AGIR ENSEMBLE CONTRE LA FRAUDE AUX PAIEMENTS

Bancontact Company lutte contre la fraude à travers **trois approches complémentaires** :

1. Un schéma de paiement sécurisé
2. Des mécanismes de sécurité intégrés dans Bancontact Pay
3. Des initiatives de sensibilisation pour aider les utilisateurs à reconnaître et éviter les tentatives de fraude

Cette combinaison de mesures permet de garantir des paiements sécurisés et de mieux protéger les consommateurs en Belgique.

1. Un écosystème de paiement sécurisé

Un paiement Bancontact implique plusieurs acteurs, des banques aux commerçants, en passant par les partenaires techniques. Au cœur de cet écosystème, Bancontact Company fait le lien entre ces acteurs et facilite le partage d'informations utiles pour mieux identifier les signaux suspects.

La sécurité de cet écosystème repose également sur des audits externes réguliers, incluant des tests d'intrusion et des évaluations des dispositifs de prévention de la fraude. Ces contrôles contribuent à maintenir un niveau de sécurité élevé et cohérent pour l'ensemble des acteurs de l'écosystème Bancontact.

2. Des mécanismes de sécurité intégrés dans Bancontact Pay

1) Vérification sécurisée des utilisateurs via itsme

L'application Bancontact Pay utilise itsme pour vérifier l'identité des nouveaux utilisateurs ainsi que celle des utilisateurs qui réactivent leur compte. Cette méthode d'identification sécurisée contribue à limiter les risques d'usurpation d'identité lors de la création ou de la réactivation d'un compte.

Près de 70 % des nouveaux utilisateurs et 92 % des utilisateurs qui réactivent leur compte utilisent itsme pour accéder à Bancontact Pay, ce qui contribue à réduire le risque de fraude pour ces groupes.

2) Détection et blocage des faux sites web et des URL frauduleuses

Bancontact Company surveille activement les sites web et les URL frauduleux susceptibles d'usurper son identité ou d'exploiter ses marques, y compris Bancontact Pay.

Entre janvier 2025 et juin 2026, 3 465 URL ont été analysées dans le cadre d'une surveillance ciblée des marques Bancontact, elle-même intégrée à un dispositif mondial couvrant 741 millions d'URL.

3) Détection et blocage des comptes suspects

Des outils dédiés permettent d'identifier les comportements à risque et, le cas échéant, de bloquer les comptes suspects. Les appareils associés à ces comptes peuvent également être mis sur liste noire afin d'empêcher leur réutilisation à des fins frauduleuses.

Depuis 2021, 19 300 comptes ont été bloqués afin de limiter les possibilités d'action des fraudeurs.

4) Tests de sécurité réguliers

Bancontact Pay fait l'objet de tests de sécurité réguliers visant à identifier d'éventuelles vulnérabilités et à renforcer la résistance de l'application face aux tentatives de fraude.

5) Renforcement continu des contrôles

Bancontact Company continue de développer de nouveaux mécanismes de protection afin de renforcer la sécurité des utilisateurs et de limiter les risques d'arnaques.

Plusieurs mesures ont été mises en œuvre et sont encore prévues en 2026, notamment des contrôles supplémentaires lors de l'ajout d'une carte dans Bancontact Pay, le renforcement de l'identification via itsme, ainsi que l'envoi de notifications lorsqu'un nouvel appareil est associé à un compte.

3. Des initiatives de sensibilisation pour aider les consommateurs à reconnaître la fraude

En complément des mécanismes de sécurité intégrés à ses solutions de paiement, Bancontact Company mène des actions de sensibilisation afin d'aider les consommateurs à reconnaître les situations suspectes et à adopter les bons réflexes avant d'agir.

Ces conseils sont notamment diffusés via sa newsletter et ses réseaux sociaux. En 2024, Bancontact Company a également collaboré avec Plantyn pour sensibiliser les plus jeunes aux paiements digitaux sécurisés et aux tentatives de fraude.

Par ailleurs, Bancontact Company lancera cette année plusieurs projets d'accompagnement et d'éducation destinés aux jeunes qui entrent progressivement dans leur vie de consommateurs. L'objectif est de les aider à adopter les bons réflexes pour mieux comprendre les risques liés aux paiements digitaux et aux tentatives de fraude.