



# Financial Fraud and Internet Banking: Threats and Countermeasures

By François Paget, McAfee® Avert® Labs

## Table of Contents

<b>Some Figures</b>	3
U.S. Federal Trade Commission Statistics	3
CyberSource	4
Internet Crime Complaint Center	4
<b>In Europe</b>	5
<b>The Many Faces of Fraud</b>	6
Small- and large-scale identity theft	7
Carding and skimming	8
Phishing and pharming	8
Crimeware	9
Money laundering	10
Mules	10
Virtual casinos	11
Pump and dump	12
Nigerian advance fee fraud (419 fraud)	12
Auctions	14
Online shopping	16
Anonymous payment methods	17
<b>Protective Measures</b>	18
Scoring	18
Europay, MasterCard, and Visa (EMV) standard	18
PCI-DSS	19
Secure Sockets Layer (SSL) and Transport Secured Layer (TLS) protocols	19
SSL extended validation	20
3-D Secure technology	21
Strong authentication and one-time password devices	22
Knowledge-based authentication	23
Email authentication	23
<b>Conclusion</b>	24
<b>About McAfee, Inc.</b>	26

Financial fraud has many faces. Whether it involves swindling, debit or credit card fraud, real estate fraud, drug trafficking, identity theft, deceptive telemarketing, or money laundering, the goal of cybercriminals is to make as much money as possible within a short time and to do so inconspicuously.

This paper will introduce you to an array of threats facing banks and their customers. It includes some statistics and descriptions of solutions that should give readers—whether they are responsible for security in a financial organization or a customer—an overview of the current situation.

### Some Figures

#### U.S. Federal Trade Commission Statistics

In the United States, many observers have been trying for several years to prove that financial fraud is stabilizing or decreasing. The U.S. Federal Trade Commission (FTC) is responsible for protecting consumers and monitoring competition. Its annual reports show a leveling off in the number of complaints between 2004 and 2006.<sup>1</sup> In 2007, however, the figures increased slightly.<sup>2</sup> All three FTC indicators are now on the rise.

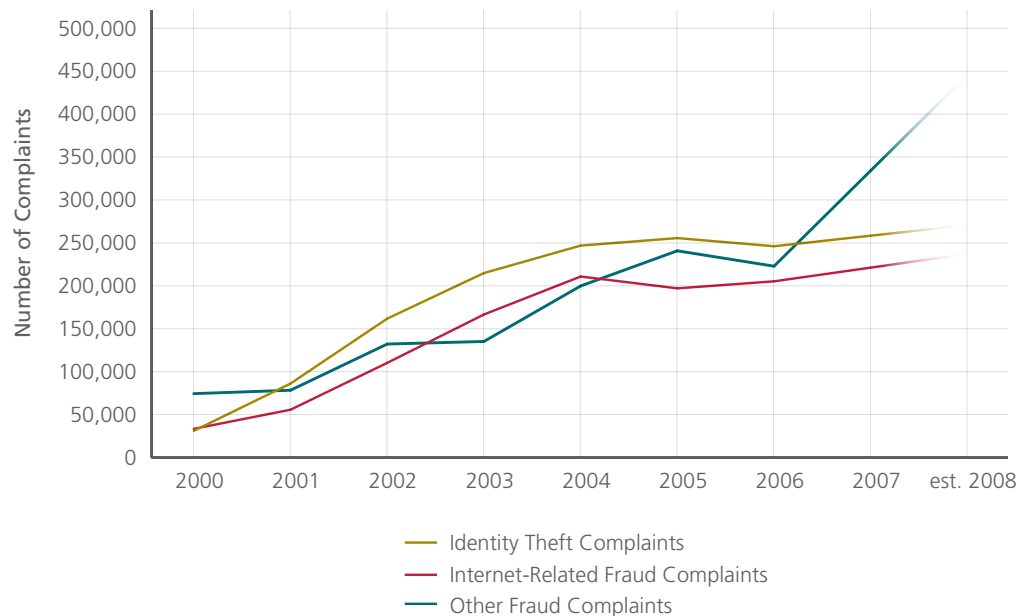


Figure 1: Annual consumer statistics from the U.S. Federal Trade Commission for consumers. (Source: FTC)

In 2008, the FTC no longer separated Internet-related fraud complaints from the total.<sup>3</sup> Figure 2 shows its new breakdown. For 2008, only 58 percent of all fraud complaints reported the method of initial contact. Of those complaints, 52 percent cited email, while another 11 percent started with an Internet website. Only 7 percent of consumers who provided statistics reported the telephone as the initial point of contact.

1. Consumer Fraud and Identity Theft Complaint Data:

Year 2004: <http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf>.

Year 2005: <http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf>.

Year 2006: <http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf>.

2. Year 2007: <http://www.consumer.gov/sentinel/pubs/Top10Fraud2007.pdf>.

3. Consumer Fraud and Identity Theft Complaint Data: Year 2008. <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf>

Contact Method	CY-2006		CY-2007		CY-2008	
	Complaints	Percentages*	Complaints	Percentages*	Complaints	Percentages*
Internet—Email	138,195	45%	152,131	50%	193,817	52%
Mail	50,317	16%	42,330	14%	51,837	14%
Internet—Web Site/Others	46,687	15%	45,447	15%	40,596	11%
Phone	39,365	13%	33,733	11%	26,067	7%
Other	31,722	10%	33,481	11%	57,695	16%
Total Reporting Contact Method	306,286		307,122		370,012	

\* Percentages are based on the total number of CSN fraud complaints for each calendar year where consumers reported the company’s method of initial contact: CY-2006 = 306,286; CY-2007 = 207,122; and CY-2008 = 370,012. 58% of consumers reported this information during CY-2008. 71% and 53% for CY-2006 and CY-2007, respectively.

Figure 2 Consumer Sentinel Network fraud complaints by contact method. (Source: CSN)

### CyberSource

Fraud as a percentage of online revenue—in the United States and Canada combined—has decreased over the past few years. It stabilized at 1.4 percent three years ago, according to CyberSource, an electronic payment and security vendor.

Overall revenue losses have nevertheless shown a marked increase. As the growth of online sales slowed during 2008, recorded losses are estimated at US\$4 billion for the American market alone. This is an increase of 11 percent in value, after a 20 percent rise the previous year.<sup>4</sup>



Figure 3: Payment fraud statistics for the American market. Although the rate of revenue loss due to online payment fraud was stable in 2008, total dollars lost to fraud have increased due to online sales growth. (Source: CyberSource 10th Annual Online Fraud Report)

### Internet Crime Complaint Center

The Internet Crime Complaint Center,<sup>5</sup> working in partnership with the U.S. Federal Bureau of Investigation (FBI) and the National White Collar Crime Center, also collects data. In 2008, Americans filed 33.1 percent more complaints than in 2007, and the total amount of money stolen online reached

4. CyberSource. 10th Annual, 2009 Edition, "Online Fraud Report." <http://forms.cybersource.com/forms/FraudReport2009NACYB5www020309>.  
 5. Internet Crime Complaint Center, "2008 Internet Crime Report." [http://www.nw3c.org/downloads/2008\\_IC3\\_Annual%20Report\\_3\\_27\\_09\\_small.pdf](http://www.nw3c.org/downloads/2008_IC3_Annual%20Report_3_27_09_small.pdf).

a historic record. The claims center registered almost 275,000 complaints, representing a loss of US\$265 million, or 10.6 percent more than in 2007.

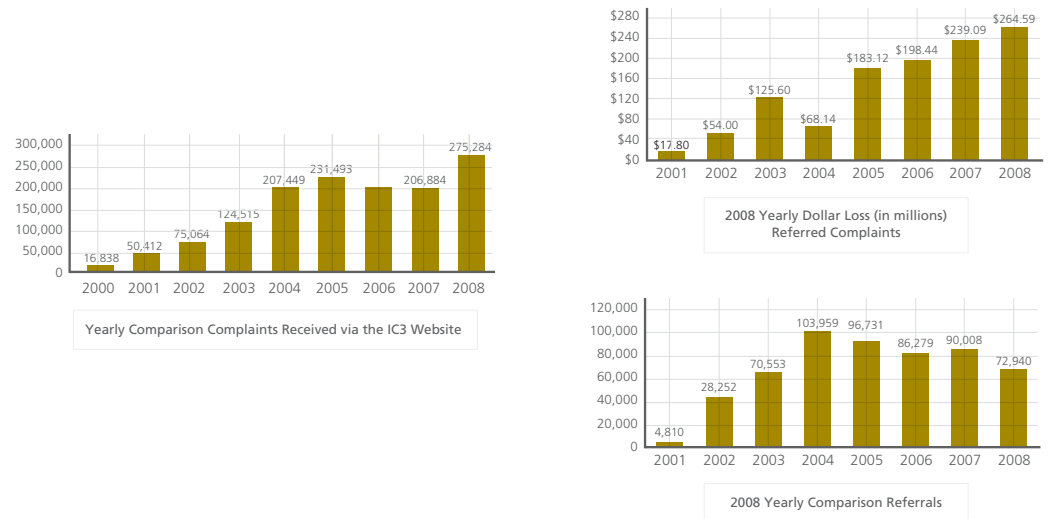


Figure 4: Internet Crime Complaint Center statistics for America. (Source: IC3 2008 Internet Crime Report)  
Half of all cases involved a monetary loss of less than \$1,000. One-third (33.7 percent) of those filing complaints reported losses between \$1,000 and \$5,000. Only 15 percent indicated a loss greater than \$5,000.

Complaint Type	% of Reported Total Loss	Average Loss per Complaint Reporting a Loss
Check Fraud	7.8	\$3,000
Confidence Fraud	14.4	\$2,000
Nigerian Letter Fraud	5.2	\$1,650
Computer Fraud	3.8	\$1,000
Non-delivery (merchandise and payment)	28.6	\$800
Auction Fraud	16.3	\$610
Credit/Debit Card Fraud	4.7	\$223

Figure 5: Amounts lost to fraud, by type, for U.S. individuals reporting a loss. (Source: IC3 2008 Internet Crime Report)

Auction fraud and the failure to deliver purchases are the most widely reported complaints. Other complaints relate to credit card fraud or even advance-fee fraud (scam). Email and web pages are the two main mechanisms for approaching victims. We find that a frequently reported scam concerns the purchase or sale of pets.

The majority of complaints come from men. Nearly half are 30 to 50 years old, and one-third of them live in one of the four most populated states in the United States: California, Florida, Texas, and New York.

**In Europe**

During the same period (2004 to 2007) and consistent with the overall North American figures, the Association for Payment Clearing Services statistics also showed a decrease in online banking fraud. In Great Britain, the sharp rise in 2006 did not continue the following year. The figures for 2007 were even

lower than the 2005 figures. This note of optimism is greatly tempered today by the results from the first half of 2008, which show a 185 percent increase compared to last year.<sup>6</sup>

	January–June 2004	January–June 2005	January–June 2006	January–June 2007	January–June 2008	Increase, 2007–2008
Online banking fraud losses (in millions)	£4	£14.5	£22.4	£7.5	£21.4	185%
Phishing incidents	126	312	5,087	7,224	20,682	186%
“Mule” recruitment offers	NA	196	468	655	873	33%

Figure 6: Online banking fraud, phishing, and money mule advertisements in the United Kingdom. (Source: APACS, the U.K. payments association)

In France, there is particular concern about risks involving remote online payments. According to the 2007 report from the Observatory for Payment Cards Security,<sup>7</sup> these transactions, which represent only five percent of the total number of “paperless” transactions (for example, transfers, debits, and cards), account for 44 percent of fraud (versus 32 percent in 2006).

In one year, e-fraud on domestic transactions went up 97 percent to €26.4 million in France.

As for international transactions, the Observatory provides figures relating only to transactions that were made using French cards abroad. Here too, we find that the rate of fraud on remote payments is higher for Internet payments than for other types of remote transactions.

Remote Payment Fraud		Amount of Fraud (in millions of euros)	
		2006	2007
Domestic transactions	By mail or phone	€19.8	€23.8
	Online	€13.4	€26.4
French issuer, foreign recipient	By mail or phone	€5.7	€7.6
	Online	€20.3	€27.4

Figure 7: Fraud distribution by transaction type in France. (Source: Observatoire de la sécurité des cartes de paiement)

Another tracking organization, the Central Office for the Fight Against ICT Related Crimes, states that 80 percent of the calls received in 2007 pertain to Internet scams.

### The Many Faces of Fraud

Often poorly protected, the personal computer is a favorite target for cybercriminals. Users are too often seduced by a wonderful offer or alerts that appear to be coming from their banks.

Mirror (phishing) sites or sites hosting malware are behind many of the attacks. The United States, Russia, China, Canada, France, and the Republic of Korea are the leading countries hosting malware, according to the Anti-Phishing Working Group.<sup>8</sup> Security firm RSA frequently adds Germany, and more recently Luxembourg, to this list.<sup>9</sup>

6. APACS, “APACS announces latest fraud figures.” <http://www.apacs.org.uk/APACSannounceslatestfraudfigures.htm>.

7. Observatory for Payment Cards Security, “2007 Annual Report.” [http://www.banque-france.fr/observatoire/telechar/rap\\_an\\_2007.pdf](http://www.banque-france.fr/observatoire/telechar/rap_an_2007.pdf).

8. APWG, “Phishing Activity Trends Report, Q1/2008.” [http://www.antiphishing.org/reports/apwg\\_report\\_Q1\\_2008.pdf](http://www.antiphishing.org/reports/apwg_report_Q1_2008.pdf).

9. RSA, “RSA Online Fraud Report, July 2008.” [http://www.rsa.com/solutions/consumer\\_authentication/intelreport/FRARPT\\_DS\\_0708.pdf](http://www.rsa.com/solutions/consumer_authentication/intelreport/FRARPT_DS_0708.pdf).

As for the brains, the former Soviet bloc countries are often singled out. Rumors even claim that the leaders of the powerful Russian Business Network (RBN) are closely linked to the government.<sup>10</sup> Until November 2007, the RBN's "bulletproof" hosting service allowed many of their affiliates to conduct all sorts of illegal activities. For about US\$600 per client per month, the organization pretended to handle complaints directed to them, all while allowing their protégés to continue their wrongdoings. With one million sites, several million available IP addresses, and four million visitors per month, the business was profitable.<sup>11</sup> Various inquiries conducted in France and in the United States have disrupted the business. As RBN disappeared, suspicion quickly turned toward the Turkish ISP Abdallah Internet Hizmetleri (AIH),<sup>12,13</sup> and then two United States ISPs (Atrivo and EstDomains).<sup>14,15</sup>

Today, experts wonder whether they are faced with a successive migration of RBN customers to other havens or whether the Russian organization has quietly set up underground networks of alliances and Mafia-like influence to continue administering a large portion of those involved in financial fraud online.

### Small- and large-scale identity theft

A person's identity forms the basis for his or her legal personality. In the real world, this identity is defined by civil status and is protected by law. In the virtual world, a person's identity is more far-reaching and its outline less clear. Some digital data dealing with an individual's identity (such as account names, user names, and passwords) provide access to private data. All these digital identifiers, which are not considered to be elements of a person's legal personality, are increasingly desirable.

The client workstation is the favorite target for cybercriminals, but many cases of lost backups or discoveries of compromised business or bank networks demonstrate that identity theft is also practiced on a large scale.<sup>16</sup>

Records Exposed	Duration	Date Reported	Organizations	Origin
94,000,000	July 2005–December 2006	January 17, 2007	TJX Companies	Deficiencies in the wireless network allowed the data theft
40,000,000	September 2004–May 2005	June 19, 2005	CardSystems, Visa, MasterCard, American Express	Malicious script injected via a web application
30,000,000	April 2003–April 2004	June 24, 2004	America Online	Data stolen by employees and sold to spammers
26,500,000	May 3, 2006	May 22, 2006	U.S. Department of Veterans Affairs	Personal data on a laptop computer stolen during a burglary
25,000,000	October 2007	November 20, 2007	HM Revenue and Customs, TNT	Loss of two CDs
17,000,000	2006–2008	October 6, 2008	T-Mobile, Deutsche Telekom	Data stolen and found online for sale
12,500,000	February 27, 2008	May 7, 2008	Archive Systems, Bank of New York Mellon	Loss of unencrypted tapes
11,000,000	July–Aug. 2008	September 6, 2008	GS Caltex	Employees made copies of personal data to sell
8,637,405	May 2001–March 2006	March 12, 2007	Dai Nippon Printing Company	Data stolen by a former contract worker and sold to a criminal group
8,500,000	2002–June 2007	July 3, 2007	Certegy Check Services, Fidelity National Information Services	Data stolen by employee and sold to a third party for marketing purposes

Figure 8: Largest data loss incidents. (Source: McAfee Avert Labs)

10. VeriSign iDefense. "Global Threat Research Report: Russia," page 23. <http://www.verisign.com/static/042139.pdf>.

11. VeriSign. "Uncovering Online Fraud Rings: The Russian Business Network," (webcast recording). <http://www.verisign.com/>.

12. David Bizeul, "Russian Business Network study," [http://bizeul.org/files/RBN\\_study.pdf](http://bizeul.org/files/RBN_study.pdf).

13. The Shadowserver Foundation, "RBN 'Rizing': Abdallah Internet Hizmetleri (AIH)." [http://digitalninjitsu.com/downloads/RBN\\_Rizing.pdf](http://digitalninjitsu.com/downloads/RBN_Rizing.pdf).

14. Jart Armin et al., "Atrivo—Cyber Crime USA." <http://hostexploit.com/downloads/Atrivo%20white%20paper%20090308ad.pdf>.

15. Washington Post, "EstDomains: A Sordid History and a Storied CEO."

[http://voices.washingtonpost.com/securityfix/2008/09/estdomains\\_a\\_sordid\\_history\\_an.html](http://voices.washingtonpost.com/securityfix/2008/09/estdomains_a_sordid_history_an.html).

16. Open Security Foundation, "DataLossDB." <http://datalossdb.org/>.

Although the number of incidents affecting several million or more data records is continuing to grow, the TJX case remains prominent in everyone's minds. Since March 2007, several resellers and users of this data have been arrested and convicted in connection with this case.<sup>17</sup> One of them, known as "Lord Kaisersose," was arrested in France in June 2007.<sup>18</sup>

### Carding and skimming

Criminals frequent and contribute to many carding sites that can be found very easily on the Internet. There, they buy or sell access to bank accounts, stolen card numbers, dumps from magnetic strips, and entire personal profiles.

On May 2, 2008, we found a set of bank accounts for sale. The most expensive was also the most highly funded: an account at European bank BNP Paribas with a balance of €30,792, selling online for just €2,200. In addition to the cut rate, the seller offered a 24-hour guarantee: if the buyer could not log in within that period or if the account no longer contained the money, a replacement account would be provided.

Bank Name	Country	Balance	Price
Bank of America	USA	...	Sold
Asmouth Bank	USA	\$16,040	€700
Washington Mutual Bank	USA	\$14,400	€600
Washington Mutual Bank	USA	\$7,950+£2,612	€500
Washington Mutual Bank	USA	...	Sold
MBNA America Bank	USA	\$22,003	€1,500
Banco Bradesco S.A.	Brazil	\$13,451	€650
Citibank	UK	£10,044	€850
NatWest	UK	£12,000	€1000
BNP Paribas Bank	France	€30,792	€2200
Caja de Ahorros de Galicia	Spain	€23,200	€1200
Caja de Ahorros de Galicia	Spain	€7,846	€500
Banc Sabadell	Spain	€25,663	€1450

Figure 9: Screen shot from a carding website.

### Phishing and pharming

Phishing is a well-known technique for obtaining confidential information from a user by posing as a trusted authority. Most often with the help of a deceptive email, the attacker redirects the victim to a mirror site.

With the help of a Trojan, it is also possible to infiltrate the link between the IP address and the server name it responds to. This is known as pharming.

In both cases, victims believe they are browsing legitimate sites. Unaware that 80 percent of bank emails are fraudulent,<sup>19</sup> many users will not hesitate to enter personal information. According to PhishTank's monthly statistics, the most popular target is PayPal.<sup>20</sup> The results show PayPal in first place by a wide margin, with other popular companies shifting positions slightly each month. eBay, which closely trailed PayPal in 2007, is often in second place.

17. Department of Justice, "Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers." <http://www.usdoj.gov/criminal/cybercrime/gonzalezIndict.pdf>.

18. U.S. District Court, District of Columbia, "Affidavit in Support of Complaint for Forfeiture."

<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 Authentication: <http://www.reuters.com/article/pressRelease/idUS191046+31-Jan-2008+MW20080131>.

20. Stats, April 2009. <http://www.phishtank.com/stats/2009/04/>.



Targets	Valid Phishing Attacks in 2009			
	January	February	March	April
PayPal	9,575	6,245	9,605	7,575
Internal Revenue Service	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: Most popular targets for phishing. (Source: PhishTank)

Although the statistics vary, the brands attacked are primarily American and English banks, according to authorities. RSA says that 72 percent of attacks are carried out against American banks, although the Anti-Phishing Working Group—an American organization devoted to eliminating scams and fraud on the Internet—reports that half of them target European organizations. Gartner estimated that the average loss per victim in the United States is US\$886.<sup>21</sup>

### Crimeware

Besides phishing, Trojans are widely popular among criminals. This class of crimeware includes password stealers and keyloggers, which log keystrokes, take screen captures, and send all data to collector sites. The amount of crimeware is increasing, and it is more effective than ever. Crimeware is often associated with rootkits, stealth programs that make crimeware completely hidden or invisible to many security tools.

Crimeware is also appearing more frequently in targeted attacks. It can then slip through detection unnoticed if the tools are unable to identify it generically or through a behavioral analysis.

A lot of crimeware is focused on virtual worlds and online games, perhaps 30 percent to 40 percent of all the hundreds of thousands of password stealers detected by McAfee VirusScan®. Much of the crimeware is detected under generic terms, but some large families are more finely classified.

- *PWS-Banker*—Bank connections
- *PWS-MMORPG*—Various multiplayer online games
- *PWS-LDPinch*—Gathers information about the system hosting it, seeks passwords stored on the disk (ICQ, TheBat, dial-up connection)
- *PWS-Legmir*—“Legend of Mir” games
- *Keylog-Ardamax*—Captures keystrokes
- *PWS-Lineage*—“Lineage” games
- *PWS-Onlinegames*—Various multiplayer online games

These are the current top password stealers; the chart below shows their frequency over the last two years.

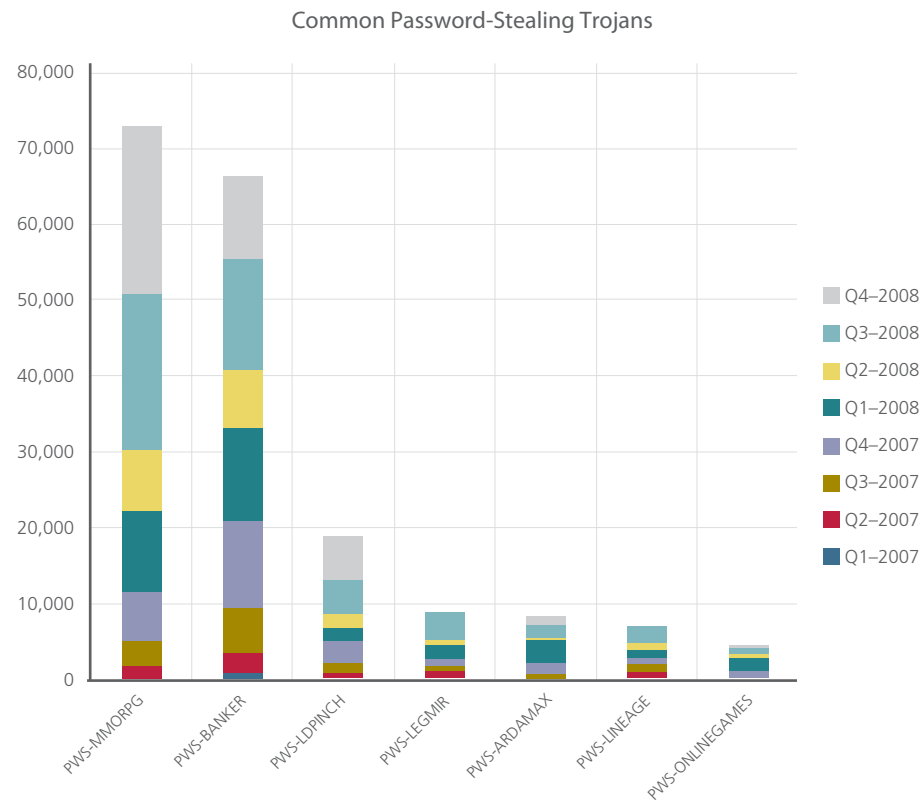


Figure 11: Variants among password-stealing malware. (Source: McAfee Avert Labs)

### Money laundering

Money laundering is required for nearly every criminal activity. In addition to the many traditional methods (including electronic funds transfer, fictional companies with foreign banks, cash smuggling, bank fraud, and informal money exchange brokers), other modern procedures, such as “mules” and virtual casinos, have emerged on the Internet.

#### Mules

Named for the transport method that smugglers used to move illegal goods, today the term describes individuals recruited over the Internet who serve as intermediaries for recovering cash in funds that were illegally acquired through phishing, keylogging, and other scams. For each transaction, the mule deducts between five percent and 10 percent of the committed amount, forwarding the balance via an anonymous money transfer service, such as WebMoney, e-gold, or Western Union.

Mules are often thought of as gullible people who were tricked by a professional-looking offer (via spam or dedicated sites). In fact, mules are rarely innocent victims. Many people who are not very concerned about the law and who are looking for easy money do not hesitate to volunteer. Today, the mule’s job is becoming a profession in itself. Recent arrests in France and in other countries demonstrate this. Four mules were formally questioned and placed under court-ordered supervision in connection with a case in May 2008.<sup>22</sup> They were at the heart of a scam targeting PayPal and eBay and were accused of “organized fraud” and “organized fraud concealment.” An accomplice, a 17-year-old hacker, is said to

22. 01net. “Quatre ‘mules’ arrêtées pour escroquerie via PayPal.” <http://www.01net.com/editorial/379382/quatre-mules-arretees-pour-escroquerie-via-paypal/>.

be currently living in Tunisia. Together, the mules are alleged to have scammed 19 French Internet users for total spoils of around €20,000. Investigators have hinted of at least another 10,000 possible victims.

In September 2007, to see how one of these offers work, I responded to a work-at-home proposal on the Internet. I then received an FAQ detailing the business.

#### Frequently Asked Questions about Freelance Job:

Q1: What do I need to do?

A: Your functions will include controlling our money flow and conducting part of the transactions. You will receive payments from our leading clients to your bank account at a time and date convenient to you and then forward the money to us. Your commission for each transaction will amount to 7%. We do NOT require any investment money on your part.

Q2: Why don't your customers make payments directly to you?

A: Customers do not transfer payments directly to us because we have no any other branches in Europe (only in United Kingdom). So we save the money on production costs and you earn 7%, which makes in profitable for both parties.

Q3: Please give me an example of the job process.

- A: 1. The customer sends the payment via his (her) bank account and notifies us. \*
2. We inform you by phone and email that the transfer is made. And send you an email (example): "Transfer has been made to your bank account. Amount is 5000 EUR from our customer Peter Tischler from Berlin, Germany. Check your account tomorrow please, withdraw money and send Western Union or MoneyGram to Kate Lewis, UK, London."
3. You go to your bank and withdraw funds.
4. Take your 7% from amount and go to Western Union or MoneyGram with remaining cash, send it to Kate Lewis, UK, London.
5. You send us details of Western Union or MoneyGram transfer and scanned copy of transfer's receipt via email.

\* Our manager will call you before bank transfer, if you are not able to receive the transfer then we'll make the transfer another day. So you can combine the work with your own schedule.

Figure 12: An FAQ from a mule recruitment site.

After an initial contact by email, I received a work contract. Considering the apparent professionalism of my contact person and the quality of the documents that I saw, an uninformed individual could fall for it. Computer security companies, banking, and the police communicate increasingly more often about these threats, but several exchanges I've had recently with the general public indicate that a lot of education is still necessary.

#### Virtual casinos

There were around 15,000 active online gambling sites in 2006.<sup>23</sup> It's unlikely that this figure has decreased since then. As there are currently only 1,766 online gambling sites operating with a license,<sup>24</sup> clandestine activity (sites conducting their business without a license) represents more than 87 percent of what is available on the Internet.

The absence of a legal structure lets anyone anonymously register an Internet site and then charge customers via an anonymous offshore bank account or virtual money system. Most of the major Russian cybercriminal groups active today (including ex-RBN and Yambo Financial) began their criminal activities through child pornography and online casinos.

23. CERT-LEXSI, "Cybercriminality of online gambling," July 2006. [http://www.lexsi.com/telecharger/gambling\\_cybercrime\\_2006.pdf](http://www.lexsi.com/telecharger/gambling_cybercrime_2006.pdf).

24. Casino City, "Online Gaming Jurisdictions" <http://online.casinocity.com/jurisdictions/index.cfm?sorttab=n/a&sortlist=sites&filterlist=&numberpage=25&searchall=1>.

### Pump and dump

Social engineering tricks, such as the circulation of false news items in forums, have long been used to manipulate the stock exchange. In 2006, we saw the rise of a popular twist in this technique: pump-and-dump stocks, a manipulation of low-priced (penny) stock usually from unattractive companies.

After purchasing a large number of shares at its low price, the manipulating purchaser would use spam techniques to send out enthusiastic messages designed to artificially raise the stock price. One or two days later, after an increase in the market, the spammer would sell at an artificially high price and reap a profit.

A study by researchers at Purdue University in Indiana and Oxford University in England noted a significant increase in both price and volume of shares traded for spammed stocks, from the day before touting begins until the day of the most active spamming.<sup>25</sup> Laura Frieder, coauthor of the study, explained who—besides the spammers themselves—were doing the trading. “Firstly, there are naive investors who are greedy and maybe not so smart—similar to the people who send thousands of dollars to Nigeria or pass on chain letters,” said Frieder. “If they attach even a very small probability of success to the idea that they can make money, they figure it’s worth a try.”<sup>26</sup>

There are people who know that the information is worthless, but they figure that if other people don’t know that, there might be a chance to make a buck. “If I think that other people are going to buy and push up the price, I might buy if I think I can get in early enough, reap a little bit of that gain, and get out,” she said.

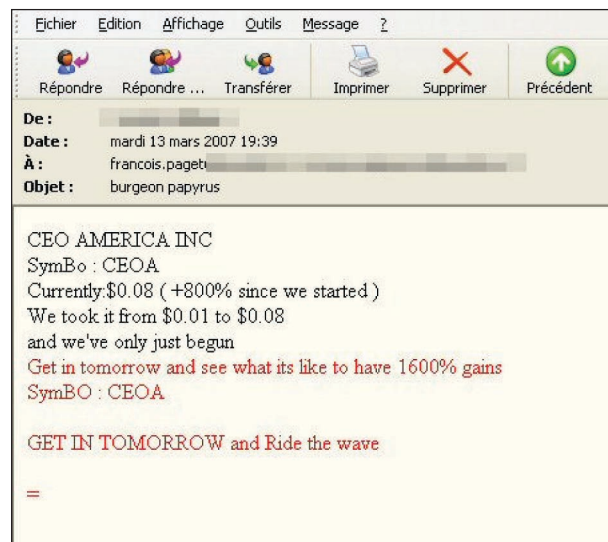


Figure 13: Pump and dump email.

The general distrust from small shareholders, the meager profits collected, and the fact that undesirable people have occasionally tried to manipulate the stock have contributed to the loss of interest and effectiveness in this form of fraud. Not having lived up to the expectations of those who invented it, pump and dump has declined in frequency.

### Nigerian advance fee fraud (419 fraud)

Named after the section of Nigerian law that covers it, “419” fraud is extremely popular and lucrative. The hoax often arrives as an email from a family member of a (usually African) dignitary. The sender explains that following the death of an influential member of his family, a large sum of money is

25. Frieder, Laura L. and Jonathan Zittrain, “Spam Works: Evidence from Stock Touts and Corresponding Market Activity.” <http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Spam%20Works.pdf>.

26. CBC, “Stock Spam: The New Boiler Room.” <http://www.cbc.ca/news/background/personalfinance/stock-spam.html>

blocked in a bank account somewhere. With the recipient's help and using the victim's financial backing for the money transfer, the sender says that it would be possible to release the money. Substantial compensation is offered to whoever agrees.

Once contact is established, the crooks request an advance. This may involve opening a bank account or paying some fees. It is followed by a series of expenses and troubles that sometimes lead to physical threats. And, of course, the blocked money does not actually exist.

In France, grammatical or spelling mistakes in the emails actually seem to build trust among unsuspecting people, rather than scare them away. The same goes for the very professional appearance of the official documents that follow.

CFA			€	S

**RECU OFFICIEL DE DEPOT DE FONDS**

RECEIVED FROM / RECU DE: MR. KONAN JOSEPH

DENOMINATION: USS 100 5.300.000USS

CURRENCY / DEVISE: USS 50, USS 20, USS 10

MONTANT TOTAL / TOTAL SUM: CINQ MILLIONS TROIS CENT MILLE DE DOLLARS AMERICAIN (5.300.000 US\$)

BUT DU DEPOSIT / 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

CAISSIER / RECEIVER'S CASHIER: Mme ELISABETH PETE

DATE: 14 Février 2003

INSPECTE PAR / INSPECTED BY: MR. KASSI EUGENE

POSITION: DIRECTEUR DES OPERATIONS BANCAIRES

A/C N°: COMPTE BLOQUE 596103487921

Stamp: BANQUE ATLANTIQUE CI SIGNATURE

Figure 14: A contract for advance fee fraud.

According to 419 AFF statistics, losses reached US\$4.3 billion in 2007:<sup>27</sup>

Country	Losses (in millions of US\$)
United States	830
United Kingdom	580
Spain	355
Germany	280
Japan	270
France	235
China	205
Australia	166
Italy	159
Canada	158

Figure 15: Losses from advance fee fraud in 2007, by companies and individuals. (Source: 419 AFF)

In France, one naive victim recently lost €1 million!

Lottery emails announcing that your email address was selected in a drawing to win millions belong to the same category of scams. The goal is to encourage the victims to spend some money while leading them to believe that it will come back to them a hundredfold.

### Auctions

Auction fraud is one of the biggest concerns among authorities. In a survey conducted in May 2008 by ConsumerWebWatch, we discovered that more than one in four New York state residents who have used an online auction (mostly eBay, Amazon.com, and Overstock.com) have experienced a scam or deceptive practice.<sup>28</sup> Eleven percent of users of online auction sites reported that they never received the goods they bid on, making this the most common complaint. In addition, seven percent of survey respondents who received their goods said that they were not in usable condition. Other complaints included not being told a key detail about the item before it arrived (seven percent) and being sent an item of lesser value than the one they actually bid on and won (seven percent).

When confronted with some kind of fraud, more than half in most age groups said they tried to resolve the problem directly with the seller. About 40 percent of victims said they filed a formal complaint with PayPal, the online payment service owned by eBay. More than 25 percent left negative feedback for the seller. In general, comparatively few respondents chose to contact law enforcement, a lawyer, or the Federal Trade Commission.

Requests for transfers via an alternative and anonymous transfer service as well as false payments are further problems that can affect both buyers and sellers. In the case of false payments to a seller, the criminal (the buyer) claims to live in a foreign country and requests a bank identifier code or an international bank agency number from the seller. This often involves the sale of a vehicle that an intermediary for the buyer will pick up. The seller's account is credited, and the car is picked up very quickly. Some time later, the payment is cancelled because the transfer was not a true transfer but, thanks to the bank identifier code, a simple check deposit. The check being insufficiently funded, stolen, or forged, the transaction is cancelled. The intermediary is often a mule.

27. 419 AFF and the media: [http://www.ultrascan.nl/html/\\_the\\_media.html](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. <http://www.consumerwebwatch.org/pdfs/surveyprerelease.pdf>.

Another sign of fraud involves asking someone to wire Western Union or MoneyGram funds. Here's an example:



Figure 16: Fake offer of a car auction.

Having suspected fraud relating to a Volkswagen offered at €7,400, a buyer contacts the seller to test his good faith. Here's the seller's reply:

*"Hello,*

*I found your message, and I thank you.*

*The vehicle has a 1900 cm<sup>3</sup> diesel engine. This engine is very nice, flexible, and powerful, very good performance for the money overall.*

*This vehicle is in perfect condition, non-smoker, no accidents, no dents, and no scratches. It sits in a garage. The maintenance book is up-to-date, all services have been done at Volkswagen dealers. I am the first owner, all the papers are in order: the maintenance book, registration, the affidavit of no lien, etc. So, there won't be any problems because it was purchased and registered in France.*

*I am currently in England, where I just got married and started my life with my family. I am selling the vehicle because of the transfer (from France to England), and because I have a company car, I have to sell the car quickly. My car is sitting in the garage at my old house in France (75003 Paris), which I just sold. In 3 weeks, the new owner is moving in, so I'm in a hurry to sell this car as quickly as possible.*

*I'm well below the market price.*

*If you want to buy the car, which is like new, give me your information (full name and address) to send to eBay. They will then send you all of the information we need to complete this transaction quickly and securely.*

*I hope all that makes sense. I look forward to receiving your contact information to confirm you as my buyer.*

*Looking forward to hearing from you!"*

After a few more exchanges in which the seller continued to avoid questions concerning his identity and the buyer's desire to see the car, the buyer received a fake email from eBay, which requested a transfer of €3,000 via Western Union. (This time, the buyer was not tricked; moreover, he knew that eBay prohibits the use of Instant Cash Transfer Services.)<sup>29</sup>



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

### Online shopping

The process of buying directly online, without a prior bid, is also subject to many attacks. You should always avoid sites that do not offer secured payments. Spam is often used to attract gullible buyers. If the products exist at all, they are often counterfeits or placebos. In its 2007 security report, IronPort<sup>30</sup> uncovered an attack that more closely resembled organized crime than online commerce.

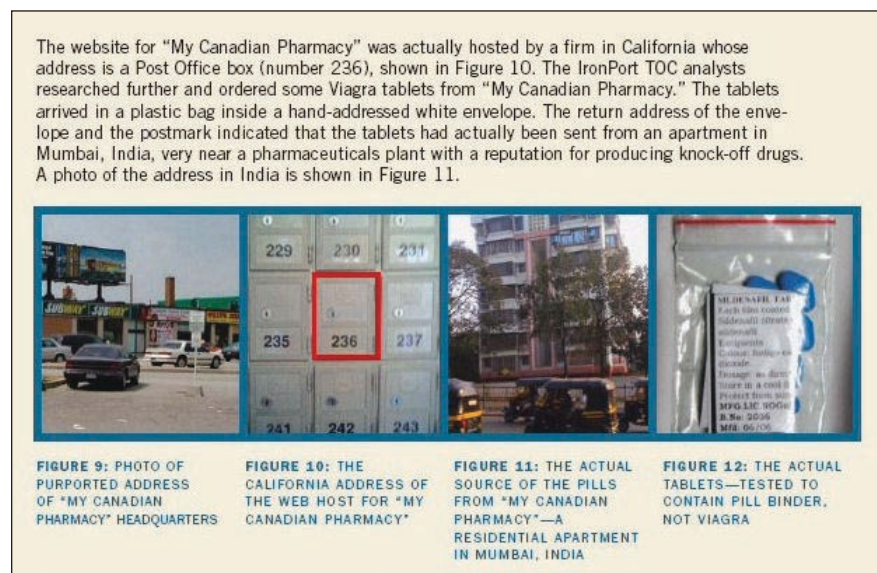


Figure 18: Extract from the "Canadian pharmacy" scam. (Source: IronPort Internet Security Trends for 2007 Report)

Another method of duping buyers consists of getting positioned prominently in search engines. The client is then redirected to a shopping site selling all sorts of pills, counterfeits, or software at one-tenth of their normal price. It is much easier, for example, to find counterfeit Vertu phones from the luxury division of Nokia for sale than it is to find originals.



Originals VERTU phones:	VERTU Replica phones:
Are manufactured at one of NOKIA's factories	Are manufactured at one of NOKIA's factories in Hong Kong
Range between 5000 and 68,000 Euros in price	Cost between 550 and 1500 Euros
Are made of amorphous 'Liquidmetal'	Are made of top-quality steel and titanium
Contain gold and platinum	Are covered by real gold and silver using hi-tech IPG methods
Are laced with diamonds and rubies	Are laced with semi-precious stones from Swarovsky
Have sapphire glass	Have a durable plastic anti-gleam screen
Are covered with top-quality leather from Northern Europe	Are covered with top-quality natural leather, which is no worse than that from Northern Europe

**NEW PRODUCTS:**



 <p><b>VERTU SIGNATURE GOLD HALF PAVE DIAMONDS</b> An exclusive VERTU Signature replica with Diamond Crystals and...</p> <p><b>\$999.00</b> Original Price: \$68,500.00</p> <p><a href="#">Details</a> <a href="#">Add to Cart</a></p>	 <p><b>VERTU SIGNATURE GOLD POLISHED</b> Simply a CLASSIC! The VERTU Signature Gold Polished Replica phone is ceramic...</p> <p><b>\$859.00</b> Original Price: \$13,000.00</p> <p><a href="#">Details</a> <a href="#">Add to Cart</a></p>
---	--

Figure 19: Counterfeiting website.

### Anonymous payment methods

Criminals prefer payments using services such as e-gold and WebMoney. There are about twenty such services in the world. They are anonymous and convenient.

In France, unlike notaries and banks approved by the banking commission, online payments services are not required to file statements of suspicion to TRACFIN (the French acronym for Information Processing and Action Against Clandestine Financial Networks) when there is suspicious activity or when a transaction exceeds a certain amount.

In the United States, the Financial Crimes Enforcement Network<sup>31</sup> is responsible for collecting bank statements, analyzing them, and actively advising investigation services regarding money laundering. This administrative service was integrated into the Department of the Treasury.

Here are a few leading money-transfer services:

- *e-gold*—Founded in 1996, its headquarters are in Florida. The authorities have long suspected the company of involvement in illegal activities. Its founders and some of its partners are currently under investigation.
- *Western Union*—This American company has branches in more than 200 countries. The service, which should be used only for money transfers to family members, is often misused.
- *WebMoney*—This Russian company carries out US\$7 million in transactions daily. It has four million customers, not all of whom are honest.

Other services—including MoneyGram, Money Express, Ria, Flouss, and DabaDaba—are also used in suspicious money transfers linked to criminal activities.



Figure 20: A Russian website that offers a service for distributed denial-of-service (DDoS) attacks

### Protective Measures

Financial fraud often starts with the diversion of personal information. A trash or recycling bin, a telephone conversation, or a poorly protected computer can be the starting point for fraud.

Businesses are often vulnerable as well. Stolen laptops and data loss can lead to lasting damage to its brand image and heavy financial consequences for the company itself or its customers. In this respect, banks find themselves on the front line.

Although it is impossible to completely eliminate the chance of becoming a victim of identity theft, individuals can effectively reduce their risk by following some commonsense recommendations. (We discussed many of these recommendations in the McAfee Avert Labs paper “Identity Theft.”)<sup>32</sup> Here we will identify a few techniques that are directly associated with the banking world.

### Scoring

Scoring is a risk-analysis technique that estimates the likelihood of a successful end (without fraud) to a transaction. Scoring gives weight to the various pieces of information related to the purchase and its buyer (email address, contact information, origin of the IP address, size of the order, and other data). The transaction is or is not authorized depending on the total score obtained.

### Europay, MasterCard, and Visa (EMV) standard

EMV is the standard for smart-card payments. This standard makes it mandatory to pay with cards that have an integrated chip rather than a magnetic strip. The Bank for International Settlements is pushing for the new international EMV standard to be adopted throughout Europe and then worldwide. By 2010, there may be more than 800 million smart cards in circulation.<sup>33</sup>

32. [http://www.mcafee.com/us/local\\_content/white\\_papers/wp\\_id\\_theft\\_en.pdf](http://www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf).

33. CARTES 2007, “CARTES & IDentification 2007 evaluate the SEPA situation.”  
[http://fr.cartes.com/ExposiumCms/cms\\_sites/SITE\\_319050/ressources319050/cp\\_sepa-fr.pdf..](http://fr.cartes.com/ExposiumCms/cms_sites/SITE_319050/ressources319050/cp_sepa-fr.pdf..)

### PCI-DSS

Facing up to the evolution of cybercrime, the Visa and MasterCard networks established a standard aimed at protecting cardholders when they purchase online. The Payment Card Industry Data Security Standard (PCI DSS) makes it possible to improve transaction security and banking data storage. It's an international standard that is also supported by other card networks, such as American Express, JCB, and Diners Club.

Organizations that accept payment card transactions are duly bound to comply with this standard. If they do not, they may be prohibited from manipulating cardholder data. They can also be fined up to US\$500,000 if data is lost or stolen.

PCI-DSS sets forth 12 security conditions, Visa's "Digital Dozen." They are organized into six categories:<sup>34</sup>

- Establishing and maintaining a secure network
  - » Set up and maintain a firewall configuration to protect cardholder data
  - » Do not use the default passwords or other security settings provided by suppliers
- Protecting cardholder data
  - » Protect stored data
  - » Encrypt cardholder data and all other sensitive information transmitted through public networks
- Maintaining a vulnerability management program
  - » Use and regularly update anti-virus programs and software
  - » Develop and maintain the security of systems and applications
- Implementing strict access-control measures
  - » Limit access to only the cardholder data that the user needs ("need to know")
  - » Assign a unique identifier to each person who has access to the computer
  - » Limit physical access to cardholder data
- Regularly testing and monitoring the networks
  - » Track and monitor all access to network resources and cardholder data
  - » Regularly test the security processes and systems
- Maintaining an information security policy
  - » Maintain an information security policy for your employees and contractors

### Secure Sockets Layer (SSL) and Transport Secured Layer (TLS) protocols

SSL and its Version 3.1, called TLS, are ways of securing transactions carried out over the Internet. These protocols were developed by Netscape in collaboration with MasterCard, Bank of America, MCI, and Silicon Graphics.

SSL and TLS are based on public-key cryptography to guarantee security while transferring data. The method establishes a secure (encrypted) channel of communication between two machines (a client and a server) after an authentication step. They include the following features:<sup>35</sup>

- *Authentication*—The client must be able to verify the server's identity. Since SSL 3.0 (currently the most widespread version), the server can also request that the client authenticate itself. This feature is provided through the use of certificates.
- *Confidentiality*—The client and the server must be assured that their conversation cannot be heard by a third party. This feature is provided by an encryption algorithm.
- *Identification and integrity*—The client and the server must be assured that the transmitted messages have not been truncated or modified (maintaining integrity) and that they come from the expected sender. These features are provided by the data signature.

### How SSL works

These are the steps an SSL server goes through to authenticate a user.

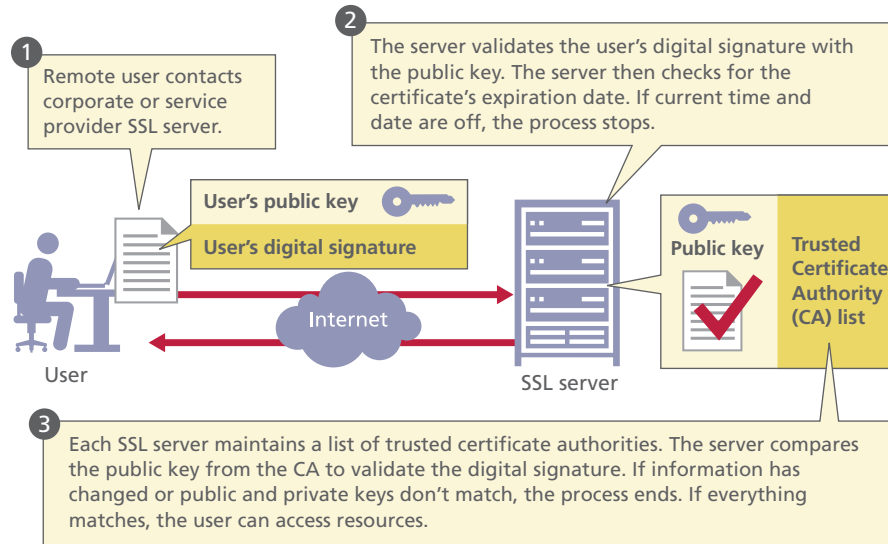


Figure 21: An analysis of SSL. (Source: Netscape)

Because SSL 2.0 became too weak and vulnerable, effective encryption requires either SSL 3.0 or TLS 1.0.

There are other protocols that ensure network security. Although they offer features that rival SSL and TLS, the others are considered primarily as complementary protocols. These are Secure Shell (SSH) and Internet Protocol Security (IPSec).

- SSH is an application-level protocol that offers a secure alternative to classic utilities—such as rlogin, rsh, and telnet—which do not offer confidentiality
- IPSec provides a security mechanism at the network layer (IP). It is primarily used for implementing virtual private networks.

A closed lock icon in the browser indicates the use of an SSL session. For examples, see below.



Figure 22: Some SSL session lock icons. (Source: McAfee Avert Labs)

### SSL extended validation

Internet Explorer 7, running on Windows Vista or XP, marks websites in green if they are deemed secure and have an extended validation SSL certificate. The presence of this certificate guarantees that the communication is secure. It also makes information available to the user about the website's owner, whose identity is displayed in the address bar. Firefox Version 3 and Opera Version 9.5 will support this certificate.

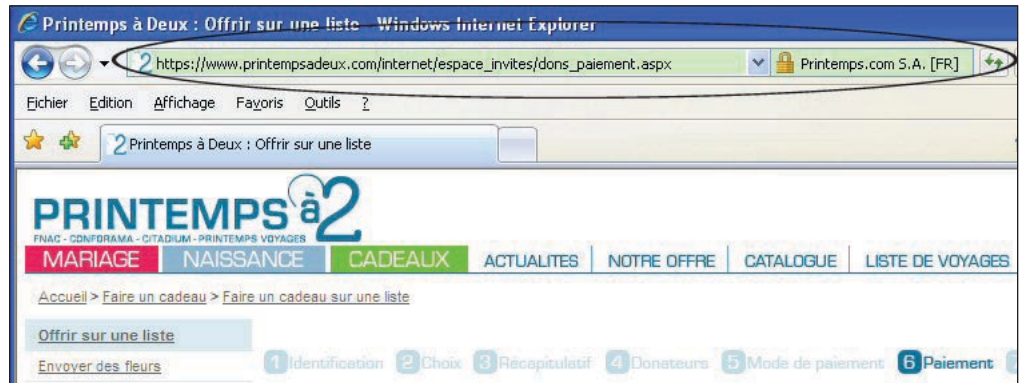


Figure 23: An SSL extended validation session. (Source: McAfee Avert Labs)

### 3-D Secure technology

The online payment architecture 3-D Secure (for three-domain security) was launched in 2001 by Visa and MasterCard. Based on SSL and TLS, it offers authentication validated by a third party. 3-D Secure consists of preregistering customers who would like to pay over the Internet, and then it is used by merchants during each remote online transaction to verify whether customers are truly registered.

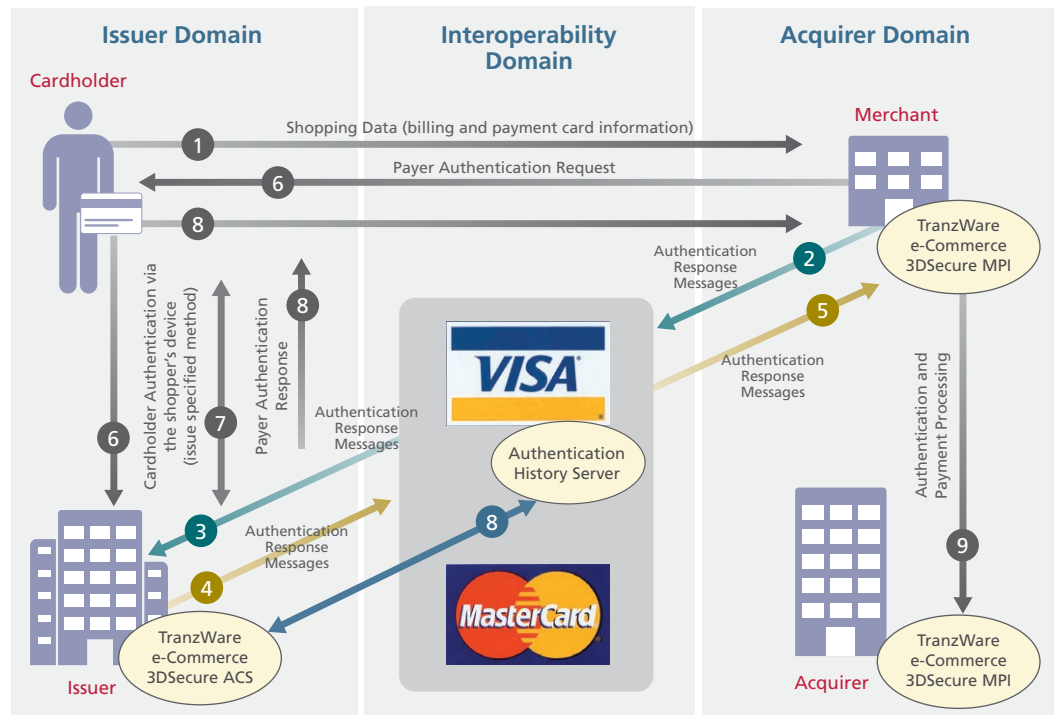


Figure 24: The 3-D Secure model. (Source: Compass Plus<sup>36</sup>)

Each of the three domains corresponds to a user type:

- Issuer domain, which includes a cardholder authentication feature
- Interbank domain, which allows the other two domains to communicate over the Internet
- Acquirer domain

3-D Secure describes the progression of information among the three domains to carry out card payments, distributing the responsibilities equally among the domains:

- The cardholder's bank authenticates its customer
- The merchant's bank authenticates its merchant
- The interbank domain allows the merchant to begin authenticating the buyer the same way, regardless of the method used by the buyer

#### Strong authentication and one-time password devices

Traditional authentication by username and password has long shown its limits (for example, trivial passwords, passwords written on paper next to the computer, passwords sent as plain text over the Internet, crimeware). These limits have created a need for stronger authentication that uses three elements:

- What the user knows: password, PIN, secret question
- What the user has: cards, authenticators, certificates
- What the user is: a biometric element

Strong authentication uses at least two of these factors.

A one-time password (OTP) is very flexible. As its name implies, it is designed to be valid only one time. Using an OTP device adds a second authentication factor:

- The first concerns something the user has, for example, a credit card that supports OTP
- The second is something the user knows, for example, a password or PIN. This is used to unlock the object that supports the OTP.



Figure 25: A one-time password calculator. (Photo source: [www.reseaux-telecoms.net](http://www.reseaux-telecoms.net)<sup>37</sup>)

There are various ways to generate OTPs:

- A “token” or calculator—Compact devices that display and refresh the OTP
- A smart card—Connected to a laptop or desktop computer, this can be used to generate the password
- A mobile phone, PDA, or computer—These devices sometimes have special software for generating passwords

One example is the PayPal Plug-in,<sup>38</sup> which is offered by PayPal in association with MasterCard. With each transaction, the plug-in generates a MasterCard account number. It is no longer necessary to enter your PayPal account number on a site that may not inspire confidence. The application works with every site that accepts MasterCard payments.

In France, the virtual banking card concept is not new. Since 2002, the GIE Carte Bleue offers a service with Visa that is equivalent to Visa’s e-Carte Bleue. Today, customers can get these services from several banks: LCL, Société Générale, Banque Populaire, La Banque Postale, and Caisse d’Epargne. But this method of shopping is not yet popular.

Secure cards are also not new. Bank of America offers one, as do Citibank and Discover. These features allow clients to use their cards online without exposing their actual card numbers to the vendors. However, what is different with PayPal’s secure card is that buyers can use a secure card almost anywhere online without having actual credit cards (if they link the payments to their bank accounts). Or, they can use any card of their choosing as a secure card for purchases, thus sparing the need to rely on BofA’s, Citi’s, or Discover’s secure payment tools.

In February 2008, four major British banks announced that they were deploying OTP calculators, which work with their owners’ bank cards, to their customers. In exchange for entering its secret code on the keypad, the calculator provides a password that can be used only once.

### Knowledge-based authentication

Knowledge-based authentication is widely used in the United States. The traditional method consists of answering questions such as “What is your mother’s maiden name?” or “In what city were you born?” Yet it is often easy for an attacker to find the answers. The recent hacking of Sarah Palin’s email box is just one example.<sup>39</sup>

Using dynamically generated secret questions improves this method. In this case, the system creates a question at runtime whose answer you should know, such as the amount of one of your payments, the amount of a recent expense, or even your address from the previous year. The question is created dynamically, and the answer is not stored for later use. Although the customer is likely to answer fairly quickly, a criminal will surely not be able to. This system is still not widely used, but the vendor Verid was purchased by EMC in June 2007.<sup>40</sup>

### Email authentication

In addition to payment security methods, there are several methods of authentication that help fight phishing:

- Sender Policy Framework is a standard for preventing the falsification of addresses. It relies on DNS servers to create a list of authorized IP addresses to send emails from a specific domain.
- Sender ID Protocol, from Microsoft, supports the Sender Policy Framework
- DomainKeys Identified Mail makes it possible to validate an identity associated with a message during its transfer via the Internet. This identity can then be held responsible for the message.

38. Bank Systems & Technology, “PayPal’s Plug-in Provides Payment Parity.” [http://www.banktech.com/blog/archives/2008/03/paypals\\_plugin.html](http://www.banktech.com/blog/archives/2008/03/paypals_plugin.html).

39. Michelle Malkin, “The story behind the Palin email hacking.” <http://michellemalkin.com/2008/09/17/the-story-behind-the-palin-e-mail-hacking/>.

40. VNUnet, “EMC purchases Verid, a specialist in knowledge-based authentication.” <http://www.vnunet.fr/news/groupe-emc-rach-te-verid-sp-2018533>.

### Conclusion

Nine years after the “I love you” virus appeared, many Internet users remain vulnerable. Optimists say that users are less impulsive about double clicking on email attachments and that they are beginning to be wary about unusual requests, such as a mirror site may present. This may be true, but new Internet subscribers form an inexhaustible reserve of naive people.

To reach the gullible as well as the experienced, cybercriminals are developing new attack methods and new traps. One example is clickjacking. Also known as UI redress attack, this web-related structural weakness can fool users when they view a web page made of two layers. While users believe they are performing actions on the visible layer, they are actually interacting with a transparent layer on top of the visible layer. These attacks consist of two steps: intercepting the click and rerouting its intention. Once the click has been intercepted, the attacker can make a user do almost anything without his knowledge—make purchases or money transfers, add a trusted contact, and more. To counter this weakness, browsers are beginning to add security features that prevent clicks on “hidden” elements.

Against a background of financial crises, cybercriminals are taking advantage with a multitude of fake banking sites.

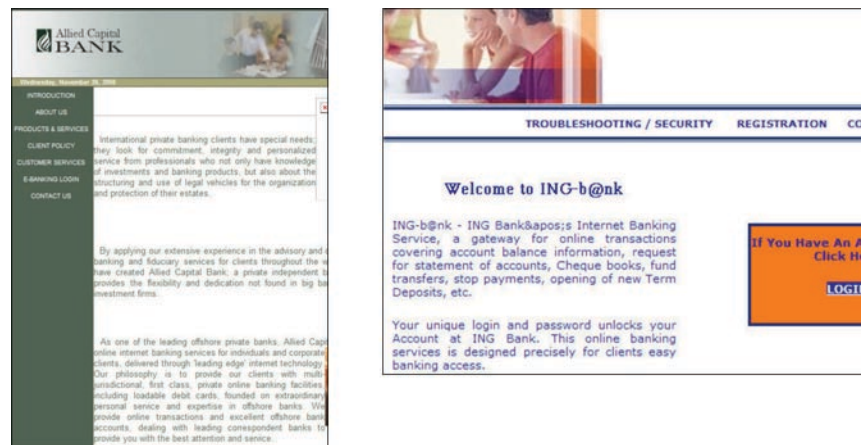


Figure 26: Fake bank sites. (Screen capture by McAfee Avert Labs)

These are not mirror sites, but sites created from scratch to attract vulnerable people whose authentic banks have perhaps denied them a loan. To abuse people who are already victims of financial problems is scandalous. This shows, as if more proof were necessary, that today's crooks have no misgivings about taking advantage of the most vulnerable among us.

In recent years, the increase in online transactions has been matched by an increase in fraud. The ability to manage your account online, the lack of contact between parties (between buyer and seller, and between naive Internet user and unscrupulous crook), the fact that communications take place directly between two computers, and the fact that an agreement requires a bank card number to be entered all multiply the risks.



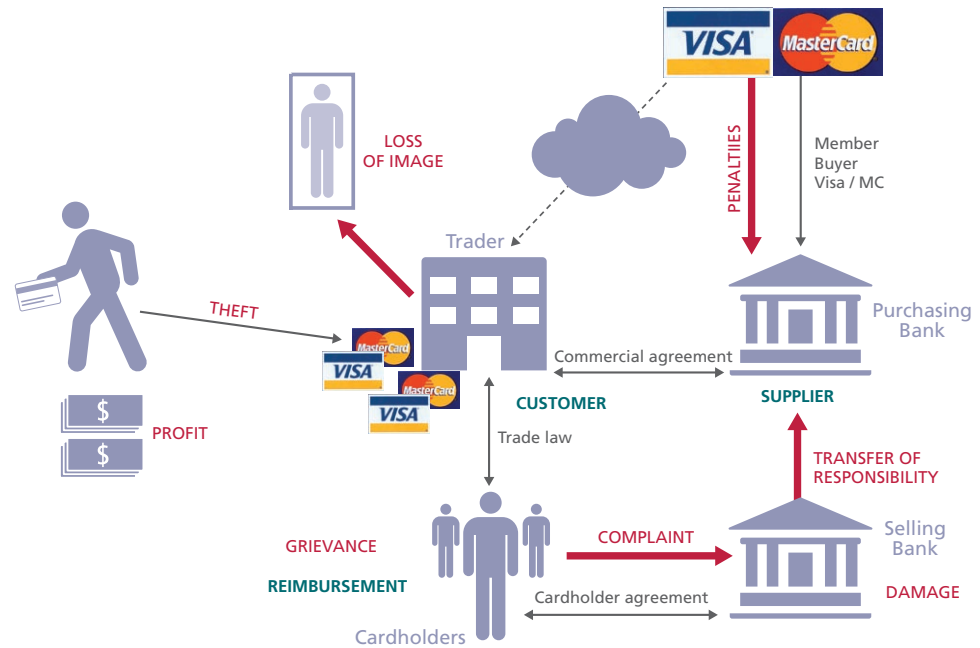


Figure 27: The players of online sales confront their problems. (Source: CLUSIF<sup>41</sup>)

Payment using bank cards is still regarded as one of the best methods of paying over the Internet. When the number of transactions was still low, the inherent risk could be deemed “tolerable” by the different parties. But today, with such high volumes, the brand image of some traders is deteriorating. Consumers are annoyed, and they complain, and banks are suffering losses they would rather avoid.

Faced with crime that is continually becoming more professional, banks and large online sales companies are strengthening their infrastructures to better protect themselves. For their part, small and medium-size businesses, for which e-commerce is the key to a prosperous future, have a vital need for security solutions that help them earn or keep the confidence of their customers. Because of the lack of training or pure negligence, these companies sometimes find themselves helpless in the face of attacks that are increasingly more sophisticated and underhanded.

Security solutions from recognized vendors that implement tools and software for managing records and vulnerabilities help companies comply with security standards. At the other end of the chain, increasing awareness among users and the availability of more intuitive and transparent security tools for computers are key development areas for the future.



François Paget is a senior malware research engineer at McAfee Avert Labs in France. He has been involved in malware research since 1990 and was a founding member of Avert Labs in 1995. Paget is a regular conference speaker at French and international security events, author of a book and numerous articles, and general secretary of the French Information Security Club (CLUSIF).

#### About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. <http://www.mcafee.com>.

This document is intended only to provide general educational information to McAfee customers and potential customers. McAfee provides this document and the information contained herein "as is," with no implied or expressed warranties as to the accuracy, merchantability, or fitness for a particular purpose. Advice and opinions contained herein are those of the authors and do not necessarily reflect the views or opinions of McAfee, Inc.