



KORT GUIDE · RISIKO · IDENTITETSSVINDEL

Ny kunde, falsk identitet?

Signaler kontrolleret, før du binder dig.

Den, der tilmelder sig eller ansøger om en kontrakt, starter med at oplyse, hvem vedkommende er. Denne korte guide viser, hvordan PaperOffice leverer e-mailadresse, IP-adresse, enhed og ID-dokument som signaler, du kan kontrollere. Til butikker, platforme, udlejere og detailhandlere, der sælger på afbetaling.

DET VIGTIGSTE

Hver kontrol giver felter, din regel kan handle på: en anbefaling for e-mailen, markeringer for VPN og Tor, et enheds-ID samt ID-dokumentets felter med deres kildeplacering. Dit team træffer beslutningen.

01 · PROBLEMET

Navnet er rigtigt. Personen bag det er ikke det.

En ny kunde underskriver en kontrakt online, og smartphonen sendes på afbetaling. Navn, adresse og e-mailadresse ser ægte ud. Først når betalingerne udebliver, står det klart: data tilhører en anden, eller personen findes slet ikke.

HVORFOR DET SKER

Stjålne og opdigtede data

Swindlere bruger rigtige navne og adresser fra datalæk eller blander dem med opdigtede oplysninger. På formularen ser begge dele ens ud.

Skjul på netværket

Engangsadresser, VPN, Tor og lejede servere skjuler, hvem der bestiller. Den samme person kan oprette mange konti med ringe indsats.

ID'er i en fart

I butikken får ID-kopien et hurtigt blik og indtastes. En tastefejl eller et manglende felt glider let igennem.

SÅDAN OPDAGER DU DET

- E-mailadressen kommer fra en engangstjeneste, eller dens domæne har ingen mailserver.
- Tilmeldingen kommer via VPN, Tor eller et datacenter i stedet for en almindelig forbindelse.
- IP-adressens land passer ikke til den oplyste adresse.
- Den samme enhed optræder i flere tilmeldinger under forskellige navne.
- Oplysningerne på formularen og på ID-dokumentet afviger fra hinanden.

02 · FREMGANGSMÅDEN MED PAPEROFFICE

Fra signal til beslutning.

PaperOffice leverer signaler om e-mail, netværk, enhed og dokument via REST API, SDK og i appen. Hvad der følger, afhænger af din regel: lad være med at gå videre, spørg igen, send til gennemgang eller afvis.

1

Vurdér e-mailadressen

POST /fakeemail/check kontrollerer engangsdomæner, MX-poster, SPF og DMARC og returnerer risk_score samt anbefalingen ACCEPT, REVIEW eller REJECT.

MODUL: [OPDAGELSE AF FALSKE E-MAILS](#)

2

Kontrollér netværk og placering

/ip2location/full returnerer land, region og udbyder samt is_vpn, is_proxy, is_tor og is_datacenter. Feltet type angiver den liste, der matchede.

MODUL: [VPN-REGISTRERING](#)

3

Genkend enheden

Browser-SDK'en returnerer et visitor_id pr. enhed. Ved næste login kontrollerer /fingerprint/verify, om det er samme enhed, og risk.factors nævner alt usædvanligt.

MODUL: [ENHEDSFINGERAFTRYK](#)

4

Læs ID-dokumentet

En IDP Agent læser navn, fødselsdato, adresse, dokumentnummer og udløbsdato fra et foto eller en scanning, hver værdi med sin placering i originalen.

MODUL: [IDP AGENT](#)

5

Beslut

Din applikation kombinerer felterne til en regel, fx: en engangsadresse eller Tor betyder gennemgang af en person. Dit team træffer beslutningen.

03 · I APPEN

Nøgler, SDK, agent: sådan sætter du det op.

Signalkontrollerne kører via REST API og SDK, ID-dokumentet via en IDP Agent i appen. Navnene svarer til appen.

1

En API-nøgle til din backend

Under **API & Udvikler** > **API-nøgler** bruger du **Opret ny nøgle** til at oprette en **API-nøgle**. Din backend bruger den til at kontrollere e-mail og IP. Du kan kopiere nøglen der når som helst.

2

En nøgle til browser-SDK'en

Under **API & Udvikler** > **API-nøgler** bruger du **Opret ny nøgle**, vælger typen **Offentliggørelsesnøgle** og indtaster dit websites domæner. Din side indlæser derefter fingerprint-SDK'en med den.

3

Opret en IDP Agent til ID'er

Vælg et eksempelfoto, og klik derefter på **Handlinger** > **Agenter og arbejdsgange** > **IDP** og **Opret ny agent**. Vælg en skabelon til ID-dokumenter, eller beskriv felterne med dine egne ord.

4

Kontrollér værdier mod kilden

I fanen **Datafelter** står hver værdi ved siden af uddraget fra ID-dokumentet. Visningen **IDP Review** viser alle dokumenter med åbne felter.

5

Arbejd igennem gennemgangsopgaver

Mangler et påkrævet felt, oprettes en opgave i den valgte gennemgangskø. Under **Workflow AI** > **Human In The Loop-opgaver** ser en person ID'et og felterne og fuldfører gennemgangen.

TIP FRA PRAKSIS

Vej flere signaler sammen En VPN alene har ofte harmløse grunde. Den bliver meningsfuld sammen med en engangsadresse eller en enhed, der allerede er knyttet til andre konti i dit system. Definér, hvornår en person gennemgår.

04 · ET EKSEMPEL

En telefonforhandler. Kontrakter med afbetaling.



En mobilforhandler med seks butikker og en onlinebutik sælger smartphones med abonnementer og afbetalingsaftaler. I butikken kopierer teamet ID'et og indtaster data, online er en formular nok. Gang på gang udebliver betalingerne, og kunderne kan ikke nås.

FØR

- I butikken kopieres ID'et, og det indtastes felt for felt i kontraktformularen.
- Online accepteres enhver e-mailadresse, også engangsadresser.
- Ansøgninger via VPN eller datacentre ser ud som alle andre.
- Ingen bemærker, at én enhed allerede har indsendt flere ansøgninger.

MED PAPEROFFICE

- Onlineformularen kontrollerer e-mailadressen, og ved REVIEW går ansøgningen til gennemgang.
- IP-kontrollen melder VPN, Tor og datacenter, og ansøgningen sammenligner landet med adressen.
- Hver ansøgning gemmer visitor_id, så enheder, der bruges flere gange, skiller sig ud.
- I butikken læser en IDP Agent ID'et fra et foto, og teamet kontrollerer værdierne mod kilden.

Et eksempel til illustration; virksomheden og processen er opdigtet. Afklar med din databeskyttelsesrådgiver, hvilke ID- og enhedsdata du indsamler, og hvor længe du gemmer dem.

05 · TJEKLISTE

Ti punkter for din kundeoprettelse.

Gennemgå punkterne med salg, IT og databeskyttelse. Hvert punkt kan kontrolleres i din egen virksomhed.

- | | |
|---|---|
| ☐ Hver tilmelding kontrollerer e-mailadressen, før kontoen aktiveres. | ☐ For REVIEW og REJECT er det defineret, hvad der sker: spørg igen, send til gennemgang eller afvis. |
| ☐ Din backend sender kundens IP-adresse til API'et i parameteren ip. | ☐ VPN, Tor og datacenter vurderes hver for sig, med en regel for hvert tilfælde. |
| ☐ IP-adressens land sammenlignes med den oplyste adresse. | ☐ visitor_id gemmes med hver konto og hver ansøgning. |
| ☐ Hvis en kendt konto logger ind fra en ukendt enhed, beder din applikation om en ekstra faktor. | ☐ En IDP Agent læser ID-dokumenter, og de påkrævede felter er defineret. |
| ☐ For sletningsanmodninger er vejen via POST /privacy/forgit dokumenteret. | ☐ Formål, retsgrundlag og opbevaringsperiode for enhedsdata er aftalt med databeskyttelse. |

06 · OFTE STILLEDE SPØRGSMÅL

Hvad teams vil vide før de går i gang.

Tjekker PaperOffice ID'er biometrisk?

PaperOffice arbejder uden ansigtsmatch. En IDP Agent læser felterne i ID-dokumentet med deres kildeplacering, og de øvrige kontroller leverer signaler om e-mail, netværk og enhed. Dit team afgør, om en identitet er bekræftet.

Hvad med personer, der bruger en VPN af gode grunde?

En VPN er et signal, som din regel vejer. Svaret skelner mellem VPN, proxy, Tor og datacenter og nævner den matchende liste i feltet type. Adresser fra blokeringslister optræder også under is_vpn.

Hvordan kommer kontrollerne ind i vores portal?

Via REST API fra din backend, via fingerprint-SDK'en med en Offentliggørelsesnøgle, der er bundet til dine domæner, og via MCP. Du uploader ID-dokumenter i et workspace, hvor en IDP Agent kører.

Hvor kommer risikoscoren fra?

Fra e-mailkontrollen: risk_score fra 0 til 100, risk_level fra MINIMAL til CRITICAL og anbefalingen ACCEPT, REVIEW eller REJECT. Enhedskontrollen leverer sine egne risikofaktorer, fx en VPN eller en umulig rejsehastighed.

Kan jeg finde den samme enhed bag flere konti?

Ja, hvis du gemmer visitor_id med hver konto. Så optræder det samme ID på flere konti. /fingerprint/similar finder enheder med lignende træk, og /fingerprint/linked finder enheder fra samme netværk.

Hvordan håndterer jeg sletningsanmodninger?

POST /privacy/forget sletter enhedsprofilen, forbindelserne, historikken og advarslerne for en identifikator i din organisation. En blokeringsmarkering forhindrer, at den samme identifikator registreres igen.

07 · SÅDAN KOMMER DU I GANG

Kontrollér din næste tilmelding med rigtige signaler.

Opret en konto på app.paperoffice.ai, generér en API-nøgle under **API & Udvikler** > **API-nøgler**, og kontrollér din første adresse med `POST /fakeemail/check`. Faktureringen sker efter forbrug; detaljerne står på prissiden.

Tilføj e-mailkontrollen

Din tilmeldingsformular sender adressen via din backend til `/fakeemail/check` og handler efter feltet `recommendation`.

Tilføj IP og enhed

`/ip2location/full` til netværk og placering, fingerprint-SDK'en til `visitor_id`. Gem begge dele sammen med ansøgningen.

Lad ID'er blive læst

Opret en IDP Agent med en ID-skabelon, og lad den køre automatisk efter behandlingen i workspace'et til ansøgninger.

DATABLADE OM EMNET

Opdagelse af falske e-mailspaperoffice.ai/downloads/paperoffice-ai-datasheet-fake-email-detector.pdf**VPN-registrering**paperoffice.ai/downloads/paperoffice-ai-datasheet-anonymity-detector.pdf**IP-lokalisering API**paperoffice.ai/downloads/paperoffice-ai-datasheet-ip-location.pdf**Enhedsfingeraftryk**paperoffice.ai/downloads/paperoffice-ai-datasheet-device-fingerprint.pdf**IDP Agent**paperoffice.ai/downloads/paperoffice-ai-datasheet-idp-intelligent-document-processing-da.pdf

MERE OM EMNET

Identitetssvindpaperoffice.ai/da/solutions/risiko/ai-identitetstyveri-detektion-forebyggelse

MERE OM EMNET

paperoffice.ai/da/solutions/risiko/ai-identitetstyveri-detektion-forebyggelse

PRISER

paperoffice.ai/en/pricing

KONTAKT

paperoffice.ai/da/kontakt