



# McAfee North America Criminology Report

Organized crime and the Internet 2007

**McAfee®**

# Introduction

“The simple bottom line is that crime often *does* pay in the digital world.”

—*Sheridan Scott, commissioner of competition*

The 2006 McAfee® Virtual Criminology Report predicted the future of cybercrime. It would become more professional and more specialized. New criminal organizations would emerge. The “take” from cybercrime would increase. Unhappily, these predictions have come true. The report opened with a quotation from Willie Horton, the famous bank robber, who explained that he preferred to rob banks because that is where the money is. To the well-equipped and organized criminal, the Internet is much like a bank.

The Internet’s anonymity and global reach make it a low-risk, high-return environment for crime. Shadowy organizations, black markets, and for-hire specialists exist unseen on the same Internet that millions of consumers and businesses use every day. Several recent developments deserve particular attention. These include the growing sophistication of cybercrime tools and the speed at which they appear; the increased ability of cybercriminals to use the Internet to organize and equip



***Despite real progress in law enforcement, estimates show that as few as 5 percent of cybercriminals are caught and convicted.***

themselves; and the growing perception among cybercriminals, despite real progress in law enforcement, that they face little or no risk of arrest. (Estimates show that as few as 5 percent of cybercriminals are caught and convicted.) Pseudonyms or stolen online identities provide criminals an anonymous cover.

The 2007 McAfee Virtual Criminology Report examines developments in online organized crime; the threat it poses to computer networks and users; and how users and organizations can protect themselves.

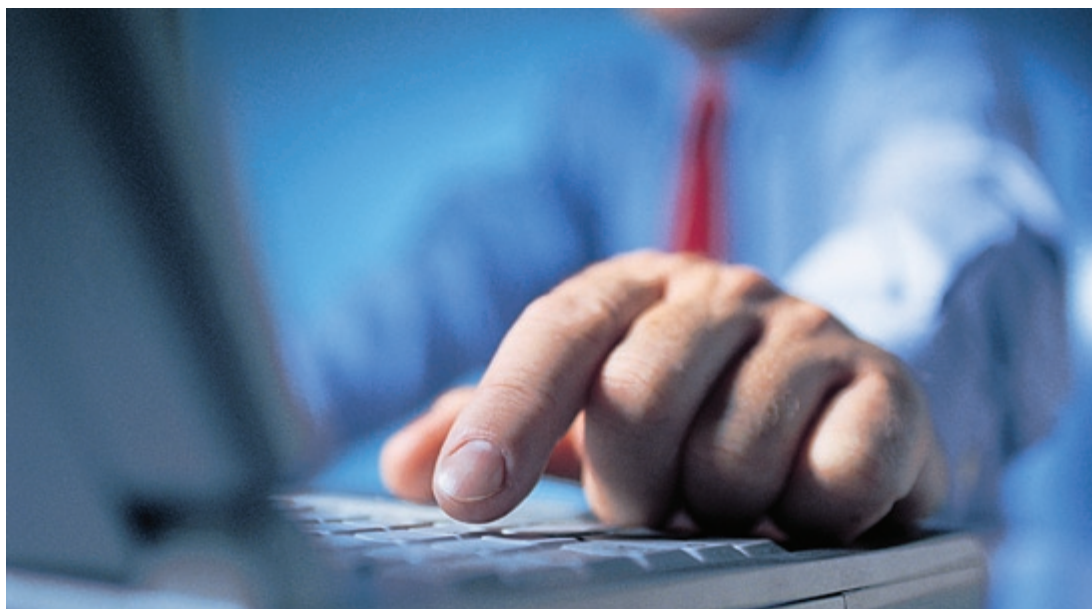
# Entrepreneurs of Crime

“The average take on a bank robbery is \$3,000. The persons committing that crime run an extremely high risk of something bad happening to them. You can run a phishing scam and make hundreds of thousands of dollars.”

—Thomas X. Grasso, FBI

There are over a billion Internet users worldwide. All are connected into a huge global network of computers. Billions of dollars move across these networks every year. The volume and value of these transactions continues to grow. Online transactions in Canada increased 38 percent, reaching almost \$40 billion last year. In the U.S., retail e-commerce increased 25 percent in 2006, to \$108 billion. The Commerce Department reports that online business-to-business transactions reached roughly \$2 trillion. That same year, online banking customers grew by roughly 30 percent in North America. Western Europe and Asia are experiencing similar growth.

The combination of millions of customers and huge sums of money is attracting criminals. A 2002 government study found that 5 percent of Canadian Internet users had their computers hacked. A 2006 survey of Canadian businesses found that almost two-thirds had lost income, customers, and productivity due to cybercrime. For many of those businesses, cybercrime cost more



*The cybercriminals who launch these attacks are very different from the scruffy teenagers who caught the attention of the press a few years ago.*

than traditional crime. A recent study of online banking found that 2 million Americans—five percent of online banking customers—had their

accounts illegally accessed and were robbed. The average loss was \$1,200; total losses for the banking industry reached over \$2 billion. One

North American credit card company reported \$100 million in fraud losses in 2005, of which \$30 million occurred online. One 2005 FBI estimate put the cost of cybercrime in the U.S. at \$67 billion.

The cybercriminals launching these attacks differ from the scruffy teenagers who caught the media's attention a few years ago. Before 2000, lone cybercriminals committed the bulk of computer-related crimes. These individuals hacked for publicity and notoriety, not for profit.

Amateur hackers who break into computer networks for these reasons continue to exist, but they no longer are the primary threat to security. Professional cybercriminals now have the skills, knowledge, and connections to support large-scale, high-value criminal enterprises online. Clearly, cybercriminals today are after money, not fame. They are organized, specialized, pervasive, and sophisticated. Some operate in traditional gangs. Others form ad hoc small teams as opportunities arise. Individuals often serve a particular function, such as gaining computer access and control or private data collection.

Criminals can make a lot of money from the Internet with relatively little risk. The web's anonymity makes the risk of prosecution very low. It is easy to impersonate a victim or to counterfeit a legitimate web site. Attacks can be launched remotely, from anywhere on the globe, and for low cost. The problems of collecting evidence in another country, and the intangible nature of cybercrime evidence, further protect

## From Amateur to Pro—Cybercriminals by Class and Type



**Bot-herders**—Cybercriminals who infect thousands of computers with malicious programs, turning them into tools for crime. The programs allow the bot-herder to command the captured computer to perform some action. Bot-networks are available for rent or sale on cybercrime web sites.

**Carders**—Cybercriminals who specialize in identity theft and online credit card fraud. Carders can draw on extensive Internet resources to acquire stolen identity and credit card information, and use it to commit fraud. Carding is lucrative, easy, and becoming more attractive to "street-level" criminals who might have once confined their crimes to petty theft.

**Cybergangs**—Groups of career criminals and hackers

whose use computer skills to commit crime in cyberspace. The groups are often based in countries with weak cybercrime laws. They can be organized or loose networks of criminals, located worldwide, who agree to cooperate for a particular criminal operation.

**Cybermules**—The expendable members of a cybergang. Cybermules receive goods or money and then pass it on to the hackers who first obtained the data. They are the most likely gang member to be caught.

**Cyberpunk**—An online delinquent who uses his or her computer skills to break into computer systems and networks. The term comes from science fiction novels including *Neuromancer* and *Shockwave Rider*. Money is usually not their primary motive, although some eventually use their skills for crime. Many cyberpunk attacks are *cybergraffiti*, an embarrassing defacement of a target web site.

**Hackers and crackers**—*Hacker* originally described someone who enjoys programming, using

computers, and devising effective and unorthodox solutions to interesting problems. Unlike script kiddies and cyberpunks, hackers are often skilled programmers. Increasingly, due to media usage, the term describes someone who gains unauthorized access to a computer or a network. The hacker community calls these individuals *crackers*. Hackers and crackers often operate alone and are motivated by social goals, such as prestige in the hacker community.

**Phishers, pharmers, and spammers**—Cybercriminals who specialize in one area of cybercrime. They often hire out their skills to other criminal organizations.

**Script kiddy**—Sometimes called an "aspiring hacker," a script kiddy is technologically unsophisticated and usually younger than 20. Script kiddies exploit computer vulnerabilities using pre-written commands obtained online. They usually do not know how the commands work, but still can inflict real damage.

## Criminology Report

cybercriminals. The scale of these automated attacks is immense, involving thousands of victims. Moreover, the stolen material—intellectual property or financial data—is easily transportable via the same Internet from which it was stolen.

The Internet enables cybercriminals to use less hierarchical structures than traditional gangs do. Loose confederations form even though members may live thousands of miles apart and never meet in person. This helps make cybercrime fast and flexible, and its community nature makes it difficult for law enforcement to penetrate or keep up with cybergangs. Successful prosecution is a challenge, too, because many cybercriminals operate from jurisdictions with weak laws and little capability or interest in cooperating with international police forces.

Online criminal networks, with names like Darkprofits, Superzonda, Hangup, and



*The FBI believes that crime syndicates—especially in Russia and the other countries of the former Soviet Union—are realizing how much money they can make with little or no overhead.*

“Researchers have concluded that the criminal organizations of the 21st century are characterized by a large degree of fluidity and structural complexity. As opposed to the popular stereotypes, they utilize diverse forms and sizes of clusters, network structures, and groups, often but not invariably transnational with occasional local home-bases, as suited for their diverse forms of illegal activities, and as dictated by emerging opportunities across the globe.”

—RCMP, *“The Changing Structure of Organized Crime Groups”*

Shadowcrew, are loose and informal alliances that span national borders. The FBI believes that crime syndicates—especially in Russia and the other countries of the former Soviet Union—are realizing how much money they can make with little or no overhead. One estimate is that groups from these regions commit a third of all cybercrime.

Superzonda specialized in spam. Located in South America, the gang used viruses to take over poorly

protected computers around the world and use them to send millions of spam messages every day. Superzonda even took over an anti-spam web site and used the email addresses of people who sent in complaints. The Hangup Team, though based in Russia, had several thousand members in Europe and the Americas. It specialized in malware that stole financial data and passwords. Shadowcrew’s specialty was identity theft and credit card fraud. The gang was broken up in 2004 after authorities arrested its leaders, but many members still operate in other groups.

The move of organized crime into cybercrime is in some ways a generational change. As younger criminals, familiar with information technology, move into organized crime, they see the benefits of adapting their computer skills to the criminal activities they pursue. The FBI believes that terrorist sympathizers have begun using phishing schemes to fund the groups they support.

# The Tools of Cybercrime

“Botnets are one of the greatest facilitators of cybercrime these days.”

—Wendi Whitmore, special agent, Air Force Office of Special Investigations

Cybercriminals need not be master programmers. Web sites sell or rent the software, botnets, or personal data cybercriminals need. Other web sites sell thousands of credit card numbers or email addresses, offering discount rates for bulk purchases.

There are three basic avenues for cybercrime: exploiting existing software vulnerabilities; tricking a computer user into downloading a malicious program; or *social engineering*, in which the criminal tricks a victim into providing access to their computer or network. The greatest risk lies in the exploitation of software vulnerabilities. Once a vulnerability is identified, cybercriminals can automatically search the Internet for computers with these vulnerable programs.

Creating malware requires a high degree of computer skills, but once developed, the cybercrime community shares and trades vulnerabilities and the tools to exploit them.



***A computer can be infected with malware in several ways, whether its user opens a malicious email attachments, downloads a program, or simply visits a fraudulent web site.***

Whoever is first to find a vulnerability usually posts it on web sites for the whole community to exploit. As a result, some estimates suggest malware infects a vulnerable computer within minutes after it logs onto the Internet.

Malware can infect a computer in several ways. Most often a user opens a malicious email attachment, downloads a program, or simply visits a fraudulent web site. Cybercriminals have started to use instant messaging and bogus web sites that lure

## Criminology Report

victims when they misspell the name of a popular web site. Another strategy cybercriminals employ is to place corrupted versions of popular files onto legitimate peer-

integration, and the growth of international financial services to make cybercrime transnational, letting criminals commit crimes in one location while safely ensconced elsewhere.

or turn the host into a *bot*—a computer that executes instructions provided by the cybercriminal, usually without the knowledge of the computer's owner. Using these tools, an attacker could steal information, disrupt networks, or erase valuable data.

### Selling the Tools

**(Note:** The following text is from a Russian spyware site called Ratsystems.)

*Welcome to RAT Systems Crew Official Web Site*

*Our team is specialised in spyware development. We code all types of spyware, from remote administration tools with GUI to simple keyloggers. Our main direction is to create effective and powerful spyware. Coding is not just hobby for us; it is our job and style of life.*

*In general, we're against destructive payloads and the spreading of viruses. Coding spyware is not a crime. Our team is not interested in massive infections. We do not use our or any other spyware for illegal purposes. All our work is absolutely legal and we are not installing our or any other spyware on someone's computer without notification.*

to-peer networks. This is how the Mydoom virus started out before spreading to email.

The availability of sophisticated *shareware* tools for cybercrime from hacker or *warez* sites give even inexperienced cybercriminals weapons to commit Internet crimes. These include online hacking manuals, do-it-yourself virus kits, and bulletin boards with tips and advice. The growing connection between hackers and criminals, combining criminal skills and computer expertise, creates new risks for companies. Finally, cybercriminals have been quick to exploit global connectivity, economic

Cybercriminals use a variety of software tools to locate poorly defended computers—preferably those with always-on broadband connections. Companies in some industries, such as banks and electrical utilities, report that their computer networks are probed hundreds or thousands of times every day. These industries usually repulse such attacks because they have an innate interest in security. Those with lower security concerns likely do not know when they are under attack.

The cybercriminal's goal is to covertly load and run malware on the receiving computer. This malware can secretly steal valuable data

Viruses began as a means for hackers to demonstrate skills, but have become a delivery vehicle of choice for cybercriminals. Sophisticated virus writers often deploy several variants to test their effectiveness. Since virus writers often share code, a virus may re-appear in a different or improved form several times. Virus writers often produce new, improved generations of the same virus within weeks of the first release.

Some viruses or Trojans target specific actions or communities. One Trojan activated a keylogger program whenever certain words appeared in a browser (i.e., "my account" or "account number"). The keylogger recorded the account number and password and then forwarded them to the cybercriminal. The Trojan also installed a remote control program on the infected computer. One virus targeted individuals whose company email address came from one of more than a thousand financial institutions.

Cybercriminals are careful to hide malware in a disguised or encrypted file, making it hard for the average user to detect it. Some

## Criminology Report

encryption prevents the user from changing or removing the program. These viruses and Trojans show a new level of sophistication and expertise in cybercrime.

Some cybercriminals even use malware on one another, disabling a target computer's anti-spyware programs as a form of competition. Other cybercrime programs contain their own anti-spyware programs that remove competing cybercriminals' spyware from the host computer.

The most successful of these tools allow a hacker to place malevolent programs on a computer without the user's knowledge. These programs can then execute harmful instructions, transmit data to an external address, or provide the hacker access and control. Cybercriminals assemble networks of these infected computers for use in denial of service (DoS) attacks, for spamming, or for advertising and tracking. Using someone else's computer as a proxy makes it difficult to track who committed the crime.

Infected computers that remain under the control of the cybercriminal are known as *bots* (short for robots). A *botnet*—a number of bots assembled into a network—is a collection of these infected machines, in which attackers have used worms or viruses to plant backdoor components that can be centrally controlled and used to launch simultaneous attacks. Spammers, hackers, and other cybercriminals acquire or

rent botnets, which can grow quite large. For example, in 2005, police in the Netherlands caught two Dutch hackers who had assembled a botnet with over 1.5 million computers by using *Toxbot*, a program they had written.

Expert cybercriminals may hack a popular and legitimate web site and place malicious software on it. As a result, unsuspecting web site visitors may unwittingly download the software onto their own machines. This year, for example, unknown cybercriminals hacked one of the web sites for the 2007 Super Bowl. Visitors looking for stadium information unwittingly started a program that then attempted to download a Trojan

and a keylogger. Although this particular web site was temporarily shut down and rapidly secured, the tactic remains popular.

Instead of lurking on a dark street corner to snatch a wallet or a purse, a cybercriminal can attack tens of thousands of people simultaneously, with little risk of harm or capture. Criminals can implant programs to disrupt or steal information from one computer, or to provide a base for attacks on others. A single criminal using a botnet can send a million emails within minutes for the cost of a few cents, and count on finding hundreds of inadequately protected computers to raid or capture.

### Cybercrime Alert—February 2, 2007\*

"...the official web site of Dolphin Stadium has been compromised with malicious code. The Dolphin Stadium is currently experiencing a large number of visitors, as it is the home of Sunday's Super Bowl XLI. The site is linked from numerous official Super Bowl web sites and various Super Bowl-related search terms return links to the site.

"A link to a malicious JavaScript file has been inserted into the header of the front page of the site. Visitors to the site execute the script, which attempts to exploit two vulnerabilities: MS06-014 and MS07-004. Both of these exploits attempt to download and execute a malicious file.

"The file that is downloaded is a NsPack-packed Trojan keylogger/backdoor, providing the attacker with full access to the compromised computer. The filename is w1c.exe and its MD5 is ad3da9674080a9edbf9e084c10e80516.

"Please do not visit the site until it has been cleaned."

\*See: <http://www.websense.com/securitylabs/alerts/alert.php?AlertID=733>

## An Expanding Arsenal for Cybercrime

**Blended threats**—A cybercrime attack that combines multiple cyber tools, such as an email virus and a Trojan or other malware.

**Bots and zombies**—A bot (short for robot) is a computer in which a worm or virus has installed programs that run automatically and allow cybercriminals access and control. A botnet is a collection of these infected machines. Botnets mainly infect consumer systems that have always-on Internet connections. They are the weapon of choice for cybercriminals to commit fraud and extortion. Spammers, hackers, and other cybercriminals are acquiring or renting botnets for as little as \$200 to \$300 an hour.

Zombies automatically execute commands from someone other than the user, without the user's knowledge. Zombies are created by placing executable code on a user's machine, often through use of a Trojan. A cybercriminal can gain control of the computer and have it automatically execute a command to initiate a DoS attack, send spam, or other malicious activities.

**Bundling**—Covertly attaching a virus or spyware to a benign or legitimate download, such as a screensaver, a game, freeware, or an image. When the user downloads and installs the legitimate file, they are unwittingly giving permission to install the criminal program.

**Denial of service (DoS)**—An attack to prevent the normal functioning of a computer network or system and to prevent access by authorized users. A *distributed denial of service* (DDoS) attack uses thousands of computers captured by a worm or Trojan to launch tens of thousands of email messages

at the target in a very short time. Attackers can cause DoS attacks by destroying or modifying data or by using zombie computers to bombard the system with emails until its servers are overloaded and other users can no longer gain access.

**IP address hijacking**—Cybercriminals take advantage of vulnerabilities in Internet servers to take over a legitimate Internet address and reroute traffic from it to them.

**Keylogging**—A program that covertly records the keys typed by a computer user and stores the data for either later access or secretly sends the information to the author. A keylogger's advantage is that the cybercriminal does not need to trick a computer user into supplying sensitive information. The keylogger simply records what the user does during a legitimate transaction.

**Packet sniffer**—Software that monitors network traffic to capture and analyze data. Specialized sniffers capture passwords.

**Ransomware**—Spyware that secretly encrypts data on an infected computer and then flashes a message on the user's screen demanding the user pay the cybercriminal to obtain the key to decrypt it.

**Rootkit**—A set of tools used by an intruder after hacking a computer. The tools allow the cybercriminal to maintain access, prevent detection, build in hidden backdoors, and collect information from both the compromised computer and from other computer systems on the network. Rootkits are available for most major operating systems.

**Screen grabbers**—Software that copies the information on your computer screen—a *screenshot*—when you log into a web site of interest to cybercriminals, such as an online banking site. The grabber captures passwords and account information and relays them to the cybercriminal.

**Scripts**—Short programs or lists of commands, usually available as shareware from hacker sites, that can be copied, remotely inserted into a computer, and used to attack and disrupt computer operations.

**Spyware**—Software that surreptitiously gathers information from a computer. Spyware is typically bundled covertly with another program. The user does not know that installing one also installs the other. Once installed, the spyware monitors user activity on the Internet and transmits that information to someone else. Spyware can also gather and relay information on email addresses, passwords, and credit card numbers.

**Trojan**—A malicious program that users unwittingly download and install. Some Trojans pretend to be a benign application. Many hide in a computer's memory as a file with a nondescript name. Trojans contain commands that a computer automatically executes without the user's knowledge. Sometimes this can be to act as a zombie and send spam or participate in a DDoS attack, or it can be a keylogger or other monitoring program that collects data and sends it covertly to the attacker. Many Trojans now also attempt to disable anti-virus programs. Many people use the term to refer only to non-replicating

malicious programs, thus making a distinction between Trojans and viruses.

**Virus**—A program or piece of code that spreads from computer to computer without the users' consent. Viruses cause an unexpected and negative event when run by a computer. They contaminate legitimate computer programs and often arrive via emails with clever titles to attract the curious reader.

**War-driving**—Wi-Fi networks are increasingly used by retailers who use hand-held price checkers and other wireless devices. Wi-Fi is attractive to cybercriminals because it can be difficult to secure wireless networks. "War-driving," where hackers or criminals drive around a city looking for open access points, is a crime that offers cybercriminals easy access to networks and valuable data. One of the largest credit card information thefts so far, involving millions of card numbers, was the result of "war-driving" and a poorly secured wireless network.

**Worms**—Wholly contained viruses that travel through networks, automatically duplicate themselves, and mail themselves to other computers whose addresses are in the host computer. They propagate by sending copies of themselves to other computers through email or Internet Relay Chat (IRC).

# Theft, Fraud, and Extortion

“The existing identity infrastructure of the Internet is no longer sustainable. The level of fraudulent activity online has grown exponentially over the years and is now threatening to cripple e-commerce. Something must be done now before consumer confidence and trust in online activities is so diminished as to lead to its demise.”

—Ann Cavoukian, information and privacy commissioner of Ontario

Most cybercrime falls into one of three categories: theft, fraud, or extortion. The Internet has made these crimes easier and safer to commit. There are few reliable or easy ways to determine the identity of someone on the Internet. The ease with which criminals can use impersonation and anonymity makes cybercrime both attractive and successful.

Low cost is also to blame for the spread of cybercrime. Phishers, for example, will send out tens of thousands or even millions of fraudulent emails for pennies. They can purchase or rent the email lists from cybercrime sites and forums. While the phisher will receive back only a few hundred emails containing personal and account information, the money they extract more than justifies the initial expense.

Distance and connectivity also help. The attack can be launched from anywhere in the world. Cybercriminals reside in Eastern Europe, the former Soviet Union, Brazil, Argentina, and China—anywhere there is programming

talent, including Canada and the U.S. These cybercriminals often recruit low-level criminals—sometimes called *cybermules*—in their target countries to help them. These “mules” may not always know that they are participating in a crime. The mule serves as a front, receiving cash obtained by internet fraud, a portion of which they will transfer back to their boss. The mule takes most of the risk and gets the smallest reward. If the mule is caught, the cybercriminal who organized the crime, and

stands to reap the bulk of the financial reward, remains free.

One subset of cybercriminals focuses exclusively on credit card theft. Known as *carders*, these criminals have developed a thriving online community using private, encrypted chat rooms and online forums with names like CardersMarket (once described as “the Wal-Mart of the Underground”). These forums are careful to assert that they are innocent of illegal activity; that staff will remove any criminal

## Carder Forums: How-to Advice for Cybercriminals

### Some Unchangeable Digits in Visa Credit Cards

Written by Stargazer and Borashi, Midwest Phreakers Alliance

*Let's start with the 4190 credit cards... 4190 format is like this: 4190-00AB-xxxx-xxxx. Notice that the 5th and 6th digit are both 0. This is a must! I have never seen one without the two 0's there. The A & B are two numbers that we have not figured out yet... in the A slot, the number 8 appears to dominate. The x's are randomized. I do not understand the checksumming, but a program such as CC.MAKER written by Phantom Viper will help you with that.*

content; and that discussion of techniques violates no laws. Forum members exchange tips on how to exploit credit card data, sell or rent credit card information, and trade or sell cybercrime software. Many of the sites change their web address every few months to evade law enforcement, notifying customers and members of the new location via chat or bulletin boards. Though cybercriminals may begin transactions on a forum or web site, they usually conclude them in private chatrooms or on closed bulletin board, where they are more difficult to track. Cybercriminals transfer money safely by using anonymous online payment services like e-gold.

Cybercrime does not rely entirely on technology. Social engineering is an important element, too. It tricks or deceives the recipient into taking an action or revealing information. Phishing is an example—some users will respond unthinkingly to a request that appears to be from a legitimate institution. Social engineering does not require the same degree of computer skills. Some successful attacks blend vulnerability exploitation and social engineering; for example, an email may use an attractive subject line to get a reader to open it, which will then launch a hidden program that will take advantage of software vulnerabilities on the host computer.

Social engineering is a key element of identity theft. Most identity theft is committed the traditional way: someone with physical access

to your mail or private documents takes advantage of that access. The most likely suspects are family members or friends. The 2006 *Identity Fraud Survey Report* notes that 47 percent of victims could identify the source of the data compromise and 36 percent of victims could identify the person who misused their information. However, we know that

more than a 50 percent increase since 2003 when the Federal Trade Commission (FTC) reported 9.9 million American adult identity-theft victims. The average loss in 2006 was \$3,257, up from \$1,408 in 2005. At the same time, the percentage of funds dropped from 87 percent in 2005 to 61 percent in 2006.



***One subset of cybercriminals focuses exclusively on credit card theft. Known as carders, these criminals have developed a thriving online community using private, encrypted chat rooms and online forums.***

cybercriminals increasingly commit identity theft as a means to enable other crimes, and the share of identity thefts committed using the Internet appears to be increasing.

Approximately 15 million Americans were victims of identity theft-related fraud in the 12 months ending in mid-2006, according to a survey by Gartner, Inc. These statistics represent

Some criminals are highly sophisticated and able to plan and execute long-term attack strategies. The multiple releases of the *Sobig* virus over the course of 2003, for example, appear to have been an effort by its authors to test and refine the virus. *Sobig* was encrypted to slow defense efforts. Once installed, it automatically downloaded more spyware from another web site.

## Categories of Cybercrime

**Extortion**—Cyberextortion affects both companies and individuals. In the Internet version of a protection racket, criminal gangs will threaten companies with disruption of their networks, DoS attacks, or the theft of valuable information unless they pay a ransom. Reputation threats, in which a hacker threatens to deface a company's web site, are often part of an extortion scheme. Damaging information will go public unless the victim pays. In other cases, the cybercriminal will encrypt a user's data and then demand payment to send them the key to unlock it. A new twist involves emails—sometimes from an alleged hit man—threatening consumers with bodily harm unless they pay.

**Fraud (phishing, pharming, spoofing, hijacking)**—Anonymity and the opportunities for misrepresentation make fraud the foundation of most cybercrime. Advance-fee frauds exploit greed and cupidity by offering, often through an email that purports to be from a relative of a prince or dictator, a chance to gain a share of millions. The email asks for the recipient's bank account or a payment as part of a money-laundering scheme that will release the millions in loot. In another variant, a cybercriminal buys a cheap stock, touts it in online chatrooms, and sells when the stock price rises because of the false information.

Phishing, currently the best-known form of fraud, occurs when an email purporting to be from a bank, credit card company, or retailer asks the user to go to a web site and supply account information. Phishing has become

increasingly sophisticated, with false web sites that are indistinguishable from the legitimate company. Often phishers use psychological techniques, such as announcing that your account has been suspended, to fool the unsuspecting into providing information. Some cybercrime sites offer do-it-yourself phishing kits for less than \$300.

Pharming, a more sophisticated attack,



is harder to detect because it attacks the DNS system that routes Internet traffic. The malware does not reside on the victim's computer. Pharming automatically redirects traffic to a false web site. Sometimes a simple typing error in entering the legitimate name will take the consumer to the criminal site. In other cases, the consumer can enter the right information, but the cybercriminal has changed the DNS address to redirect the request to a criminal web site. When the consumer places an order, the criminal gains not only the money from the transaction but also the account information.

Hijacking is similar to pharming. A cybercriminal hijacks a legitimate Internet domain name and redirects its traffic to his or her servers. In a recent case, a hijacker gained control of a legitimate ISP's domain name and had the email from all of the ISP's customers redirected to an unknown server located in Canada. The cybercriminals gained access to thousands of emails for a few days without the knowledge of the customers.

**Money laundering**—The volume of transactions, the anonymity, the availability of alternatives to cash, and the lack of consistent record-keeping make the Internet ideal for money-laundering. The Financial Action Task Force (FATF), a group of national law-enforcement agencies concerned with financial crimes, found that criminals use online banking, Internet casinos, and web-based financial services. Specially legitimate transactions, such as a purchase from an auction site, can exchange funds without attracting much notice. One new technique is to recruit consumers to act as accomplices. Cybercriminals first transfer stolen money to the accomplice's account. Then, the intermediary transfers the money to an overseas account, keeping a percentage as a fee. Accomplices usually do not know who hired them.

**Spamming**—A crime in many countries, including the United States. Spammers frequently use the tools of cybercrime. These include botnets, which use individual computers to launch thousands of emails at

no expense to the spammer. The Messaging Anti-Abuse Working Group, an organization founded by companies including AOL, Microsoft, and Bell Canada, estimates that more than 80 percent of all email is spam. Spammers also buy stolen email addresses, which are sold on many cybercrime web sites. In September 2004, the U.S. government estimated that spammers send out as many as 200 million messages a day. The *Washington Post* reported that spam costs U.S. businesses \$10 billion a year. The convergence between spyware and spam means spam is not just an annoying advertisement but also a delivery vehicle for programs that attack computers.

**Theft of information and intellectual property**—Cybercriminals can extract personal identification information or credit information from a company's database and affect thousands of consumers. Cybercriminals can also steal a company's own financial information and valuable intellectual property (designs, blueprints, and marketing plans). While the reported cost of information theft is declining, many crimes remain unreported or undiscovered. IP theft remains one of the greatest Internet risks a company can face.

# The Challenge for Law Enforcement

Global law enforcement agencies have strengthened national laws and international cooperation to catch, prosecute, and deter cybercriminals. Despite this progress, however, cybercrime continues to grow. The Internet increases in value every day, but its security cannot keep up. It remains an anonymous place in which cybercriminals safely can operate.

Many victims are reluctant to report cybercrime. For large corporations or banks, the damage to their reputations often outweighs the losses from the crime. This embarrassment and the underreporting it produces help to make cybercrime a low-risk activity.

Another challenge faced by law enforcement is the continued presence of cybercrime “havens”—countries with skilled programmers and either weak or disinterested law enforcement. The states of the former Soviet Union attract cybercriminals because they meet these criteria, but criminal programmers also operate in South America and Asia.



*Global law enforcement agencies have made some progress in catching, prosecuting, and deterring cybercriminals. Nevertheless, cybercrime continues to grow.*

Cybercriminals operate in North America and Europe, but they are more likely to be caught and prosecuted.

The core of the problem is national sovereignty, or the right of a country to govern itself. A major obstacle to prosecuting

cybercrime is the difficulty of establishing which police force has jurisdiction; the victim may live in one country, the attack may have been launched from another, and the criminal may live in a third. Enforcing one country's laws in another is complex and time-

consuming. There have been steps to expand cooperation, however. The best examples are the G8 24/7 High Tech Crime Network and the Council of Europe Cybercrime Convention.

The G8 agreement establishes round-the-clock points of contact, which are crucial for dealing with fast-breaking cybercrimes before evidence is destroyed. Under the agreement, officials in 45 countries provide immediate assistance in terrorist or criminal cases involving electronic evidence. Although the G8 arrangement is informal in the sense that a country can decline to honor a request, it has proven to be very useful in prosecuting cybercrime.

The Convention defines cybercrime as offenses committed against “the integrity, availability, and confidentiality of computer systems and telecommunication networks,” or the use of networks or their services to commit traditional offenses, including money laundering, offering illegal services, violation of copyright, violations of “human dignity and the protection of minors.” This convention provides an adequate legal framework and ensures a common approach by different countries to simplify cooperation.

Having equivalent laws in place reduces the problems of sovereignty. If a foreign police force requests assistance for something that would be a crime in one’s own country, that assistance is easier to provide. There are 43 signatories and 15 parties to the Convention—

about a third of the world’s nations—so many countries still lack an adequate legal framework for cybercrime.

The issues created by sovereignty and the transnational aspect of cybercrime are compounded by technologies that make it difficult to identify perpetrators and collect evidence. Digital evidence is fragile and transitory, and pre-digital techniques for evidence collection are ineffective. Many police forces still lack the resources and capability to operate effectively in cyberspace.

This problem can be solved. Countries can devote more resources to combat cybercrime and make it a high priority. Internationally, work

continues to strengthen existing cooperative groups and networks and to increase the number of signatories to the Council of Europe Convention. Existing organizations like Interpol and APEC (the Asia-Pacific Economic Council) are paying greater attention to cybercrime. Ultimately, it may be possible for nations to agree to increase formal cooperation in prosecuting cybercrime. These improvements, combined with technological progress in improving authentication and making networks more secure, will ultimately tamp down cybercrime, but this will take years to accomplish.



*The issues created by the transnational aspect of cybercrime are compounded by technologies that make it difficult to collect evidence. Digital evidence is fragile and transitory, and pre-digital techniques for evidence collection are ineffective.*

# The Future of Cybercrime

“No one is safe these days on the Internet, where bad people operate with apparent abandon. A private citizen without a badge or a search warrant is hopelessly outgunned by hackers who can virtually hop across international borders in moments. It can be nearly impossible even for federal authorities to catch these criminals.”

—Ted Bridis, technology reporter

What does the future hold for cybercrime? More of the same. The combination of factors that enable cybercrime will be slow to change. Networks will continue to be insecure. Some consumers and some companies will still be careless. Cooperation between countries will remain slower than the spread of the Internet. Moreover, the value of e-commerce will continue to increase.

Cybercrime will migrate to new technologies. Wireless networks create a new opportunity for cybercriminals to obtain access to valuable information and to hide their tracks. The spread of mobile devices, such as PDAs and Internet-enabled mobile phones that connect to the Internet, make them a target for virus writers. Once data with financial value is stored on these mobile devices, cybercriminals will begin to exploit them.

The increase in cybercrime does not mean the end of the Internet or e-commerce.



*The spread of mobile devices, such as PDAs and mobile phones that connect to the Internet, make them a target for virus writers.*

What it means is slower growth and higher costs. Cybercriminals prefer easy targets, so companies and individuals that pay attention to security requirements will be relatively safe. Those who ignore cybersecurity will suffer. Cybercrime will always be with us, but

reasonable goals for governments in the next few years would be to slow its growth and to increase the likelihood of prosecution. When criminals believe that cybercrime is no longer risk-free, fewer of them will engage in it. Until that time, cybercrime will continue to increase.

# Further Information

## **Press Inquiries, Canada**

Kathy Swail  
McAfee, Inc.  
Direct line: 514.830.5776  
Email: [kathy\\_swail@mcafee.com](mailto:kathy_swail@mcafee.com)

David Eisenstadt  
The Communications Group Inc.  
Direct line: 416.696.9900  
E-mail: [deisenstadt@tcgpr.com](mailto:deisenstadt@tcgpr.com)

## **Press Inquiries, U.S.**

Francie Coulter  
McAfee, Inc.  
Direct line: 408.992.8407  
Email: [francie\\_coulter@mcafee.com](mailto:francie_coulter@mcafee.com)

## **General Information**

For additional information,  
please call 888.847.876  
or visit [www.mcafee.com](http://www.mcafee.com).

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, [www.mcafee.com](http://www.mcafee.com)

McAfee and/or additional marks herein are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2007 McAfee, Inc. All rights reserved. 6-cr-na-002-0507