Protégez votre compte de commerçant contre les tests de carte

Que sont les tests de carte?

Les tests de carte (aussi appelés « fraude liée aux cartes bancaires », « énumération » ou « tests de compte ») sont utilisés par les fraudeurs pour soumettre des opérations non autorisées dans le but de trouver les renseignements valides d'une carte qu'ils pourront ensuite utiliser pour commettre des fraudes ailleurs. La méthode de tests de carte la plus courante consiste à cibler le site Web ou l'application mobile d'un commerçant et d'y soumettre plusieurs opérations au moyen d'un processus automatisé. Ces opérations peuvent prendre la forme d'achats, de préautorisations ou de vérifications à l'ajout d'une carte.

Quelles sont les répercussions des tests de carte sur les commerçants?

Les tests de carte ont de nombreuses répercussions négatives sur les commerçants, notamment :

- **Contestations des titulaires de carte :** Les opérations approuvées risquent d'entraîner des contestations de la part des titulaires de carte, surtout si elles ne sont pas remboursées. Ces contestations sont coûteuses et nuisent à la réputation du commerçant.
- **Frais supplémentaires :** Les tests de carte peuvent entraîner des tentatives d'opération excessives et des frais de non-conformité supplémentaires de la part des réseaux de cartes de paiement. Les tentatives d'opération excessives sont définies par les réseaux de cartes de paiement comme étant des tentatives d'autorisation continues (au moyen d'un même numéro de carte), ce qui se traduit généralement par des opérations refusées, par exemple : 10 refus ou plus dans une période de 24 heures ou 15 refus ou plus dans une période de 30 jours. Pour en savoir plus, consultez le document *Réseau de cartes de paiement – Changements apportés aux codes de refus, aux règles et aux frais* à l'adresse suivante : https://www.td.com/ca/fr/entreprises/comment-faire/solutions-aux-commercants/centre-de-ressources/annonces-et-avis/.
- **Augmentation des refus :** Les tests de carte créent une association négative avec l'entreprise du point de vue des réseaux de cartes de paiement et des émetteurs de cartes, ce qui peut entraîner le refus d'un plus grand nombre d'opérations, même lorsque les tests de carte ont cessé.

Comment est-ce que Solutions aux commerçants TD aide à protéger les commerçants contre les tests de carte?

Solutions aux commerçants TD a mis en place des contrôles visant à atténuer les répercussions des tests de carte, comme de la surveillance, des rapports et des alertes. Malheureusement, ces contrôles à eux seuls ne peuvent pas empêcher les tests de carte. Les commerçants doivent prendre des mesures pour empêcher les opérations non autorisées sur leurs sites Web ou leurs applications mobiles.

Que dois-je faire si mon compte de commerçant est utilisé pour des tests de carte?

La première chose à faire est de déterminer si les tests de carte passent par votre site Web ou directement à votre passerelle de paiement. Si les tests de carte passent par votre site Web, veuillez passer en revue les recommandations ci-dessous.

Si les tests de carte passent directement à votre passerelle de paiement, vos clés d'interface de programmation d'applications (API) risquent d'être compromises et doivent être changées. Si cela se produit, vous devez examiner la façon dont vous gérez vos clés d'API pour vous assurer qu'elles sont sécuritaires. Vous devez également faire attention aux tentatives d'hameçonnage visant à obtenir vos clés d'API.

Peu importe la forme que prennent les tests de carte, il est important de rembourser toute opération approuvée par l'entremise de ceux-ci afin d'éviter d'autres répercussions sur votre réputation et d'autres contestations.

Comment puis-je protéger mon site Web contre les tests de carte?

Habituellement, la prévention des tests de carte nécessite des changements au niveau du code, ce qui exige que les commerçants fassent appel à leurs développeurs. Si vous utilisez une plateforme, veuillez communiquer avec votre fournisseur. Vous pouvez également travailler avec votre fournisseur de passerelle de paiement pour vous assurer d'utiliser les outils de prévention de la fraude dont il dispose. Cela peut comprendre des outils comme 3-D Secure, le code de vérification de la carte 2 (CVV2), le Service de vérification d'adresse (SVA) ou d'autres outils d'évaluation liés à la fraude. Bien que ces outils n'empêchent pas directement les tests des cartes, ils décourageront les fraudeurs de cibler votre site Web en entraînant un plus grand nombre de tentatives de tests de carte, et donc un refus.

Comment protéger votre site Web contre les tests de carte

CAPTCHA

- Mettez en place des contrôles CAPTCHA pour empêcher le lancement automatisé d'opérations par des robots et des scripts.
- Assurez-vous que votre solution CAPTCHA est configurée pour empêcher les tests de carte en ajustant les seuils disponibles et en vous assurant de l'utiliser dans le flux de paiement ou d'ajout de carte.

Surveillance et limites

- Surveillez la vitesse des opérations, petites ou importantes. Les opérations de tests de compte sont habituellement de faible montant. Établissez des limites en fonction des montants ou des fourchettes d'opérations et du nombre d'opérations dans une période donnée.
- Surveillez la vitesse pour divers éléments de données, comme l'appareil, l'adresse IP, l'adresse courriel, etc.
- Analysez les différences de fuseau horaire et les incohérences dans la langue du navigateur par rapport à l'adresse IP et à l'appareil du titulaire de carte. Classez ces opérations comme présentant un risque élevé et effectuez un examen plus rigoureux.
- Surveillez les adresses IP associées à un grand nombre de refus. Limitez ou bloquez temporairement ces adresses IP.
- Repérez les cas d'utilisation et de consommation excessive de la bande passante pour un même utilisateur. Limitez ou bloquez ces utilisateurs.
- Dans les opérations, repérez les éléments communs liés à un même appareil. Par exemple, plusieurs opérations peuvent être effectuées à partir de différents comptes, mais avec la même adresse courriel ou le même ID d'appareil.
- Recherchez les ouvertures de session provenant de nombreuses adresses IP pour un même compte de paiement.
- Limitez le nombre de comptes qui peuvent être créés par une même adresse IP dans une période établie. Surveillez la fréquence des changements apportés aux modes de paiement dans les comptes.

Sessions utilisateurs

- Limitez le nombre de cartes qui peuvent être ajoutées par compte et par session.
- Mettez fin aux sessions d'utilisateurs invités qui demeurent actives pendant un certain temps.
- Au moment de vérifier un compte, insérez des pauses aléatoires (p. ex., ralentissements) afin de ralentir les attaques qui dépendent du temps.
- Incluez des vitesses de session HTTP, qui limitent le nombre d'opérations par session d'utilisateur, et réglez la session pour qu'elle expire après quelques secondes d'inactivité.
- Verrouillez un compte si l'utilisateur entre incorrectement un nom d'utilisateur ou un mot de passe dans les données d'authentification jusqu'à un nombre de tentatives donné.

Outils de réseau

- Mettez en place une application Web de pare-feu.
- Utilisez les outils de base pour la détection, la prévention et le retrait des réseaux zombies. Des outils comme les systèmes de détection des intrusions dans les réseaux, les trousses de détection de programmes malveillants furtifs, les analyseurs de réseaux et les programmes spécialisés anti-robots peuvent offrir une protection plus sophistiquée contre les réseaux zombies.

Détection de la falsification de requêtes intersites (attaques CSRF)

- Mettez en place des jetons CSRF pour prévenir les attaques automatisées simples.
- Assurez-vous que toutes les pages du *site* sont dotées d'un protocole HTTPS et protégées par un jeton CSRF.