Politiques Sécuritaires

Niveaux de sécurité

Visa a créé de multiples niveaux de systèmes et de programmes de détection et de prévention de la fraude. Il s'agit d'une façon de plus pour Visa de vous protéger.

1. Responsabilité zéro

Lorsque vous utilisez votre carte Lidar Visa pour faire des achats à n'importe quel endroit, vous êtes protégé contre l'utilisation non autorisée de votre carte ou des renseignements sur votre compte. Grâce à la politique Responsabilité zéro de Visa[1], votre responsabilité pour les transactions non autorisées[2] sur votre compte s'élève à 0 FCFA : vous ne payez rien.

[1] La politique Responsabilité zéro de Visa protège les cartes émises au Canada et ne s'applique pas aux transactions anonymes effectuées avec les cartes Visa prépayées*, Visa Approvisionnement, Visa Entreprise et Visa Commerciale ou à toute autre transaction non traitée par Visa. En cas d'utilisation non autorisée, les titulaires de carte Visa doivent en aviser immédiatement leur institution financière. Pour connaître les restrictions ou les limites particulières, ou pour obtenir tout autre détail, veuillez vous reporter à la documentation de l'institution qui vous a émis la carte.

* Une carte Visa prépayée sera considérée comme étant anonyme, si l'identité du titulaire de carte n'a pas été validée par l'institution financière émettrice de la carte (par exemple, une carte prépayée Visa Cadeau).

[2] Les institutions financières peuvent exclure de la politique Responsabilité zéro une transaction effectuée par une personne autorisée à effectuer des transactions sur le compte ou une transaction effectuée par un titulaire de carte qui dépasse l'autorisation accordée par le titulaire de compte.

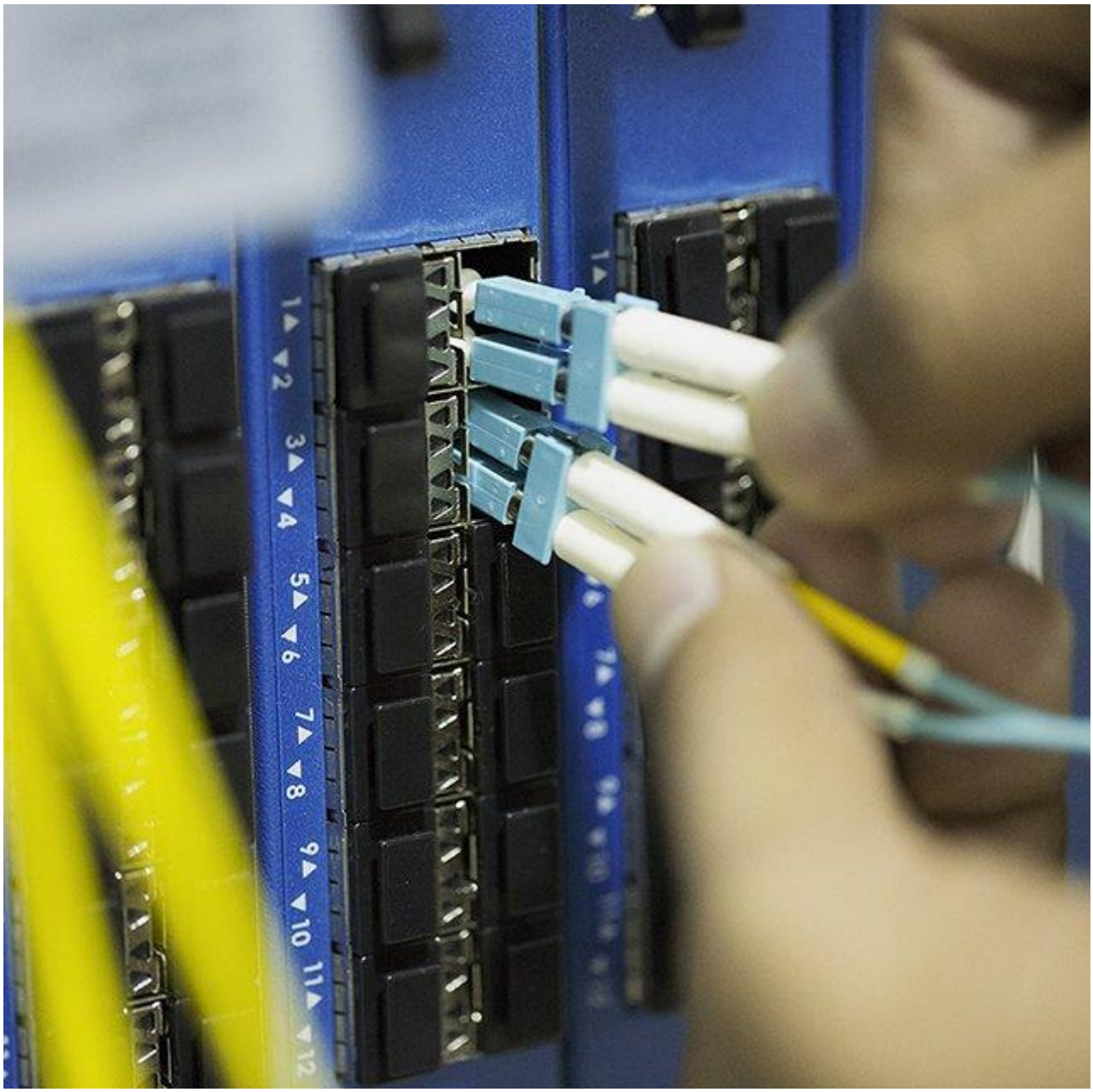
2. Vérifié par Visa

Vérifié par Visa est une solution mondiale conçue pour rendre les achats en ligne plus sécurisés, qui permet de s'assurer que les paiements sont effectués par le titulaire légitime d'un compte Visa. L'un des objectifs de Vérifié par Visa est de continuer à renforcer la confiance que consommateurs accordent au magasinage en ligne, de sorte que cette confiance soit semblable à celle accordée à un environnement physique.

Vérifié par Visa travaille souvent en coulisses lorsque vous magasinez en ligne. Votre banque vous demandera parfois de fournir des renseignements supplémentaires pour confirmer l'achat. Ce processus contribue à assurer que vous êtes la seule personne à utiliser votre carte en ligne.

Visa offre une protection exhaustive contre la fraude, mais Vérifié par Visa va encore plus loin en ajoutant un niveau de sécurité supplémentaire lorsque vous saisissez les renseignements de votre carte de crédit en ligne.

En saviour plus



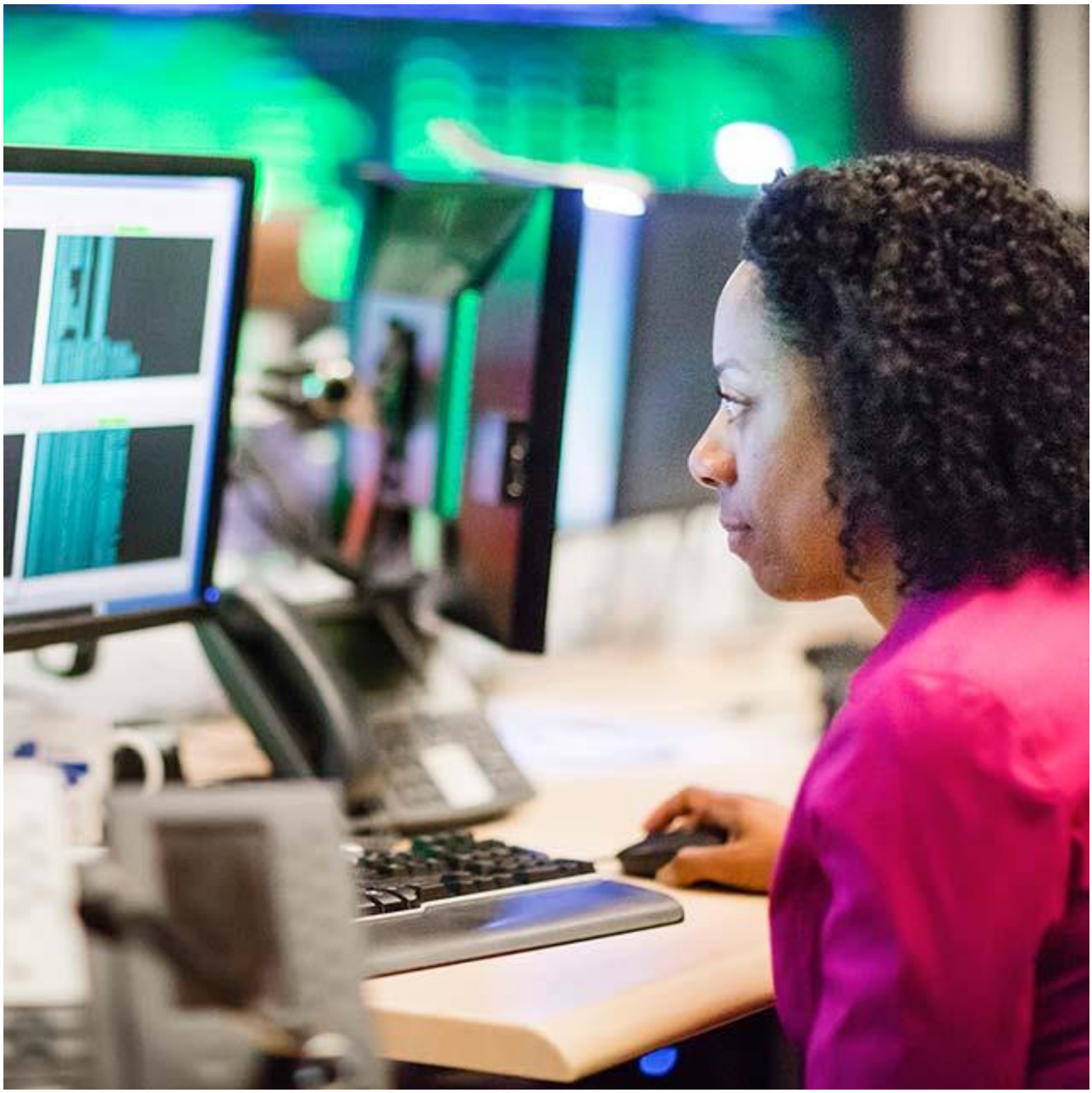
3. Réseaux neuronaux

Les réseaux neuronaux surveillent les transactions par carte Visa 24 heures sur 24, 7 jours sur 7, afin de repérer toute situation d'achat inhabituelle, par exemple, lorsque votre carte est utilisée simultanément pour effectuer un achat à Abidjan et à Dubaï. Si une transaction douteuse comme celle-là se produit, l'institution financière émettrice de votre carte Lidar communiquera avec vous. Ajoutez ce niveau aux autres niveaux de sécurité de Visa, et il s'agit d'une façon de plus pour Visa de vous protéger.

4. Sécurité de la puce EMV

Les cartes Lidar emploient la technologie de la puce EMV pour rendre plus sécuritaires les paiements. Les cartes à puce sont presque impossibles à contrefaire. Elles sont utilisées actuellement dans plus de 130 pays, facilitant ainsi davantage vos déplacements avec la carte Visa.

La technologie de la carte à puce n’est qu’un autre des nombreux niveaux de sécurité déjà offerts par Visa à ses titulaires de carte et à ses marchands.



5. Vérification d’adresse

Grâce au Service de vérification d’adresse, lorsque vous utilisez votre carte Lidar pour effectuer un achat en ligne, par la poste ou par téléphone, le marchand peut demander à l’institution financière qui traite les transactions de vérifier votre adresse. Cette vérification permet de fermer un autre accès à la fraude par carte de crédit. Ajoutez ce niveau aux autres niveaux de sécurité de Visa, et il s’agit d’une façon de plus pour Lidar de vous protéger.

6. Code de trois chiffres

Le code de trois chiffres, ou CVV, est utilisé par les marchands qui acceptent les cartes Visa afin d'assurer que l'acheteur est en possession d'une carte véritable. Ainsi, lorsque vous passez une commande par téléphone ou en ligne, c'est presque comme si vous étiez présent. Ajoutez ce niveau aux autres niveaux de sécurité de Visa, et il s'agit d'une façon de plus pour Lidar de vous protéger.

Politique Responsabilité zéro

Utilisez votre carte Lidar pour faire des achats partout, que ce soit sur Internet ou dans un magasin, et vous êtes protégé contre les transactions non autorisées effectuées avec votre carte Lidar. La politique Responsabilité zéro de Visa élimine la responsabilité du consommateur en cas de transactions frauduleuses.

Aucune responsabilité pour le consommateur en cas de transaction frauduleuse

La politique Responsabilité zéro de Lidar vous offre une protection contre la fraude**. Si quelqu'un vole votre numéro de carte Lidar, vous ne paierez rien pour les activités frauduleuses portées à votre compte. Cette politique s'applique à n'importe quel article acheté à l'aide de votre carte ou de votre numéro de carte Lidar, y compris les achats effectués sur Internet.

** Les titulaires de carte Lidar doivent établir qu'ils ne sont pas responsables de la transaction, conformément à toutes les ententes pertinentes de l'institution financière émettrice. Ne s'applique pas aux transactions effectuées à un GAB ou aux transactions avec NIP non traitées par Lidar. Les montants de crédit provisoire individuels peuvent être retenus, retardés, limités ou annulés par un émetteur en fonction de facteurs comme la négligence grave ou la fraude, le retard à signaler une utilisation non autorisée de la carte, l'enquête et la vérification d'une réclamation et l'état et l'historique du compte.

Si vous remarquez une activité frauduleuse effectuée avec votre carte, communiquez rapidement avec votre institution financière pour la signaler. Il est important de surveiller continuellement vos relevés mensuels afin de repérer toute transaction non autorisée. Votre contrat de titulaire de carte vous donne la définition d'une transaction non autorisée.

La Fraude par Hameçonnage

Les Canadiens sont confrontés à un nombre croissant d'arnaques téléphoniques par hameçonnage, où les fraudeurs prétendent appartenir à une organisation légitime (institution financière, entreprise, agence gouvernementale, etc.) afin d'essayer de leurrer les Canadiens à partager des renseignements personnels tels que leurs numéros de compte bancaire, mots de passe, numéros de carte de crédit voire même leurs numéro de sécurité sociale.

Fonctionnement

Les fraudeurs peuvent utiliser un message enregistré, un courriel et même parfois une vraie personne pour vous dire que votre carte a été la cible d'une tentative de fraude. Ils peuvent vous demander de vérifier votre identité à l'aide d'un numéro de carte de crédit, d'une date d'expiration, d'un numéro d'identification personnel (NIP) ou d'autres renseignements. Ces appels peuvent sembler légitimes, mais il faut demeurer prudent : les fraudeurs peuvent facilement tromper votre système d'identification de l'appelant en affichant un numéro qui semble provenir d'une entreprise crédible.

Ne mordez pas à l'hameçon

Lidar rappelle aux porteurs de carte, de ne pas partager leurs renseignements personnels par téléphone, sms ou courriel. Votre institution financière possède déjà ces renseignements, qui ont été obtenus à l'ouverture de votre compte.

Conseils pour éviter d'en être victime

Voici quelques conseils supplémentaires pour aider les porteurs de carte à se protéger eux-mêmes et à protéger leurs finances personnelles :

- Lidar et les institutions financières n’appelleront jamais ou n’enverront jamais de courriel aux porteurs de carte pour demander des renseignements personnels sur le compte
- Ne fournissez jamais de renseignements sauf si vous avez vous-même initier la communication
- Ne vous sentez pas obligé(e) de fournir votre numéro de carte par téléphone
- Demandez des détails : si l’appelant est incapable de vous répondre, l’appel n’est probablement pas légitime
- Plutôt que de demander un numéro de rappel, faites votre propre recherche sur l’appelant afin d’obtenir son numéro de téléphone légitime
- Signalez les appels, sms ou courriels suspects en appelant le numéro au dos de votre carte

Pour en savoir plus, cliquez ici. (ça renvoi à une page PDF sur l’hameçconnage)