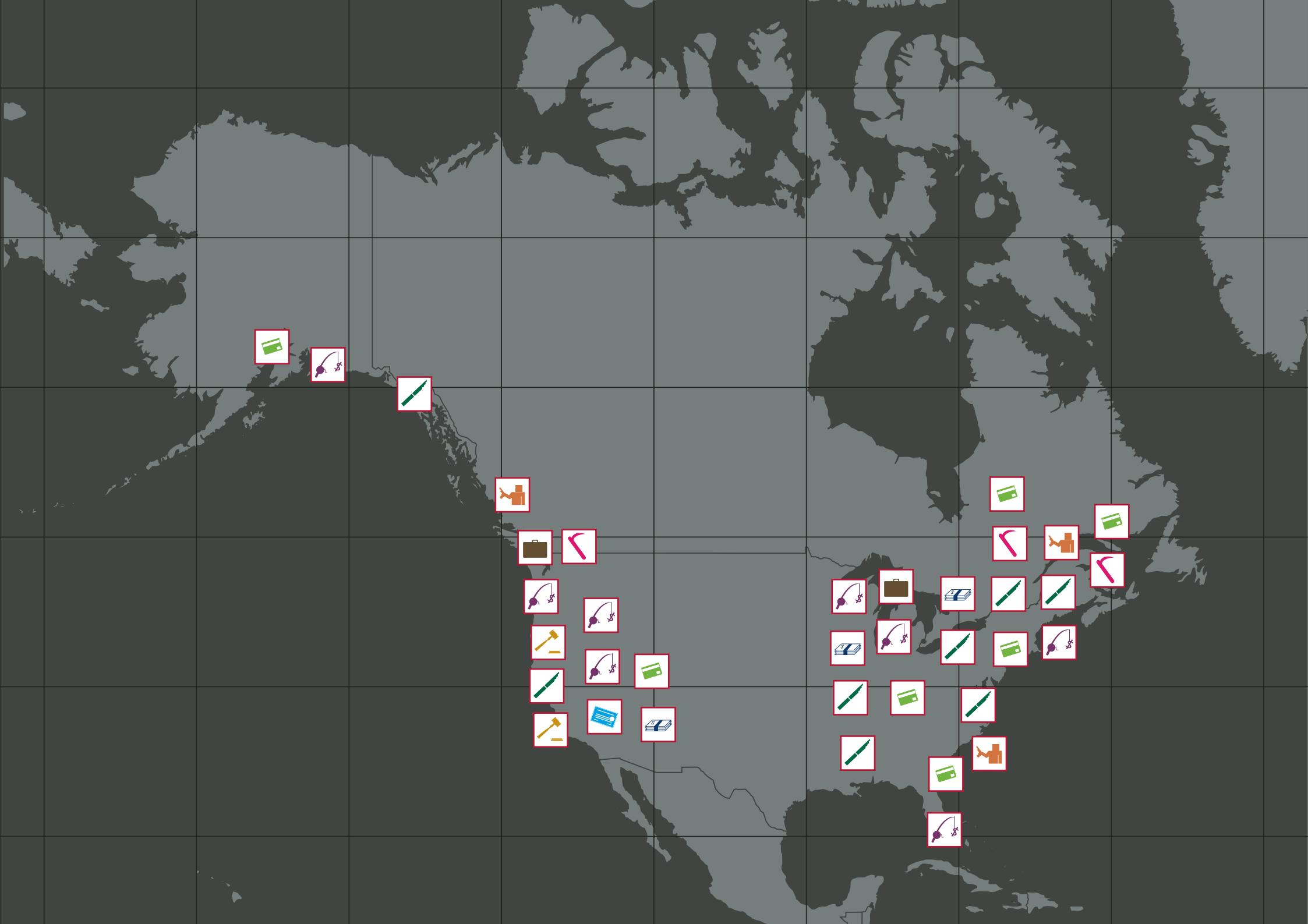
# McAfee Virtual Criminology Report:

North American Study into
Organized Crime and the Internet



July 2005


Share Scams
Online Protection Racket
Organized Crime Phishing
Corporate Espionage
Political Crime
Hacking
Bot-Nets for Hire
Credit Card Fraud
Money Laundering



# CONTENTS

# INTRODUCTION

Information technologies change how societies operate, so it should be no surprise that they have changed crime as well. Computers, computer networks, and the Internet have become an integral part of business and social activity. The value of the information available through computers and networks attracts criminals, an attraction that will only grow as information technology reshapes economic life. At the start of the computer age, *computer crime* meant stealing a PC or gaining illegal access to a mainframe to get information or extra processing time. Today, computer crime spans a wide range of offenses that target companies and the value stored on computer networks.

*"E-mail and the Web are arguably the most widely used forms of communication and information-sharing today. Millions of people use the Internet every day. So do many kinds of criminals.*

*We have entered a new phase of malicious activity. Cybercrime is now driven by those out to make money, which has led to growing involvement by organized criminals. They will capitalize on every opportunity to exploit new technologies and the general lack of awareness surrounding security—and their methods are becoming more subtle and sophisticated every day. As such, proactive protection is becoming imperative—it is the only way to offer users absolute confidence.*

*As a leader in anti-virus and intrusion prevention solutions, McAfee® is at the forefront of helping consumers and businesses better understand the threats they face online—and showing them the best ways in which they can protect themselves.*

*Although the growth of cybercrime sounds like a worrying trend, everyone can protect themselves and their personal information simply and with a little common sense."*

—Lee Fisher, McAfee Security Strategist

Increasingly, *the money* is in computers or on the Internet; one FBI estimate put the cost of cybercrime at about $400 billion in 2004.

The McAfee Virtual Criminology Report reveals how a new class of criminals is using the Internet in new, systematic, and professional ways to commit illegal acts. It examines emerging areas of concern, including the use of new technologies such as *bot-nets*—networks of computers that can be controlled remotely. The report suggests how businesses and individuals can protect themselves against criminal activity. The report examines how organized crime and cybercrime are developing, and looks at the future threat this activity could pose to home computers, government computer networks, and to computer systems in the business sector.

*"Because that's where the money is…"*

—Statement attributed bank robber Willie Sutton, as to why he robbed banks, 1952

Two years ago, McAfee researchers were seeing roughly 300 potentially malicious threats emerging each month, but today the figure has rocketed to 2,000, largely due to the growing number of bots. Cybercrime is also mirroring traditional offline criminal activity, with an estimated 85 percent of malware written purely for profit.

Commissioned by McAfee and authored by Dr. James A. Lewis, a Senior Fellow at the Center for Strategic and International Studies, the McAfee Virtual Criminology Report reveals how organized crime and cybercrime are developing, and looks into the future at the threat this activity poses to home computers, as well as to government infrastructure, and to computer systems in the financial and health sectors.

# SECTION ONE

## Cybercrime, New and Improved

The Internet began as a kind of online science park, used mainly to exchange research information among a community of users who were generally known to each other. With its commercialization and massive growth, the Internet changed into a new and exciting arena for economic activity involving tens of millions of anonymous users. The anonymity and global reach of the Internet make it a low-risk, high-return environment for crime.

The value of Internet activities and the wealth stored on computers is the source of the attraction. While e-commerce represents only a fraction of total commerce, it reached almost $70 billion in the U.S. at the end of 2004, an increase of 24 percent over 2003. A third of the U.S. workforce is online—roughly 50 million people—an important consideration since more than half of e-commerce transactions are made from work and since the online workers very often are engaged in higher-value activities than their offline colleagues. Sixty million residents of North America—almost half of the Internet user population in Canada and the U.S.—have online bank accounts. The combination of banking and commerce draws criminals more than anything else.

> *"Information is itself the target. Information is the world's new currency."*
>
> —Ralph Basham, Director, United States Secret Service

With the Internet's global reach, the temptation is irresistible for these criminal entrepreneurs. The value of information and transactions on computer networks has grown to the point where cybercrime has become an organized, *professional* activity. Cybercriminals take advantage of vulnerabilities in networks and computers to gain access to valuable information, such as personal identification information, financial data, or intellectual property.

CASE STUDY: **Operation Firewall**

**In an investigation codenamed *Operation Firewall*, U.S. and Canadian authorities announced in October 2004 the arrest of twenty-eight people from six countries involved in a global organized cybercrime ring. The underground criminal groups had names like Shadowcrew, Carderplanet, and Darkprofits. They operated Web sites to buy and sell credit card information and false identities, to share information on how to commit fraud, and to sell the tools needed to commit such crimes. They bought and sold almost 1.7 million stolen credit card numbers. Financial institutions have estimated their losses to be more than $4.3 million.**

Criminals now use the Internet for extortion, fraud, money laundering, and theft. Information technology lets them carry out these crimes more efficiently and with less risk. Victims can be found automatically. The use of pseudonyms or online identities provides an anonymity that is attractive to criminals. Some sources estimate that perhaps only 5 percent of cybercriminals are ever caught and convicted. The Internet provides criminals a way to move money rapidly among bank accounts and countries. The nature of the Internet makes it difficult for police to follow transactions to gather evidence, and national laws differ enough to make prosecution difficult.

### *Categories of Cybercrime*

*Extortion*—In the Internet variant of a protection racket, criminal gangs will threaten companies with disruption of their networks, denial of service attacks, or the theft of valuable information unless they pay ransom or ***security consultant*** fees into an offshore bank account.

*Reputational Damage*—A hacker or a competitor can deface a company's Web site, causing not just embarrassment but loss of sales. Reputational threats are often part of an

extortion scheme: damaging information will be made public unless the victim pays. In other cases, spite or a desire to inflict harm means that the attack will be executed without warning.

*Fraud*—The anonymity and opportunities for misrepresentation found on the Internet make fraud easy. Fraud comes in several forms. Advance-fee frauds exploit greed and cupidity by offering, often through an e-mail that purports to be from a relative of a prince or dictator, a chance to gain a share of millions. The e-mail 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, the cybercriminal touts a certain stock on an online chatroom. When the stock price rises because of the false information, the cybercriminal cashes in. Or the cybercriminal can create a false Web site that mimics an online retailer. Sometimes, a simple typing error in entering the legitimate name will take the consumer to the criminal site. When the consumer places an order, the criminal gains not only the money from the transaction but the consumer's account information. In some cases, cybercriminals illicitly access databases and tamper with records to gain some advantage. Auction fraud is another common variant—the winning bidder pays a spurious seller for a high-value good and receives nothing or junk in return.

*"This is a multi-billion-dollar industry, with well-funded hackers searching everywhere to discover vulnerabilities and exploit them for identity theft,"*

—Alan Paller,
head of SANS Institute

*Phishing*—Currently the best known form of fraud, phishing begins with an e-mail purporting to be from a bank, credit card company, or retailer asking 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 the phisher will use psychological techniques, such as announcing that ***your account has been suspended***, to coerce the unsuspecting into providing information. Some cybercrime sites offer do-it-yourself phishing kits for less than $300.

*Service Disruption*—A cybercriminal can use an Internet attack to disrupt a key service. Denial of service attacks are one method, but worms and viruses containing malicious code are another. A major auto manufacturer was one of many companies that had to shut down its e-mail network for a few days because of the Love Letter virus. Some viruses will wipe clean computer memories, erasing payroll records or invoices. The threat of service disruption can be part of an extortion scheme or a potential area of risk for some critical infrastructure.

*Information Theft*—The most damaging category of Internet crime, information theft can take several forms. Cybercriminals can extract personal identification information or credit information from a company's database and affect thousands of consumers. Cybercriminals can also extract a company's own financial information. Finally, cybercriminals can steal valuable intellectual property (designs, blueprints, and marketing plans) from a company. While the reported cost of information theft is declining, it remains one of the greatest Internet risks a company can face.

*Money Laundering*—The growth of global financial services makes it easy to conduct banking operations across borders over the Internet. The Financial Action Task Force, a group of national law enforcement agencies, notes that "Within the retail banking sector, services such as telephone and Internet banking allow customers to execute transactions on a non face-to-face basis from any location with telephone or internet access." While use of the Internet provides law enforcement agencies a greater ability to trace transactions through electronic records, the volume of transactions, the anonymity, and the lack of consistent record-keeping make it attractive to criminals and terrorists.

**The success of cybercriminals poses new and difficult challenges for law enforcement. The anonymity and global connectivity of the Internet lets cybercriminals engage online in traditional crimes such as extortion, drug-running, or pornography on a greatly expanded scale. Crimes can be committed across national borders or from different continents. Criminals do not need to be physically present to commit the crime. This reduces the risk of capture and prosecution and makes the job of law enforcement that much harder.**

# Comparisons between real-life crime and cybercrime

All of the online versions of these crimes offer criminals a number of advantages:

1 **Criminals do not need to be physically present at the scene to commit the crime.**

2 **These crimes can be committed across geographies, i.e., someone in Russia could commit a crime in the U.S./ Canada/France/UK/Germany/Italy, etc.**

3 **Using computers, the crime is carried out automatically, at high speed and attacks a vast number of victims at the same time, making it harder to track and prosecute.**

**Protection Rackets**

In the old world shopkeepers were forced to pay a ransom to organized criminal gangs to stop their shops being robbed or set on fire.

**Online Extortion**

Today organized criminals try to force e-businesses to pay a ransom to *protect* online shops from online attacks.

**Bank Robbery**

Old-fashioned bank robbery: gangs rob high street banks/ security vans.

**Hacking**

Hacking into a bank's computer systems and transferring money over electronic payment systems.

**Credit Card Theft**

Criminals steal credit card statements and utility bills from garbage cans to fraudulently use the identity of their victims.

**Boiler Room Share Scams**

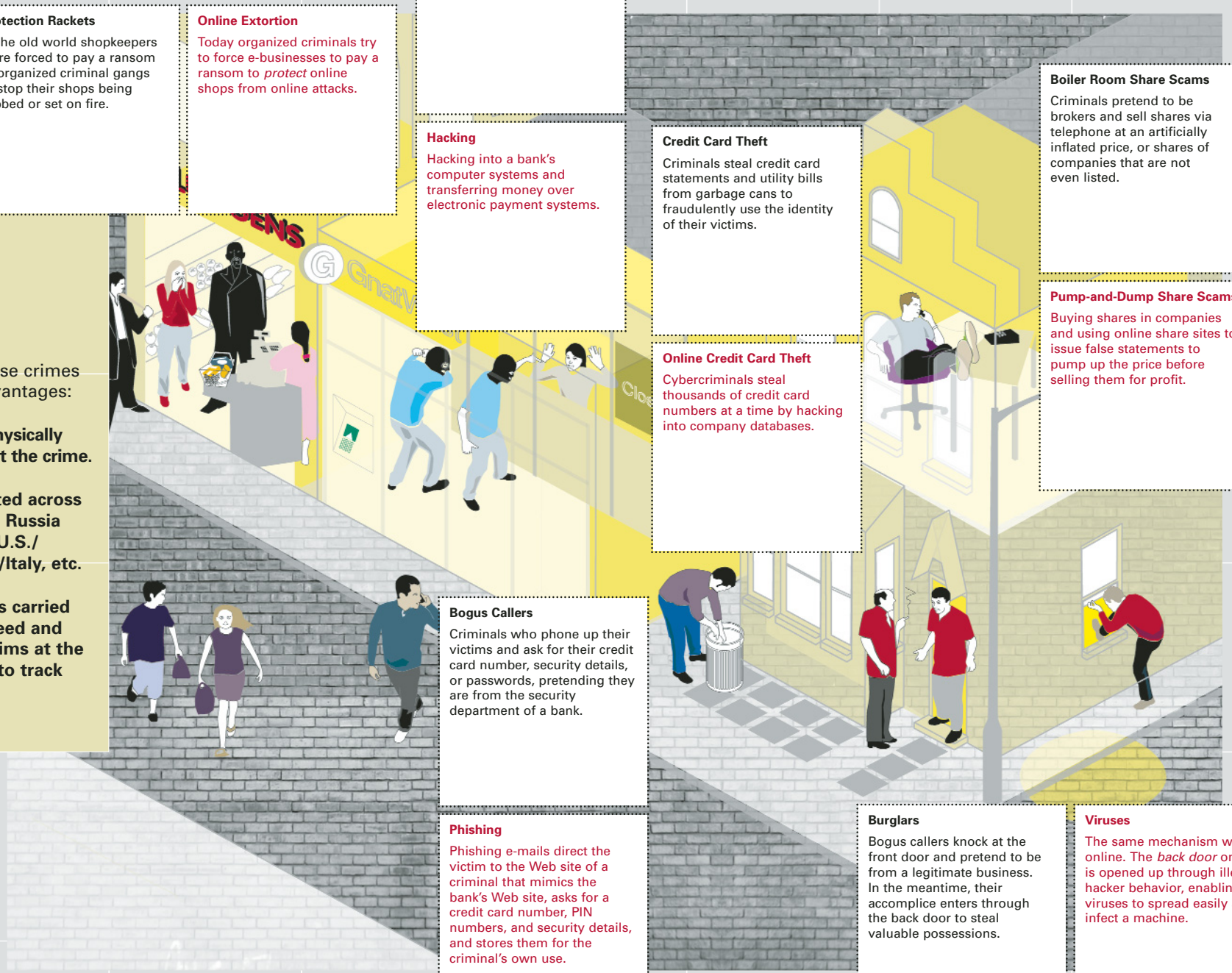
Criminals pretend to be brokers and sell shares via telephone at an artificially inflated price, or shares of companies that are not even listed.

**Pump-and-Dump Share Scams**

Buying shares in companies and using online share sites to issue false statements to pump up the price before selling them for profit.

**Online Credit Card Theft**

Cybercriminals steal thousands of credit card numbers at a time by hacking into company databases.



**Bogus Callers**

Criminals who phone up their victims and ask for their credit card number, security details, or passwords, pretending they are from the security department of a bank.

**Phishing**

Phishing e-mails direct the victim to the Web site of a criminal that mimics the bank's Web site, asks for a credit card number, PIN numbers, and security details, and stores them for the criminal's own use.

**Burglars**

Bogus callers knock at the front door and pretend to be from a legitimate business. In the meantime, their accomplice enters through the back door to steal valuable possessions.

**Viruses**

The same mechanism works online. The *back door* on a PC is opened up through illegal hacker behavior, enabling viruses to spread easily and infect a machine.

The transnational aspect of cybercrime is compounded by technological developments that pose new and difficult challenges for the identification of perpetrators and the collection of evidence. Digital evidence is fragile and transitory and pre-digital techniques for evidence collection are often ineffective. The growing sophistication of cybercriminals is a serious challenge to law enforcement. Many police forces still lack the capability to operate effectively in cyberspace. In part, this is due to the absence of adequate laws for cybercrime. Many countries still lack an adequate legal framework for the deterrence and punishment of cybercrimes or rely on an uneven patchwork of legislation. Disagreement over what constitutes a crime; inadequate, uneven, or absent authorities for governments to investigate and prosecute cybercrime; and paper-based procedures for international cooperation have at times hampered international cooperation on cybercrime.

Sophisticated shareware tools for cybercrime available on hacker or warez sites give even inexperienced cybercriminals the weapons they need to commit crime on the Internet. These can range from online hacking manuals and do-it-yourself virus kits to sophisticated tools that require some expertise to use. The growing connection between hackers and professional criminals provides a marriage of criminal skills with computer know-how to create a new level of risk for companies. Finally, cybercriminals have been quick to exploit global connectivity, economic integration, and the growth of international financial services to make cybercrime transnational, letting criminals commit crimes in another country or continent while safely ensconced somewhere else.

CASE STUDY: **Operation Cyber Chase**

**In April 2005, an investigation codenamed *Operation Cyber Chase* led U.S. authorities from the Drug Enforcement Agency, the FBI, and other agencies to an Internet pharmacy that sold $20 million worth of controlled drugs to thousands of people around the world. The online pharmacy did not require prescriptions, only a credit card number and address. Based in India, the Internet ring supplied drugs for 200 Web sites. The foreign distributor shipped the drugs in bulk to Philadelphia and other sites in the United States, where the drugs would be repackaged and shipped to customers. Authorities have seized $7 million from banks and 7 million doses of drugs, and arrested twenty-three people in eleven cities in the United States, India, and Canada. The online buyers paid higher-than-market prices, leading police to suspect that many were abusing the drugs. Federal authorities obtained most of the buyers' names and credit card numbers and may refer the information to authorities in the states where they live.**

*"We haven't seen a big move with the traditional Mafia groups to the Internet…not like we have with the Eastern European hacking groups. But as the money becomes more and more widely publicized, they probably will."*

—David Thomas, Chief, FBI Computer Intrusion Section

Before 2000, cybercriminals acting alone committed the bulk of computer-related crimes. For these individual hackers, publicity and notoriety—not profit—were the main motivation. Hackers want bragging rights in their online world. The psychology of hackers shows the attraction of cyberspace for them. Hackers tend to be young, disaffected males, although an increasing number of young women are joining their ranks. Hacking is an important part of their identity. John Suler, a psychologist of cyberspace at Rider University writes: "What motivates the hacker? Some are captivated by the challenge and excitement of venturing into forbidden territories…Some are motivated by a rebellious nature…In extreme cases, a hacker—and especially hacker wannabes—feel pressured to demonstrate that they are better and smarter than anyone…false bravado and desperate needs to prove oneself may be more common in the hacker wannabe than in the truly skilled hacker."

Hackers motivated by these social or personal goals will continue to be a feature of the Internet. But in the last few years, cybercrime has moved from amateurs and hackers to professional criminals. Criminals have realized the huge financial gains to be made from the Internet with relatively little risk. They bring the skills, knowledge, and connections needed for large scale, high-value criminal enterprise that, when combined with computer skills, expand the scope and risk of cybercrime.

Some aspects of cybercrime—spyware or phishing—have attracted considerable public attention, but there is less attention to the connections among the various attacks and the growing sophistication of cybercrime. Cybercrime offers criminals several advantages. It also lets them move into new fields for crime. The Internet is having the same effect on crime that it has on other organizations, moving them towards flatter, less hierarchical structures and a greater reliance on loose confederations. Online criminal networks are often informal alliances that span national borders.

***Hierarchy of Cybercriminals***

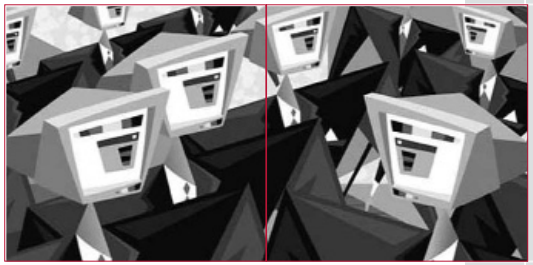
*Script Kiddy*—A technologically unsophisticated attacker, usually under the age of 20, who uses a macro file or other lists of commands written by someone else to exploit computer vulnerabilities. Script kiddies usually do not know how the program they execute works.

*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 such as ***Neuromancer*** and ***Shockwave Rider***. Financial gain is usually not their primary motive. Many cyberpunk attacks are ***cyber graffiti***, an embarrassing defacement of a target Web site.

*Hackers and Crackers*—Hacker originally described a person who enjoys learning programming languages and playing with computer systems. Many of these skilled programmers often have a libertarian bent to their politics. Increasingly, the term has a pejorative sense because it is used in the press to describe someone who gains unauthorized access to a computer or network. The hacker community calls these individuals ***crackers***. Hackers often operate alone and are motivated by social goals (a desire for prestige in the hacker community) more than for financial gain. Hackers often use a specialized jargon to identify their Web sites and tools. The most common convention is to use "z" instead of "s" to indicate the plural, as in ***warez*** (software), ***hackz*** (hacking techniques) and ***crackz*** (software that can remove license restrictions from software).

*Cyber Gangs*—Groups of career criminals and hackers who have acquired the computer skills necessary to move their activities into cyberspace. Very often, the groups are based in countries with weak cybercrime laws, but they can also be loose, fluid networks of criminals located in a number of different countries who agree to cooperate for a particular criminal operation.

The most interesting development may be the ability of these more advanced criminal groups to plan and execute long-term attack strategies that are of little interest to the socially motivated hacker or script kiddy. 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 and once installed, it automatically and without the users' knowledge downloaded more spyware from another Web site. Many viruses or trojans target specific actions or communities. One trojan activated a keylogger program whenever certain words like *my account* or *account number* appeared in a browser. It also installed a remote control program on the infected computer. Another virus targeted individuals whose company e-mail address came from one of more than a thousand financial institutions. These viruses and trojans show a new level of sophistication and expertise in cybercrime.



*"Computer networks, electronic transfers of vast sums of money, virtual businesses—all taking place in a cyber world that provides untold opportunity but also the virtual anonymity and possibilities for rip-offs of a reach and dimension that would not have been possible even a decade ago."*

—RCMP Commissioner Giuliano Zaccardelli, January 27, 2005

# Section Two

## Attack of the Zombies

There are two basic avenues for cybercrime: exploiting vulnerabilities in operating systems and other software programs, or *social engineering*, where the criminal tricks a victim into providing access to their computer or network. Once vulnerability is identified in a software program, cybercriminals can automatically search for computers with these vulnerable programs (often those that have not kept their updates current), using specialized tools that comb the Internet. Some estimates say an unprotected computer will be found and infected only minutes after it logs onto the Internet. This approach to cybercrime requires a high degree of computer skills initially, but once developed, vulnerabilities and tools to exploit them are shared and traded among the cybercrime community.

***The Case of the Hired Hacker***

*A businessman hired a sixteen-year-old New Jersey hacker to disable the Web sites of his competitors. The hacker launched a program that placed bots on 2,000 unprotected computers that he then used for a distributed denial of service attack. The attacks were repeated over five months and damaged not only the target companies, but also their Internet service providers (ISP) and, in a cascading effect, hundreds of other unrelated companies that used the same ISP. The FBI estimated that the attacks cost all the companies over $2 million, and arrested both hacker and businessman in March 2005.*

*"This is an example of a growing trend: that is, denial of service attacks being used for either extortionate reasons, or to disable or impair the competition. It's a growing problem and one that we take very seriously, and one that we think has a very destructive impact and potential."*

—FBI Supervisory Special Agent Frank Harrill

Social engineering does not require the same degree of computer skill. Social engineering gets around defenses by tricking computer users into providing information or unwittingly giving permission for the criminal program to install itself and reside on their computer. Some successful attacks blend vulnerability exploitation and social engineering—an e-mail 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.

Cybercriminals are becoming more sophisticated in their attack techniques and technologies, and have moved to using automated tools and networks of hacked computers. Criminals take advantage of the distributed computing power found on modern networks to launch attacks automatically, at high speed, and against a vast number of victims simultaneously. Criminals can implant programs that run without the owners' knowledge, to disrupt or steal information from that computer, or to provide a base for attacks on another target. A single criminal can send a million e-mails within minutes for the cost of a few cents, and count on finding hundreds of inadequately protected computers to raid or capture. Criminal Web sites can bundle spyware or virus with legitimate downloads. Some spam or phishing e-mails now allow criminals to access a company or personal mailing lists containing many more.

Computer users can find their computers infected with malware in several ways, including opening malicious e-mail attachments, downloading programs, or simply visiting a fraudulent Web site. Cybercriminals have also begun to use instant messaging and bogus e-mail news services. Peer-to-peer networks (P2P) for file sharing have been a boon to cybercriminals. P2P software grants other participants on the network expanded access to computers and involves the download of large files. It is easy to bundle malicious code with a legitimate download. One strategy is for criminals to join the network, identify the most downloaded files, and then place a corrupted version of the popular file on a computer, knowing that peer-to peer programs on other network members' computers

will find and automatically download both the malicious and legitimate programs. The MyDoom virus, for example, started on a peer-to-peer network and then spread to e-mail.

Viruses have been a leading form of attack for cybercriminals and, according to the FBI, the most costly for business. Viruses began as a means for hackers to demonstrate their prowess, but they have become the delivery vehicle of choice for cybercriminals. Virus writers are now very sophisticated and often deploy several variants of the virus to test their effectiveness. Virus writers may also share code, so a virus may be relaunched in a different or improved form several times over the course of a year. Virus writers will often produce new, improved generations of the same virus within weeks of the first release. Advances in computing technology will probably provide new opportunities for viruses. They will soon target voice mail systems, wireless networks, handheld devices, and game consoles.

In 2004, virus writers even began to compete with each other for control of victims' computers. One virus, Netsky, removed its competitors from infected computers as it loaded itself, leading other virus writers to respond with new versions and a war of words against each other in hacker chatrooms and Web sites.

Currently, the most damaging form of cybercrime uses a two-phase attack. The first phase of the attack is to locate and covertly control as many computers as possible. The second phase is to use this unwitting network of computers for criminal purposes.

Cybercriminals use a variety of software tools to locate poorly defended computers—preferably those computers with always-on broadband connections—in homes, universities, and companies. Companies in some industry sectors, such as banks and electrical utilities, report that their computer networks are probed hundreds or thousands of times every day. These are sectors with an innate interest in security. Other sectors where security concerns are lower are probably unaware that they are under similar attack. The goal of the criminal virus writer is to covertly plant malware on the receiving computer. This malware can secretly provide valuable data stored or entered on the host computer, or it can be used to turn the host into a *bot*—a computer that executes instructions provided by the cybercriminal, usually without the knowledge of the computer's owner.

***Cybercrime Tools***

*Bots*—A bot (short for robot) is a computer on which a worm or virus has installed programs that run automatically and allow cybercriminals access and control. Cybercriminals use viruses or bots to search for vulnerable computers where they can load their own programs or store data. A bot network is a collection of these infected machines, often compromised weeks or months earlier by attackers using worms or viruses to plant backdoor components that can be centrally controlled and used to launch simultaneous attacks. Spammers, hackers, and other cybercriminals are acquiring or renting bot networks, making it harder for authorities to track down the real culprits.

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

*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 computer user downloads and installs the legitimate file, they are unwittingly also giving permission to install the criminal program.

*Denial of Service*—An attack specifically designed to prevent the normal functioning of a computer network or system and to prevent access by authorized users. A ***distributed denial of service*** attack uses thousands of computers captured by a worm or trojan to launch tens of thousands of e-mail messages at the target in a very short time. Attackers can cause denial of service attacks by destroying or modifying data or by using zombie computers to bombard the system with e-mails until its servers are overloaded and other users can no longer gain access.

*Packet Sniffer*—Software program that monitors network traffic. Attackers use packet sniffers to capture and analyze data transmitted via a network. Specialized sniffers capture passwords as they cross a network.

*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 computers systems on the network. Rootkits are available for most major operating systems.

*Spyware*—Software that gathers information without the users' knowledge. 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 in the background to someone else. Spyware can also gather and relay information on e-mail addresses, passwords, and credit card numbers.

*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.

*Social Engineering*—Social engineering is not limited to cybercrime, but it is an important element for cyber fraud. Social engineering tricks or deceives the recipient into taking an action or revealing information. The reasons given seem legitimate but the intent is criminal. Phishing is an obvious example—a certain percentage of users will respond unthinkingly to a request that appears to be from a legitimate institution.

*Trojan*—A malicious program unwittingly downloaded and installed by computer users. 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 it can act as a zombie and send spam or participate in a distributed denial of service 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.

*Worm*—Worms are 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 e-mail or Internet Relay Chat (IRC).

*Virus*—A program or piece of code that spreads from computer to computer without the users' consent. They usually cause an unexpected and negative event when run by a computer. Viruses contaminate legitimate computer programs and are often introduced through e-mail attachments, often with clever titles to attract the curious reader.

*Zombie*—A computer running programs that give control to someone other than the user. 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 (and usually covertly) execute a command to initiate a denial of service attack, send spam, or perform other activities.

The goal of many cybercriminals is to infect thousands of computers and turn them into a network of devices that attack in unison on command—a *bot-net* or network of robots. A bot-net is a collection of computers that have already been compromised by worms or viruses. Some malware packages even include their own server software to ease the bot's surreptitious connection to the Internet.

Those who succeed in creating bot-nets have created a very powerful tool for crime. Spammers, hackers, and other cybercriminals are acquiring or renting bot-nets—some owners will rent their networks to others for as little as $200 to $300 an hour. Cybercriminals have recognized the value of bot-nets, which are becoming the weapon of choice for fraud and extortion.

Bot-nets are crucial for distributed denial of service attacks, spam, and phishing—the theft of personal financial data. Spammers and phishers use the bot networks to contact thousands of potential victims. Carnegie Mellon's CERT stopped publishing the number of computer crime incidents in 2004, writing, "Given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks." Bot-nets enable one form of online extortion. The cybercriminal uses the computers under their control to bombard a company's Web sites with thousands of e-mails—a distributed denial-of-service attack. The cybercriminals then send an e-mail threatening renewed bombardment unless the company pays them.

Online fraud is a growth area for cybercrime. The Internet creates ambiguities into the process of identification—one bit looks much like another—that makes fraud easier. An assertion of identity is removed from any context in which we could judge its validity. There are no external clues and no opportunity for the judgments that accompany the use of physical credentials. Ambiguous identities are a major source of uncertainty and risk in the digital networks that span the globe, and an area of opportunity for cybercrime.

Internet scams, which trick people through fake Web sites and tales of woe into providing credit card and bank information, are threatening to swamp the FBI's Internet crime center with the volume of attacks. And while these scams used to come primarily from hackers in the United States, FBI officials and computer experts are seeing growing signs that the culprits are now members of organized crime and terrorist groups working from abroad.

One leading anti-phishing consortium estimates that 75 million to 150 million phishing e-mails are sent every day on the Internet. Another report found that 57 million Americans received phishing e-mails in 2004. Three percent of the 57 million suffered losses that totaled to $1.2 million. Even though the response rate is only one tenth of one percent, this is still 60,000 victims. Phishing e-mails now make up more than half of the 15,000 monthly citizen complaints filed to the FBI's Internet crime center. Companies are currently reporting 100,000 incidents a month. The FBI has had to upgrade its databases to keep up with the influx.

The FBI suspects that the phishers' growing skill is a sign of the introduction of experienced criminals into the fraud schemes. They believe that crime syndicates—especially in Russia and the former Soviet Union have begun to realize how much money they can make with little or no overhead. One estimate is that a third of all cybercrime is committed by groups from these regions. The FBI also believes that terrorist sympathizers operating outside of North America have also begun using phishing schemes to steal identities to make money after being shut out by counterterrorism measures from their traditional avenues of funding.

Prosecution of online extortionists is difficult. Experts believe there are a large number of unknown cases never reported to the police. Online betting companies have been the target of extortion scams, but are reluctant to talk openly about their experiences for fear of attracting more unwanted attention. They are also keen to play down the problem for fear of undermining confidence in the industry. One large Internet retailer, worried about its reputation, removed a link to an Internet fraud hotline from its site.

CASE STUDY: **Online Extortion**

**The $8 billion online-gambling industry has seen hundreds of attacks in the last year. One manager told how in January 2004 a flood of blank incoming e-mail messages inundated servers and slowed customer traffic to a crawl. Shortly thereafter, the company received an e-mail in broken English. It told the company to wire $40,000 to ten different accounts in Eastern Europe if it wanted its computers to stay online to receive customers' bets.**

# Section Three

## Looking to the Future

The move to a networked world and an information economy only increases the incentives for cybercriminals and the scope for their activities. As people and companies rely more and more on the Internet to do business, and as an essential means of communication, the more opportunity there is for cybercriminals to make money illegally—and the greater the risk of malicious attacks on users.

***Rising Threats to Mobile Devices***

Mobile wireless devices, such as cell phones or personal digital assistants (PDA), offer an attractive new target for cybercrime. So far, most cases have involved pranks—a celebrity's PDA is hacked and her phone list and pictures are posted on the Web, or the recipients get an SMS message and their phones' memory is erased. As wireless devices spread in number and as the applications that run on mobile devices increase, the temptation to turn some of these pranks into more serious crimes like embezzlement, extortion, and identity theft will grow. In the near future, cell phones will be more like computers, offering Web browsing and act as credit cards, allowing a user to automatically phone in a charge. When information that is more valuable is stored in the phone or PDA, cybercriminals will be attracted. Spam will play an important role as a delivery vehicle for trojans and viruses to mobile devices, just as it is now used for computers.

***Voice over Internet Protocol (VoIP)***

VoIP is not yet a major target for cybercrime. However, as VoIP spreads, it could offer criminals new opportunities to exploit computer vulnerabilities in the provision of telephone services.

***From E-Mail to Malicious Software***

The number of viruses that use e-mail as a delivery vehicle is declining. E-mail delivery will still be attractive to cybercriminals, but they will increase the use of other methods to get malicious code onto a computer.

***Exploitation of Wi-Fi Networks***

Wi-Fi networks are growing rapidly in number and coverage. Wi-Fi is inherently attractive to cybercriminals because of the difficulty of securing wireless networks from intrusion. *War driving* where hackers or criminals drive around a city looking for open access points is a new kind of crime that offers cybercriminals easy access to networks and valuable data. Kevin Mitnick, a reformed hacker says "The new wireless vulnerabilities are even worse than the old methods."

***Spam and Spyware***

Spam is often seen as an annoying marketing ploy that clogs inboxes and Internet connections. Cybercriminals have seized on spam as a reliable delivery vehicle for bots, trojans, and other spyware. In September 2004, the U.S. government estimated that each spammer sends out as many as 200 million messages a day. Spyware, like spam, is a questionable Internet tool that was originally used for marketing. Now it is increasingly being adopted by sophisticated cybercriminals. Several estimates put the percentage of infected computers to be over 50 percent.

CASE STUDY: **War Driving**

**In December 2004, two men sitting in a car in the parking lot of a home improvement store repeatedly hacked into the company's national computer network, altering its computer programs and gaining access to credit card numbers and other information. The intruders gained access to the company's national network by logging onto a user account over a single store's wireless network. Once in the system, the intruders gained access to stores in six states plus the headquarters' computer system. The hackers altered the software used by the company to process credit card transactions nationwide and installed a malicious program that disabled several of the company's computers.**

***Phishing and Identity Theft***

The weaknesses of digital identity management and the ability to use false identities to tap into global credit card and financial networks will continue to make this form of fraud attractive to cybercriminals. Although improvements in software and authentication technology will reduce some areas of risk for identity theft, social engineering will continue to provide opportunity for crime and new technological vulnerabilities like the ability to illegally duplicate some biometric identification data will likely be discovered.

*"Our information infrastructure is regularly probed for weaknesses countless times every day by hackers. Worms and viruses that can cripple vital systems propagate with frightening speed. These cyber incidents can cause billions of dollars in economic damages, and can pose a real physical risk when they disrupt vital infrastructure."*

—Margaret Bloodworth, Deputy Minister, Public Safety and Emergency Preparedness, May 25, 2005

# Conclusion

Cybercrime is not going to go away. As computer security improves, the cost of the damage it causes may fall, and it may evolve into different forms of attack, but as computers become more deeply embedded in daily activity, criminals will continue to use them. Individuals can defend against cybercrime by practicing a reasonable degree of computer hygiene, by installing anti-virus and anti-spyware programs and keeping systems updated and by exercising a reasonable degree of caution. Expanded use of encryption and authentication technologies will make the criminals' task more difficult. The information technology industry has begun the long and arduous process of building more secure computers and networks.

*"With the Council of Europe's Convention, we've seen that with the laws in place, people can be effectively prosecuted."*

—Paul Kurtz, Executive Director, Cyber Security Industry Alliance and a former White House cyber security official

Increased funding for law enforcement, including training in cyber forensics, improved vehicles for international cooperation (like the efforts in the G-8 to create national points of contact for cybercrime), and effective national laws (modeled on the Council of Europe Cybercrime Treaty) will also help narrow the opportunities for cybercriminals.

Carnegie Mellon's CERT Coordination Center's 2004 Annual Report states, "In every way, the next twenty years will bring more of everything. More threats, more attacks, more resources at risk, more interconnection, more communication, more emergencies."

It is hard to say if we are at the high tide of computer crime and can expect levels to drop in the future, or whether cybercrime will increase even further. What we can say is that as long as people use computers, criminals will attack them.

# APPENDIX

## National Law Enforcement Agencies

***Canada***

***Royal Canadian Mounted Police (RCMP)***—The RCMP is the leading law enforcement agency in Canada for cybercrime. The RCMP's Technological Crime program provides support services to investigators in the RCMP, to other Canadian police services or government agencies, and, in the case of Internet investigations, to any accredited international police service or agency. Individual RCMP divisions also have cybercrime responsibilities. For example, the National Capitol Region's A Division has an integrated technological crime unit (ITCU) that investigates computer crimes such as hacking, industrial espionage, denial of service, and viruses, and provides technological support to divisional investigators and other police forces. The Quebec RCMP's ITCU has twenty police officers who work in computer investigations and support conventional investigations.

***The Department of Justice, Federal Prosecution Service, eProsecutions Secretariat***—The Department of Justice, eProsecutions Secretariat's staff provides expertise in cybercrime to help prosecutors and to develop policy and legislation in response to new development and trends in computer-related crime.

***Competition Bureau***—Canada's Competition Bureau is an independent law enforcement agency responsible for the administration and enforcement of Canada's competition and consumer protection laws. It participates with the RCMP and other government agencies in efforts against phishing, spam, and fraud.

***United States***

***Department of Justice Computer Crimes and Intellectual Property Section (CCIPS)***—The CCIPS implements the Department of Justice's national strategies for combating computer and intellectual property crimes. CCIPS works with other government agencies, the private sector, academic institutions, and foreign counterparts to prevent, investigate, and prosecute computer crimes.

***Federal Bureau of Investigation***—The FBI is responsible for investigating cyber attacks by foreign adversaries and terrorists. The FBI also works to prevent criminals and malicious actors from using the Internet for theft or fraud. The FBI's cyber division coordinates and supervises FBI investigations of federal violations involving the Internet or computer networks for espionage, terrorism, or criminal activities.

***InfraGard***—An FBI program to create partnerships between FBI field offices and private sector companies to support FBI investigations. The program has 14,800 private sector members in eighty-four local chapters nationwide. Infragard's primary goal is sharing information and intelligence on cyber threats.

***Regional Forensic Computer Labs***—The FBI supports Regional Forensic Computer Labs (RCFL) through its RCFL National Program Office. RCFL are forensics laboratories that provide technical assistance in the examination of digital evidence in support of criminal investigations. There are currently seven RCFL in five states around the country and another six are planned for 2006.

***U.S. Secret Service***—The Secret Service investigates the criminal misuse of electronic technology for credit card fraud, unauthorized computer access, cellular and land line telephone service tampering, the production of false identification, counterfeit currency, threats made against the President, and other crimes. The Financial Crimes Division's Electronic Crimes Branch houses the equipment and personnel for electronic investigations and provides service to special agents located in more than 125 domestic and foreign offices.

***Immigration and Customs Enforcement (ICE)***—ICE is an investigative arm of the Department of Homeland Security. ICE's Cybercrimes Center investigates Internet crime cases involving child pornography, money laundering, arms and drug trafficking, and intellectual property rights violations.

***Federal Trade Commission***—The Federal Trade Commission investigates complaints involving spam, fraud, identity theft, and spyware, and takes legal action against violators.

## Major Cities' High-Tech Crimes Units

Many major cities in the U.S. and Canada, such as Vancouver, Edmonton, New York, Austin, and Los Angeles, have also created high-tech crime units responsible for investigating cybercrime. These units have specially trained investigators who know computers, how to collect and store digital evidence, and how to connect with the IT community for assistance. Some units specialize in particular criminal activities, such as financial crimes and fraud. Toronto police, in cooperation with the RCMP and with Microsoft®, have created a Child Exploitation Tracking System (CETS) that allows police to communicate and match data rapidly. Other police forces in Canada are making use of CETS, and the FBI has tested the system in the U.S.

# GLOSSARY

**Bot:** Rogue computer code used to operate a denial of service attack.

**Cybercrime:** Term used to describe all crime committed using computers, especially the Internet.

**Cyber Corporate Espionage:** Legitimate businesses using cybercrime to attack competitors or steal sensitive business information.

**Distributed Denial of Service (DDoS):** Hackers link thousands of computers and activate them to bombard a company Web site with bogus queries, paralysing normal operations before issuing a blackmail demand.

**Extortion:** Obtaining money from a third party by use of a threat.

**Hacking:** Unauthorized access to a computer, network, or Web site of a third party.

**Phishing:** Using spoof e-mails or directing people to fake Web sites to fool them into divulging personal financial details so criminals can access their accounts.

**Pump and Dump:** Organized criminals buy up cheap shares in a company, spread false business information via the Internet to increase the share price (pump), and then sell the shares at the high price (dump).

**Script Kiddies:** Hackers, usually teenage computer geeks, who disrupt a system for fun rather than financial gain.

**Trojan Horse:** A malicious program that appears to be harmless through the fact it is hidden.

**Zombie**: A computer that has been infected and is under the control of another person.

# FURTHER INFORMATION

## Press Inquiries, U.S.

**Tracy Ross**
McAfee, Inc.
Direct line: 408.346.5965
E-mail: tracy_ross@mcafee.com

**Ryan Lowry**
Porter Novelli
Direct line: 415.975.2294
E-mail: ryan.lowry@porternovelli.com

## Press Inquiries, Canada

**Kathy Swail**
McAfee, Inc.
Direct line: 514.428.2561
E-mail: kathy_swail@mcafee.com

**David Eisenstadt**
The Communications Group Inc.
Direct line: 416.696.9900
E-mail: deisenstadt@tcgpr.com

**Beth Merrick**
The Communications Group Inc.
Direct line: 416.696.9900
E-mail: bmerrick@tcgpr.com

## General Information

For additional information, please call 888.847.8766
or visit www.mcafee.com.

**McAfee, Inc.**
3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com