



KORT GUIDE · RISK · IDENTITETSBEDRÅGERI

Ny kund, falsk identitet?

Signaler kontrolleras innan du binder dig.

Den som registrerar sig eller ansöker om ett avtal börjar med att påstå vem den är. Den här korta guiden visar hur PaperOffice levererar e-postadress, IP-adress, enhet och id-handling som signaler som du kan kontrollera. För butiker, plattformar, hyresvärdar och återförsäljare som säljer på avbetalning.

DET VIKTIGASTE

Varje kontroll ger fält som din regel kan agera på: en rekommendation för e-postadressen, flaggor för VPN och Tor, ett enhets-ID och fält för id-handlingen med deras källplats. Ditt team fattar beslutet.

01 · PROBLEMET

Namnet stämmer. Men personen bakom det gör inte det.

En ny kund skriver på ett avtal online, och smarttelefonen levereras på avbetalning. Namn, adress och e-postadress ser äkta ut. Först när betalningarna uteblir blir det tydligt: uppgifterna tillhör någon annan, eller så finns personen inte alls.

VARFÖR DET HÄNDER

Stulna och uppdiktade uppgifter

Bedragare använder riktiga namn och adresser från dataintrång eller blandar dem med uppdiktade uppgifter. På formuläret ser båda likadana ut.

Gömmor sig i nätverket

Engångsadresser, VPN, Tor och hyrda servrar döljer vem som beställer. Samma person kan öppna många konton med liten möda.

Id-handlingar i brådskan

Vid disken får kopian av id-handlingen en snabb blick och skrivs in. Ett tryckfel eller ett saknat fält slinker lätt igenom.

SÅ MÄRKER DU DET

- E-postadressen kommer från en engångstjänst, eller dess domän saknar en e-postserver.
- Registreringen kommer via ett VPN, Tor eller ett datacenter i stället för en vanlig anslutning.
- Landet för IP-adressen stämmer inte med den angivna adressen.
- Samma enhet förekommer i flera registreringar under olika namn.
- Uppgifterna på formuläret och på id-handlingen skiljer sig åt.

02 · SÅ GÖR DU MED PAPEROFFICE

Från signal till beslut.

PaperOffice levererar signaler om e-post, nätverk, enhet och dokument, via REST API, SDK och i appen. Vad som sedan händer är upp till din regel: släppa igenom, fråga igen, skicka till granskning eller avvisa.

1

Bedöm e-postadressen

POST /fakeemail/check kontrollerar engångsdomäner, MX-poster, SPF och DMARC och returnerar risk_score samt rekommendationen ACCEPT, REVIEW eller REJECT.

MODUL: [IGENKÄNNING AV FALSKA E-POSTADRESSER](#)

2

Kontrollera nätverk och plats

/ip2location/full returnerar land, region och leverantör samt is_vpn, is_proxy, is_tor och is_datacenter. Fältet type anger vilken lista som matchade.

MODUL: [VPN-IDENTIFIERING](#)

3

Känn igen enheten

Webbläsar-SDK:t returnerar ett visitor_id per enhet. Vid nästa inloggning kontrollerar /fingerprint/verify om det är samma enhet, och risk.factors anger allt ovanligt.

MODUL: [ENHETSFINGERAVTRYCK](#)

4

Läs id-handlingen

En IDP Agent läser namn, födelsedatum, adress, dokumentnummer och utgångsdatum från ett foto eller en skanning, varje värde med sin plats i originalet.

MODUL: [IDP AGENT](#)

5

Besluta

Din applikation kombinerar fälten till en regel, till exempel: en engångsadress eller Tor innebär granskning av en person. Ditt team fattar beslutet.

03 · I APPEN

Nycklar, SDK, agent: så ställer du in det.

Signalkontrollerna körs via REST API och SDK, id-handlingen via en IDP Agent i appen. Namnen stämmer med appen.

1

En API-nyckel för din backend

Under **API & Utvecklare > API-Schlüssel** använder du **Skapa ny nyckel** för att skapa en **API-nyckel**. Din backend använder den för att kontrollera e-post och IP. Du kan kopiera nyckeln där när som helst.

2

En nyckel för webbläsar-SDK:t

Under **API & Utvecklare > API-Schlüssel** använder du **Skapa ny nyckel**, väljer typen **Publicerbar nyckel** och anger din webbplats domäner. Din sajt laddar då fingeravtrycks-SDK:t med den.

3

Skapa en IDP Agent för id-handlingar

Markera ett exempelfoto, och välj sedan **Åtgärder > Agenter & arbetsflöden > IDP** och **Skapa ny agent**. Välj en mall för id-handlingar eller beskriv fälten med egna ord.

4

Kontrollera värden mot källan

På fliken **Datafält** sitter varje värde bredvid utdraget från id-handlingen. Vyn **IDP Review** visar alla dokument med öppna fält.

5

Arbeta igenom granskningsuppgifter

Om ett obligatoriskt fält saknas skapas en uppgift i den valda granskningskön. Under **Workflow AI > Human In The Loop-uppgifter** ser en person id-handlingen och fälten och slutför granskningen.

TIPS FRÅN PRAKTIKEN

Väg flera signaler tillsammans Ett VPN har ofta ofarliga skäl i sig självt. Det blir meningsfullt tillsammans med en engångsadress eller en enhet som redan är kopplad till andra konton i ditt system. Definiera när en person ska granska.

04 · ETT EXEMPEL

En mobilhandlare. Avtal med avbetalning.



En mobilhandlare med sex butiker och en onlinebutik säljer smarttelefoner med avtal och avbetalningsplaner. I butiken kopierar teamet id-handlingen och skriver in uppgifterna, online räcker ett formulär. Gång på gång uteblir betalningarna och kunderna går inte att nå.

FÖRE

- I butiken kopieras id-handlingen och skrivs in i avtalsformuläret fält för fält.
- Online godtas varje e-postadress, även engångsadresser.
- Ansökningar via VPN eller datacenter ser ut som alla andra.
- Ingen märker att en enhet redan lämnat in flera ansökningar.

MED PAPEROFFICE

- Onlineformuläret kontrollerar e-postadressen, och vid REVIEW går ansökan till granskning.
- IP-kontrollen rapporterar VPN, Tor och datacenter, och ansökan jämför landet med adressen.
- Varje ansökan lagrar visitor_id, så att enheter som använts flera gånger sticker ut.
- I butiken läser en IDP Agent id-handlingen från ett foto, och teamet kontrollerar värdena mot källan.

Exempel för illustration, företaget och processen är påhittade. Stäm av med ditt dataskyddsombud vilka id- och enhetsuppgifter du samlar in och hur länge du behåller dem.

05 · CHECKLISTA

Tio punkter för din kundregistrering.

Gå igenom punkterna tillsammans med försäljning, IT och dataskydd. Varje punkt kan kontrolleras i din egen verksamhet.

- | | |
|--|--|
| ☐ Varje registrering kontrollerar e-postadressen innan kontot aktiveras. | ☐ För REVIEW och REJECT är det bestämt vad som händer: fråga igen, skicka till granskning eller avvisa. |
| ☐ Din backend skickar kundens IP-adress till API:t i parametern ip. | ☐ VPN, Tor och datacenter bedöms var för sig, med en regel för varje fall. |
| ☐ Landet för IP-adressen jämförs med den angivna adressen. | ☐ visitor_id lagras med varje konto och varje ansökan. |
| ☐ Om ett känt konto loggar in från en okänd enhet frågar din applikation efter en andra faktor. | ☐ En IDP Agent läser id-handlingar, och de obligatoriska fälten är definierade. |
| ☐ För raderingsbegäranden är vägen via POST /privacy/forget dokumenterad. | ☐ Syfte, rättslig grund och bevarandetid för enhetsuppgifter är överenskomna med dataskyddet. |

06 · VANLIGA FRÅGOR

Vad team vill veta innan de börjar.

Kontrollerar PaperOffice id-handlingar biometriskt?

PaperOffice arbetar utan ansiktsjämförelse. En IDP Agent läser fälten i id-handlingen med deras källplats, och de övriga kontrollerna levererar signaler om e-post, nätverk och enhet. Ditt team avgör om en identitet bekräftas.

Hur är det med personer som använder ett VPN av goda skäl?

Ett VPN är en signal som din regel väger. Svaret skiljer på VPN, proxy, Tor och datacenter och anger den matchande listan i fältet type. Adresser från blockeringslistor visas också under is_vpn.

Hur kommer kontrollerna in i vår portal?

Via REST API från din backend, via fingerprint-SDK:t med en **Publicerbar nyckel** kopplad till dina domäner, och via MCP. Du laddar upp id-handlingar i ett Workspace där en IDP Agent körs.

Var kommer riskpoängen ifrån?

Från e-postkontrollen: risk_score från 0 till 100, risk_level från MINIMAL till CRITICAL och rekommendationen ACCEPT, REVIEW eller REJECT. Enhetskontrollen levererar egna riskfaktorer, till exempel ett VPN eller omöjligt resande.

Kan jag upptäcka samma enhet bakom flera konton?

Ja, om du lagrar visitor_id med varje konto. Då förekommer samma ID på flera konton. /fingerprint/similar hittar enheter med liknande egenskaper, /fingerprint/linked enheter från samma nätverk.

Hur hanterar jag raderingsbegäranden?

POST /privacy/forget raderar enhetsprofilen, kopplingarna, historiken och varningarna för en identifierare i din organisation. En blockeringsmarkering förhindrar att samma identifierare registreras igen.

07 · SÅ HÄR BÖRJAR DU

Kontrollera nästa registrering med verkliga signaler.

Skapa ett konto på app.paperoffice.ai, generera en API-nyckel under **API & Utvecklare > API-Schlüssel** och kontrollera din första adress med POST `/fakeemail/check`. Faktureringen sker efter användning, detaljerna finns på prissidan.

Lägg till e-postkontrollen

Ditt registreringsformulär skickar adressen via din backend till `/fakeemail/check` och agerar på fältet för rekommendation.

Lägg till IP och enhet

`/ip2location/full` för nätverk och plats, fingerprint-SDK:t för `visitor_id`. Lagra båda tillsammans med ansökan.

Låt id-handlingar läsas

Skapa en IDP Agent med en id-mall och låt den köras automatiskt efter bearbetningen i Workspace för ansökningar.

DATABLAD OM DETTA ÄMNE

Igenkänning av falska e-postadresserpaperoffice.ai/downloads/paperoffice-ai-datasheet-fake-email-detector.pdf**VPN-identifiering**paperoffice.ai/downloads/paperoffice-ai-datasheet-anonymity-detector.pdf**IP-plats-API**paperoffice.ai/downloads/paperoffice-ai-datasheet-ip-location.pdf**Enhetsfingeravtryck**paperoffice.ai/downloads/paperoffice-ai-datasheet-device-fingerprint.pdf**IDP Agent**paperoffice.ai/downloads/paperoffice-ai-datasheet-idp-intelligent-document-processing-sv.pdf

MER OM DETTA ÄMNE

Identitetsbedrägeripaperoffice.ai/sv/solutions/risk/ai-identitetsbedrageri-detektering-forebyggande

MER OM DETTA ÄMNE

paperoffice.ai/sv/solutions/risk/ai-identitetsbedrageri-detektering-forebyggande

PRISER

paperoffice.ai/en/pricing

KONTAKT

paperoffice.ai/sv/kontakt