Rapport

Fraude financière et opérations bancaires en ligne : menaces et contre-mesures

François Paget, McAfee® Avert® Labs

Sommaire

La fraude financière revêt de multiples aspects. Qu'il s'agisse d'escroquerie, d'utilisation frauduleuse de cartes de débit ou de crédit, de fraude immobilière, de trafic de stupéfiants, d'usurpation d'identité, de publicités trompeuses ou de blanchiment d'argent, les cybercriminels n'ont qu'un seul but : gagner un maximum d'argent, rapidement et le plus discrètement possible.

Ce rapport se penche sur les multiples menaces auxquelles sont confrontés les banques et leurs clients. Les statistiques et les descriptions de solutions présentées ici devraient permettre aux lecteurs, qu'ils soient responsables de la sécurité d'une organisation financière ou simplement clients, de se faire une idée de la situation actuelle.

Quelques chiffres

Statistiques de la FTC (Commission fédérale américaine du commerce)

Aux Etats-Unis, de nombreux observateurs tentent depuis plusieurs années de prouver que la fraude financière entre dans une phase de stabilisation, voire de régression. La FTC, la Commission fédérale américaine du commerce, est un organisme chargé de la protection des consommateurs et de la régulation de la concurrence. Ses rapports annuels montrent effectivement une stabilisation du nombre de plaintes entre 2004 et 2006[1]. En 2007, toutefois, ces chiffres ont connu une légère augmentation[2]. Et à l'heure actuelle, les trois indicateurs de la FTC sont en hausse.

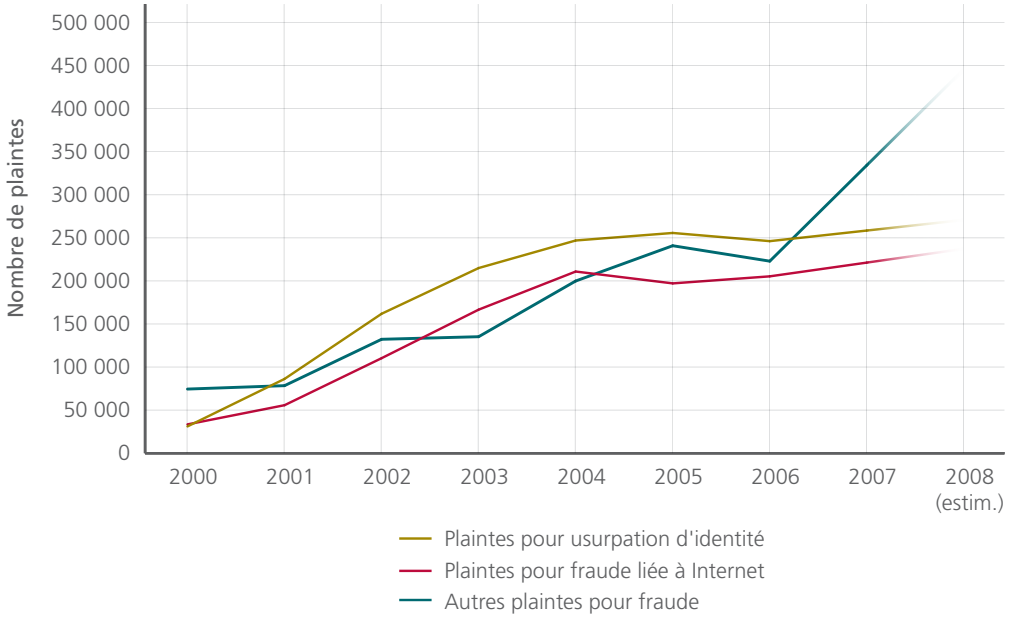


Figure 1 : Statistiques annuelles sur les plaintes des consommateurs de la Commission fédérale américaine du commerce. (Source : FTC)

En 2008, la FTC ne distinguait plus les plaintes déposées pour des fraudes liées à Internet du total[3]. La figure 2 illustre cette nouvelle répartition. Pour l'année 2008, seuls 58 % de toutes les plaintes pour fraude mentionnaient la méthode de contact initial. La messagerie électronique a été citée pour 52 % de ces plaintes et un site Web Internet, pour 11 % d'entre elles. Seuls 7 % des utilisateurs ayant participé aux statistiques ont signalé le téléphone comme point de contact initial.

1. « Consumer Fraud and Identity Theft Complaint Data » (Données sur les plaintes pour fraudes à la consommation et à l'usurpation d'identité) – Année 2004 : *http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2004.pdf*
   Année 2005 : *http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2005.pdf*
   Année 2006 : *http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2006.pdf*
2. Année 2007 : *http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2007.pdf*
3. « Consumer Fraud and Identity Theft Complaint Data » (Données sur les plaintes pour fraudes à la consommation et à l'usurpation d'identité) – Année 2008 : *http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf*

	Année 2006		Année 2007		Année 2008	
Méthode de contact	Plaintes	Pourcentages*	Plaintes	Pourcentages*	Plaintes	Pourcentages*
Internet — Messagerie électronique	138 195	45 %	152 131	50 %	193 817	52 %
Courrier postal	50 317	16 %	42 330	14 %	51 837	14 %
Internet — Sites web/autres	46 687	15 %	45 447	15 %	40 596	11 %
Téléphone	39 365	13 %	33 733	11 %	26 067	7 %
Autre	31 722	10 %	33 481	11 %	57 695	16 %
Total des plaintes mentionnant la méthode de contact	306 286		307 122		370 012	

* Les pourcentages sont basés sur le nombre total de fraudes signalées à CSN pour chaque année civile et où la méthode de contact initial de la société a été mentionnée : 2006 = 306 286 ; 2007 = 307 122 et 2008 = 370 012. 58 % des consommateurs ont mentionné cette information pour l'année 2008 et respectivement 71 % et 53 % pour les années 2006 et 2007.

Figure 2 : Plaintes déposées pour fraudes auprès de Consumer Sentinel Network par méthode de contact. (Source : CSN)

CyberSource

En ce qui concerne les Etats-Unis et le Canada, le pourcentage de fraude par rapport aux revenus générés par les transactions en ligne a diminué au cours des dernières années. Selon CyberSource, fournisseur de services de paiement électronique et de solutions de sécurité, il s'est stabilisé à 1,4 % il y a trois ans.

Toutefois, les pertes de revenus globales ont montré une nette augmentation. Tandis que la croissance des ventes en ligne s'est poursuivie avec un ralentissement en 2008, l'on a enregistré des pertes estimées à 4 milliards de dollars pour le seul marché américain. Cette augmentation de 11 % suit la hausse de 20 % enregistrée l'année précédente[4].

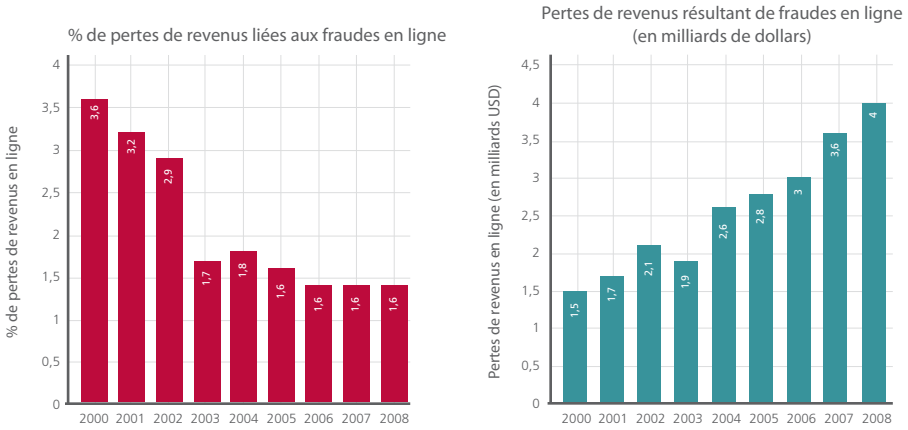


Figure 3 : Statistiques des fraudes aux paiements pour le marché américain. Bien que le pourcentage de pertes de revenus résultant des fraudes aux paiements en ligne soit resté stable en 2008, le montant total des pertes liées aux fraudes a augmenté en raison de la croissance des ventes en ligne. (Source : *10e rapport annuel sur la fraude en ligne de CyberSource)*

Internet Crime Complaint Center (IC3)

L'Internet Crime Complaint Center[5], en collaboration avec le FBI (Federal Bureau of Investigation) et le National White Collar Crime Center, recueille également des données en matière de fraude. En 2008, les Américains ont déposé 33,1 % de plaintes en plus qu'en 2007 et le montant total volé en ligne a atteint un record historique. Le centre des réclamations a enregistré près de 275 000 plaintes, représentant une perte de 265 millions de dollars, soit 10,6 % de plus qu'en 2007.

4. CyberSource, 10e édition annuelle 2009, « Online Fraud Report » (Rapport sur les fraudes en ligne). *http://forms.cybersource.com/forms/FraudReport2009NACYBSwww020309*
5. Internet Crime Complaint Center, « 2008 Internet Crime Report » (Rapport 2008 sur la cybercriminalité). *http://www.nw3c.org/downloads/2008_IC3_Annual%20Report_3_27_09_small.pdf*

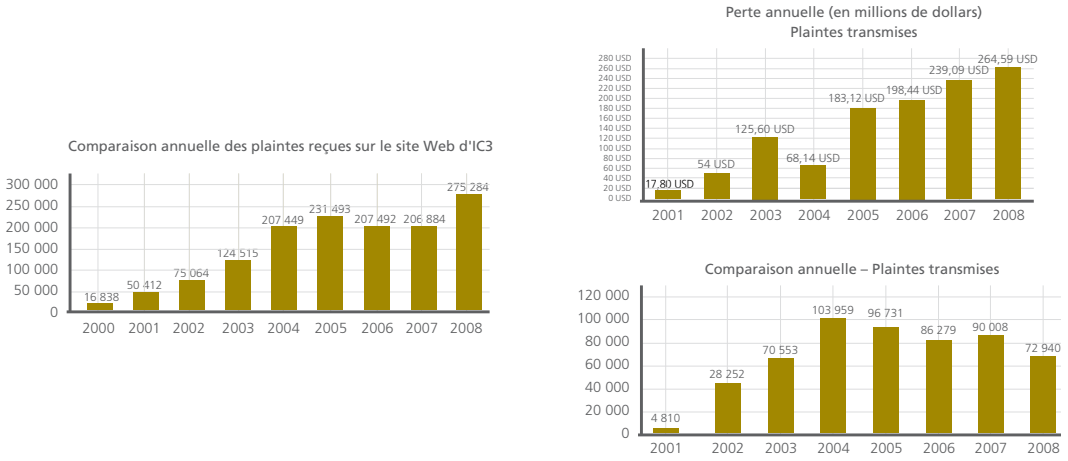


Figure 4 : Statistiques de l'Internet Crime Complaint Center (IC3) pour l'Amérique. (Source : Rapport 2008 sur la criminalité Internet de l'IC3)

Dans la moitié des dossiers, la perte monétaire était inférieure à 1 000 dollars. Un tiers (33,7 %) des plaignants a déclaré des pertes comprises entre 1 000 et 5 000 dollars. Seuls 15 % faisaient état de pertes supérieures à 5 000 dollars.

Type de plainte	% de la perte totale déclarée	Perte moyenne par plainte avec perte signalée
Fraude aux chèques	7,8	3 000 USD
Fraude par abus de confiance	14,4	2 000 USD
Fraude nigériane	5,2	1 650 USD
Fraude informatique	3,8	1 000 USD
Non-livraison de marchandises et non-exécution de paiements	28,6	800 USD
Fraude sur les sites d'enchères	16,3	610 USD
Fraude liée aux cartes de crédit/débit	4,7	223 USD

Figure 5 : Montants perdus pour fraudes, répartis par type, pour les citoyens américains ayant déclaré une perte. (Source : *Rapport 2008 sur la criminalité Internet de l'IC3)*

Les fraudes sur les sites d'enchères et la non-livraison de marchandises sont les motifs de plaintes les plus fréquents. D'autres plaintes concernent les fraudes par cartes de paiement ou les fraudes nigérianes, exigeant le paiement d'acomptes. Les e-mails et les pages web sont les deux principales méthodes de contact des victimes. Une escroquerie assez courante concerne l'achat ou la vente d'animaux domestiques.

Les plaignants sont généralement de sexe masculin. Près de la moitié ont entre 30 et 50 ans et un tiers vit dans l'une des quatre zones les plus peuplées des Etats-Unis, à savoir la Californie, la Floride, le Texas et l'Etat de New York.

La situation en Europe

Au cours de la même période (2004 à 2007), à l'instar des chiffres globaux de l'Amérique du Nord, les statistiques de l'Association for Payment Clearing Services ont également témoigné d'une diminution de la fraude bancaire en ligne. En Grande-Bretagne, la hausse importante enregistrée en 2006 ne s'est pas poursuivie l'année suivante. Au contraire, les chiffres de 2007 étaient inférieurs à ceux de l'année 2005. Cette note optimiste a été largement tempérée par les résultats du premier semestre 2008, qui montrent une augmentation de 185 % par rapport à l'année dernière[6].

6. APACS, « APACS announces latest fraud figures » (Publication par l'APACS des derniers chiffres sur les fraudes). *http://www.apacs.org.uk/APACSannounceslatestfraudfigures.htm*

	Janvier à juin 2004	Janvier à juin 2005	Janvier à juin 2006	Janvier à juin 2007	Janvier à juin 2008	Augmentation pour 2007–2008
Pertes dues à la fraude bancaire en ligne (en millions)	4 £	14,5 £	22,4 £	7,5 £	21,4 £	185 %
Arnaques par phishing	126	312	5 087	7 224	20 682	186 %
Offres de recrutement de « mules »	N/A	196	468	655	873	33 %

Figure 6 : Fraude bancaire en ligne, phishing et offres de recrutement de « mules » au Royaume-Uni. (Source : APACS, l'association britannique des paiements)

En France, ce sont les risques liés aux paiements à distance qui suscitent le plus d'inquiétude. D'après le rapport 2007 de l'Observatoire de la sécurité des cartes de paiement[7], 44 % des fraudes (contre 32 % en 2006) concernent ces transactions, qui constituent seulement 5 % du nombre total de transactions électroniques (par exemple, virements, retraits et transactions par carte).

En une seule année, la fraude électronique sur les transactions nationales a augmenté de 97 % pour atteindre 26,4 millions d'euros en France.

Pour ce qui est des transactions internationales, l'Observatoire fournit uniquement des chiffres liés aux transactions réalisées avec des cartes françaises à l'étranger. Ici aussi, on constate que le taux de fraudes sur les paiements à distance est plus élevé pour les paiements via Internet que pour n'importe quel autre type de transactions à distance.

		Montant des fraudes (en millions d'euros)	
Fraudes associées aux paiements à distance		2006	2007
Transactions nationales	Par courrier ou téléphone	19,8 €	23,8 €
	En ligne	13,4 €	26,4 €
Emetteur français, destinataire étranger	Par courrier ou téléphone	5,7 €	7,6 €
	En ligne	20,3 €	27,4 €

Figure 7 : Distribution des fraudes par type de transaction en France. (Source : Observatoire de la sécurité des cartes de paiement)

Un autre organisme de surveillance, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), indique que 80 % des appels reçus en 2007 concernent des arnaques Internet.

Une fraude aux multiples facettes

Souvent mal protégé, l'ordinateur personnel est une cible de prédilection pour les cybercriminels. Les utilisateurs sont souvent séduits par une offre alléchante ou se laissent fréquemment piéger par des avertissements semblant provenir de leurs banques.

Les sites en miroir (phishing) ou les sites hébergeant des logiciels malveillants (malwares) sont derrière de nombreuses attaques. D'après l'Anti-Phishing Working Group[8], les Etats-Unis, la Russie, la Chine, le Canada, la France et la République de Corée sont les principaux pays hébergeant des logiciels malveillants. L'éditeur de solutions de sécurité RSA ajoute souvent l'Allemagne, et plus récemment le Luxembourg, à cette liste[9].

7. Observatoire de la sécurité des cartes de paiement, « Rapport annuel 2007 ». *http://www.banque-france.fr/observatoire/telechar/rap_an_2007.pdf*
8. APWG, « Phishing Activity Trends Report, Q1/2008 » (Rapport sur les tendances en matière de phishing – 1er trimestre 2008). *http://www.antiphishing.org/reports/apwg_report_Q1_2008.pdf*
9. RSA, « RSA Online Fraud Report, July 2008 » (Rapport de RSA sur les fraudes en ligne – juillet 2008). *http://www.rsa.com/solutions/consumer_authentication/intelreport/FRARPT_DS_0708.pdf*

Selon de nombreuses sources, les cerveaux, quant à eux, proviendraient principalement des pays de l'ancien bloc soviétique. Certaines rumeurs laissent même entendre que la puissante organisation criminelle russe RBN (Russian Business Network) entretient des relations étroites avec le gouvernement[10]. Jusqu'en novembre 2007, le service d'hébergement hypersécurisé du RBN permettait à nombre de ses affiliés de se livrer à toutes sortes d'activités illégales. Pour environ 600 dollars par mois et par client, l'organisation affirmait gérer les plaintes dont celui-ci faisait l'objet tout en permettant à ses protégés de poursuivre leurs méfaits. Avec un million de sites, plusieurs millions d'adresses IP disponibles et quatre millions de visiteurs par mois, il s'agissait d'une activité très lucrative[11], à laquelle il a toutefois été possible de mettre un terme grâce à plusieurs enquêtes menées en France et aux Etats-Unis. Avec la disparition de RBN, les soupçons se sont rapidement tournés vers trois fournisseurs d'accès Internet : d'abord Abdallah Internet Hizmetleri (AIH)[12,13] (Turquie) et ensuite Atrivo et EstDomains[14,15] (Etats-Unis).

Aujourd'hui, les experts se demandent si ces fournisseurs servent de nouveaux repaires aux anciens clients de RBN ou si c'est l'organisation russe elle-même qui a discrètement mis en place des réseaux clandestins d'alliances et d'influence mafieuse pour continuer à administrer une grande partie des cybercriminels impliqués dans les activités de fraude financière en ligne.

Usurpation d'identité à petite et grande échelle

L'identité d'une personne constitue la base de sa personnalité juridique. Dans le monde réel, elle est définie par l'état civil et protégée par la loi. Dans le monde virtuel, l'identité d'une personne a une portée bien plus grande, d'autant plus difficile à délimiter. Certaines données numériques liées à l'identité d'un individu (noms de compte, noms d'utilisateur et mots de passe) permettent d'accéder à ses données privées. Tous ces identifiants numériques, qui ne sont pas considérés comme des éléments de la personnalité juridique d'une personne, font l'objet de toutes les convoitises.

Le poste de travail d'un client est la cible favorite des cybercriminels, mais de nombreux incidents liés à des sauvegardes perdues ou à des réseaux bancaires ou d'entreprise compromis prouvent que le vol d'identité est également pratiqué à grande échelle[16].

Enregistrements exposés	Durée	Date de déclaration	Organisations	Origine
94 000 000	Juillet 2005 à décembre 2006	17 janvier 2007	Groupe TJX	Vol de données perpétré à la suite de l'exploitation de failles dans le réseau sans fil
40 000 000	Septembre 2004 à mai 2005	19 juin 2005	CardSystems, Visa, MasterCard et American Express	Script malveillant injecté via une application web
30 000 000	Avril 2003 à avril 2004	24 juin 2004	America Online	Données volées par des employés et vendues à des spammeurs
26 500 000	3 mai 2006	22 mai 2006	Ministère américain des Vétérans	Données personnelles d'un ordinateur portable volées pendant un cambriolage
25 000 000	Octobre 2007	20 novembre 2007	Département des douanes et des impôts (Royaume-Uni), TNT	Perte de deux CD
17 000 000	De 2006 à 2008	6 octobre 2008	T-Mobile, Deutsche Telekom	Données volées et mises en vente sur Internet
12 500 000	27 février 2008	7 mai 2008	Archive Systems, Bank of New York Mellon	Perte de bandes non cryptées
11 000 000	Juillet à août 2008	6 septembre 2008	GS Caltex	Données personnelles copiées par des employés dans le but de les vendre
8 637 405	Mai 2001 à mars 2006	12 mars 2007	Dai Nippon Printing Company	Données volées par un ancien employé contractuel et vendues à un groupe criminel
8 500 000	De 2002 à juin 2007	3 juillet 2007	Certegy Check Services, Fidelity National Information Services	Données volées par un employé et vendues à un tiers pour des actions de marketing

Figure 8 : Fuites de données majeures. (Source : McAfee Avert Labs)

10. VeriSign iDefense, « Global Threat Research Report: Russia » (Rapport de recherche sur les menaces dans le monde : Russie), page 23. *http://www.verisign.com/static/042139.pdf*
11. VeriSign, « Uncovering Online Fraud Rings: The Russian Business Network » (Les réseaux de fraudes en ligne dévoilés : le réseau russe Russian Business Network), séminaire web. *http://www.verisign.com/*
12. David Bizeul, « Russian Business Network study » (Etude sur le réseau russe Russian Business Network). *http://bizeul.org/files/RBN_study.pdf*
13. The Shadowserver Foundation, « RBN 'Rizing': Abdallah Internet Hizmetleri (AIH) » (RBN se relève : AIH). *http://digitalninjitsu.com/downloads/RBN_Rizing.pdf*
14. Jart Armin et al., « Atrivo—Cyber Crime USA » (Atrivo ou la cybercriminalité aux Etats-Unis). *http://hostexploit.com/downloads/Atrivo%20white%20paper%20090308ad.pdf*
15. Washington Post, « EstDomains: A Sordid History and a Storied CEO » (EstDomains : une histoire sordide et un PDG plein d'histoires). *http://voices.washingtonpost.com/securityfix/2008/09/estdomains_a_sordid_history_an.html*
16. Open Security Foundation, « DataLossDB ». *http://datalossdb.org/*

Bien que le nombre de divulgations de données affectant plusieurs millions d'enregistrements ou plus ne cesse d'augmenter, l'affaire TJX reste la plus importante à ce jour. Depuis mars 2007, plusieurs revendeurs et utilisateurs de ces données ont été arrêtés et condamnés dans le cadre de cette affaire[17]. L'un deux, connu sous le nom de « Lord Kaisersose », a été appréhendé en France en juin 2007[18].

Fraude à la carte bancaire par carding et skimming

Les criminels fréquentent et alimentent de nombreux sites de « carding », permettant de créer de fausses cartes virtuelles au départ de données dérobées, qui sont monnaie courante sur Internet. Ils y achètent ou vendent des accès à des comptes bancaires, des numéros de cartes volés, des copies de pistes magnétiques et des profils personnels complets.

Le 2 mai 2008, nous avons identifié une série de comptes bancaires à vendre. Le plus cher était également le compte le mieux approvisionné : il s'agissait d'un compte de la banque BNP Paribas affichant un solde de 30 792 euros, vendu en ligne pour seulement 2 200 euros. En plus du prix réduit, le vendeur offrait une garantie de 24 heures. Si l'acheteur n'arrivait pas à se connecter au cours de cette période ou si le compte n'était plus approvisionné, un autre compte lui était proposé en échange.

Nom de la banque	Pays	Solde	Prix
Bank of America	Etats-Unis	...	Vendu
Asmouth Bank	Etats-Unis	16 040 USD	700 €
Washington Mutual Bank	Etats-Unis	14 400 USD	600 €
Washington Mutual Bank	Etats-Unis	7 950 USD + 2 612 £	500 €
Washington Mutual Bank	Etats-Unis	...	Vendu
MBNA America Bank	Etats-Unis	22 003 USD	1 500 €
Banco Bradesco S.A.	Brésil	13 451 USD	650 €
Citibank	Royaume-Uni	10 044 £	850 €
NatWest	Royaume-Uni	12 000 £	1 000 €
BNP Paribas	France	30 792 €	2 200 €
Caja de Ahorros de Galicia	Espagne	23 200 €	1 200 €
Caja de Ahorros de Galicia	Espagne	7 846 €	500 €
Banc Sabadell	Espagne	25 663 €	1 450 €

Figure 9 : Données relatives à divers comptes bancaires mis en vente, extraites d'un site de carding.

Phishing et pharming

Le phishing est une technique bien connue visant à obtenir des informations confidentielles d'un utilisateur en se faisant passer pour une organisation de confiance. La victime est généralement abusée par un e-mail trompeur qui la redirige vers un site miroir.

A l'aide d'un cheval de Troie, il est également possible d'infiltrer la liaison entre l'adresse IP et le nom du serveur auquel elle répond. C'est la technique dite du pharming.

Dans les deux cas, les victimes pensent accéder à des sites légitimes. Non conscients du fait que 80 % des e-mails bancaires sont frauduleux[19], de nombreux utilisateurs n'hésitent pas à fournir des informations personnelles. Selon les statistiques mensuelles de PhishTank, la cible la plus populaire est PayPal[20]. Les résultats montrent que PayPal occupe de loin la première place et que le classement des autres sociétés varie légèrement chaque mois. eBay, qui suivait PayPal de près en 2007, arrive souvent en deuxième position.

17. Ministère américain de la Justice, « Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers » (Un réseau de piratage des ventes au détail accusé de voler et de distribuer des numéros de cartes de crédit et de débit d'importants détaillants américains). *http://www.usdoj.gov/criminal/cybercrime/gonzalezIndict.pdf*
18. Tribunal de district américain, District de Columbia, « Affidavit in Support of Complaint for Forfeiture » (Déclaration sous serment en soutien d'une plainte pour déchéance de droits). *http://docs.justia.com/cases/federal/district-courts/district-of-columbia/dcdce/1:2007cv01346/126695/1/1.pdf*
19. « Leading Companies & Non-Profits Realize the Benefits of Brand and Consumer Protection Through Email Authentication » (Des grandes entreprises et des sociétés à but non lucratif prennent conscience des avantages de la protection des marques et des consommateurs par le biais de l'authentification par e-mail). *http://www.reuters.com/article/pressRelease/idUS191046+31-Jan-2008+MW20080131*
20. Stats (« Statistiques »), avril 2009. *http://www.phishtank.com/stats/2009/04/*

Cibles	Attaques par phishing réussies en 2009			
	Janvier	Février	Mars	Avril
PayPal	9 575	6 245	9 605	7 575
IRS (Administration fiscale américaine)	469	326	96	426
eBay	720	292	459	356
Google	336	203	169	330
Bank of America Corp.	231	204	429	290
HSBC Group	272	97	265	228

Figure 10 : Cibles les plus populaires des attaques par phishing. (Source : PhishTank)

D'après les autorités, bien que les statistiques varient, les marques principalement ciblées sont des banques anglaises et américaines. Selon la société RSA, 72 % des attaques sont menées contre des banques américaines, bien que l'APWG, le groupe de travail antiphishing dont la vocation est de lutter contre les arnaques et les fraudes sur Internet, indique que la moitié des attaques visent des organisations européennes. Gartner estime que la perte moyenne par victime aux Etats-Unis s'élève à 886 dollars[21].

Logiciels criminels

Outre le phishing, les chevaux de Troie sont très en vogue auprès de la communauté des cybercriminels. Cette catégorie de logiciels criminels (crimewares) comprend les dérobeurs de passe et les enregistreurs de frappe, qui enregistrent des séquences de touches, prennent des captures d'écran et envoient les données à des sites chargés de les collecter. Le nombre de ces logiciels est en augmentation et leur efficacité ne cesse de croître. Les logiciels criminels sont souvent associés aux rootkits, des programmes furtifs qui rendent ces logiciels invisibles à de nombreux outils de sécurité.

Les logiciels criminels sont également de plus en plus utilisés dans le cadre des attaques ciblées. Ils peuvent alors échapper à la détection si les outils ne sont pas capables de les identifier à l'aide de la détection générique ou d'une analyse de comportement.

Une grande partie de ces logiciels sont concentrés dans les mondes virtuels et les jeux en ligne puisqu'on y trouve entre 30 et 40 % des centaines de milliers de dérobeurs de mots de passe détectés par McAfee VirusScan®. La plupart d'entre eux sont détectés sous une forme générique mais certaines grandes familles font l'objet d'une classification plus granulaire.

- *PWS-Banker* — Connexions bancaires
- *PWS-MMORPG* — Divers jeux en ligne multijoueurs
- *PWS-LDPinch* — Collecte d'informations sur le système qui l'héberge, recherche des mots de passe stockés sur le disque dur (ICQ, TheBat, connexion par numérotation)
- *PWS-Legmir* — Jeux « Legend of Mir »
- *Keylog-Ardamax* — Enregistrement de la frappe
- *PWS-Lineage* — Jeux « Lineage »
- *PWS-Onlinegames* — Divers jeux en ligne multijoueurs

21. 257 dollars en 2005 et 1 244 dollars en 2006. D'après l'étude de Gartner, le phishing aurait coûté 3,2 milliards de dollars (2,2 milliards d'euros) aux internautes américains en 2007. 64 % des victimes ont été indemnisées ou remboursées. *http://www.gartner.com/it/page.jsp?id=565125*

Il s'agit des dérobeurs de mots de passe les plus répandus à l'heure actuelle. Le graphique ci-dessous illustre leur fréquence au cours des deux dernières années.

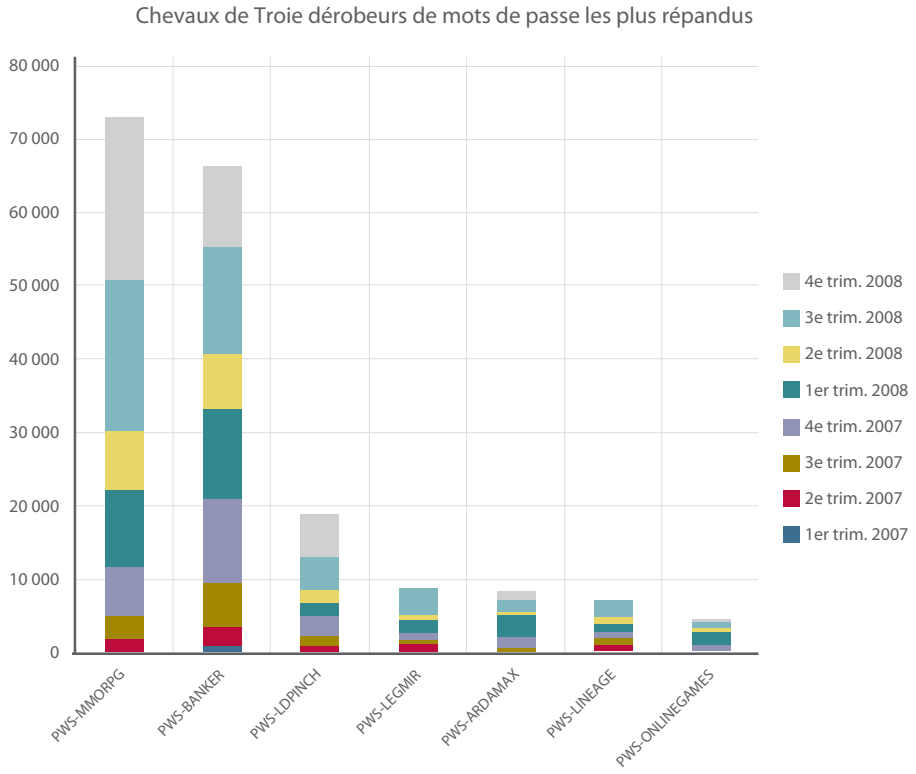


Figure 11 : Variantes de logiciels malveillants dérobeurs de mots de passe. (Source : McAfee Avert Labs)

Blanchiment d'argent

Pratiquement toutes les activités criminelles nécessitent un blanchiment d'argent. Outre les nombreuses méthodes traditionnelles (y compris les transferts de fonds électroniques, le recours à des sociétés fictives dans les banques étrangères ou à des courtiers en devises non agréés, la contrebande d'espèces ou encore la fraude bancaire), d'autres procédures récentes, comme l'emploi de « mules » et les casinos virtuels, ont fait leur apparition sur Internet.

Les « mules »

Les « mules » (ou passeurs d'argent), qui doivent leur nom à la méthode de transport utilisée par les contrebandiers pour acheminer les marchandises illégales, sont des individus recrutés via Internet pour servir d'intermédiaires afin de récupérer les fonds illicitement acquis lors des arnaques par phishing, les enregistrements de frappe et autres escroqueries. Pour chaque transaction, ce passeur déduit entre 5 et 10 % du montant obtenu et transfère le solde via un service de transfert anonyme, par exemple WebMoney, e-gold ou Western Union.

On pense souvent à tort que les mules sont des personnes naïves qui ont été abusées par une offre d'emploi en apparence légitime (via le spam ou des sites spécialisés). Mais elles sont rarement innocentes. Bien des personnes peu scrupuleuses et en quête d'argent facile n'hésitent pas à se porter volontaires. Aujourd'hui, le travail de mule devient une profession en soi. De récentes arrestations en France et dans d'autres pays le prouvent. Quatre de ces passeurs d'argent ont été interpellés et placés sous contrôle judiciaire dans le cadre d'une affaire en mai 2008[22]. Ils étaient au cœur d'une arnaque visant PayPal et eBay et ont été accusés d'escroquerie en bande organisée et de recel d'escroquerie en bande organisée.

22. 01net, « Quatre "mules" arrêtées pour escroquerie via PayPal ». *http://www.01net.com/editorial/379382/quatre-mules-arretees-pour-escroquerie-via-paypal/*

On pense qu'ils ont été aidés par un complice, un pirate informatique de 17 ans, vivant actuellement en Tunisie. Les mules sont soupçonnées d'avoir escroqué 19 internautes pour un butin approchant les 20 000 euros, mais les enquêteurs parlent d'au moins 10 000 autres victimes potentielles.

En septembre 2007, pour savoir comment fonctionne l'une de ces offres, j'ai répondu à une proposition de télétravail sur Internet. J'ai ensuite reçu une liste de questions fréquemment posées sur l'emploi proposé.

Questions fréquemment posées concernant le travail d'indépendant :

Q1 : En quoi consiste ce poste ?

R : Votre fonction consiste à contrôler notre flux monétaire et à prendre en charge une partie des transactions. Vous recevez des paiements de nos principaux clients sur votre compte bancaire à l'heure et la date qui vous conviennent, puis nous transférez l'argent. Votre commission pour chaque transaction s'élève à 7 %. Nous n'exigeons AUCUN investissement d'argent de votre part.

Q2 : Pourquoi vos clients n'effectuent-ils pas les paiements directement sur votre compte ?

R : Les clients n'effectuent pas les paiements directement sur notre compte car nous n'avons pas de succursale en Europe (en dehors du Royaume-Uni). Cette solution profite aux deux parties, puisque nous économisons sur les coûts de production et que vous percevez une commission de 7 %.

Q3 : Pouvez-vous me donner un exemple de déroulement d'une transaction ?

R : 1. Le client envoie le paiement via son compte bancaire et nous prévient.*

2. Nous vous informons par téléphone du transfert effectué. Nous vous envoyons également un e-mail du type suivant : « Un transfert d'argent a été effectué sur votre compte bancaire. Le montant est de 5 000 euros et émane de notre client Peter Tischler de Berlin, en Allemagne. Veuillez vérifier votre compte demain, retirer l'argent et l'envoyer par Western Union ou MoneyGram à Kate Lewis, à Londres, au Royaume-Uni. »

3. Vous vous rendez dans votre banque et retirez l'argent.

4. Vous empochez votre commission de 7 % et vous rendez dans une agence Western Union ou MoneyGram avec le reste de l'argent afin de l'envoyer à Kate Lewis, à Londres, au Royaume-Uni.

5. Vous nous envoyez par e-mail les détails du transfert via Western Union ou MoneyGram, ainsi qu'une copie numérisée du reçu du transfert.

* Notre responsable vous contactera avant le transfert bancaire. Si vous n'êtes pas en mesure de recevoir celui-ci, nous l'effectuerons un autre jour. Vous pouvez par conséquent organiser ce travail en fonction de votre agenda.

Figure 12 : Questions fréquemment posées sur un site de recrutement de mules.

Après un premier contact par e-mail, j'ai reçu un contrat de travail. Compte tenu de l'apparent professionnalisme de la personne de contact et de la qualité des documents qu'il m'a été donné de voir, il serait facile, par ignorance, de tomber dans le panneau. Les publications sur le sujet des sociétés spécialisées dans la sécurité informatique, du secteur bancaire et des forces de police se multiplient, mais à la lumière de mes échanges récents avec la communauté des utilisateurs, une campagne de sensibilisation ne serait pas superflue.

Les casinos virtuels

En 2006, on recensait près de 15 000 sites de jeux de hasard actifs[23]. Il est peu probable que ce chiffre ait diminué depuis lors. Seuls 1 766 des sites de jeux de hasard disposant d'une licence à l'heure actuelle[24], plus 87 % des sites proposés sur Internet réalisent une activité clandestine (sans licence).

L'absence de cadre juridique permet à quiconque d'enregistrer un site Internet dans l'anonymat puis de facturer les clients via un compte bancaire anonyme dans un paradis fiscal ou un système monétaire virtuel. La plupart des groupes de cybercriminels russes actifs aujourd'hui (y compris l'ex RBN et Yambo Financial) ont commencé leurs activités criminelles par de la pornographie à caractère pédophile et les casinos en ligne.

23. CERT-LEXSI, « Cybercriminalité des Jeux en Ligne », juillet 2006. *http://www.lexsi.com/telecharger/gambling_cybercrime_2006.pdf*
24. Casino City, « Online Gaming Jurisdictions » (Les juridictions des jeux de hasard). *http://online.casinocity.com/jurisdictions/index.cfm?sorttab=n/a&sortlist=sites&filterlist=&numperpage=25&searchall=1*

Manipulation des titres boursiers

Des techniques d'ingénierie sociale telles que la circulation de faits d'actualité mensongers dans les forums sont depuis longtemps utilisées pour manipuler les marchés boursiers. 2006 a marqué l'avènement d'une version modifiée de cette technique : le « pump and dump », ou la manipulation des titres boursiers à moins d'un dollar (« penny stock ») de sociétés souvent peu attrayantes.

Après avoir acheté un volume important d'actions à un cours bas, le manipulateur a recours au spam pour envoyer des messages enthousiastes destinés à faire grimper artificiellement le cours de l'action. Un ou deux jours plus tard, après une augmentation du cours, le spammeur revend ses titres à un prix artificiellement élevé et engrange un bénéfice.

Les résultats d'une étude menée par des chercheurs de la Purdue University (Indiana) et l'université d'Oxford (Angleterre) ont montré une hausse sensible du cours et du volume d'actions ayant fait l'objet d'une campagne de spam entre le jour précédant l'envoi des messages racoleurs et le jour le plus actif de la campagne[25]. Laura Frieder, coauteur de l'étude, a identifié deux profils de spéculateurs en plus des spammeurs eux-mêmes. « D'une part, il y a les investisseurs naïfs, cupides mais pas toujours très futés, dont le profil s'apparente beaucoup à celui des utilisateurs qui envoient des milliers de dollars au Nigéria ou transmettent les lettres en chaîne », a déclaré Laura Frieder. « S'ils pensent avoir ne fût-ce qu'une toute petite chance de réaliser un profit, ils se laisseront tenter[26] ».

D'autres, en revanche, sont conscients que ces informations ne valent rien mais pensent que, si d'autres l'ignorent, ils ont peut-être une chance d'encaisser une plus-value. « S'ils estiment que d'autres personnes vont investir et faire augmenter le prix de l'action, ils vont essayer d'acheter suffisamment tôt, réaliser un petit profit puis vendre aussitôt ».

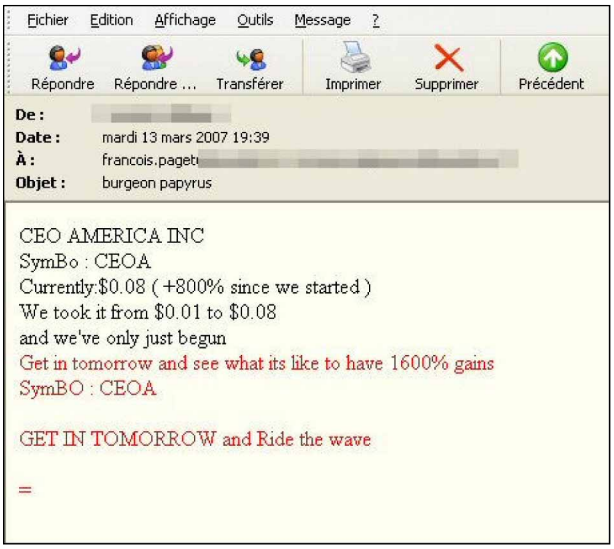


Figure 13 : E-mail destiné à la manipulation de titres boursiers

La méfiance des petits actionnaires, le profit limité qu'il est possible de réaliser et les tentatives de manipulation des titres par des indésirables ont contribué à rendre cette forme de fraude moins intéressante et efficace. N'ayant pas donné les résultats escomptés, cette technique est devenue plus rare.

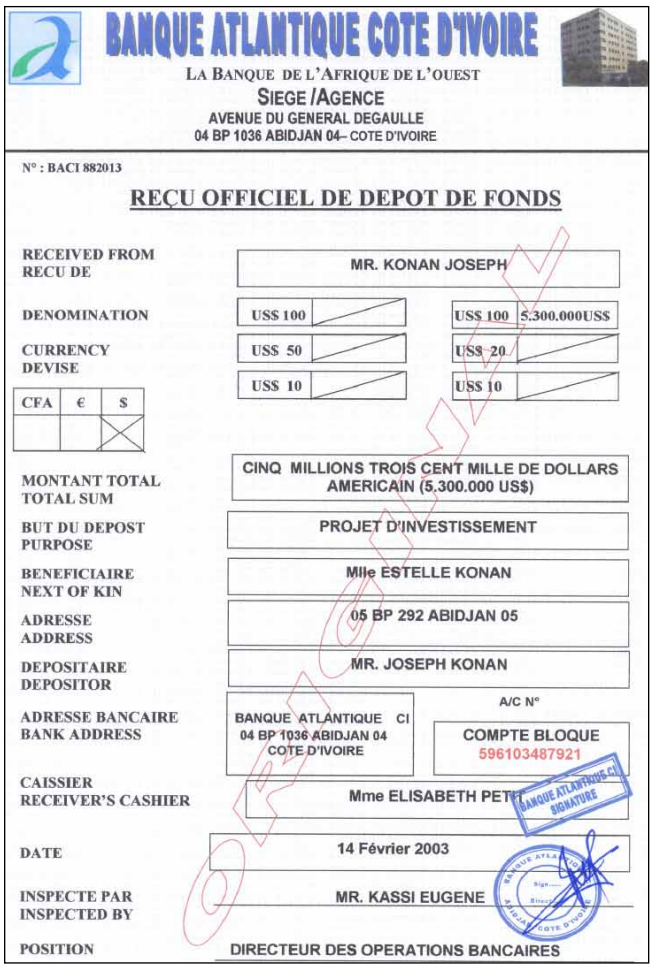
25. Laura Frieder et Jonathan Zittrain, « Spam Works: Evidence from Stock Touts and Corresponding Market Activity » (Le spam à l'œuvre : preuves du racolage boursier et de l'activité correspondante du marché). *http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Spam%20Works.pdf*
26. CBC, « Stock Spam: The New Boiler Room » (Le spam boursier : la nouvelle « salle de courtage »). *http://www.cbc.ca/news/background/personalfinance/stock-spam.html*

La fraude nigériane (fraude 4-1-9)

La fraude 4-1-9, qui doit son nom à l'article de la législation nigériane qui la décrit, est une arnaque extrêmement populaire et lucrative. Elle se présente souvent sous la forme d'un e-mail émanant d'un membre de la famille d'un dignitaire (généralement africain). L'expéditeur y explique que, suite à la mort d'un membre influent de sa famille, une somme d'argent importante est bloquée sur un compte bancaire. Avec l'aide du destinataire et en tirant parti de son soutien financier pour le transfert des fonds, l'expéditeur déclare qu'il serait possible de faire libérer les fonds. Une rémunération non négligeable est offerte à quiconque acceptera de participer à l'opération.

Une fois le contact établi, l'escroc demande une avance, par exemple par l'ouverture d'un compte bancaire ou le paiement de certains frais. Cette première transaction est suivie d'une série de dépenses et de problèmes qui s'accompagnent parfois de menaces physiques. Naturellement, les fonds bloqués n'existent pas.

En France, les fautes d'orthographe ou de syntaxe dans les e-mails ont tendance à rassurer les naïfs plutôt qu'à les inquiéter. Il en va de même pour l'apparence très officielle des documents envoyés par la suite.



BANQUE ATLANTIQUE COTE D'IVOIRE

LA BANQUE DE L'AFRIQUE DE L'OUEST

SIEGE /AGENCE

AVENUE DU GENERAL DEGAULLE

04 BP 1036 ABIDJAN 04– COTE D'IVOIRE

N° : BACI 882013

REÇU OFFICIEL DE DEPOT DE FONDS

RECEIVED FROM / RECU DE	MR. KONAN JOSEPH
DENOMINATION	US$ 100 ; US$ 100 5.300.000US$
CURRENCY / DEVISE	US$ 50 ; US$ 20 ; US$ 10 ; US$ 10
CFA / € / $	$ X
MONTANT TOTAL / TOTAL SUM	CINQ MILLIONS TROIS CENT MILLE DE DOLLARS AMERICAIN (5.300.000 US$)
BUT DU DEPOST / PURPOSE	PROJET D'INVESTISSEMENT
BENEFICIAIRE / NEXT OF KIN	Mlle ESTELLE KONAN
ADRESSE / ADDRESS	05 BP 292 ABIDJAN 05
DEPOSITAIRE / DEPOSITOR	MR. JOSEPH KONAN
ADRESSE BANCAIRE / BANK ADDRESS	BANQUE ATLANTIQUE CI 04 BP 1036 ABIDJAN 04 COTE D'IVOIRE
A/C N°	COMPTE BLOQUE 596103487921
CAISSIER / RECEIVER'S CASHIER	Mme ELISABETH PETIT
DATE	14 Février 2003
INSPECTE PAR / INSPECTED BY	MR. KASSI EUGENE
POSITION	DIRECTEUR DES OPERATIONS BANCAIRES

BANQUE ATLANTIQUE CI SIGNATURE

Figure 14 : Exemple de contrat utilisé pour une fraude nigériane.

Selon les statistiques recueillies sur la fraude nigériane, les pertes s'élevaient à 4,3 milliards de dollars en 2007[27] :

Pays	Pertes (en millions de dollars)
Etats-Unis	830
Royaume-Uni	580
Espagne	355
Allemagne	280
Japon	270
France	235
Chine	205
Australie	166
Italie	159
Canada	158

Figure 15 : Pertes dues à la fraude nigériane en 2007, pour les sociétés et les particuliers. (Source : Ultrascan Research Services)

En France, une victime très crédule a récemment perdu un million d'euros !

Les e-mails de la loterie qui annoncent la sélection de votre adresse e-mail dans un tirage dont le prix s'élève à plusieurs millions d'euros relèvent de la même catégorie d'arnaques. Le but est d'encourager les victimes à dépenser une certaine somme tout en les persuadant qu'ils pourront gagner cent fois plus.

Les sites d'enchères

La fraude aux enchères est l'une des préoccupations majeures des autorités. Une étude réalisée en mai 2008 par ConsumerWebWatch a révélé que, dans l'Etat de New York, plus d'un utilisateur d'un site d'enchères en ligne (généralement eBay, Amazon.com et Overstock.com) sur quatre a été victime d'une arnaque ou abusé d'une façon quelconque[28]. 11 % des utilisateurs de ces sites ont déclaré n'avoir jamais reçu les marchandises dont ils s'étaient portés acquéreurs ; il s'agit de la plainte la plus courante associée à ces sites. En outre, 7 % des personnes interrogées qui avaient reçu les marchandises ont indiqué que celles-ci étaient inutilisables. Autres motifs de plaintes : le fait qu'une information majeure relative à l'article n'a pas été communiquée avant sa réception (7 %) et que la valeur de l'article reçu était inférieure à celle de l'enchère (7 %).

Lorsqu'ils sont victimes d'une forme quelconque de fraude, plus de la moitié des plaignants, pratiquement toutes catégories d'âge confondues, ont déclaré avoir tenté de résoudre le problème directement avec le vendeur. Près de 40 % des victimes ont dit avoir déposé une plainte formelle auprès de PayPal, système de paiement en ligne appartenant à eBay. Plus de 25 % ont publié des commentaires négatifs sur le vendeur. En comparaison, très peu des personnes interrogées ont choisi de contacter les autorités, un avocat ou la FTC.

Les demandes de transfert par l'intermédiaire d'un service de transfert anonyme de même que les faux paiements sont d'autres problèmes susceptibles d'affecter vendeurs et acheteurs. Dans le cas de faux paiements à un vendeur, le criminel (l'acheteur) prétend vivre à l'étranger et demande un code d'identification de la banque (BIC) ou un numéro de compte bancaire international (IBAN) au vendeur. Ce type d'affaires implique souvent la vente d'un véhicule dont un intermédiaire vient prendre possession pour le compte de l'acheteur. Le compte du vendeur est crédité et l'intermédiaire vient très rapidement prendre livraison de la voiture. Plus tard, le paiement est annulé car il ne s'agissait pas d'un véritable transfert mais, grâce au code BIC, d'un simple dépôt de chèque. Comme il s'agit d'un chèque sans provision, volé ou falsifié, la transaction est annulée. L'intermédiaire est souvent une mule.

27. Ultrascan Research Services, « 419 AFF and the media » (La fraude nigériane et les médias). *http://www.ultrascan.nl/html/__the_media.html*
28. « Consumer Reports WebWatch Survey: More than 25 Percent of New Yorkers Stung in Online Auction Site Scams » (Enquête de Consumer Reports WebWatch : plus de 25 % des New-Yorkais piégés par des escroqueries sur des sites d'enchère en ligne). *http://www.consumerwebwatch.org/pdfs/surveypressrelease.pdf*

Un autre type de fraude consiste dans la demande de transfert de fonds via la Western Union ou MoneyGram. En voici un exemple :

Figure 16 : Fausse offre d'enchère de véhicule.

Soupçonnant une fraude pour la vente d'une Volkswagen proposée au prix de 7 400 euros, un acheteur contacte le vendeur pour s'assurer de sa bonne foi. Voici une traduction de la réponse du vendeur :

> *Bonjour,*
>
> *J'ai bien reçu votre message et vous en remercie.*
>
> *Le véhicule est équipé d'un moteur diesel de 1 900 cm³. Le moteur est très souple, puissant et représente un très bon rapport qualité-prix.*
>
> *Le véhicule est en parfait état, n'a jamais été accidenté, est très bien entretenu (non fumeurs) et ne présente aucune bosse ni éraflure. Il se trouve dans un garage. Le carnet d'entretien est à jour et tous les entretiens ont été réalisés dans des garages Volkswagen agréés. J'en suis le premier propriétaire et tous les papiers sont en ordre : carnet d'entretien, immatriculation, certificat de non-gage, etc. Il n'y aura aucun problème car le véhicule a été acheté et immatriculé en France.*
>
> *Je réside actuellement en Angleterre, où je viens de me marier. Je vends le véhicule pour cause de déménagement (de France en Angleterre) et, comme j'ai une voiture de société, je souhaite le vendre rapidement. La voiture est dans le garage de mon ancienne maison en France (75003 Paris), que je viens de vendre. Comme le nouveau propriétaire emménage dans trois semaines, je suis assez pressé...*
>
> *Le prix que je propose est très inférieur à celui du marché.*
>
> *Ma voiture est vraiment en parfait état. Si vous voulez l'acheter, communiquez-moi vos coordonnées (nom complet et adresse) que j'enverrai à eBay. Ils vous enverront ensuite toutes les informations dont vous avez besoin pour effectuer la transaction rapidement et en toute sécurité.*
>
> *J'espère avoir répondu à toutes vos questions. Merci de m'envoyer vos coordonnées, je pourrai ainsi vous réserver le véhicule et vous envoyer la confirmation.*
>
> *Sincères salutations,*

Après quelques autres échanges où le vendeur continue d'éviter de répondre aux questions concernant son identité et à la demande de l'acheteur de voir le véhicule, celui-ci reçoit un faux e-mail d'eBay, lui demandant de verser 3 000 euros via la Western Union. (Cette fois, l'acheteur ne se laisse pas abuser car il sait qu'eBay interdit l'utilisation de ce type de services de transfert instantané[29].)

29. eBay Security & Resolution Center (Espace Sécurité d'eBay). *http://pages.ebay.com/SECURITYCENTER/mrkt_safety.html*

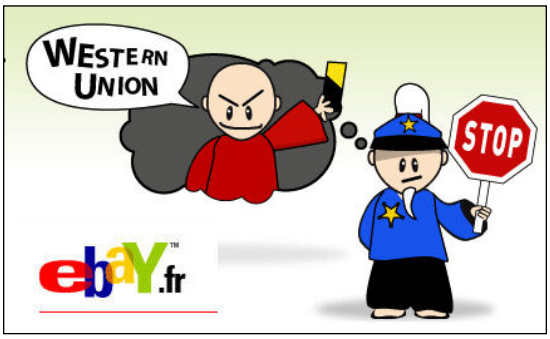


Figure 17 : Logo eBay. (Source : eBay France)

Achats en ligne

L'achat direct d'articles en ligne, sans enchère préalable, est également visé par de nombreuses attaques. Il est évidemment primordial d'éviter les sites qui n'offrent pas de système de paiement sécurisé. Le spam est la technique la plus répandue pour attirer les acheteurs crédules. Si l'article ou le médicament existe, il s'agit souvent respectivement d'une contrefaçon ou d'un placebo. Dans son rapport 2007 sur la sécurité, IronPort[30] a identifié une attaque qui tenait plus du crime organisé que du commerce électronique.

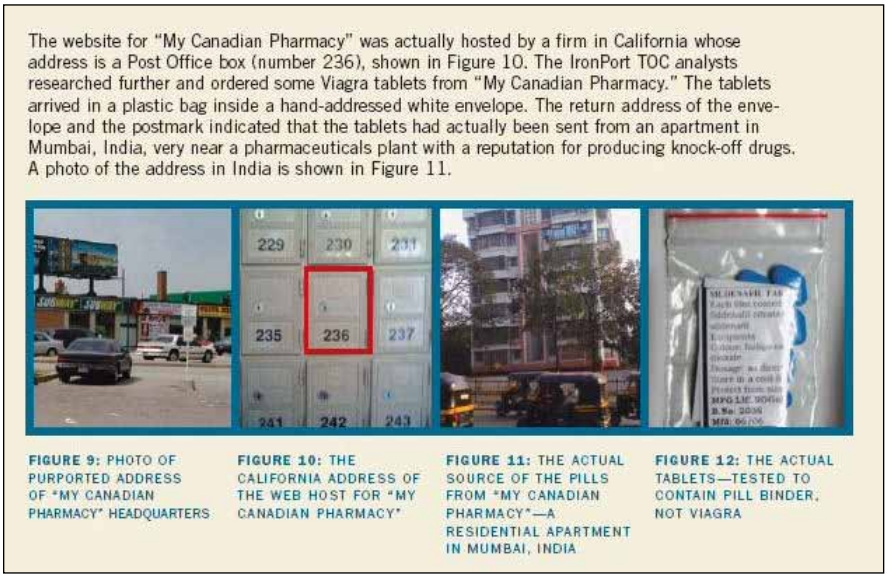


Figure 18 : Extrait de l'arnaque « My Canadian Pharmacy ». (Source : *Rapport 2007 d'IronPort sur les tendances en matière de sécurité Internet*)

Pour tromper les acheteurs, une autre méthode consiste à s'assurer une grande visibilité dans les moteurs de recherche. Le client est ainsi redirigé vers un site d'achats en ligne qui vend des médicaments, des articles de contrefaçon ou des logiciels dix fois moins chers que leur prix d'origine. Il est bien plus facile, par exemple, de trouver des téléphones Vertu contrefaits de la division de luxe de Nokia que d'acheter les modèles originaux.

30. IronPort, « Internet Security Trends for 2007 » (Tendances en matière de sécurité Internet pour 2007) (p. 9–11). *http://www.ironport.com/pdf/ironport_trend_report.pdf*

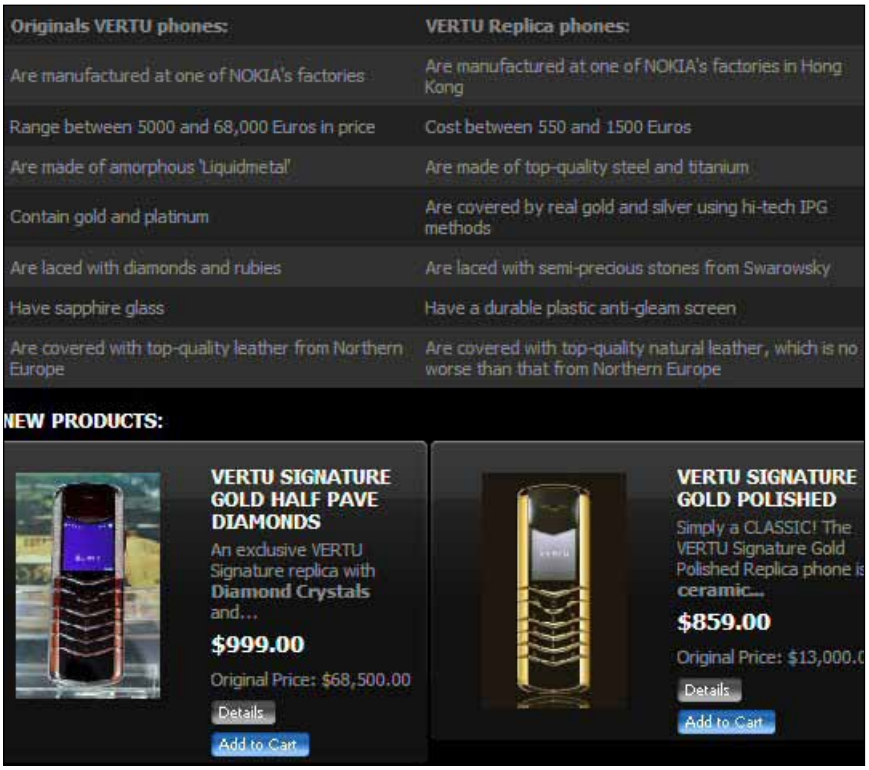


Figure 19 : Site web de contrefaçons.

Méthodes de paiement anonymes

Les criminels préfèrent avoir recours à des services de paiement tels qu'e-gold et WebMoney. Il existe environ vingt services de ce type dans le monde, en réalité anonymes et très pratiques.

En France, à la différence des notaires et des banques approuvées par la commission bancaire, les services de paiement en ligne ne doivent pas envoyer des déclarations de soupçon à TRACFIN (Traitement du renseignement et action contre les circuits financiers clandestins) en cas d'activités suspectes ou de transactions pour des montants supérieurs à un seuil donné.

Aux Etats-Unis, le FCEN (Financial Crimes Enforcement Network)[31] est responsable de la collecte des extraits bancaires, de leur analyse et du renvoi des activités suspectes aux services d'enquête chargés des dossiers de blanchiment d'argent. Ce service administratif a été intégré au ministère du Trésor américain.

Voici quelques exemples de services de transfert de paiements connus :

- *e-gold* — Fondée en 1996, cette société a son siège en Floride. Les autorités la soupçonnent depuis longtemps de participer à des activités illégales. Ses fondateurs et certains de ses partenaires font actuellement l'objet d'une enquête.
- *Western Union* — Cette société américaine possède des filiales dans plus de 200 pays. Elle propose des services qui sont normalement réservés aux transferts d'argent à des membres de la famille, mais sont souvent utilisés par des personnes mal intentionnées.
- *WebMoney* — Cette société russe réalise chaque jour des transactions pour un montant de 7 millions de dollars. Elle possède 4 millions de clients, certains moins honnêtes que d'autres.

D'autres services, dont MoneyGram, Money Express, Ria, Flouss et DabaDaba, sont également utilisés dans le cadre de transferts de fonds suspects liés à des activités criminelles.

31. *http://www.fincen.gov/*

Figure 20 : Site web russe qui offre un service pour des attaques par déni de service distribué.

Mesures de protection

La fraude financière commence souvent par le détournement d'informations personnelles. Une corbeille ou une poubelle, une conversation téléphonique ou un ordinateur mal protégé peuvent constituer le point de départ de la fraude.

Les entreprises sont également vulnérables. Le vol d'ordinateurs portables et les fuites de données peuvent porter atteinte à leur image de marque et avoir des répercussions financières importantes pour les sociétés elles-mêmes ou leurs clients. A cet égard, les banques se retrouvent en première ligne.

Bien qu'il soit impossible d'éliminer complètement le risque d'usurpation d'identité, les utilisateurs peuvent au moins le limiter en suivant quelques recommandations fondées sur le simple bon sens. (Ces recommandations ont été présentées en détail dans le livre blanc de McAfee Avert Labs sur l'usurpation d'identité[32]). Dans ce rapport, nous nous concentrerons sur quelques techniques qui concernent directement le secteur bancaire.

Notation

La notation est une technique d'analyse du risque destinée à évaluer la probabilité qu'une transaction aboutisse (si elle n'est pas frauduleuse). Cette notation attribue une pondération aux diverses informations associées à l'achat et à l'acheteur (adresse e-mail, coordonnées, origine de l'adresse IP, importance de la commande et d'autres données). La transaction est approuvée ou refusée selon le score total obtenu.

Norme EMV (Europay, MasterCard et Visa)

EMV est la norme en vigueur en matière de paiements par carte à puce. Cette norme exige que les paiements soient effectués par des cartes à puce et non des cartes à piste magnétique. La Banque des règlements internationaux (BRI) souhaite que la nouvelle norme EMV internationale soit adoptée d'abord dans toute l'Europe puis dans le reste du monde. D'ici à 2010, il devrait y avoir plus de 800 millions de cartes à puce en circulation[33].

32. *http://www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf*
33. CARTES 2007, « CARTES & IDentification 2007 fait le point sur le SEPA ». *http://fr.cartes.com/ExposiumCms/cms_sites/SITE_319050/ressources319050/cp_sepa-fr.pdf*

Norme PCI DSS

Face à l'évolution du cybercrime, les réseaux Visa et MasterCard ont élaboré une norme visant à protéger les titulaires de carte lors de leurs achats en ligne. PCI DSS, la norme de sécurité des données du secteur des cartes de paiement, permet d'améliorer la sécurité des transactions et le stockage des données bancaires. Il s'agit d'une norme internationale également adoptée par d'autres réseaux, notamment American Express, JCB et Diners Club.

Les organisations qui acceptent les transactions par cartes de paiement doivent respecter les dispositions de la norme. Dans le cas contraire, elles peuvent se voir interdire l'accès aux données des titulaires de carte. Les amendes peuvent s'élever à 500 000 dollars en cas de vol ou fuite des données.

La norme PCI DSS prévoit 12 dispositions relatives à la sécurité numérique élaborées par Visa. Elles sont connues sous le nom de « Digital Dozen » et sont regroupées en six catégories [34] :

- Mettre en place et gérer un réseau sécurisé
  - » Installer et gérer une configuration de pare-feu afin de protéger les données des titulaires de carte
  - » Ne pas utiliser les valeurs par défaut du fournisseur pour les mots de passe et les autres paramètres de sécurité
- Protéger les données des titulaires de carte
  - » Protéger les données des titulaires de carte stockées
  - » Crypter la transmission des données des titulaires de carte et autres informations sensibles sur les réseaux publics ouverts
- Disposer d'un programme de gestion des vulnérabilités
  - » Utiliser et mettre à jour régulièrement un logiciel antivirus
  - » Développer et gérer des applications et systèmes sécurisés
- Mettre en œuvre des mesures de contrôle d'accès rigoureuses
  - » Limiter l'accès aux données des titulaires de carte aux cas de nécessité professionnelle absolue
  - » Attribuer une identité d'utilisateur unique à chaque personne disposant d'un accès informatique
  - » Limiter l'accès physique aux données des titulaires de carte
- Surveiller et tester régulièrement les réseaux
  - » Suivre et surveiller tous les accès aux ressources du réseau et aux données des titulaires de carte
  - » Tester régulièrement les systèmes et procédures de sécurité
- Disposer d'une politique en matière de sécurisation de l'information
  - » Disposer d'une politique en matière de sécurisation de l'information pour les employés et les sous-traitants

Protocoles SSL (Secure Sockets Layer) et TLS (Transport Layer Security)

SSL et sa version 3.1, appelée TLS, sont des protocoles de sécurisation des transactions réalisées via Internet. Ils ont été développés par Netscape en collaboration avec MasterCard, Bank of America, MCI et Silicon Graphics.

SSL et TLS sont basés sur le cryptage par clés publiques pour garantir la sécurité lors du transfert des données. Cette méthode de cryptage établit un canal de communication sécurisé (crypté) entre deux ordinateurs (un client et un serveur) après une étape d'authentification. La procédure s'organise comme suit[35] :

- *Authentification* — Le client doit être en mesure de vérifier l'identité du serveur. Depuis SSL 3.0 (la version la plus répandue actuellement), le serveur peut également demander au client de s'authentifier. Cette fonction est assurée par l'utilisation de certificats.
- *Confidentialité* — Le client et le serveur doivent être certains que leur conversation ne peut être entendue par un tiers. Cette fonction est assurée par un algorithme de cryptage.
- *Identification et intégrité* — Le client et le serveur doivent être certains que les messages transmis n'ont pas été tronqués ni altérés et qu'ils proviennent de l'expéditeur prévu. Ces fonctions sont assurées par la signature des données.

34. GFI Software, « Le standard PCI DSS simplifié ». *http://www.gfsfrance.com/fr/whitepapers/pci-dss-made-easy.pdf*
35. Vincent Limorte, François Verry et Sébastien Fontaine, « SSL et TLS ». *http://www.authsecu.com/ssl-tls/ssl-tls.php*

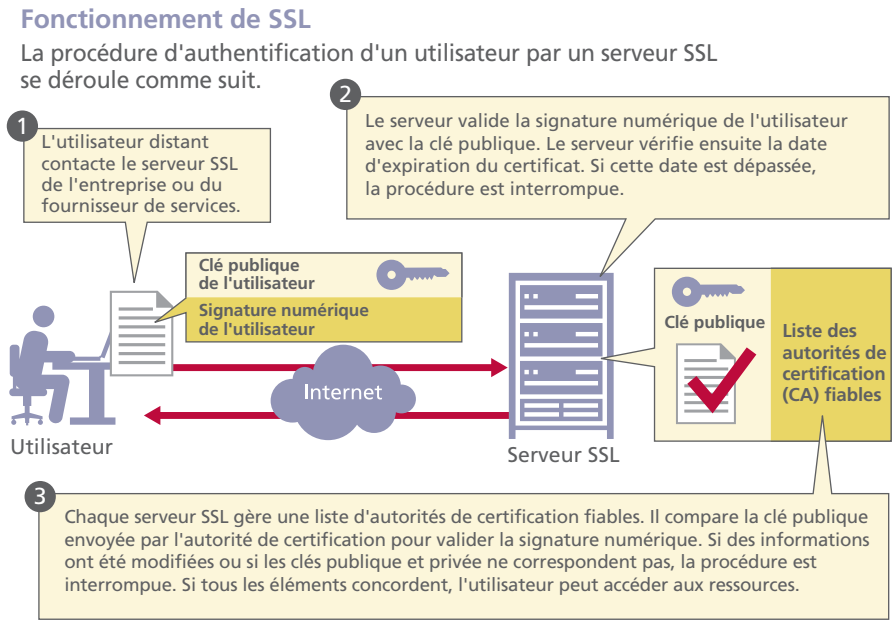


Figure 21 : Analyse du protocole SSL. (Source : Netscape)

La version SSL 2.0 étant devenue vulnérable et trop peu sûre, la norme SSL 3.0 ou TLS 1.0 a été adoptée pour garantir un cryptage efficace.

Il existe d'autres protocoles permettant d'assurer la sécurité des réseaux. Bien qu'ils offrent des fonctionnalités similaires à SSL et TLS, ils sont principalement considérés comme des protocoles complémentaires. Il s'agit des protocoles Secure Shell (SSH) et Internet Protocol Security (IPSec).

- SSH est un protocole de la couche Application qui offre une alternative sécurisée aux utilitaires classiques, tels que rlogin, rsh et telnet, lesquels ne garantissent pas la confidentialité.
- Quant à IPSec, il fournit un mécanisme de sécurité au niveau de la couche Réseau (IP). Il est principalement utilisé pour l'implémentation des réseaux privés virtuels (VPN).

L'icône représentant un verrou fermé dans la fenêtre du navigateur indique qu'il s'agit d'une session SSL. L'illustration ci-dessous propose quelques exemples.

Figure 22 : Exemples d'icônes représentant des sessions SSL. (Source : McAfee Avert Labs)

Validation étendue SSL

Internet Explorer 7, exécuté sous Windows Vista ou XP, marque les sites web en vert s'ils sont considérés comme sécurisés et s'ils possèdent un certificat SSL à validation étendue (EV). La présence de ce certificat garantit une communication sécurisée. Il propose également à l'utilisateur des informations sur le propriétaire du site web, dont l'identité est affichée dans la barre d'adresse. Firefox version 3 et Opera version 9.5 prendront également en charge ce certificat.

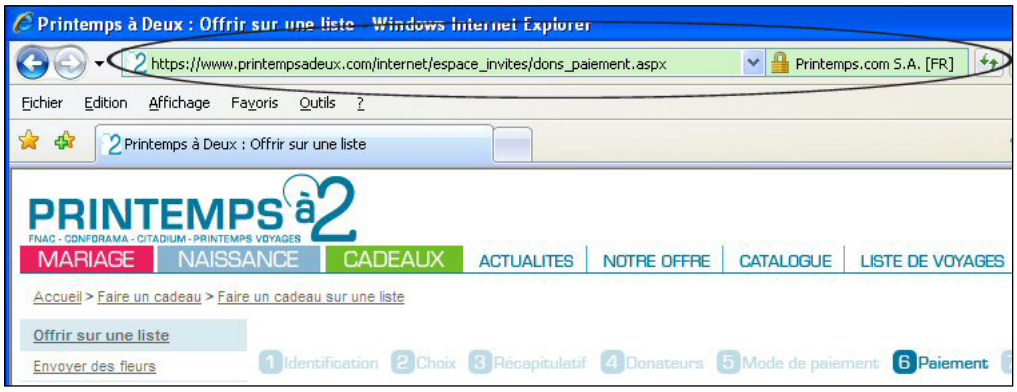


Figure 23 : Session SSL à validation étendue. (Source : McAfee Avert Labs)

Technologie 3-D Secure

L'architecture de paiement en ligne 3-D Secure (modèle à trois domaines) a été lancée en 2001 par Visa et MasterCard. Basée sur SSL et TLS, elle propose une authentification validée par un tiers. Le système 3-D Secure consiste à enregistrer préalablement les clients qui souhaitent effectuer un paiement via Internet. Il est ensuite utilisé par les marchands lors de chaque transaction en ligne distante pour vérifier si les clients sont effectivement enregistrés.

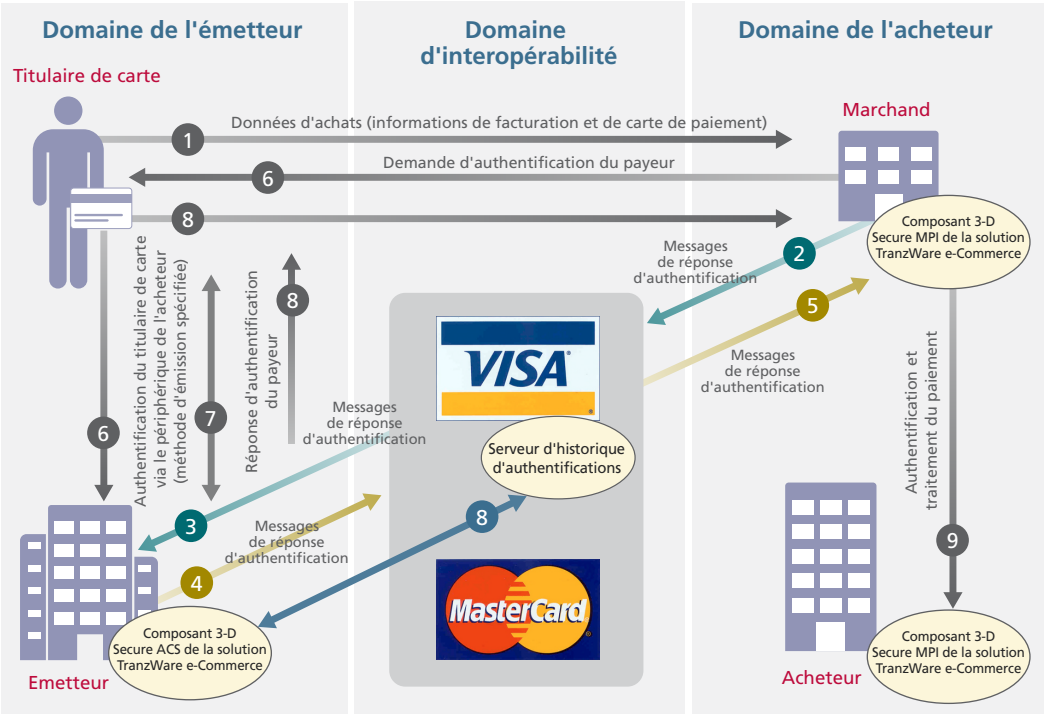


Figure 24 : Modèle 3-D Secure. (Source : Compass Plus[36])

36. *http://www.compassplus.com/TranzWare_e-Commerce.html*

Chacun des trois domaines correspond à un type d'utilisateur :

- Domaine de l'émetteur, qui inclut une fonction d'authentification du titulaire de carte
- Domaine interbancaire, qui permet aux deux autres domaines de communiquer via Internet
- Domaine de l'acheteur

3-D Secure décrit la progression des informations entre les trois domaines pour effectuer les paiements par carte, en distribuant les responsabilités de façon égale entre les domaines :

- La banque du titulaire de carte authentifie son client.
- La banque du marchand authentifie son marchand.
- Le domaine interbancaire permet au marchand d'utiliser le même moyen pour l'authentification initiale de l'acheteur, indépendamment de la méthode utilisée par l'acheteur.

Authentification forte et périphériques de génération de mots de passe à usage unique

L'authentification traditionnelle à l'aide d'un nom d'utilisateur et d'un mot de passe a depuis longtemps montré ses limites (mots de passe élémentaires, écrits sur un bout de papier à côté de l'ordinateur ou transmis en texte brut sur Internet et logiciels criminels, par exemple). D'où la nécessité d'une authentification plus forte basée sur trois éléments :

- Les connaissances de l'utilisateur : mot de passe, code PIN, question secrète
- Des éléments en possession de l'utilisateur : cartes, informations d'authentification, certificats
- Les caractéristiques physiques de l'utilisateur : un élément biométrique

L'authentification forte combine au moins deux de ces facteurs.

Les mots de passe à usage unique (ou OTP, pour one-time password) se caractérisent par une très grande flexibilité. Comme leur nom l'implique, ils sont conçus pour n'être valides qu'une seule fois. L'utilisation d'un périphérique de génération de tels mots de passe s'appuie sur deux facteurs d'authentification :

- Un objet en la possession de l'utilisateur, tel qu'une carte de crédit prenant en charge les mots de passe à usage unique
- Une information connue de l'utilisateur, telle qu'un mot de passe ou un code PIN, qui permet de déverrouiller l'objet prenant en charge le mot de passe à usage unique

Figure 25 : Calculettes de génération de mots de passe à usage unique. (Source de la photo : www.reseaux-telecoms.net)[37]

37. Source de la photo : *http://www.reseaux-telecoms.net/actualites/lire-deploiement-massif-de-calculettes-otp-pour-securiser-les-banques-en-ligne-en-grande-bretagne-17674.html*

Les mots de passe à usage unique peuvent être générés par divers moyens :

- Un jeton matériel (« token ») ou une calculette — Ces périphériques compacts affichent et actualisent les mots de passe à usage unique.
- Une carte à puce — Connectée à un ordinateur portable ou de bureau, elle peut être utilisée pour générer le mot de passe.
- Un téléphone mobile, un assistant numérique personnel (PDA) ou un ordinateur — Ces périphériques intègrent parfois des logiciels spéciaux de génération de mots de passe.

Le plug-in PayPal[38], proposé par PayPal en association avec MasterCard, est un exemple d'un tel programme. A chaque transaction, il génère un numéro de compte MasterCard. Vous n'êtes par conséquent plus obligé de saisir votre numéro de compte PayPal sur un site qui ne vous inspire pas pleinement confiance. Cette application fonctionne sur tous les sites acceptant les paiements par MasterCard.

En France, le concept de carte bancaire virtuelle n'est pas neuf. Ainsi, le GIE Carte Bleue offre, en association avec Visa, un service équivalent au service e-Carte Bleue de Visa depuis 2002 et plusieurs banques proposent aujourd'hui de tels services à leurs clients, parmi lesquelles LCL, Société Générale, Banque Populaire, La Banque Postale et Caisse d'Epargne. Cette technique de sécurisation des achats n'est cependant pas très répandue.

Les cartes sécurisées ne sont pas une nouveauté non plus. Ainsi, Bank of America en propose une, à l'instar de Citibank et de Discover. Ces cartes permettent aux clients d'effectuer des transactions en ligne sans révéler leur numéro de carte réel aux vendeurs. Cependant, à la différence de la carte sécurisée de PayPal, ces cartes sécurisées peuvent être utilisées sur quasiment tous les sites en ligne même si l'acheteur ne possède pas de carte de crédit réelle (en liant les paiements à son compte bancaire). Celui-ci peut également se servir d'une carte quelconque en tant que carte sécurisée pour ses achats, évitant ainsi de faire appel aux outils de paiement sécurisés de Bank of America, Citibank ou Discover.

En février 2008, quatre grandes banques britanniques ont annoncé à leurs clients le déploiement d'un système reposant sur des calculettes OTP, fonctionnant en tandem avec la carte bancaire du titulaire. Il consiste, pour le client, à saisir son code secret sur le pavé, en échange de quoi la calculette fournit un mot de passe utilisable une seule fois.

Authentification basée sur la connaissance

L'authentification basée sur la connaissance est très répandue aux Etats-Unis et consiste traditionnellement à répondre à des questions du type « Quel est le nom de jeune fille de votre mère ? » ou « Dans quelle ville êtes-vous né ? ». Il n'est cependant généralement pas très difficile pour les pirates de trouver les réponses, comme en témoigne le récent piratage de la boîte de messagerie électronique de Sarah Palin[39].

L'utilisation de questions secrètes générées de manière dynamique permet d'améliorer cette technique. Dans ce cas, le système génère une question sur le vif dont vous êtes supposé connaître la réponse, telle que le montant d'un de vos paiements ou d'une dépense récente, ou encore votre précédente adresse. La question est créée dynamiquement et la réponse n'est pas enregistrée en vue d'une utilisation ultérieure. Si le client ne devrait pas éprouver de difficultés à y répondre dans des délais assez courts, il n'en va pas de même pour les pirates. Ce système n'est pas encore utilisé à très grande échelle, mais son fournisseur, Verid, a été racheté par EMC en juin 2007[40].

Authentification par e-mail

Outre les techniques de sécurisation des paiements, plusieurs méthodes d'authentification contribuent à lutter contre le phishing :

- Sender Policy Framework, un standard qui vise à empêcher la falsification des adresses en s'appuyant sur des serveurs DNS pour créer une liste des adresses IP autorisées à envoyer des e-mails depuis un domaine spécifique
- Sender ID Protocol, de Microsoft, qui prend en charge Sender Policy Framework
- DomainKeys Identified Mail, qui permet de valider une identité associée à un message lors de son transfert via Internet, identité qui peut alors être identifiée comme à l'origine du message

38. Bank Systems & Technology, « PayPal's Plug-in Provides Payment Parity » (Le plug-in de PayPal assure la parité des paiements). *http://www.banktech.com/blog/archives/2008/03/paypals_plugin.html*
39. Michelle Malkin, « The Story Behind the Palin Email Hacking » (Les dessous du piratage de la boîte de messagerie de Sarah Palin). *http://michellemalkin.com/2008/09/17/the-story-behind-the-palin-e-mail-hacking/*
40. VNUnet, « EMC rachète Verid, spécialiste de l'authentification basée sur la connaissance ». *http://www.vnunet.fr/news/groupe-emc-rach-te-verid-sp-2018533*

Conclusion

Neuf ans après l'apparition du virus « I love you », de nombreux internautes demeurent vulnérables. Les optimistes affirment que ceux-ci se montrent moins impulsifs à l'heure d'ouvrir des pièces jointes et commencent à se méfier davantage des requêtes inhabituelles susceptibles d'émaner d'un site miroir. C'est sans doute vrai, mais les peu familiarisés à Internet constituent une réserve inépuisable de naïfs prêts à se laisser abuser.

Pour atteindre les plus crédules comme les plus expérimentés, les cybercriminels mettent sans cesse au point de nouveaux pièges et techniques d'attaque. C'est ainsi qu'est né le « clickjacking » (ou détournement de clic). Egalement connue sous le nom de « UI redress attack », cette faille structurelle liée au Web permet de duper les utilisateurs visualisant des pages web constituées de deux couches. Au lieu d'effectuer des actions sur la couche visible, comme ils le croient, les utilisateurs interagissent en fait avec une couche transparente placée sur cette couche visible. Ces attaques comportent deux étapes : l'interception du clic et le réacheminement de l'intention de celui-ci. Une fois le clic intercepté, l'auteur de l'attaque peut amener l'utilisateur à exécuter quasiment n'importe quelle opération à son insu — effectuer des achats ou des transferts d'argent, ajouter un contact de confiance, etc. Pour contrer cette faille, les navigateurs commencent à intégrer des fonctions de sécurité empêchant les clics sur des éléments « cachés ».

Sur fond de crise financière, les cybercriminels exploitent une multitude de faux sites bancaires.

Figure 26 : Faux sites bancaires. (Capture d'écran de McAfee Avert Labs)

Il ne s'agit pas ici de sites miroirs, mais de sites créés de toutes pièces pour attirer des personnes vulnérables auxquelles de véritables banques ont peut-être refusé un prêt. Abuser ainsi des personnes déjà en proie à des problèmes financiers est tout simplement scandaleux et démontre une fois de plus l'absence de scrupule des escrocs d'aujourd'hui, qui n'hésitent pas à profiter des plus vulnérables.

Ces dernières années, la croissance des transactions en ligne s'est accompagnée d'une augmentation des fraudes. La possibilité de gérer ses comptes en ligne, l'absence de contact entre les parties (entre l'acheteur et le vendeur ou encore entre l'internaute naïf et l'escroc sans scrupule), l'établissement de communications directes entre les ordinateurs et l'obligation de fournir un numéro de carte bancaire pour conclure un contrat sont autant de facteurs qui contribuent à la multiplication des risques.

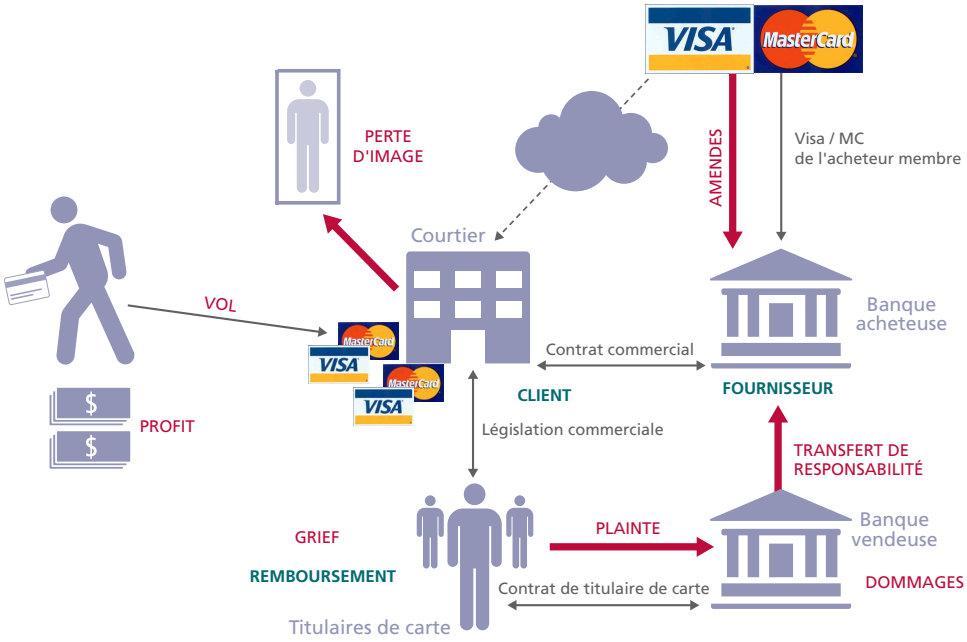


Figure 27 : Les acteurs de la vente en ligne et les problèmes auxquels ils sont confrontés. (Source : CLUSIF[41])

La carte bancaire est toujours considérée comme l'une des solutions les plus pratiques pour payer ses achats sur Internet. A l'époque où le nombre de transactions était peu élevé, le risque inhérent pouvait encore être jugé « tolérable » par les différentes parties. Mais face à l'explosion du volume de transactions, l'image de marque de certains vendeurs ressort ternie, les consommateurs sont agacés et n'hésitent pas à déposer plainte, tandis que les banques essuient des pertes dont elles se passeraient volontiers.

Face à une criminalité de mieux en mieux organisée, les banques et les grandes sociétés de vente en ligne renforcent aujourd'hui leurs infrastructures afin de mieux se protéger. De leur côté, les petites et moyennes entreprises, pour qui le commerce électronique est la clé de leur réussite future, ont un besoin vital de solutions de sécurisation qui les aident à gagner ou garder la confiance de leurs clients. Mais que ce soit par manque de formation ou par pure négligence, ces entreprises se retrouvent parfois totalement démunies face aux attaques toujours plus sophistiquées et sournoises.

Les solutions de sécurité de fournisseurs reconnus qui mettent en œuvre des outils et logiciels de gestion des dossiers et des vulnérabilités aident les entreprises à se conformer aux normes de sécurité. A l'autre bout de la chaîne, une meilleure sensibilisation des utilisateurs et la mise à disposition d'outils informatiques plus intuitifs et transparents constituent des voies d'évolution clés pour l'avenir.

41. « PCI DSS : Le paradoxe français ». *http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-CONFORMITE-SECURITE-2008-GROUPEMENT-CARTE-BANCAIRE.pdf*

François Paget est chargé de recherche sur les logiciels malveillants chez McAfee Avert Labs en France. Il participe aux recherches sur les logiciels malveillants depuis 1990 et figurait parmi les membres fondateurs d'Avert Labs en 1995. François Paget intervient régulièrement lors de conférences organisées dans le cadre d'événements sur la sécurité en France et à l'étranger. En plus d'être l'auteur d'un ouvrage et de nombreux articles, il occupe le poste de secrétaire général du Club de la sécurité de l'information français (CLUSIF).

A propos de McAfee, Inc.

Basé à Santa Clara en Californie, McAfee, Inc. est la plus grande entreprise au monde entièrement vouée à la sécurité informatique. McAfee consacre tous ses efforts à trouver des réponses aux plus grands défis de sécurité de notre époque. Il fournit dans le monde entier des solutions et des services proactifs et réputés, qui assurent la sécurisation des systèmes et des réseaux et permettent aux utilisateurs de se connecter, de surfer ou d'effectuer leurs achats sur Internet en toute sécurité. Avec le soutien d'une équipe de recherche saluée par de nombreux prix, McAfee crée des produits innovants à l'intention des particuliers, des entreprises, du secteur public et des fournisseurs de services, pour les aider à se conformer aux réglementations, à protéger leurs données, à prévenir les perturbations dans le flux des activités, à identifier les vulnérabilités ainsi qu'à surveiller et à améliorer en continu leurs défenses. http://www.mcafee.com/fr

McAfee S.A.S.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.mcafee.com/fr

6168rpt_fraud-report_0409_fnl_ETMG