

Protection à l'ouverture des comptes BioCatch

Des nouveaux clients qui n'en sont pas vraiment

Les institutions financières investissent de plus en plus dans les canaux numériques pour répondre aux besoins des clients là où ils se trouvent, en offrant plus de fonctionnalités, de produits et de services en ligne que jamais. Outre les fonctionnalités bancaires courantes, 82 % des institutions financières offrent la possibilité d'ouvrir un compte courant en ligne¹. Bien que ce virage numérique offre aux entreprises une formidable opportunité d'acquérir davantage de clients, les cybercriminels menacent ces opportunités en exploitant les faiblesses du processus d'ouverture de compte.

Face à l'abondance d'informations personnelles identifiables (IPI) facilement disponibles sur le dark web, les cybercriminels utilisent des identités volées ou synthétiques pour ouvrir de nouveaux comptes et emprunter ou blanchir de l'argent, accumulant ainsi les pertes liées à la fraude et introduisant un risque pour la réputation de l'entreprise.

La fraude à l'ouverture de compte étant une pratique de plus en plus répandue et difficile à détecter, les entreprises recherchent des solutions innovantes pour améliorer la détection des fraudes et réduire les frictions avec les clients.

Une ouverture du compte en toute confiance

Forte de plus d'une décennie d'expérience dans l'analyse des comportements numériques, la plateforme BioCatch possède une capacité inégalée à distinguer les utilisateurs authentiques des cybercriminels au moment de l'ouverture d'un compte, protégeant ainsi les entreprises et leurs clients contre un large éventail de menaces de fraudes, parmi lesquelles :



Usurpation d'identité

Comptes ouverts en utilisant l'identité d'une autre personne. Les fuites de données et les attaques par hameçonnage fournissent la matière indispensable aux usurpations d'identité.



Fraude par identité synthétique

Comptes ouverts à l'aide de données légitimes combinées à des données synthétiques pour créer une nouvelle identité.



Comptes mules

Comptes ouverts dans le but de déplacer des fonds volés. Les comptes mules sont essentiels au processus d'encaissement des criminels.

Dites non aux criminels, oui aux nouveaux clients

BioCatch adopte une approche innovante pour protéger l'ouverture de compte, en surveillant les comportements numériques physiques et cognitifs d'un utilisateur afin de détecter la fraude et l'usurpation d'identité et d'améliorer l'expérience client. Les utilisateurs authentiques ont un comportement naturel différent de celui des fraudeurs ; grâce à la visibilité continue des sessions et aux fonctions de profilage avancées, la plateforme BioCatch fait apparaître des modèles de comportement qui racontent une histoire : celle d'un cybercriminel ou celle d'un prospect authentique.

¹ Source : The Financial Brand, Digital Banking Report Research, août 2020



CYBERCRIMINELS vs UTILISATEURS AUTHENTIQUES



Le comportement est révélateur

Contrairement aux contrôles traditionnels de prévention de la fraude qui reposent majoritairement sur des éléments susceptibles d'être compromis ou modifiés, le comportement des utilisateurs ne peut jamais être volé, usurpé ou reproduit. La plateforme BioCatch utilise la biométrie comportementale et l'analyse cognitive pour analyser des milliers d'attributs comportementaux tout au long d'une session d'ouverture de compte, ce qui permet de repérer les indices, mêmes subtils, d'une activité criminelle. La plateforme BioCatch délivre de puissantes informations sur les risques liés à l'ouverture d'un compte, parmi lesquelles :

Maîtrise du processus : dans quelle mesure l'utilisateur connaît-il le processus de demande d'ouverture d'un compte ?

Un cybercriminel utilisant à plusieurs reprises des identités compromises ou synthétiques démontrera un niveau élevé de connaissance du processus d'ouverture de compte par rapport à un utilisateur authentique.

Méconnaissance des données : dans quelle mesure l'utilisateur connaît-il ses données personnelles ?

Un cybercriminel n'a pas connaissance des données personnelles et peut procéder à des suppressions excessives ou recourir à des techniques de copier-coller ou à des outils automatisés pour saisir des informations qui seraient intuitives pour un utilisateur authentique.

Comportement expert : l'utilisateur possède-t-il des compétences informatiques avancées par rapport à la population générale ?

Un cybercriminel fait souvent preuve de compétences informatiques avancées que l'on retrouve rarement chez les utilisateurs authentiques. Citons par exemple l'utilisation de raccourcis avancés, d'outils de développement, de touches spéciales ou le passage d'une application à l'autre.

Analyse de l'âge : la vitesse de frappe et les swipes correspondent-ils à la tranche d'âge de l'utilisateur ?

Certains comportements évoluent avec l'âge, comme le temps nécessaire pour passer de la touche Contrôle à une touche alphabétique lors de la saisie de données, l'orientation de l'appareil mobile et les habitudes de déplacement.

Avantages de la protection à l'ouverture des comptes BioCatch

Réduire les pertes dues à la fraude

Détectez les indices les plus subtils d'un comportement criminel sans avoir jamais vu l'utilisateur

Obtenez des résultats immédiats

Tirez parti des modèles de risque avancés de BioCatch pour détecter les fraudes immédiatement après le déploiement

Augmentez l'acquisition client

Réduisez considérablement les faux refus et les abandons de demandes pour acquérir plus de clients en toute sécurité



Obtenez des résultats dès le premier jour

La protection à l'ouverture des comptes BioCatch est efficace dès son déploiement, la collecte continue de données comportementales permettant d'obtenir des scores de risque et des informations comportementales exploitables. Pour permettre une action en temps réel, les informations de BioCatch sont fournies au moyen d'un ensemble d'outils puissants sur plateforme et via des API.



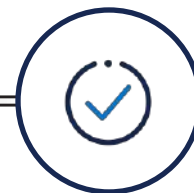
Déployez

Commencez immédiatement à collecter les comportements des utilisateurs en intégrant les SDK brevetés BioCatch



Analysez

Distinguez les utilisateurs authentiques des cybercriminels à l'aide des modèles de risque avancés de BioCatch



Agissez

Réduisez les risques en temps réel en tirant parti des scores de risque et des informations comportementales de BioCatch.

Changez la donne pour votre établissement

800 000 £

de pertes dues à la fraude évitées en trois mois

Une des cinq plus grandes banques britanniques a empêché des milliers de tentatives de fraude à l'ouverture de compte dans le cadre d'offres promotionnelles.

+ de 90 %

d'amélioration de la précision des alertes de fraude dans les premières semaines

Une grande banque de la région Asie-Pacifique a obtenu des résultats immédiats en détectant des centaines d'ouvertures de comptes frauduleuses immédiatement après le déploiement.

1 million de dollars

de nouveaux revenus

Un des cinq principaux émetteurs de cartes aux États-Unis a généré de nouveaux revenus annuels en réduisant considérablement les faux refus et les abandons de demandes.



BioCatch est le leader en matière de biométrie comportementale. Cette technologie consiste à analyser le comportement numérique physique et cognitif d'un utilisateur en ligne afin de protéger les individus et leurs biens. Notre mission est d'utiliser le pouvoir du comportement et de fournir des informations exploitables afin de créer un monde numérique où l'identité, la confiance et la facilité coexistent en toute fluidité. Des institutions financières de premier plan du monde entier utilisent BioCatch pour lutter plus efficacement contre la fraude, favoriser la transformation numérique et accélérer leur croissance. Avec plus d'une décennie d'analyse de données, plus de 60 brevets et une expérience inégalée, BioCatch continue d'innover pour résoudre les problèmes de demain. Pour en savoir plus, rendez-vous sur www.biocatch.com

www.biocatch.com

E-mail : info@biocatch.com

[@biocatch](https://twitter.com/biocatch)

[in/company/biocatch](https://www.linkedin.com/company/biocatch)