dix points pour votre intégration client.

Passez ces points en revue avec les ventes, l'informatique et la protection des données. Chacun peut être vérifié dans votre propre activité.

- ☐ Chaque inscription contrôle l'adresse e-mail avant l'activation du compte.
- ☐ Votre backend transmet l'adresse IP du client à l'API dans le paramètre ip.
- ☐ Le pays de l'adresse IP est comparé à l'adresse indiquée.
- ☐ Si un compte connu se connecte depuis un appareil inconnu, votre application demande un second facteur.
- ☐ Pour les demandes de suppression, la voie via POST /privacy/forget est documentée.
- ☐ Pour REVIEW et REJECT, il est défini ce qui se passe : redemander, envoyer à l'examen ou refuser.
- ☐ VPN, Tor et centre de données sont évalués séparément, avec une règle pour chaque cas.
- ☐ Le visitor_id est enregistré avec chaque compte et chaque demande.
- ☐ Un IDP Agent lit les pièces d'identité, et les champs obligatoires sont définis.
- ☐ La finalité, la base légale et la durée de conservation des données d'appareil sont convenues avec la protection des données.

06 · QUESTIONS FRÉQUENTES

Ce que les équipes veulent savoir avant de commencer.

PaperOffice vérifie-t-il les pièces d'identité de manière biométrique ?

PaperOffice fonctionne sans correspondance faciale. Un IDP Agent lit les champs de la pièce d'identité avec leur emplacement source, et les autres contrôles fournissent des signaux sur l'e-mail, le réseau et l'appareil. Votre équipe décide si une identité est confirmée.

Qu'en est-il des personnes qui utilisent un VPN pour de bonnes raisons ?

Un VPN est un signal que votre règle pondère. La réponse distingue VPN, proxy, Tor et centre de données et nomme la liste correspondante dans le champ type. Les adresses figurant dans des listes de blocage apparaissent aussi sous is_vpn.

Comment les contrôles arrivent-ils dans notre portail ?

Via la REST API depuis votre backend, via le SDK d'empreinte avec une **Clé publiable** liée à vos domaines, et via MCP. Vous téléversez les pièces d'identité dans un Workspace où tourne un IDP Agent.

D'où vient le score de risque ?

Du contrôle de l'e-mail : risk_score de 0 à 100, risk_level de MINIMAL à CRITICAL et la recommandation ACCEPT, REVIEW ou REJECT. Le contrôle de l'appareil fournit ses propres facteurs de risque, comme un VPN ou une vitesse de déplacement impossible.

Puis-je repérer le même appareil derrière plusieurs comptes ?

Oui, si vous enregistrez le visitor_id avec chaque compte. Le même identifiant apparaît alors sur plusieurs comptes. /fingerprint/similar trouve les appareils aux caractéristiques proches, et /fingerprint/linked trouve les appareils du même réseau.

Comment traiter les demandes de suppression ?

POST /privacy/forget supprime le profil d'appareil, les liens, l'historique et les alertes pour un identifiant de votre organisation. Un marqueur de blocage empêche d'enregistrer à nouveau le même identifiant.

07 · COMMENT COMMENCER

Contrôlez votre prochaine inscription avec des signaux réels.

Créez un compte sur app.paperoffice.ai, générez une clé API sous **API et Développeur > Clés API** et contrôlez votre première adresse avec `POST /fakeemail/check`. La facturation se fait au paiement à l'usage ; les détails figurent sur la page Tarifs.

Ajouter le contrôle e-mail

Votre formulaire d'inscription envoie l'adresse via votre backend à `/fakeemail/check` et agit sur le champ recommandation.

Ajouter IP et appareil

`/ip2location/full` pour le réseau et la localisation, le SDK d'empreinte pour le `visitor_id`. Enregistrez les deux avec la demande.

Faire lire les pièces d'identité

Créez un IDP Agent avec un modèle de pièce d'identité et laissez-le tourner automatiquement après le traitement dans le Workspace des demandes.

FICHES TECHNIQUES SUR CE SUJET

Détection des faux e-mails

paperoffice.ai/downloads/paperoffice-ai-datasheet-fake-email-detector.pdf

Détection VPN

paperoffice.ai/downloads/paperoffice-ai-datasheet-anonymity-detector.pdf

API de localisation IP

paperoffice.ai/downloads/paperoffice-ai-datasheet-ip-location.pdf

Empreinte d'appareil

paperoffice.ai/downloads/paperoffice-ai-datasheet-device-fingerprint.pdf

IDP Agent

paperoffice.ai/downloads/paperoffice-ai-datasheet-idp-intelligent-document-processing-fr.pdf

POUR ALLER PLUS LOIN

Fraude à l'identité

paperoffice.ai/fr/solutions/risque/ai-fraude-identite-detection-prevention



POUR ALLER PLUS LOIN

paperoffice.ai/fr/solutions/risque/ai-fraude-identite-detection-prevention

TARIFS

paperoffice.ai/fr/tarifs

CONTACT

paperoffice.ai/fr/contact