# Internet Users at Risk:
# The Identity / Privacy Target Zone

**© Stephen E. Arnold**
President, Arnold Information Technologies
Postal Box 320
Harrod's Creek, Kentucky 40027 U.S.A.
*Web Site:* http://www.arnoldit.com
*Contact:* ait@arnoldit.com

"Security on the Internet. There is none. Get over it" is a statement that has been attributed to Scott McNealy, President of Sun Microsystems—and about a dozen other high-profile technology executives. The pithy statement echoes one-line gags from Groucho Marx. But privacy and security in a public network is not a joker.

## Privacy Target Zone

Anyone who uses the Internet without stringent privacy measures enters an "Internet Target Zone."

As the Internet swells beyond 200 million users worldwide, concerns about protecting privacy may be ballooning even faster. There is growing evidence that the general public has begun to sense just how tenuous their right to privacy has become. A recent *Business Week* / Harris poll found that 57 percent of Americans believe that "the government should pass laws now for how personal information can be collected and used on the Internet."

Neither the telephone, the motion pictures, the radio, or broadcast television engendered the fast-changing, spectre-like security challenges of the Internet. Enter the zone. Take your chances at:

**Online Shopping.** Consider electronic commerce credit transactions. Electronic commerce runs on credit card transactions. Handing over a credit card at a restaurant causes little if any security jitters. A *newbie* or Internet newcomer to the Internet encounters a fuzzier, less tangible world. In a restaurant, a customer who is a victim to credit card theft believes he can go back to the establishment, find the owner or manager, and seek satisfaction. On the Internet, the crime can be as difficult to grasp as a shadow, a digital one at that.

Almost two-thirds of Internet users who shop online more than once a week are women, according to a new survey by PeopleSupport, an Internet customer service provider. About 19 percent of Internet users shop online once a week, 22 percent do so once a month and 43 percent are infrequent Internet shopper. Just under 16 percent have never shopped online. Over 60 percent of frequent shoppers have been online for more than five years but 20 percent have only been using the Web for less than three months. Just over a third those who shop online more than once a week would prefer to get product information by electronic mail, while 26.5 percent would like live text chat, six percent self-help and 32 percent a toll-free number.[1]

Millions of online shoppers click “Yes, I would like to receive information about this product” buttons. Blithely indifferent to opt-in marketing schemes, these consumers are throwing gasoline on the privacy inferno.

**Monitoring Actions.** Clicks, downloads, preferences, purchases, electronic mail, voice messages sent via Internet telephony—all these actions can be watched, processed, and counted. A generation of children are coming of age when classrooms are viewable by parents who want to keep tabs on their progeny.

In a small town near Louisville, Kentucky—hardly a hotbed of Internet innovation—the Web cams have arrived. One wonders how students will react to the radical change in classroom pri-

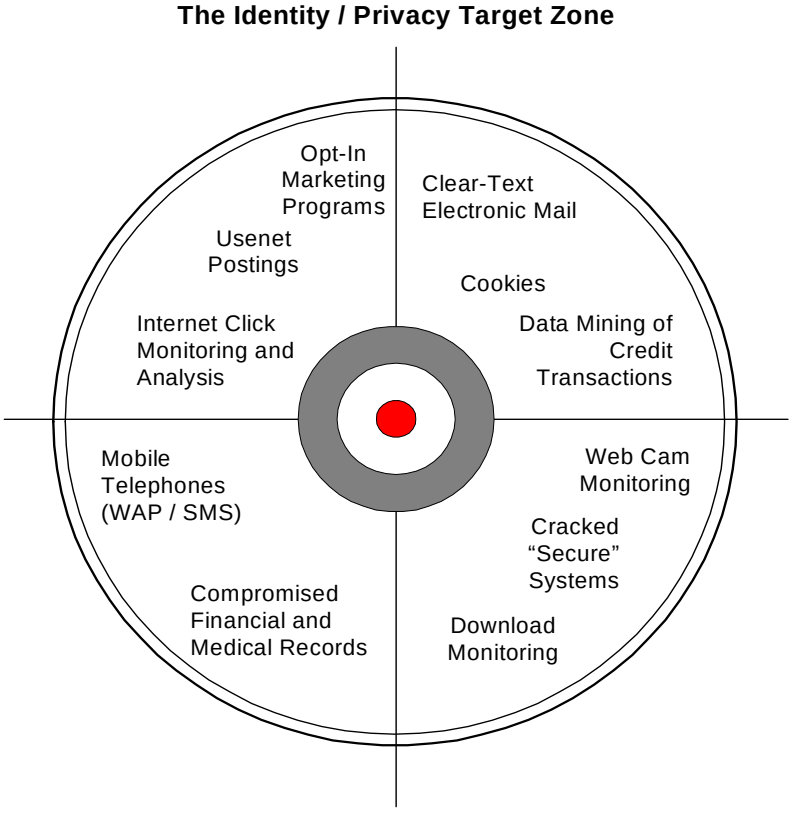



**FIGURE 1. An Internet user becomes a target for wrongdoers who would like to capture information that can be used to create a false identity, purchase products without concern for payment, and obtain information that could be used for illegal or improper activities.**

1. These data come from a recent study sponsored by Peoplesoft. The results were posted by Nua, an Internet consultancy, at:www.nua.ie/surveys/ in July 2000.

vacy. One wonders if a pedophile will use the feed to select and target victims after he or she snags a user name and password.


**FIGURE 2. A school in rural Kentucky will allow parents and other authorized "viewers" to observe classroom activities at this school for pre-high school students.**

Security has another connotation as well. The Internet revolution embraces digital video as readily as millions of electronic mail messages. A relative, voyeurs, or worse can check up on their progeny by clicking to a Web site. Web cams—video cameras that feed their signal into an Internet server—broadcast the activities in front of the CCD lens.[2] What if a pederast compromises the system and uses it to target a victim.

**Data Mining.** Amazon.com is one of the most respected Internet retailers by the general public. Amazon offers customers a way to "personalize" their shopping experience. By providing information to Amazon, the customer can get access to what Amazon calls "recommendations." Using sophisticated software tools, Amazon can map a customer to a cluster, perform some mathematical calculations, and create a list of books or records that other customers who are similar have purchased. The data mining and affinity algorithms enrich a registered user's shopping experience as though a live person were quietly, unobtrusively accompanying the customer.

2. A CCD lens is a combination of optical and digital technology. The light strikes a "charge coupled device." The "image" is converted into ones and zeroes and can be immediately fed to a server for real-time access via the Internet to the image and sound captured by the camera.

Amazon also offers “Purchase Circles,” a summary of book purchases by corporate account. A person interested in the reading at major consulting firms can quickly compare A.T. Kearney’s purchases with Booz, Allen & Hamilton’s, a feature some might find mildly entertaining.


**FIGURE 3. Amazon greets a registered user by name and suggests products that the data mining and affinity software determines would be of high interest to a particular customer. The software is making an effort to perform helpful, added value services for a registered user and increase Amazon’s sales to a particular customer**

## The Lingo of Security

The terminology of privacy and security is arcane. Part of the reason is a direct result of what might be called “security’s unspoken rule.” The rule is, “Never talk about security to untrusted individuals.” A soupçon of paranoia wafts among the world of security. There is more than a grain of truth in the old joke, “If I tell you, I will have to kill you.” The problem now is that with an exploding user community awareness of privacy, security, identity theft, and several other incendiary issues is sorely needed.

The table below provides a short list of the terminology that fills popular and trade press writing:

**TABLE 1. Security Jargon**

| Term | Definition |
|---|---|
| Affinity marketing | Once a person is placed in a cluster, mathematical algorithms can predict certain pattern or predispositions of behavior for the group. No individual action can be predicted, but in an affinity group, a certain number of individuals will adopt the predicted behavior. Affinity group marketing, therefore, allows a person in a group who bought X to be offered product Y. The marketer knows that a certain number of people will buy Y because they bought X. |
| Agents | Scripts that perform specific tasks and are equipped with some type of mechanism that allows the script to take different actions depending upon a situation. At this time agents cannot readily communicate with one another. However, inter-agent communication promises to create a new class of more flexible, effective automatic data collection and analysis functions. |
| Black or dark site | These are sites that have not been updated or sites that have closed but may be available in the cache of some servers. |
| Cookie | a handle, transaction ID, or other token of agreement between cooperating programs. 'I give him a packet, he gives me back a cookie.' The claim check you get from a dry-cleaning shop is a perfect mundane example of a cookie. Less powerful than cgi-bin scripts that can programmed to perform ET functions. Cookies are prevalent. |
| Cracking | Controversy surrounds the distinction of "cracker" and "hacker" and "cracking" and "hacking." A cracker is a person who enters a site with malicious intent. |
| Data mining | A series of routines that look at data, make decisions about how the data relate, and then output reports about the content of large collections of information that a person may not have been able to review because of the large amount of information in the collections; for example, a year's collection of American Express credit card users' transactions. |
| Encryption | Encoding a clear text message so that it is a collection of normally unreadable letters and symbols. |
| ET | A program that is sent from one computer to another, usually unbeknownst to the recipient. The program builds a collection of information and then transmits these data to its home base. "ET" is a play on the motion picture where an extraterrestrial creates wants to "phone home"; that is, send information from one remote place to a home base. |
| Hacking | A person who explores for personal satisfaction or from curiosity the ins and outs of software, hardware, and systems. |
| Identity theft | A person steals such information as another person's Social Security Number, credit card number, and checking account information. Using these "proofs" of identity, the criminal pretends to be someone else, running up charges against the dupe's accounts. |
| Kerberos | A network authentication protocol that allows one computer to provide its identity to another across an insecure network through an exchange of encrypted messages. Once identity is verified, the protocol gives each computer an encryption key for a secure session. |
| Opt-in marketing | An Internet user knowingly or unwittingly provides an electronic marketer with permission to resell or use the address for direct marketing of other products and services. |
| Password | A secret string of words and numbers that is used to prove to an online system that a person logging on to the system is the person he or she is supposed to be. |
| Pervasive network | A wireless or broadcast connection or a land-line connection to the Internet exists wherever the Internet user wants to connect. The connection can be "live" for whatever interval the Internet user requires or desires. |

**TABLE 1. Security Jargon**

| Term | Definition |
|---|---|
| PKI | Public Key Infrastructure is a system that will allow people to obtain encryption codes and permit authorized recipients to view a document that has been changed from clear text to an unreadable format. The "key" is needed to read the message. PKI assumes a standard for "keys" that is widely used and easily available. Canada is one of the leaders in PKI an is the world's first multi-certificate authority PKI. |
| Single Sign On | A software program that automatically replaces many passwords with a single point of entry. |
| Sniffer | A script that look for words, phrases, terms, concepts, and tendencies in digital messages. Sniffers are difficult to detect, since they operate at the server level and provide few, if any, traces of their presence. Network latency may provide an indication of a sniffing process' presence. Separate software is required to interpret what the "sniffer" senses. |
| Spider | A script designed to traverse a Web site by following links. It can be set up to copy an entire site or to save specific types of files or data. |
| Spoofing | Making a message or process appear to come from another source. Because systems and users "trust" known sources, spoofing allows a wrongdoer to entered the target system. |
| User name | The name an individual uses to identify himself or herself to an online system. |
| WAP SMS | The Wireless Application Protocol allows mobile devices to receive Web pages that are properly encoded. The Short Messaging Service allows a mobile device to send a text message entered with a keypad or stylus from a properly equipped device. Voice and text messages can be intercepted. |

Some evidence of the lack of solid facts about how vulnerable Internet systems are to users who want something for nothing falls readily to hand. Consider Pay Pal, an online payment system that allows a person to purchase a product from an eBay seller using a credit card. Pay Pal was designed to eliminate the need for the buyer to go to a bank, buy a money order, mail or send via an express service the payment, and then hope the seller would ship the product the day payment was received. Pay Pal cut out some of the process, making the seller happy to get the money faster and the buyer happy because leg work was chopped out of the process.

But for some new Pay Pall customers, setting up an account on a service like Pay Pal has become more annoying than the trip to the bank. The would-be Pay Pal user must wait for a secure Web site to download and then paint the scree. The customer-to-be fills out a long, complex, detailed form. One inevitable question is, "Will Pay Pal protect my personal information?"[3] The would-be user then must wait two or more weeks for a password to be mailed by U.S. Postal Service to a street address. Armed with the mailed notification, the would-be Pay Pal user then must log on the site, use the code number in the mailed letter from Pay Pal, and transfer up to $500 in funds billed to a credit card. The would-be user then must wait another seven to 12 days for the credit card account to be verified. Once the funds have been verified, another electronic mail is sent to the would-be customer with the notification that Pay Pal is now ready for use. The elapsed time can

3. Toysmart got in hot water when it advertised the sale of its customer list in the *Wall Street Journal*. The U.S. Federal Trade Commission has taken action to halt the sale of Toysmart's customer database. After Toysmart went out of business, its principal asset was the customer data. Walt Disney Co., a principal owner of Toysmart, has been tarred by the uproar over privacy concerns that exploded in a class action suit to block the sale of personal data that Toysmart allegedly said it would never divulge. Other companies that may try to sell customer information include Boo.com and CraftShop.com.

easily extend to three weeks to a month or more. The verifications include user identity, user's physical address, and credit card validity. Trust is not something Pay Pal assumes.

Why?

## More Silence, Please

Talking "off the record," finance and security executives say that more than 30 percent of Web credit card transactions cause some type of problem. A large percentage are fraudulent. Security professionals know to keep their lips zipped. Security is a problem that is best discussed by insiders—regardless of what side of the law each is on.

Network security is a serious business. A search of Lexis Nexis or Northern Light returns precious little information about security breaches at financial services firms, stock brokers, defense contractors, insurance companies, and Fortune 500 companies. Incidents occur, but the understanding is that security concern is a deal breaker. Network security is a complex job, and it is nearly impossible for technical professionals to keep up with the fixes, settings, and configurations necessary to keep hackers, crackers, thieves, and misguided teens at bay.

When a problem occurs, it has to be one too big to cover up. The Los Alamos security set up lost hard drives with sensitive nuclear information. The devices turned up behind a copy machine. The hue and cry over security fell away quickly. Yet even minor security stories are bad for business.

Equally startling is the report from ZD Net concerning America Online's privacy peccadilloes.[4] In a lawsuit naming AOL/Netscape, the plaintiff alleges that the company's Smart Download feature, which is a component of some America Online installations, illegally monitors downloads of executable files with the extension ".exe" and ".zip."

The law firm of Abbey, Gardy & Squitieri has sued AOL in federal court in New York, claiming that the software developed by Netscape Communications Inc.'s illegally monitors users' actions. AOL acquired the software when it bought Netscape in November 1998.

The Smart Download service is automatically activated whenever a user downloads files from the Web. The suit claims that Smart Download captures and transmits back to Netscape uniquely identifiable information when a person visits a Web site and downloads software.

The suit says, "Unbeknownst to the members of the Class, and without their authorization, defendants have been spying on their Internet activities." With this information, it is possible to create a profile of a customer's file transfers. The music and entertainment industries are interested in getting the names and other information about people who may have downloaded copyright music or films.

In addition to compromising the privacy of its subscribers voluntarily, AOL has also earned the dubious distinction as one of the most hacked services on the web. Just last month the company

4. Lisa M. Bowman, ZDNet News, AOL/Netscape hit with privacy lawsuit, July 07, 2000.

was once again forced to admit that vandals had broken into its service and gained access to an undisclosed number of member accounts.[5]

AOL, however, is far from being alone in drawing the ire of an ever more privacy conscious public.

An anonymous Internet user filed suit last May against Yahoo, charging that the company violated both state and federal law, as well as its own privacy policy when it handed over personal information to another company that was suing him for defamation.

Answer Think, an online consulting group, requested the information after "Aquacool_2000" posted a number of derogatory remarks about the company on a free message board maintained by Yahoo. One of the many questions at stake is what right companies have to disclose personal information about private individuals utilizing their services. Where does free speech end and fair disclosure begin?

For those who do not know how systems work, the wireless connections and the high-speed lines that bring music and video to the computing device look like magic of a high caliber. Books foster the metaphor as well. A best-seller in 1998 told the story of the Internet under the title *Where Wizards Stay Up Late*.[6] For those who have a $250 per year to spend, Privacy Times offers a newsletter that will curdle the blood of the most ardent Internet surf-and-be-damned soul.[7] Not surprisingly "instant books" have been rushed through the publishing process to capitalize on a growing anxiety about security. A recent example is Jerome Schneider and Allison Hope Weiner's *Hiding Your Money.* The subtitle hits the fear button, "Everything you need to know about keeping your money and valuable safe from predators and greedy creditors."

"Identity-theft remains at the top of the list of privacy violations," said Evan Hendricks, who runs the watchdog *Privacy Times*. If you use the Internet a lot, you have to cross your fingers and hope all that data you are forking over isn't used against you. It is very much the wild, wild West out there."

## "Virtual" Criminals

Identity theft is an old crime given a jolt of digital Internet steroids.

The Internet allows a person who steals a credit card or another's identity to be hidden from detection. The clever thief becomes a virtual identity, operating through a service that hides a person's electronic mail address. Anonymizer.com provides this service as do dozens of other Web sites.[8]

---

5. Reuters, "AOL Says Hackers Broke into Some Member Accounts," June 16, 2000.
6. The full title is *Where Wizards Stay Up Late: The Origins of the Internet* by Katie Hafner, Matthew Lyon. (January 1998).
7. www.privacytimes.com and the newsletter are published by Evan Hendricks.
8. www.aononymizer.com. Other companies offering software are services for user anonymity include Freedom by Zero Knowledge Systems and Norton Internet Security by Symantec. An interesting approach is http://geocities.com/jiboprox/.

A clever criminal uses digital sleight of hand to escape prosecution. The Software Industry Association published a white paper that tells the harrowing story of Lt. Col. Jones, who has been the victim of a criminal who uses the real Lt. Col. Jones's identity to run up tens of thousands of dollars on the victim's credit card accounts. The misuse of Lt. Col. Jones's identity began in late 1999. Nearly nine months later, the suspect has not been located.

**U.S. Military's Use of Social Security Numbers.** The trigger point for Lt. Col. Jones's credit woes began with his Social Security Number. Other credit problems begin with people who complete personal information profiles from links on public discussion groups or who fall prey to Web crooks who create a bogus electronic commerce site.[9] The unwitting Internet user provides data, and the crook closes up shop. Once vital information is in the hands of a wrongdoer, the data can be used to make purchases. Alternatively, the thief sells the data to a third party.

Law enforcement and financial services security professionals are confronted with increasingly clever criminals.

But technology is only an accelerant, not a cause. One major problem is that many organizations and companies use a person's Social Security number as a person's identification number. The Social Security Number may be used by government entities, health insurance companies, colleges and, until recently in Kentucky, as a person's driver license number.

**Old and New Crime Blend.** Stolen identity nightmares afflict about 500,000 Americans annually, and account for more than $2 billion in fraud losses but the actual figure is not likely to be known.The reason is that those who have been duped do not want the details of the incident to be made widely known. Hiding the dirty laundry of security problems is preferable to the publicity surrounding the breakdown.

Consider this story of identity theft using manual and Internet technology in a synergistic manner:

> In April 2000, Tennessee authorities indicted two men on charges of buying nearly $750,000 worth of diamonds and Rolex watches using credit card numbers stolen from current and deceased top executives, including the late publisher Nackey Loeb of *The Union Leader.* Among victims were the chief operating officer of Coca-Cola Enterprises, the chief executive officer of Hilton Hotels and the chairman and chief executive officer of Lehman Brothers Holdings, prosecutors said. Other victims included the estates of deceased executives, including a former chairman and chief executive officer of Wendy's International, a former administrator of Cedars-Sinai Medical Center in Los Angeles and Loeb, who died Jan. 8. The indictment alleged that the alleged criminals targeted prominent members of the nation's business community and obtained personal information about them. The men impersonated their victims in telephone calls to banks and credit card companies. The men changed the billing addresses on the accounts to hotels in Tennessee, Arkansas and Mississippi. The men alleg-

9. Any electronic mail software that supports Hypertext Markup Language can embed an active link to another site in the text of a message. The only safeguard is to complete personal information forms on sites where the integrity of the operator is known. Providing personal data to an unknown site is risky.

> edly chose diamonds and watches viewed on the Internet Web sites of the jewelry dealers and then arranged to send payments by using the stolen credit card numbers or arranging for banks to wire the money. The merchandise was shipped to hotels whose addresses Jackson had provided to the banks and credit card companies as the new billing addresses.The men then made reservations at the hotels in the names of his victims and notified the hotels to expect packages to be delivered to the individuals, the government alleged. One of the victim's daughters learned of scam after people claiming to be her mother called the Bank of New Hampshire trying to access the mother's checking account. The man making the call had Loeb's Social Security number and birthdate, but the bank would not provide the information to the caller because the caller did not have the account number.

**People: The Weak Link in Security.** A government employee, equipped with secure computer systems, can make a poor decision. The *Detroit News* (Gannet News Service) story of Mr. Feakes in April 2000 underscores the weak link in many systems—a careless employee filling "routine requests":

> Dave Feakes lived in Fressenden, North Dakota. Feakes purchased an independent insurance brokerage. Feakes received a call from his bank wanting to know why he had applied for a hefty loan to buy a new pickup when he had just taken one out for a new utility vehicle. A short time later a South Dakota bank called asking for payment on bounced checks totaling almost $9,000. Feakes then applied for a new driver's license. The clerk told Feakes he was not Dave Feakes. The computer spit out a license with Feakes's name and Social Security number but another man's photograph. After two years of work, Feakes figured out what happened. The thief got a copy of Feakes' birth certificate for $10 from the state of North Dakota. The con man used the birth certificate to convince the driver license clerk to create a duplicate driver's license. With the license, birth certificate and social security number, the con man called Feakes's bank. Using the lost-my-wallet story, the con man asked for Feakes's checking account information. The con man used this information to open new checking accounts and make purchases.

In each of these examples those duped had access to various online information systems. The breakdown in "security" had little to do with online systems. The failures had a great deal to do with human nature. Despite the increased vulnerabilities of certain types of online transactions, security boils down to individual behavior. The only secure computer is one that has the plug pulled and sits in the middle of a locked room.When a person can get in the room, security is compromised.

## Ignorance Equates to Vulnerability

Conjure up a mental picture of an theater. The stage is dark. The house lights are down. A magician takes the stage. A floodlight bathes him in a spot light. The audience can see every move the

magician makes clearly. With a snap of the fingers, a person levitates. A few moments later, the magician pulls hundreds of colorful silk scarves from his mouth. A few people in the audience know how the magician performed his tricks. Those who lack this knowledge shake their heads in wonderment. “Magic,” a few may say.

A pervasive network exists in such wired cities as Austin, Texas, Tokyo, Japan, and Helsinki, Finland, among others. Online connections are possible from mobile telephones that tuck into a pocket or a full-scale computer that nestles in a student’s canvas backpack.

With an ease that rivals the magician’s sleight of hand, a person can access an online service and whiz through electronic mail, buy and sell stock, or perform a mind-boggling array of functions. A newcomer to the online ecosystem often says, “Amazing” after first sampling online services.

System administrators can be gulled as easily as the average Internet user.

If the blame could be placed on the Internet user, security would be a simpler problem. The user can do everything right and still be robbed of a credit card number or worse. There are dozens of tricks a hacker can use to steal information from a server. Many of these are solely within the control of the system administrator for an Internet Service Provider or a an organization’s network administrator.

Networks, like personal computers, have to be set up. Each network operating system or NOS as the software environment is often described has dozens, if not hundreds of specialized settings. Harried network administrators or careless systems engineers may accept the default values when building a network.

Most users are blithely ignorant that the network they are using has been compromised. Some systems can be entered improperly simply by using the command prompt and a telnet session to log into the server. Some servers offer ftp or file transfer protocol services. These sites can be viewed by anyone with ftp products that come with most operating systems.

A crook can use utilities like those created by Blue Squirrel Software or Soft Byte Labs Black Widow. Black Widow, which costs about $40, can scan a Web site and present found files in an Explorer-like window. The user can retrieve just about any files associated with the site as long as other pages have a link to them. Unlinked “gems” reward the spider’s user. Black Widow also features resumeable downloads for those hard to get files. It is compatible with both HTTP and HTTPS server types. Black Widow is an off-line browser, a site scanner, a site mapping tool and a “site ripper.”

A person with more technical savvy may want to use the “rootkit” to snag system and user data.[10] A rootkit places special entries in the root of a server. These entries are then used by the hacker to create a back door to the system. A trojan horse crontab utility will allow a cracker to run a hidden series of tasks or daemons. These tasks will create vulnerabilities in a system.[11]

10.The most popular Web server is the Apache Software Foundation’s Apache server. (www.apache.org). This server can be made more secure with special add-in software. For details, consult www.apache-ssl.org.

For criminals with a strong technical background, it is possible to modify the operating system kernel itself. This can be accomplished by recompiling the operating system. Patches can be added to the operating system that provide the criminal with administrator privileges or routines that scour the server for data, compress it, and send it by electronic mail to the criminal. Another approach is to add a new kernel module to the operating system. The "enhancement" allows the criminal to access the system or perform one or more specific tasks designed to compromise privacy and security.[12]

Once a criminal has root or administrator privileges, the system is not secure. A list of cracker actions facilitated by these tricks includes:

- Rootkits. A rootkit is a group of programs (modifications of regularly used system programs) which help an intruder remain undetected after he has already compromised a system; for example, a modified "ls" program. Normally "ls" lists files, but a rootkit version may prevent the intruder's files from being listed when the actual system administrator runs the command.
- Password poaching. The intruder obtains user names and passwords. With these key pieces of information, the cracker can enter new systems with the identity of the original user.
- Account takeover. The intruder uses the accounts of the true user for his own purposes, including setting a person's electronic mail account. Bogus electronic mail accounts are frequently used to verify passwords for certain commercial sites. Thus, a criminal armed with an e-mail identity and a credit card can pyramid other scams masquerading as another person.
- Fraudulent transactions. The intruder uses the existing accounts to make fraudulent purchases. A drop address is required, and this may be gleaned from information on the server. When the delivery arrives, the cracker arranges for a third-party to "sign" for the package or if no signature is required, accept delivery.
- New account creation. Using the data found on the server or in electronic mail, the criminal creates new accounts in the name of one or more people whose information was hijacked by the The table below provides a summary of 10 ways information can be obtained to gain access to personal details about an individual. With the right pieces of information, anyone's identity can be compromised:

**TABLE 2. Tactics for Stealing Personal Information**

| Tactic | How It Works |
|---|---|
| Dumpster diving or steal a person's mail to locate credit card numbers, bank statement, or other information | One or more people go through discarded materials. The tactic is one of the most reliable and most easily used by professional and amateur alike. |
| Capture personal information from an Internet user | Ask for information as part of a qualification for accessing a site. |

11. For more information about Trojan horse programs, see www.securityfocus.com, www.phrack.infonexus.com, and www.2600.com, among others. A search of Deja.com or Remarq.com can yield useful information about these cracking techniques.

12. System administrators must be required to review security logs. Organizations without a system administrator oversight function are at risk. Windows 2000 security can be supplemented with third-party products like RSA Security's SecrID (www.rsasecurity.com). In Windows NT and 2000 the system event viewer and policy change services provide clues to cracker activity.

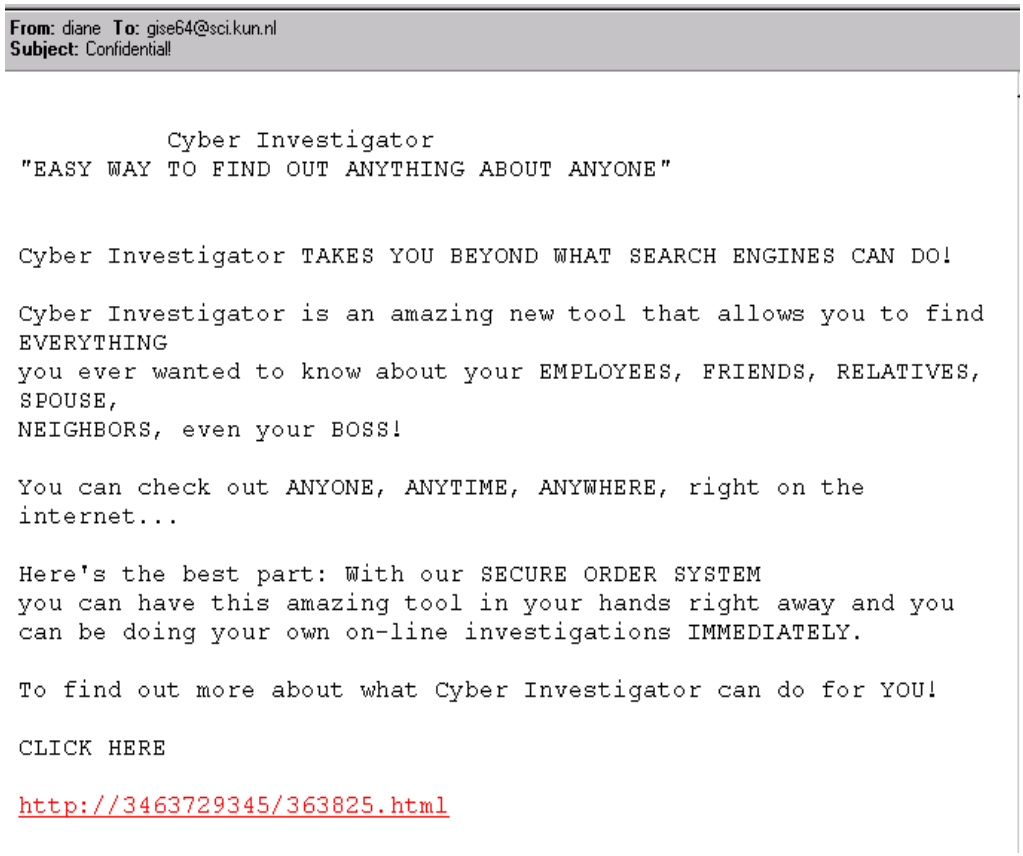
**TABLE 2. Tactics for Stealing Personal Information**

| Tactic | How It Works |
|---|---|
| Place a small file on a user's computer so that the actions of the user can be tracked. | The "cookie" allows an Internet site to record a wide range of information about a user's actions. This includes what sites were visited, what files were downloaded, etc. |
| Intercept electronic mail | Any electronic mail can be intercepted by anyone with access to the mail server account. In an ISP or information technology department, usually two or more people will have access to the mail accounts. These individuals can copy, read, and delete any mail that resides within the system. Encrypting electronic mail is a must.[a] |
| Steal a laptop or notebook | A thief grabs a computer in a notebook. Instead of taking the notebook out of the airport, the thief sits down, looks for passwords and other useful data, then discards the notebook. |
| Create a fake electronic commerce site, offer products at a great price, and require detailed personal information from would-be buyers. | A person creates a Web site and uses it to capture an individual's credit card information, shipping address, and other details. These data can be used by the thief or resold via the Internet to other individuals. |
| Snoop within a personal computer | A person gains access to a home or office legally or illegally and looks for passwords or personal information on machines or networks. |
| Gain unauthorized access to an online system and place programs on the server to allow an unauthorized person to access the system | Unless properly set up and protected, computer hooked to the network can be located and accessed by those with knowledge about networked computers. |
| Ask for the information or "social engineering" | Identify an America Online user. Call the person and ask for account information in order to verify that the system is working properly. |
| Walk up to a computer and look for passwords and log on instructions taped to the monitor, the desktop, or wall. | Users have difficulty remembering passwords and complicated log in instructions. |
| Create a public posting in a usenet forum. Provide a url or link to a Web page with a form where more information can be posted. | The person creating the link to the form can ask the duped Internet user for credit information and other data. These data can be used by the thief or sold to another party to use. |
| Use public information sources. | Individuals and Web sites provide Social Security Numbers, personal profiles, and background information for a fee. The person wanting information goes to a Web site or hires a person to obtain the data. |

a. A well-known encryption system is PGP or Pretty Good Privacy. Once the user installs the software and signs up, an encryption key is issued. A privacy key looks like this: 42 57 B3 D2 39 8E 74 C3 5E 4D AC 43 25 D2 26 D4. The software is available at http://web.mit.edu/network/pgp.html.

One of the more interesting software tools available for monitoring a person's Internet activities is a software product called Spector 2.1. Once installed on an individual's computer, Spector Spector records PC and Internet activity, much like a camcorder, and lets the person who installed the software play back the recorded information. Spector records all applications loaded, all web sites visited, all chat conversations, and all incoming and out going e-mail activity. It is possible to see what the personal computer user sees. Spector is one of the first automatic screen recording software designed for consumers and corporations. The software automatically takes snap shots of the display screen, as often as once per second, or as infrequently as once every few minutes. [13]

Stealing someone's identity is not very difficult. Typical of the Web sites that advertise they can provide a Social Security number for anyone you might choose for less than $50. If you want help, Diane, who provides her "e mail" address as gise64@sci.kun.nl offers this:



**From:** diane **To:** gise64@sci.kun.nl
**Subject:** Confidential!

Cyber Investigator
"EASY WAY TO FIND OUT ANYTHING ABOUT ANYONE"

Cyber Investigator TAKES YOU BEYOND WHAT SEARCH ENGINES CAN DO!

Cyber Investigator is an amazing new tool that allows you to find EVERYTHING
you ever wanted to know about your EMPLOYEES, FRIENDS, RELATIVES, SPOUSE,
NEIGHBORS, even your BOSS!

You can check out ANYONE, ANYTIME, ANYWHERE, right on the internet...

Here's the best part: With our SECURE ORDER SYSTEM
you can have this amazing tool in your hands right away and you can be doing your own on-line investigations IMMEDIATELY.

To find out more about what Cyber Investigator can do for YOU!

CLICK HERE

http://3463729345/363825.html

**FIGURE 4. A query to a major search engine will return links to sites that offer to obtain for a nominal fee an individual's Social Security Number. These sites come and go rapidly, but new sources of Social Security Numbers become available continually.**

For more reading, *The Unwanted Gaze: The Destruction of Privacy in America* by Jeffrey Rosen. Hardcover (May 2000)

13.The software is available at http://www.child-monitor.com/spector/. It costs about $50.

An interesting service is available from Docusearch. The operation is staffed by licensed private investigators. A selection of the reports the firm offers appears in the screen capture below:


**FIGURE 5. A person looking for specific information about a particular individual can retain a third party to locate the information. The information is usually sent to the customer in an electronic mail message. Payment is usually handled with a credit card.**

Docusearch says this about itself:

> "docusearch.com offers an array of informative searches designed to help you find the information you need to know, today! No matter where you live in this world; you can now access data about people residing in the United States. This is the information age, and information is power! Controversial? Maybe; but wouldn't you sleep easier knowing a little bit more about a prospective business partner, employee, baby-sitter, neighbor or significant other? All search requests are ordered here, on our secure server

> and the results are posted to a password protected client area, where you can view them in the comfort and privacy of your home or office. All information obtained is held strict confidence and no one is alerted or notified of your search (including the Subject). Today begins a new era in the information age. Don't be left in the dark."[14]

The company's fees range from $14 for a telephone number trace to $249 for a corporate bank account. Customers settle their accounts online with a credit card, a facsimile with the credit card information, or traditional mail service.

Not surprisingly, different cultures react in ways that some American marketers find peculiar, even perverse. The European Union takes a dim view of the American habit of mining databases, reselling electronic mail addresses, and generally stripping an individual of his or her privacy. Europeans are nervous about the exploits of their criminals as well. In June 2000, a computer cracker breached the security of an Internet Service Provider in Great Britain and tapped into credit card data for 24,000 users. The victims included scientist at the top-secret Defence Evaluation and Research AGency, senior government officials, and senior managers at British Broadcasting Corporation.

The various studies of abuses of Internet privacy point to a growing concern about abuse and that enterprises operating in the Internet ecology are not accountable.[15] Internet users put less faith in the government than in enterprises. Not surprisingly, males between the ages of 19 and 25 are most likely to exchange information over the Internet. Trusted Web sites by mainstream Web users in the United States include Yahoo! and established financial institutions.[16]

## Mathematics and Privacy Empower Data Mining

The difficulties faced by online advertising companies selling banner ads can be summed up in a single thought: People ignore them. To get around this, these companies have increased their efforts to track the public's surfing habits with "cookies"—small files of code sent form one computer to another—that can then be used to identify users and monitor their actions as they negotiate the web.

Through data mining's recursive mathematics the software can locate and identify actions that fit together. An example would be American Express's use of Cross Z fractal technology to determine from all American Express credit card transactions on Mother's Day what related purchases fit in the cluster of buyers. Link analysis is the mathematical process of identifying probable causal relationships.

As online systems become as common as automatic cash machines and as easy to use, the likelihood of security problems, including identify-related crimes, rises. Millions of Internet users key

14. The site is located at www.docusearch.com.

15. See the Cheskin Research Web site at www.cheskin.com for information about the relationship of privacy and trust in different countries.

16. Business 2.0, July 2000, provides a summary of trust factors in Internet space. See pages 166 *ff*.

in their name, address, home and work telephone, facsimile, electronic mail address, and credit card number without only a moment's hesitation and sometimes not even that.

Double Click, an Internet direct marketing company, acquired a company that aggregates marketing data and matches it to consumers' names, addresses, and affinity group or cluster.[17] Double click bought Abacus, another firm specializing in data extraction and analysis. Double Click said that it would blend the data from the two firms in such a way that more precise marketing could be performed using the Double Click data sets. Double Click stepped over the line. The U.S. Federal Trade Commission pounced, and the stock quickly shed value. Double Click, Engage, and AdForce, among others, quickly changed their tune in response to a privacy backlash. The tactics have changed. The mathematical algorithms still run, but these companies have changed their positioning strategy

There are many data mining companies. Some are esoteric like Cognos. Others are designed for Web marketers who want to run marketing campaigns to exploit similarities or tendencies in clusters of buyers. Internet sites use products from companies like Net Perceptions. The approach is to "fuzzify" statistics. In this mathematical technique, an individual user is placed in a cluster. The tendencies of the cluster are analyzed and useful information extracted and written to a report the marketer can use for an electronic mail campaign or a Web marketing program.

The trajectory of data mining technology is moving rapidly. The "opt in" marketing company Promotions.com make a strong point in their advertisements about respecting the privacy of individual users, but the company uses comparatively low-power algorithms.[18] In fact, most of the popular Internet-centric tools are not much more than undergraduate statistical routines spiffed up and rejigged for the Web. The industrial-strength programs, widely used in police and government intelligence work, are making their way into the commercial marketplace.

The Federal Bureau of Investigation uses a system called "Carnivore" that reads electronic mail, figures out the meaning, and routes the possibly useful messages from criminal suspects to FBI analysts.[19] Carnivore must be installed with the assistance of Internet Service Provides who handle mail. The system eavesdrops without the suspects knowing their message traffic has been compromised. The throughput of the system is in excess of six gigabytes (about six billion bytes or two million electronic mail messages every 24 hours). Carnivore, in the parlance of security professionals, is a sniffer. Like other sniffers, it cannot process encrypted messages encoded with such tools as Pretty Good Privacy or an equivalent software program.[20]

17.Cluster analysis is the chief claim to fame for Claritas. However, Claritas cluster analyses can easily reach six figurs. Lower cost services have sprouted to meet the demand for rough-and-ready clustering.

18."Opt in" means that the person completing an electronic mail or paper form, checks a box that gives the recipient of the card permission to use the electronic mail address in other marketing programs.

19.On the international front, Echelon performs that same function. The U.S. National Security Agency is participating in this program with Great Britain and Australia, among other countries.

20.Encrypted messages can possibly be "broken" or decoded. Encrypted messages must be processed by separate subsystems. The security agencies classify the methods for breaking encrypted messages in the hopes of keeping an advantage over individuals who believe encrypted messages are secure.

The digitization of information allows a person with the requisite knowledge to assemble a composite report on one or more people rapidly. The military and police have used products from such companies as i2 Ltd. (Cambridge, England) that can process telephone bills, credit card statements, field operatives' notes, and other types of data and create a visual picture of the relationships that exist among events and people. A typical visual representation of this type of system's outputs appears in the illustration below:

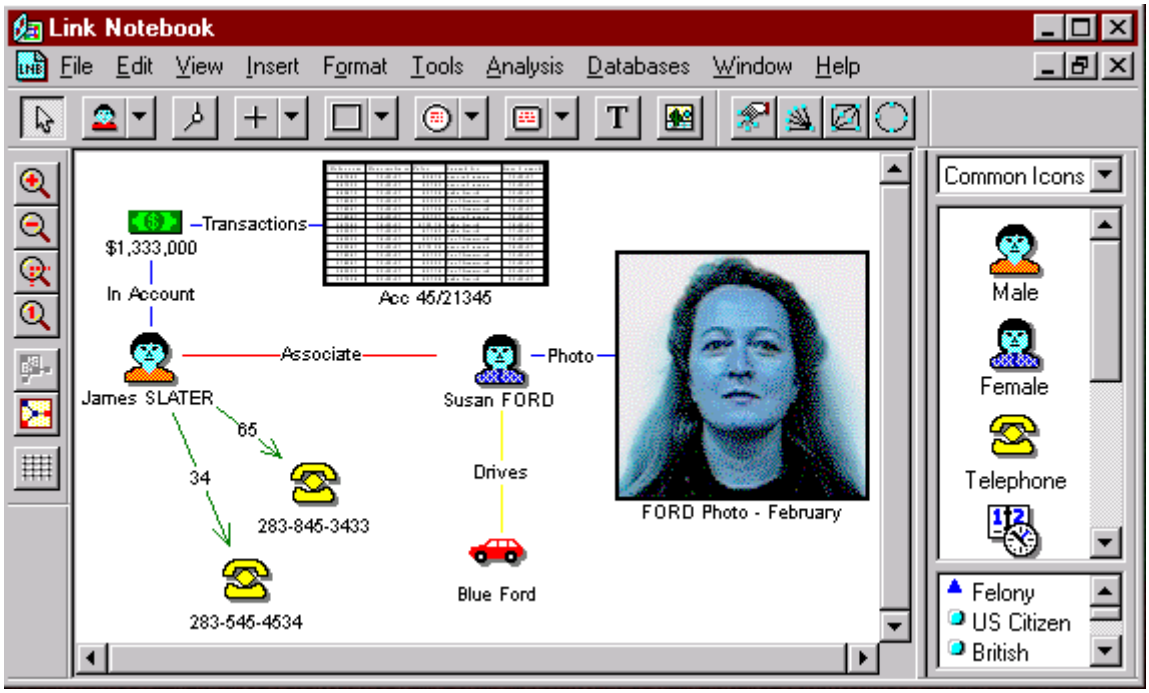



**FIGURE 6. Cambridge-based i2 Limited's software can process a wide range of data sources and construct an illustrated link diagram. A click on an object in the diagram will display the source data. An Excel table and a mug shot are shown on the "Link Notebook" screen.**

A computer user—whether by design as a Web surfer or by accident when making a mobile telephone call—leaves a well-marked trail of bright yellow digital footprints. Programs like i2 Limited's read these footprints and produce a visual picture of one's actions. If a link exists between a footprint and a picture, the image of the person will appear in the report. What types of systems leave digital footprints:

- Mobile telephones that can pinpoint one's location within three meters. Mobile telephones transmit their locations to the systems that route call to them. These data can be and are captured for various purposes.

- Banks that surreptitiously sell your financial secrets. The new publication *iMarketing News* contains dozens of advertisements for electronic mailing lists and demographic reports from major sites who resell customer data.[21] Most of these lists are based on the customer's providing permission to the site operator to send electronic mail and use the name for marketing purposes. Resale of the data is one "marketing purpose."
- Computer technology that secretly profiles you when you go online. These are the "cookies" that are ubiquitous.
- A health care system that makes your innermost medical secrets available to almost anyone. Med Records Web (www.medrecordsweb.com). The site's operators say, "We believe at Med Records Web, Inc. that a patient's, attorney, or insurance company should not have to face hurdles when it comes to obtaining copies of medical records fast and efficiently for self or for clients. The fee? $24.99 for 200 pages or less delivered online.
- Airport scanning devices that see and "sniff" for trace gases on your person and in your luggage. International points of entry are equipped with sophisticated online systems that match passport data to other databases from such companies as CPS Systems (Australia).[22]
- Tiny surveillance cameras everywhere: workplaces, campuses, lobbies, elevators, restaurants, locker rooms. Web-centric video is revolutionizing surveillance. For a sampling of what can be accomplished with "hidden cams," a quick click through www.guzei.com/live/camera/ is instructive. Be sure to load the Cyrillic character set. To buy a hidden cam outfit, consider TSS's products.[23]
- Growing pressure to require all Americans to carry a national identification card and DNA registries for everyone that would permit tracking.

21. iMarketing News is a publication of Mill Hollow Corporation. The editorial office is at 100 Sixth Avenue, New York, New York 10013. The firm's Web site is www.dmnews.com.

22. For information about the CPS Systems "border" products, visit www.cps.com.au/.

23. The TSS catalog is located at www.surveillancesolutions.com/catalog/internet/

# A Digital Bulletproof Vest

The American Bar Association offers some useful tips.[24]

**TABLE 3. Checklist for Preventing Credit / Identity Theft**

| Category | Detail |
|---|---|
| Key information to guard from identity thieves | Social Security number<br>Maiden names<br>Birthdate<br>Past addresses<br>Driver's license number |
| How criminals get your data | Ordering credit reports<br>Asking a seemingly harmless way<br>Digging through garbage<br>Stealing mail<br>Snatching purses<br>Learning it from the victim; for example, from résumés or family genealogies posted online |
| Prevention tips | Don't give out your Social Security number unless necessary (i.e., not to merchants who don't really need it)<br>Request your credit report regularly<br>Shred personal documents before putting them in the trash<br>Check W-2 for extra earnings (it could indicate someone else working under your name) |
| Victim assistance | Privacy Rights Clearinghouse: 619-298-3396, www.privacyrights.org<br>U.S. Public Interest Research Group: 202-546-9707, www.pirg.org/uspirg<br>Contact www.identitytheft.org<br>Contact the Federal Trade Commission, 877-438-4338<br>Report the problem to the Federal Bureau of Investigation at www.ifccfbi.gov<br>Contact the local police |

24.http://www.abanet.org/journal/oct98/10FIDSB.HTML

## Legislation or Technology?

Security legislation continues to flow from Washington, D.C., the European Union, and various countries where the Internet has swept into the lives of citizens and businesses. In the United States in June 2000, the Federal Trade Commission issued a call for privacy legislation. There are almost two dozen privacy bills moving through Congress in an election year.

The Platform for Privacy Preferences Project, usually referred to by the acronym P3P, began in 1997 at the Massachusetts Institute of Technology, under the auspices of the World Wide Web Consortium (W3C). The P3P initiative is focused on devising software that standardizes Internet privacy policies and render them in clear, easy-to-understand English. The partners in P3P are IBM, AT&T, Microsoft Corporation, American Express, Nokia, and the Direct Marketing Association. P3P is moving slowly, and there is little chance of the group's having a substantive impact for many months.

P3P works by asking the Internet user to complete a form that captures privacy preferences. Each P3P compliant site will use the privacy preferences to match the user's privacy preferences with the privacy policies of a particular Internet site. If the site's and the user's privacy preferences do not match, the user is given the option of overriding his or her privacy preferences and accessing the site. If the user does not want to visit a site that falls below the user's privacy threshold, the user's browser does not log on to the site. P3P does not block access to a site nor does it provide any data to a site that the user has not agreed to provide. A formal P3P specification will be posted on the Internet late in 2000.

The General Services Administration created the position of a computer security "czar." The person in this position will facilitate the establishment of government-wide security policy and guidelines across the entire government and work with the Office of Management and Budget to enforce these policies and guidelines.[25] The U.S. government federal Chief Information Officers' Council has set up a Privacy, Security, and Critical Infrastructure subcommittee. This group will explore PKI, electronic signatures, and encryption. The Department of Defense and the National Institute of Standards and Technology (NIST) have established technical working groups to address PKI and fund pilot programs. States are jumping on the bandwagon. Political in-fighting is evident between the Federal Trade Commission, the Software and Information Industry Association (SIIA) over the role of the U.S. government. Many Web sites have privacy statements, but they are often difficult to find, written in legalese, and enforced sometimes loosely, sometimes not at all.

For the foreseeable future, Internet users should guard their privacy with encryption and common sense. Companies and organizations will want to buy specialized services and tools from such firms as Internet Security Systems, an enterprise with more than 21 or the top 25 U.S. financial institutions.[26] The Golden Age of Online may be on the way, but the dark clouds of privacy and security could trigger an Ice Age in a click of Internet time.

---

25.The first person to hold this position is Barry C. West. He can be reached at barry.west@gsa.gov.

26.The company's Web site is located at www.iss.net.