Fraude à la carte bancaire : comment vous protéger !

En règle générale, les achats sur Internet sont sûrs. Les émetteurs de cartes et les banques investissent massivement dans la sécurité. Malgré cela, les cyber-escrocs parviennent à leurs fins. La dernière arnaque en date concerne les systèmes de paiement mobile. Marcel Drescher, Responsable du services des fraudes à l'UBS Card Center, nous parle de la fraude au portefeuille numérique (digital wallet) et nous dit comment s'en prémunir.

Qu'est-ce qu'un système de paiement numérique ?

Il s'agit d'informations de paiement qui, au lieu d'être enregistrées sur une carte en plastique, sont stockées sur un support numérique. Ce support peut prendre la forme d'un porte-monnaie numérique, appelé « wallet », présent sur les smartphones ou sur les montres intelligentes. Ces appareils servent ainsi à effectuer des achats, comme une carte de crédit ou de débit classique.

Quels sont les principaux types de fraude rencontrés dans les achats en ligne ?

Souvent, les données personnelles d'une carte que vous avez utilisée pour effectuer un paiement auprès d'un commerçant sont volées suite à une fuite de données et utilisées à des fins abusives.

Autre type courant d'escroquerie : l'obtention frauduleuse des données personnelles de votre carte et de vos codes d'accès par l'envoi d'e-mails d'hameçonnage. Dans ces e-mails, les malfaiteurs vous font croire, par exemple, qu'il reste encore une petite somme à payer pour la livraison d'un colis. Ils vous demandent d'effectuer ce paiement via un lien envoyé dans l'e-mail. Mais ce lien mène à une page web falsifiée. Si vous y saisissez les données personnelles de votre carte et que vous révélez également le code d'accès que vous avez reçu séparément par SMS ou par notification, les escrocs peuvent disposer librement de votre argent.

Ils obtiennent souvent les informations nécessaires par l'envoi d'un e-mail d'hameçonnage.

Qu'est-ce qu'une fraude au portefeuille numérique (digital wallet) ?

Dans ce type d'arnaque, les cyber-escrocs tentent d'enregistrer abusivement les données d'une tierce personne dans leur propre application, afin de pouvoir ensuite effectuer des paiements abusifs dans un magasin, un restaurant ou sur Internet avec leur appareil.

Comment les cyber-escrocs procèdent-ils pour ce type d'arnaque ?

Ils obtiennent souvent les informations nécessaires par l'envoi d'un e-mail d'hameçonnage. Les victimes fournissent leurs données personnelles, pensant répondre à une demande de paiement légitime. Elles transmettent également le code de confirmation, envoyé séparément par SMS, pour valider l'enregistrement dans leur portefeuille. Pour ce faire, il suffit de saisir le code sur le site web falsifié. Grâce à ces informations, les escrocs disposent alors de toutes les données nécessaires à l'authentification des transactions.

Où puis-je m'informer sur les e-mails d'hameçonnage et comment les reconnaître ?

Pour de plus amples informations, vous pouvez consulter les sites www.card-security.ch, www.cybercrimepolice.ch ou ceux de votre banque ou de l'émetteur de votre carte.

Que dois-je faire si j'ai transmis les données de ma carte et mes codes d'accès ?

Faites immédiatement bloquer votre carte et signalez que vous avez transmis vos données personnelles ou vos codes d'accès. Vous pouvez également effectuer le blocage directement et rapidement via les services web de l'émetteur de cartes. Une fois votre carte bloquée, elle est protégée contre toute utilisation abusive. Les transactions frauduleuses effectuées avant son blocage ne peuvent malheureusement plus être annulées.

Comment puis-je me protéger des attaques contre mes cartes de débit et de crédit ?

Pour vous garantir la meilleure protection, lisez entièrement et attentivement les messages que vous recevez par SMS ou par notification. Lorsque vous effectuez un paiement, même pour une somme modique, et que vous recevez par SMS un code de validation destiné à confirmer l'enregistrement de votre carte de crédit dans votre solution de paiement numérique, ne divulguez ce code en aucun cas.

En outre, il est vivement conseillé d'activer un service de notification dès qu'une transaction est effectuée par carte. Cela vous permet de garder le contrôle sur vos paiements et d'éviter les transactions abusives multiples en un laps de temps très court. Si vous recevez une notification relative à une transaction inconnue, faites immédiatement bloquer votre carte et contactez l'émetteur de la carte.

Contactez également l'émetteur de la carte en cas de doutes lors d'une demande de paiement. Il pourra vous aider et vous évitera peut-être l'utilisation abusive de vos données.

Suis-je responsable des dommages financiers liés à une fraude à la carte ?

Tout dépend du devoir de diligence exercé : si le client a respecté ses obligations conformément aux conditions générales, il sera indemnisé pour le préjudice subi. C'est par exemple le cas si les données personnelles ont été dérobées suite à une fuite de données.

En revanche, le client ne perçoit aucun dédommagement s'il transmet les données de sa carte via le lien contenu dans un e-mail d'hameçonnage. Le client doit supporter les dommages subis jusqu'au blocage de sa carte par lui-même ou par l'établissement émetteur. C'est pourquoi il est important, avant de transmettre tout code de validation, de vérifier à quelles fins ce code est émis. Faites bien attention à ce que vous validez, vérifiez le montant et le site marchand.

Marcel Drescher, Responsable du services des fraudes à l'UBS Card Center.

Marcel Drescher et son équipe se consacrent aux fraudes liées aux cartes de crédit et de débit pour la banque UBS et pour d'autres émetteurs de cartes suisses.