Les principales fraudes et arnaques des moyens de paiement

Carte bancaire, prélèvement, chèques, paiements en ligne, etc., tous ces supports de paiement vous exposent à la convoitise de nombreux escrocs.

Ces derniers développent tous les moyens (vol, arnaque, falsification, etc.) pour vous subtiliser un maximum de vos disponibilités financières.

Parfois il ne s'agit pas de vous voler vos supports de paiement mais de se procurer vos coordonnées bancaires voire simplement votre nom, prénom et adresse.

UNE MENACE AU QUOTIDIEN

Les fraudes relatives aux moyens de paiement sont en constante progression. En 2012, les fraudes concernant les attaques de distributeur automatique de billets ont progressé de 73% et les fraudes sur les points de vente ont augmentés de 250%.

En France, 61% des opérations frauduleuses sont sur internet alors que les transactions sur internet ne représentent que 9,2% des transactions.

Il existe une multitude de moyens de subtiliser vos outils de paiement voire votre bien. Il est donc important de les connaitre pour éviter de se les faire subtiliser.

VOL DE VOTRE CARTE BANCAIRE

Le saint Graal de tout fraudeur qui use des techniques les plus farfelues et les plus poussées pour se procurer toutes les informations relatives à votre carte bancaire

Piéger le distributeur automatique de paiement :

Le fraudeur installe un faux clavier sur le clavier du distributeur automatique de billet ou installe une fausse caméra de surveillance. Il récupère ainsi votre code secret que vous aurez tapé. Il lui suffit plus qu'à vous subtiliser votre carte bancaire. Souvent par la manière forte.

Certains vont encore plus loin en captant les informations directement sur votre carte bancaire en piégeant à la fois le clavier mais également le support de réception de votre carte bancaire du distributeur automatique de paiement ainsi il scanne votre carte bancaire à distance sans avoir besoin de vous voler votre carte bancaire.

L'œil qui louche

Lors de vos paiements chez des commerçants, dans une entreprise de restauration rapide par exemple, vous devez effectuer votre code secret en public. C'est à ce moment précis que l'œil « attentif » d'un fraudeur tente d'observer discrètement votre code. Il lui suffira par la suite de subtiliser votre carte.

Détournement du terminal de paiement chez le commerçant.

Certains fraudeurs poussent l'art du vol directement sur le lieu de vente. Cela fut le cas dans le sud de la France et plus particulièrement à Béziers où des terminaux de paiement chez des commerçants ont été discrètement échangés par des terminaux piégés.

Les fraudeurs récupéraient à distance toutes les informations relatives à votre carte bancaire y compris le code secret.

C'est près d'une dizaine de millions d'euros qui ont été détournés ainsi.

Complicité du commerçant

Certains fraudeurs arrivent à convaincre des commerçants de participer à leurs arnaques. Après avoir subtilisées les coordonnées d'une carte bancaire, les fraudeurs se rendent chez le commerçant-collaborateur pour effectuer des paiements nécessitant qu'une simple signature.

Détournement du courrier postal

Souvent les banques, particulièrement les banques en ligne, envoient votre carte bancaire par courrier postal. Il n'en suffit pas plus pour un fraudeur pour récupérer sans trop d'effort votre carte bancaire. Pour se faire, il intègrera les services postaux pour récupérer votre courrier ou bien il disposera d'un moyen pour accéder à votre courrier dans votre boite aux lettres.

Les distributeurs de courriers, de magazines et autres annuaires disposent d'une clé ouvrant le panneau des boites aux lettres. Une personne mal intentionnée peut ainsi accéder à votre courrier et parfois il aura la surprise d'y trouver vos clés de domicile qui lui permettront de rechercher tranquillement chez vous tous vos moyens de paiement sans que vous vous en rendiez compte.

VOL DE CHEQUE

Les chèques bancaires sont également un moyen de paiement que cherche à se procurer le fraudeur. En effet, votre chéquier présente votre nom, prénom et vos coordonnées. Il suffit alors de fabriquer

une fausse carte d'identité reprenant ces informations pour ensuite l'utiliser à volonté.

Vol de votre chéquier

Le principal canal d'action pour récupérer votre chéquier reste bien entendu le vol. Le fraudeur tentera de récupérer celui-ci dans votre bagage (sac à main, sacoche d'ordinateur), dans votre vêtement (veste, manteau) ou dans votre véhicule de transport.

Mais certains fraudeurs n'ont pas froid aux yeux et peuvent aller jusqu'à la source pour récupérer votre chéquier. En témoigne l'exemple de ce fraudeur qui subtilisa à un client de la BNP Paribas du 13ème arrondissement de Paris, son courrier de convocation pour la récupération de son chéquier. Le voleur s'est présenté à l'agence avec une carte d'identité présentant toutes les coordonnées du client mais avec une photo différente. Il a fallu toute la vigilance de la conseillère d'agence qui connaissait particulièrement bien son client pour éviter que ce dernier devienne la victime d'une fraude bancaire.

Faux chèque bancaire

Certains fraudeurs sortent tout droit du film « Attrape moi si tu peux » et sont capables de recréer des chéquiers à l'image d'une banque.

L'arnaque au faux chèque repose sur trois acteurs, l'expéditeur du chèque, le destinataire du chèque et la banque.

Dans le cadre d'une transaction, l'expéditeur (ou acheteur) fait parvenir un chèque avec une somme supérieure au montant de la transaction négociée. Il prétexte une erreur et demande à ce que le destinataire (le vendeur) lui retourne la différence moins les frais liés au dérangement dès que celui-ci aura déposé le dit chèque.

Une fois déposé, la banque du vendeur crédite la somme sur son compte. Rassuré le vendeur accepte alors de renvoyer l'excédent à son acheteur.

Ce dernier demande alors de passer exclusivement par des organismes tels que Western Union afin de récupérer au plus vite la différence.

Et ce n'est que quelques jours plus tard que votre banque vous informe que le chèque est faux.

Faux chèque de banque

Lors d'une transaction vous demandez un chèque de banque qui est pour vous une garantie. Une fois la transaction réalisée, vous déposez votre chèque de banque dans votre banque et découvrez que celui-ci est faux.

VOL DES INFORMATIONS BANCAIRES

Le vol de vos données est la principale activité des fraudeurs. Les fraudeurs s'ingénient à développer toutes les techniques possibles pour les récupérer.

En voici quelques unes :

Piratage informatique de votre ordinateur

Le classique du classique : Vous téléchargez un fichier qui contient un virus ou un cheval de Troie qui infecte votre ordinateur de manière soit à prendre le contrôle de celui-ci pour y récupérer des informations bancaires ; soit à vous observer en espérant que vous

effectuerez un paiement en ligne afin d'enregistrer le plus simplement du monde les informations de la carte bancaire que vous taperez sur votre clavier.

Piratage d'un commerçant : Le commerçant se fait pirater son serveur. Et vos coordonnées bancaires se retrouvent entre les mains du pirate.

Email frauduleux

Vous recevez un email vous invitant à mettre à jour vos informations chez un de vos fournisseurs (EDF, Opérateurs téléphoniques, Banque, etc.) voire même des services des impôts.

Vous vous retrouvez sur une page quasi similaire à celle de votre fournisseur ou service des impôts dans lequel vous êtes invité à remplir vos coordonnées et vos informations bancaires.

Toutes ces informations sont récupérées en règle générale à l'étranger par un pirate informatique qui les utilise immédiatement pour réaliser des achats voire des virements bancaires .

Récupération via Wifi, NFC

Le développement des technologies permettant l'accès à distance favorisent la tentation des fraudeurs d'accéder à vos données.

Vos appareils de communication sont vulnérables à des attaques de pirates extrêmement bien équipés pour tenter de récupérer vos données lorsque vos appareils sont branchés en mode Wifi ou NFC.

Le développement du paiement mobile NFC qui permet de réaliser un paiement avec sa carte de paiement ou son téléphone portable équipée sans avoir à taper son code est une véritable aubaine pour

les fraudeurs. Ces derniers n'ont plus besoin de vous subtiliser votre code secret ou de vous voler votre carte bancaire. Il leur suffit de développer les bons outils pour tenter de récupérer les informations de votre carte bancaire ou de votre mobile, puis de les dupliquer sur un support.

Arnaque sur Paypal

Paypal est un moyen de paiement prisé par toutes celles et tous ceux qui ne souhaitent pas communiquer leurs informations bancaires sur des sites de vente.

Le compte paypal étant limité par un montant défini, il est impossible pour un fraudeur ayant accès à ce compte de se servir sans limite.

Toutefois, les arnaques utilisant le service de paiement paypal sont nombreuses. Principalement sur les sites de vente de particulier à particulier.

Sur ces sites, l'escroc se porte rapidement acquéreur d'un objet en vente. Il propose l'envoi de la somme via paypal. Le vendeur reçoit une confirmation du transfert par email. Cet email peut être à la fois un vrai courrier provenant de paypal ou un faux courrier provenant de l'escroc.

Rassuré, le vendeur envoie alors l'objet à une adresse souvent un point relais ou à l'étranger.

Après l'envoi, le vendeur se rend compte que son compte paypal n'est pas réellement crédité. Ou bien il reçoit un vrai courrier de Paypal quelques jours plus tard lui indiquant que le transfert est bloqué car basé sur 'un moyen de paiement douteux.

Entre-temps, le fraudeur disposera de votre bien qu'il pourra

revendre ou utiliser à loisir.

Comme nous avons pu le voir les techniques de détournement de vos disponibilités financières sont très nombreuses.

Prendre connaissance de ces techniques d’escroquerie via les moyens de paiement est indispensable pour pouvoir les éviter.