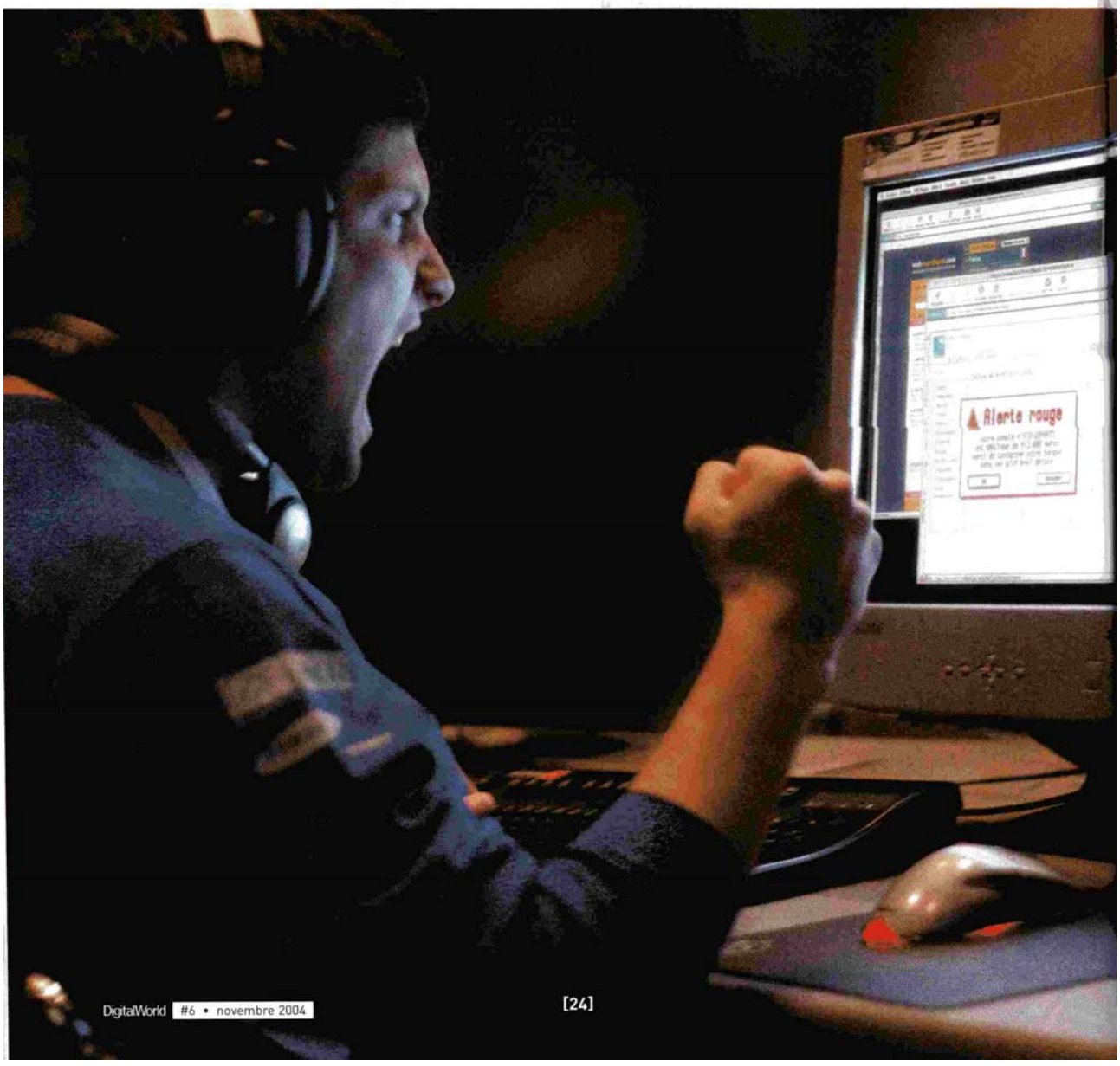
FAUT-IL EN ACHETER SUR



CORE LE WEB ?

Compte bancaire pillé, identité usurpée, transaction détournée, sites marchands clonés, les fraudes liées au commerce en ligne se multiplient. Les offres sont certes abondantes et séduisantes sur Internet, mais les achats ne sont pas sans risques.

Au début, Damien, 32 ans, pensait faire une affaire inespérée : un portable à 900 euros alors que dans une grande enseigne, il en vaut le double. Appâté par le gain – les Canadiens préfèrent le terme "hameçonner" –, notre acheteur poursuit la transaction et entame un contact direct avec le vendeur par e-mail, hors toute plate-forme d'échange de type e-bay, priceminister ou encore 2xmoinscher. On lui propose un paiement sécurisé avec Western Union (WU) et un envoi du colis *via* UPS, deux sociétés reconnues. *"Renseignements pris auprès de La Poste, qui délivre des mandats WU, un numéro MCTN sécurisait les transactions et était nécessaire pour le retrait d'argent par le destinataire"*, explique-t-il. Convaincu, il paie et reçoit un bordereau UPS qui lui permet de suivre en direct le déplacement de son colis, depuis les Etats-Unis jusqu'à son domicile. Problème, deux jours plus tard, le colis est toujours censé se trouver aux Etats-Unis et son argent, lui, s'est volatilisé.

Cette mésaventure est, à quelques détails près, celle que connaissent des dizaines d'autres internautes qui achètent ou vendent sur Internet. *"Il y a bien une recrudescence des fraudes mais elle n'est*

10 ASTUCES POUR COMMERCER SEREINEMENT

1. Ne pas répondre à un mail invitant à confirmer ou mettre à jour ses informations bancaires sur Internet, même si ce mail semble provenir de sa banque.
2. Taper l'URL d'un site directement dans le navigateur sans passer par un lien contenu dans un mail.
3. Vérifier lors de la saisie de données confidentielles que l'adresse de l'URL commence par https// au lieu de http://. Le site est alors sécurisé.
4. Désactiver la saisie semi-automatique de son mot de passe.
5. Privilégier les sites marchands qui fournissent un numéro de téléphone, un point de retrait physique et qui proposent d'autres moyens de paiement, comme le chèque ou le paiement à livraison.
6. Se méfier d'une offre trop alléchante... Elle a de fortes chances d'être douteuse.
7. Privilégier le paiement en contre-remboursement (cash and delivery).
8. Ne pas faire de commerce dans une langue méconnue.
9. Si la transaction passe par un tiers de confiance, choisir le tiers partenaire du site marchand ou vérifier son identité sur www.escrowfraud.com.
10. En cas de contact par mail direct avec le vendeur, remonter son adresse IP pour connaître son origine géographique réelle.

TROIS TECHNIQUES COURANTES DE PIRATAGE

Le phishing

Dérivé du mot fishing, qui signifie "pêche" en anglais, le phishing consiste à envoyer à un internaute un spam (un mail non sollicité) alarmiste qui l'incite à se rendre sur un site contrefait d'un marchand ou d'une institution bancaire. Le but pour le fraudeur est de convaincre l'internaute de mettre à jour ses données personnelles telles que mot de passe ou numéro de carte de crédit, pour usurper son identité, ou pire le piller.

Les alertes de sécurité

L'internaute reçoit un mail lui disant qu'en raison d'une alerte de sécurité, il doit activer un lien du mail qui le mène sur un faux site bancaire, où il est invité à saisir son nom et son code secret avant de changer ce code secret. De quoi aider le fraudeur à récolter des données essentielles pour pénétrer indûment le compte d'un client trop confiant.

Le cheval de Troie

Ce virus s'installe sur un ordinateur à l'insu de son utilisateur. Lorsque celui-ci fournit ses coordonnées bancaires à un site sécurisé pour réaliser un achat, le cheval de Troie les intercepte et les transmet au fraudeur. Le meilleur moyen pour s'en protéger consiste à installer un pare-feu (firewall) sur sa machine, plus efficace en la matière qu'un antivirus.

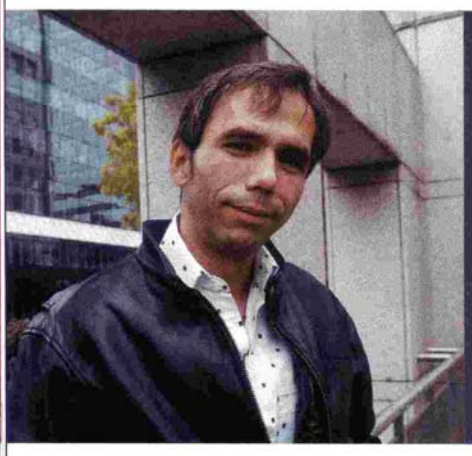
pas toujours d'un grand professionnalisme et grandit logiquement avec l'évolution du parc Internet", estime le commissaire principal Yves Crespin, en charge de la Brigade d'enquête sur les fraudes aux technologies de l'information (Befti). Et si la France restait jusque-là un peu en retrait en raison de la barrière de la langue et de la réticence des Français à commercer sur le Web, il semble que le pays soit de moins en moins épargné par le phénomène.

Pour soutirer une forte somme d'argent à un acheteur en échange d'un objet ou lui subtiliser ses données bancaires, toutes les techniques sont bonnes. Certaines sont plus inquiétantes que d'autres. *"Le phishing séduit beaucoup aujourd'hui"*, reconnaît Yves Crespin. Le "phisheur" clone un site bancaire ou marchand. Il envoie à ses futures victimes un e-mail à l'en-tête de la société, en leur demandant de mettre à jour leurs identifiants, login et mot de passe, donnant accès à leur compte. Une technique qui fait des ravages outre-Atlantique, et se développe aujourd'hui dans l'Hexagone. *"Il n'y a malheureusement pas grand-chose à faire contre. Sur 10 000 envois d'e-mails, il y aura toujours une partie pour répondre"*, se désole Yves Crespin, tout en insistant sur les signes, comme les fautes d'orthographe, qui permettent de différencier un site contrefait du site original. *"C'est un peu comme la contrefaçon d'un sac Vuitton : il y aura toujours un fil qui dépasse. Mais il y a plus dangereux et efficace que le phishing"*, prévient-il. Et cette autre menace a un nom : le cheval de Troie. Ce programme s'installe lors d'un spam ou d'un virus sur une machine à l'insu de son utilisateur. Dès que celui-ci se connecte à un site sécurisé et fournit ses données bancaires, le cheval de Troie les intercepte. Avec, pour but ultime, le pillage du compte bancaire de sa victime. *"Nous avons eu un cas de ce type"*, admet Jérôme Fourré, de la Société générale, tout en qualifiant le fait de marginal. Le phénomène, pourtant, prend de l'ampleur même s'il reste difficile à quantifier.

"L'arnaqué a un sentiment de honte", confie Damien Bierlaire, auteur d'un site (http://webarnaques.free.fr/) qui recense les dernières techniques de fraudes en vogue, et rares sont ceux qui portent plainte.

> **Le phishing, une technique à la mode**

La Befti estime ainsi que 90 % des affaires lui échappent. Face au phénomène, les sociétés s'organisent pour prévenir les internautes. Car en dehors du cheval de Troie, il est un fait établi : les fraudes réussissent souvent grâce à la naïveté, relative, de l'internaute. *"Les fraudeurs sont intelligents, ils sont capables de cloner un site et d'inciter assez finement les clients à leur faire confiance. Nous appelons cela le social engineering, c'est-à-dire arriver à ses fins en jouant sur le comportement des utilisateurs"*, précise Jérôme Fourré. La Société générale, comme la plupart des autres banques, consacre une rubrique sur son site Web aux techniques de fraudes et aux moyens de s'en prémunir. La Fédération bancaire



TEMOIGNAGE
"EN FRANCE, ON EST EXTREMEMENT PROTEGÉ"

Rodriguo a coutume d'acheter sans trop de crainte sur le Web. L'an dernier pourtant, il découvre avec surprise que sa Carte bleue a été utilisée frauduleusement sur le site Amazon, pour un montant avoisinant les 3 000 euros. *"Ma banque m'a conseillé de porter plainte pour escroquerie, ce que j'ai fait, et elle m'a intégralement remboursé alors que je n'ai souscrit à aucune assurance particulière. On est extrêmement protégé quand on fait de la vente par correspondance. Je n'ai jamais su comment on avait pu obtenir mon numéro de Carte bleue, mais je reste persuadé que je ne me le suis pas fait piraté sur le Web, mais intercepté dans la vie quotidienne. Depuis, j'ai changé de numéro et de carte, et je continue d'acheter régulièrement sur Internet. Je fais peut-être un peu plus attention mais guère plus"*, explique-t-il.

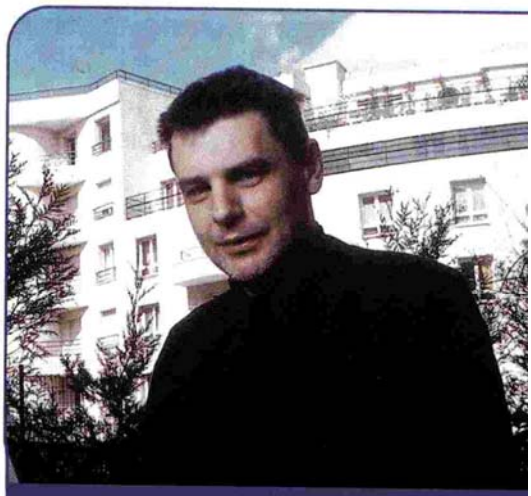
française a même édité un guide pratique téléchargeable sur son site www.lesclesdelabanque.com, indiquant quelques conseils techniques et règles de bon sens. Et de prévenir : *"Une banque n'émet jamais de courrier électronique invitant à se connecter à un site de banque à distance pour y déposer ses codes d'accès."* De nouveaux moyens de paiement ont aussi été imaginés pour sécuriser les échanges, comme l'e-Carte bleue : la banque fournit pour chaque achat sur Internet un numéro de carte utilisable une seule fois, pour une durée limitée et pour un montant prédéfini. La transaction conclue, le numéro devient inutilisable. De quoi, en théorie, protéger le client de toute malversation.

De leur côté, les sites marchands développent des outils pour "éduquer" leurs clients. Des espaces d'information distillent des conseils de prévention des fraudes. Car des éléments souvent simples permettent de confondre le pirate. Un mail alarmiste, mal orthographié et trop indiscret, a des chances d'être du phishing. Une incohérence entre le profil du vendeur et l'objet de la vente, un profil d'évaluation trop flatteur et récent, l'insistance du vendeur à conclure la transaction en direct hors du site ou encore son refus d'encaisser un paiement autre que de la monnaie liquide sont aussi douteux. E-bay, l'un des sites français les plus fréquentés par les fraudeurs, a même développé une barre outil qui repère grâce à son URL si l'utilisateur est ou non sur un site pirate : si tel est le cas, une icône rouge prévient aussitôt l'internaute. *"Nous développons des outils d'aide à la détection de comptes usurpés. Nous avons aussi un service chargé de déceler les comportements suspicieux et de repérer les faux sites pour les détruire"*, confie Esther Ohayon, responsable communication chez e-bay. D'autres techniques marchandes permettent aussi de rassurer le chaland. Sur Cdiscount, par exemple, on lui propose de laisser une partie de son numéro de carte bancaire sur Internet pour le compléter par téléphone auprès d'un opérateur virtuel.

Des outils pour "éduquer" les clients

Commercer en ligne n'a donc rien d'une sinécure. Mais que l'on se rassure : la loi est ainsi faite en France que l'internaute reste très protégé en situation de litige. Ainsi, en cas d'utilisation frauduleuse de son compte bancaire, la banque rembourse intégralement l'intéressé. Restent les échanges d'espèces. Car c'est bien à ce moment, qui clôt une transaction, que le fraudeur parvient véritablement à pêcher l'acheteur, aveuglé par sa cupidité. □

FRANCK KANTOR



TEMOIGNAGE
"IL M'A PRATIQUEMENT INSULTÉ"

Jean achète et vend régulièrement des jeux vidéo en ligne. *"Je cherchais à acheter un ordinateur sur e-bay et j'ai été appâté par une annonce attractive proposant un Mac à environ 400 euros. Il y avait pas mal de gens intéressés et j'ai engagé la discussion hors du site e-bay avec le vendeur qui disait être aux Etats-Unis. Quand on le questionnait sur le fait qu'il fallait envoyer l'argent en Roumanie, il répliquait qu'avec Western Union, la transaction était assurée. Quand on lui demandait pourquoi le prix était si bas, il expliquait un truc confus, comme quoi il travaillait dans une grande entreprise et que c'était du matériel de déstockage. Mais quand je lui ai posé des questions techniques, il n'a pas su répondre, simplement parce qu'il ne connaissait pas la machine. A la fin, je n'ai pas donné suite et il m'a pratiquement insulté. Cela m'a rendu plus méfiant, mais je continue d'acheter et de vendre comme auparavant."*

LES BONNES ADRESSES

www.bigpockets.co.uk

Ce site britannique est spécialisé dans les supports DVD et le déstockage de produits numériques. Les meilleurs prix pour les DVD-/+Rw.

www.cdiscount.fr

Spécialisé dans les opérations coup de poing, ce site, qui fait partie du groupe Casino, propose un choix restreint de produits à des prix imbattables. Attention, les quantités sont à chaque fois limitées.

www.rueducommerce.fr

Au fil des années, Rue du commerce a su bâtir une boutique virtuelle très bien fournie. Les mauvaises surprises sont rares. Les promos sont à suivre.

www.maismoinscher.com

Electroménager, téléphonie, informatique, mais aussi TV ou APN... Maismoinscher propose des produits aux meilleurs prix pour les internautes. Mais attention au délai de livraison et à la garantie uniquement assurée par le constructeur.