Astuces simples pour vous protéger de la fraude

Signez votre carte dès sa réception

Signez le dos de votre carte de crédit ou de débit quand vous la recevez. Cela vous aidera déterminer si la carte que vous rendent les commerçants est bien la même que celle que vous leur avez donnée. En effet, la duplication de carte est une méthode classique d'usurpation d'identité.

Jouez aux jeux en ligne avec prudence

Ne donnez pas d'informations cruciales concernant votre identité sur un coup de tête, même si des jeux vidéo vous y incitent.

Mettez votre adresse postale à jour

Si vous déménagez, contactez vos institutions financières, les autorités fiscales et vos agences d'évaluation de crédit et tenez-les au courant des informations concernant votre localisation actuelle. Les fraudeurs utilisent des données personnelles périmées pour accéder à vos comptes.

Shopping en ligne

Faites toujours affaire avec des marchands fiables quand vous magasinez en ligne et assurez-vous que votre achat est sécurisé grâce au cryptage, qui protège efficacement vos informations bancaires. Pour vous assurer qu'une transaction est sécurisée, assurez-vous que l'adresse du site web débute par <https://>.

Utilisez la fonction « bloquer »

Si vous soupçonnez qu'un expéditeur mal intentionné tente de vous rejoindre par courriel, n'hésitez pas à le bloquer ou à l'ajouter à votre liste de courrier indésirable.

Ne partagez pas vos informations bancaires

Ne partagez jamais vos informations bancaires avec qui que ce soit. Votre banque ne vous demandera jamais votre numéro de compte, votre NIP ou votre mot de passe par courriel.

Investissez dans un bon antivirus

Utilisez un bon antivirus et un outil contre les logiciels malveillants pour protéger votre ordinateur, vos téléphones et vos tablettes. Assurez-vous de télécharger les mises à jour de ces logiciels régulièrement.

Évitez les ordinateurs publics pour vos transactions bancaires

Évitez d'accéder à vos comptes bancaires à partir d'un ordinateur public ou d'entreprise. Si vous ne pouvez pas l'éviter, assurez-vous de le faire dans des sessions privées et déconnectez-vous dès que vous avez terminé.

Apprenez de vos erreurs

Si vous avez déjà été escroqué en ligne, partagez votre expérience avec les membres de votre famille, particulièrement les jeunes et les personnes âgées, qui sont plus susceptibles d'être dupés.

Vérifiez votre rapport de solvabilité

C'est une bonne idée de vérifier sa solvabilité de temps à autre afin de vous assurer que personne ne commet de fraude en votre nom, en faisant une demande de prêt, par exemple. Ces activités n'apparaissent pas dans vos rapports mensuels.

Chéquier

Sauf exception, ne traînez pas votre chéquier partout où vous allez. Gardez-le plutôt en lieu sûr.

Variez vos mots de passe

N'utilisez pas le même mot de passe pour vos différents comptes en ligne. Il est préférable d'avoir des mots de passe distincts pour vos courriels, vos comptes bancaires et vos comptes sur les réseaux sociaux. Ne vous servez pas de votre date de naissance ou de votre adresse comme mots de passe. Des données aussi évidentes sont faciles à décoder. Utilisez des gestionnaires comme LastPass, qui enregistrent vos mots de passe de manière sécurisée.

NIP de carte bancaire

Mémorez votre NIP et ne l'écrivez jamais nulle part, surtout pas sur votre carte.

Soyez prudent quand vous stockez vos données en ligne

Bien que stocker de l'information en ligne sur un serveur partagé puisse sauver de la précieuse mémoire sur votre ordinateur, n'utilisez jamais ces outils pour stocker vos informations financières, vos informations bancaires, vos mots de passe ou vos photos personnelles. Vous ne voulez surtout pas que tout ça se retrouve entre de mauvaises mains.

Gérez vos cartes de crédit

Si vous avez cessé d'utiliser certaines de vos cartes de crédit, appelez votre banque et annulez-les. Aussi, si vous recevez une carte de remplacement, détruisez l'ancienne immédiatement.

Attention aux points d'accès sans fil publics

Soyez prudent quand vous utilisez des points d'accès sans fil à Internet; regardez attentivement les noms des connexions sans fil car les escrocs imitent parfois des noms fiables en espérant que vous les utiliserez sans vous méfier.

Téléchargez vos applications d'une source fiable

Assurez-vous de toujours télécharger les applications bancaires à partir d'une source sûre car elles nécessitent l'entrée de beaucoup de données confidentielles.

Supprimez après la lecture

Prenez l'habitude de supprimer les messages liés à votre compte en banque après les avoir lus car ils contiennent de l'information confidentielle à propos de vos finances.

Gardez votre numéro d'assurance sociale pour vous

À moins que ce soit absolument nécessaire, ne donnez pas votre numéro d'assurance sociale.

Protégez votre téléphone avec un mot de passe

Utilisez un mot de passe pour votre téléphone ou votre tablette afin que personne ne puisse y accéder sans votre permission. Par ailleurs, ne gardez pas vos informations bancaires sur votre téléphone cellulaire.

Ne faites pas trop facilement confiance

Ne partagez pas vos informations bancaires ou de carte de crédit avec des vendeurs au téléphone.

Ignorez les liens et les pièces jointes inconnues

Soyez à l'affût des liens douteux qui promettent de vous rendre riche sans effort, qui révèlent de l'information confidentielle ou de nature pornographique et n'ouvrez jamais les pièces jointes louches. Ils pourraient infecter votre ordinateur avec des logiciels malveillants.

Examinez vos relevés mensuels de près

Les courriels de relevés de transactions bancaires et de cartes de crédit vont souvent directement dans la corbeille, mais il est avisé de les parcourir afin de vérifier si vous avez bel et bien effectué

les transactions qui y figurent. Si vous remarquez quoi que ce soit de suspect, informez immédiatement votre banque.

Évitez de révéler des renseignements personnels sur les réseaux sociaux

Évitez d'ajouter de l'information superflue sur les réseaux sociaux, comme le nom de fille de votre mère, vos numéros de téléphone ou le nom de votre animal de compagnie. Des pirates informatiques pourraient les utiliser pour accéder à vos autres comptes.

Les codes à barres 2D peuvent aussi être frauduleux

Traitez les codes 2D comme les liens suspects : ils constituent une méthode graphique pour vous diriger vers un site web.

Traitez les reçus avec respect

Vos reçus de transaction en révèlent peut-être plus que vous ne le croyez. Gardez-les en lieu sûr ou disposez-en de manière sécuritaire.

Connaissez votre cycle de facturation

Soyez toujours au courant de vos cycles de facturation et de relevés et connaissez la date de votre prochain paiement. Rester à jour vous permettra de repérer les transactions suspectes plus rapidement.

Conservez une copie de toutes vos cartes et documents

Gardez toujours des photocopies de vos documents financiers et de vos cartes en lieu sûr, au cas où les originaux seraient perdus ou volés. Vous pourrez les utiliser en attendant que ces derniers soient remplacés.

Dites oui aux factures électroniques

Adhérez à la facturation électronique. Cela vous évitera des ennuis avec les copies papier, qui pourraient tomber entre de mauvaises mains.

Ne sauvegardez pas les informations de vos cartes de crédit sur les sites de magasinage

C'est peut-être désagréable de devoir entrer vos informations de cartes de crédit chaque fois que vous magasinez en ligne, mais c'est le prix à payer pour éviter que votre carte soit utilisée de manière frauduleuse.

Signalez rapidement

Le vol ou la perte de cartes de crédit ou de tout autre document important ne doit pas être pris à la légère. N'attendez pas et informez les autorités concernées immédiatement.

<https://www.msn.com/fr-be/finance/financenewsitaly/31-astuces-simples-pour-vous-protoc3%a9ger-de-la-fraude/ss-BBLtmtw?li=BBqiJuZ&ocid=mailsignout>

Des offres frauduleuses de crédit circulent sur internet: une fois les "frais" payés, le "prêteur" disparaît

L'Autorité des services et marchés financiers (FSMA) a reçu plusieurs messages de la part de consommateurs à propos d'offres frauduleuses de crédit circulant sur internet. Elle met en garde plus spécifiquement contre les activités des sociétés irrégulièrement actives intitulées "Dell Loan Company", "Laporte Holding" et "Snel Krediet".

Ces entreprises non agréées demandent aux consommateurs souhaitant donner suite à ces propositions de verser certains montants destinés à couvrir de prétendus frais liés au crédit (frais de dossiers ou administratifs, assurances, etc.). Une fois ces "frais" payés, le "prêteur" disparaît dans la nature et il est quasiment impossible de récupérer les sommes versées, souligne l'autorité. La FSMA déconseille absolument de donner suite à des propositions de crédit d'un tel genre. Elle recommande notamment de se méfier lorsqu'un crédit est proposé par internet ou au travers des médias sociaux sans qu'une demande ait été faite au préalable. Elle conseille également de vérifier les adresses électroniques utilisées, gageant celles qui utilisent une adresse électronique professionnelle et non celles se terminant par @hotmail.com, @gmail.com et @outlook.com. Elle appelle également à douter des propositions de crédit à des conditions particulièrement avantageuses. Enfin, la FSMA demande aux citoyens à l'avertir de toute société suspecte qui n'aurait pas déjà fait l'objet d'une mise en garde.

<https://www.msn.com/fr-be/actualite/national/des-offres-frauduleuses-de-cr%C3%A9dit-circulent-sur-internet-une-fois-les-frais-pay%C3%A9s-le-pr%C3%A9teur-dispara%C3%Aet/ar-AAIhW7I?li=BBqiQ9T&ocid=mailsignout>