

Identity Theft: A New Frontier for Hackers and Cybercrime

By Claudio Cilli, Ph.D., CIA, CISA, CISM, CISSP

Internet Identity Theft

There is a relatively new and dangerous threat that people should recognize—even if they do not use a computer to carry out electronic commerce or financial operations when they interact with public and private administrations in the course of their daily lives. In truth, this is an old problem—if a person succeeds in assuming all of the characteristics that identify a victim in the archives of various administrations (fiscal registry office, banks, public offices, etc.), that person can commit criminal actions without fear of being discovered. The responsibility will be attributed to the unaware victim. A famous novel by the Italian writer Luigi Pirandello, *Il fu Mattia Pascal* depicts the opposite situation, but it is similar in some aspects. The poor victim is listed as deceased in the records of the registry office, and she is not able, due to the bureaucracy, to demonstrate that she is alive and in good health. Therefore, she cannot find a job, open a bank account, etc.

The situation shown by Pirandello was paradoxical at the time in which it was written, but today, when transactions are completed through networked computers, offices do not exchange printed documents but streams of data, and people are identified by a few thousand bytes, the problem is dramatically real.

Definition

Identity theft can be defined as the use of information about a person obtained from the Internet, with the purpose of identifying oneself as that person to take illegal actions. The Internet is not the only medium through which identities are stolen. However, it is the main one, because its increasing diffusion and the tendency to make use of it to carry out operations that used to require people to visit several offices (paying banking bills, conducting general transactions, signing contracts) have increased its dangerousness.

Why It Happens

Criminals always pay attention to the development of technologies, much more than the designers do. Before a new instrument is diffused, it is already known how to profit from its weaknesses for illicit purposes. For example, when it was first introduced, few people used the ATM, but the tools to make clones of ATM cards existed. When the data transmission era began and modems were introduced to allow computers to communicate, hackers had already discovered holes in the public telephony network and found a way to make free calls.

Identity theft is a means to commit frauds—it is not the objective. Progress has supplied cybercriminals with this new opportunity to take advantage of people, and its consequences are devastating. Identity theft can be used to:

- Commit frauds directly. The most innocuous use of a victim's data is to use the information to obtain access to pornographic sites; however, other uses, such as making big purchases with the victim's money, have far more serious consequences. The victim will work hard to demonstrate his/her innocence, but it may be impossible.
- Sell the data to others so they can commit frauds. There is already proof of data banks, paradoxically sold on the Internet, with all the necessary information to impersonate those whose data were stolen. It is a large market, and it continues to grow.
- Snatch economic information and spy on bank accounts. This is not a true identity theft, but the snatched information is used to illicitly inquire into the private sphere of the victim to gain advantages.
- Open new credit positions. The data of the victim can be used as warranty to obtain lenders and advanced financing exceeding the criminal's own possibilities, or to open checking accounts with several banks online.
- Generate new forms of illegality.

These are the most common illegal consequences of identity theft, but there is no limit to the criminal mind.

How It Happens

Identity theft is an extremely sneaky threat that can be put into effect in many ways, including:

- Stealing from a pocket/purse containing identification documents, credit cards, personal information, passwords and PINs. Passwords and PINs should never be carried together with the cards.
- Theft of correspondence or an error by the postal worker who puts mail in the wrong mailbox
- Intercepting/reading e-mail. The protocol used for e-mail, SMTP, is intrinsically insecure; it does not offer certainty about the authenticity of the sender, and it does not prevent the information in transit from being read by unauthorised users.
- Intercepting data in transit on the computer
- Penetrating the computer with special programs (spyware)
- Using personal information supplied by registering to web sites
- Obtaining information from the workplace (theft of financial and personal information) by hacking files or taking paper documents or notes left unattended

- Purchasing personal data from illegal data banks
The information necessary for assuming a victim's social profile is everywhere:
- Financial information
- Fiscal data (assurances, taxes, communications with public administration, etc.)
- Personal identifying data and banking information, which are often stored in the computer

How Identity Thieves Use Victims' Personal Information

The main consequences of identity theft, drawn from archives of investigation agencies and the complaints received from victims, are:

- Modifying the e-mail address used in the victim's relationships with others
- Opening new bank accounts with the victim's identifying data
- Using the data to obtain access to pornographic web sites that request proof of age by showing a credit card
- Withdrawing money from the victim's bank accounts
- Charging purchases on the victim's credit cards until the limit is reached

However, there are numerous other consequences to identity theft. The most significant damage suffered by victims is often not economic in nature, but emotional. Victims not only have to prove that their financial privacy has been violated, but they also have to fight long, hard battles to assert their good name and to reconstruct their economic good standing.

Identity Theft Statistics

The following statistics as well as those provided in figures 1 and 2 demonstrate the widespread threat of identity theft:

- There were more than 635,000 known cases of identity theft in 2004, up from 82,094 in 2002, 52,658 in 2001 and 21,756 in 2000. In other words, identity theft increased by 800 percent from 2002 to 2004 (source: CERT, 2003).
- Symantec has recorded 689 attacks to financial institutions; 48 percent of these were serious (source: Symantec, 2003).
- Symantec has recorded 616 attacks to e-commerce sites; 19 percent of these had serious consequences (source: Symantec, 2003).
- 24 percent of attacks perpetrated by hackers are intentional, and 76 percent are opportunistic (Symantec, 2003).
- More than 200,000 identities are stolen every year.
- The Internet gives criminals a new way to snatch personal information:
 - Criminals created a fake eBay site to steal personal credit card numbers and data entered by customers who believed the site to be the real eBay (these types of frauds are so common that a name has been given to them: phishing).
 - Criminals create sites that pretend to offer job opportunities and ask for personal information from the customers.

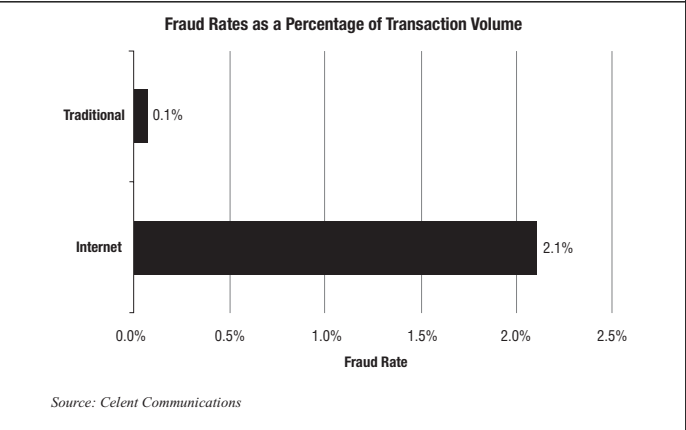
Identity theft is not just a problem in the US, where the widespread diffusion of the Internet and computer technologies is extensive, but also in many other countries and regions, such as the European Union, where identity theft has cost more than €4 billion in the last five years.

Identity theft certainly results in significant financial costs,

but there are other costs as well, such as damage, the negative impact on the banking system that generates distrust from customers, and the time involved in additional computer security training (figure 3).

Figure 1 – US Federal Trade Commission's Top Categories in 2004 for Consumer Fraud Complaints

Identity theft	39%
Internet auctions	16%
Other (miscellaneous)	12%
Shop-at-home/catalog sale	8%
Internet services and computer complaints	6%
Foreign money offers	6%
Prizes/sweepstakes and lotteries	5%
Advance-fee loans and credit protection	3%
Business opportunities, including work-at-home	2%
Telephone services	2%



Spam

A serious problem related to identity theft is spam, which is an unsolicited commercial e-mail with a massive distribution. Numerous variants exist, including requests for assistance, claims for lottery winnings and worms. Since the person who receives it did not request the message, many reply complaining (and thus send some personal data, including proof that their e-mail addresses exist), which is exactly what the sender wants.

Figure 2 – Resulting Abuses of Stolen Identities

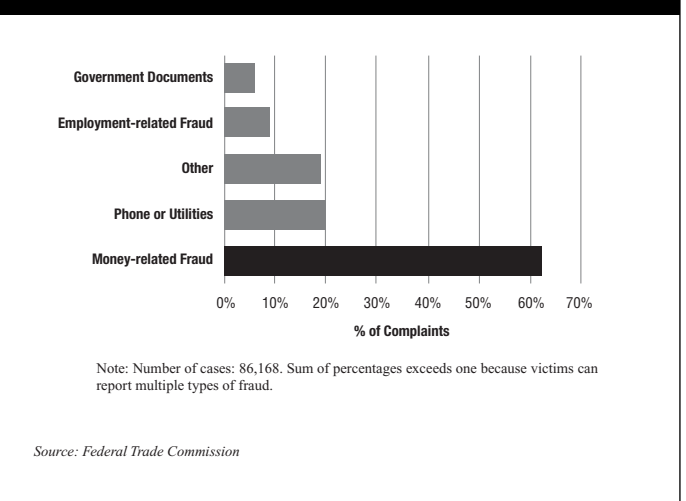
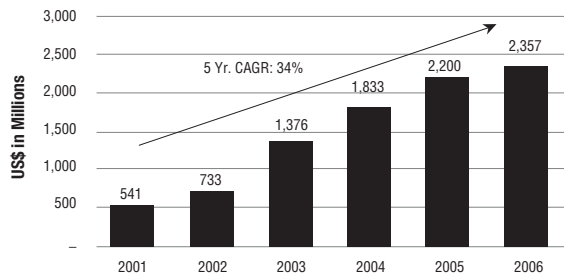


Figure 3—Indirect Identity Theft Cost Incurred by US Financial Institutions



Note: Cost includes US dollars spent on technology, legal fees, personnel and training, and consumer education.

Source: Celent Communications

Spam results in economic damage to the recipient as a result of productivity loss. In fact, the recipient spends much more time than the spammer who sends the message. What if someone falls in the trap put forth in the e-mail? Spam is the only kind of publicity paid by the addressees even if they do not buy the publicized product. The cost of writing and sending the message is insignificant. The message can be automatically sent to millions of e-mail addresses randomly generated; many correspond to real persons. Spam is convenient for the sender even if only one reader among a million buys the product. This explains its increase in use.

Various techniques have been proposed to mitigate spam, including charging senders to send the e-mail and filtering spam with proper software using two main filtering methods: blacklisting (lists sites from which spam messages come, automatically deleting messages from those sites) and content filtering (analysis of the content of messages to determine if the message should be discarded). The two methods are not completely secure, so they are often used in combination.

Spyware

Spyware is a technology that helps in obtaining information about people or organizations without their knowledge. More than 250 spyware applications currently exist on the Internet; that makes it one of the newest and most dangerous types of threat.

The prevention is not simple, and it is based almost exclusively on the potential victim's knowledge of the problem and adoption of adequate policies and procedures aimed to prevent the infections. From a technological point of view, recognizing the presence of spyware is difficult as the evidence of spyware is not obvious. Antivirus programs are not often able to signal their presence, while antispyware programs, such as Ad-aware, often are not effective, especially if they are used alone. Removing spyware is a complex activity that demands great skill. The automatic removal programs are not enough. It is necessary to act manually on critical system files.

Reducing the Risk of Becoming a Victim

The following tips are recommended for limiting the risk of becoming a victim of identity theft:

- Limit the information in purses, wallets, pockets, etc.

Information Privacy Resources

Following is a list of web sites where additional information on privacy and identity theft can be found:

- International Association of Privacy Professionals (www.privacyassociation.org)
 - Privacy International and the Electronic Privacy Information Center—Annual review of privacy laws in more than 50 countries worldwide (www.privacyinternational.org/survey)
 - US Federal Trade Commission (www.ftc.gov/privacy/index.html)
 - Electronic Privacy Information Center (www.epic.org)
 - International Security, Trust and Privacy Alliance (www.istpa.org)
 - Online Privacy Alliance (www.privacyalliance.org)
 - Privacy Exchange (www.privacyexchange.org)
 - Privacy Forum (www.vortex.com/privacy.html)
 - Privacy Page (www.privacy.org)
 - Privacy Rights Clearinghouse (www.privacyrights.org)
-
- Do not supply information to an unsolicited service.
 - Sign a contract with an identity protection service.
 - Know the people to whom you are giving personal information on the Internet and why they need it.
 - Supply only the information that is absolutely necessary to complete the transaction.
 - Make online purchases from known companies only.
 - Regularly verify credit card statements.
 - Use credit cards instead of debit cards, as credit cards allow expenses to be contested.
 - Do not supply the same password used for company network access for the web site registrations. Change passwords often, and do not to use obvious names.
 - Regularly update the antivirus software.
 - Verify the security patches available for the operating system. Install only those coming from secure and known sources.
 - Do not download files from unknown sites.
 - Use a personal firewall, especially if using a high-speed connection or DSL line for the Internet access.
 - Use software for the browser that makes use of cryptography for data sent on the Internet.
 - Before getting rid of a computer, destroy all the personal data it contains.
 - Define a policy for the hiring of staff and consultants.
 - Limit the access to company data with a policy based on the need-to-know principle.
 - Assign every customer an unequivocal identification code.
 - Install and control a network firewall.
 - Use cryptography for all personal data accessible via the Internet.
 - Use cryptography for all the data sent via the Internet.
 - Do not use the standard security settings supplied by the vendor, but personalize the configuration to individual necessities.
 - Do not leave disks, CDs or documents with personal data unattended.

- Destroy data and media that are no longer necessary.
- Regularly verify security systems and procedures.
- Carry out intrusion tests (penetration tests).
- Immediately investigate every suspected violation of privacy or improper use of financial data.
- Use only Internet service providers (ISPs) that offer assurance of security.
- Destroy every document before throwing it in the garbage.
- Sign credit cards immediately.
- Destroy expired credit cards.
- Carry only a few blank checks—not an entire checkbook.
- Conserve banking papers, financial documents, tax receipts, etc., in a secure place, possibly outside the house.
- Do not to carry tax identification numbers, passwords and PINs, passports, birth certificates, bank receipts or personal telephone numbers, unless absolutely necessary.

Conclusion

Spyware is the fastest growing online threat. Studies show that nine out of 10 Internet-connected PCs are infected with spyware. Chances are, nearly all computers are infected, putting confidential information and a computer's performance at risk. In addition, spyware programs morph frequently.

The number of identity theft crimes appears to be rapidly growing. Further collection and analysis of complaint data are necessary to better understand the nature of identity theft crimes and to devise effective prevention and enforcement policies. While identity theft has received a great deal of

attention in the past few years, there is still much to learn about such crimes. Current data sources give some indication of the prevalence of identity theft; however, more detailed information about the nature of such theft is needed. Increasing people's understanding of identity theft will enable them to determine how successful various prevention and enforcement policies are and allow for development of more effective strategies for combating identity theft.

While studies are being conducted to make the Internet more secure, there is something people can do now to lessen the potential consequences of Internet identity theft. First, follow the rules and suggestions explained in this article. Second, when faced with malware on a PC, do not panic and do not start deleting files. Identify the malware and learn as much about it as possible. People who try to execute "repairs" without proper information or skills often create more damage than any virus could. Finally, do not forget the "golden rule": always, always, ALWAYS have a backup.

Claudio Cilli, Ph.D., CIA, CISA, CISM, CISSP

is a professional information security consultant. He is responsible for IS audit and security projects for many firms, including organizations in civil and military sectors. He has designed and implemented information systems based on mainframes and distributed architecture, including disaster recovery, data and physical security, information and site protection. Cilli is the president of the ISACA Rome (Italy) Chapter and a past chair of the ISACA Standards Board.

Information Systems Control Journal, formerly the IS Audit & Control Journal, is published by the *Information Systems Audit and Control Association, Inc.* Membership in the association, a voluntary organization of persons interested in information systems (IS) auditing, control and security, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of the Information Systems Audit and Control Association and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *Information Systems Control Journal* does not attest to the originality of authors' content.

© Copyright 2005 by Information Systems Audit and Control Association Inc., formerly the EDP Auditors Association. All rights reserved. ISCA™ Information Systems Control Association™

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by the Information Systems Audit and Control Association Inc., for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org