6 Cybercrime

Objectives

After completing this chapter, the student should be able to:

- Describe the three types of computer crime;
- Describe and define the types of Internet crime that target individuals and businesses; and
- Explain the key federal laws that target Internet crime against property.

6.1 Overview

This chapter will review privacy and security breaches on the Internet that are of a criminal nature, or called cybercrime. Broadly speaking, cybercrime is defined as any illegal action that *uses* or *targets* computer networks to violate the law.

The U.S. Department of Justice (DOJ)[317] categorizes computer crime in three ways:

1. As a target: a computer is the subject of the crime (such causing computer damage). For example, a computer attacks the computer(s) of others in a malicious way (such as spreading a virus).
2. As a weapon or a tool: a computer is used to help commit the crime. This means that the computer is used to commit "traditional crime" normally occurring in the physical world (such as fraud or illegal gambling).
3. As an accessory or incidental to the crime: a computer is used peripherally (such as for recordkeeping purposes). The DOJ suggests this would be using a computer as a "fancy filing cabinet" to store illegal or stolen information.[318]

6.2 Types of Crimes

Many types of crimes are committed in today's networked environment. They can involve either people, businesses, or property. Perhaps you have been a victim of Internet crime, or chances are you know someone who has been a victim. Crimes against a person or business include auction fraud, credit card fraud, debt elimination, parcel courier email scheme, employment/business opportunities, escrow service fraud, identity theft, Internet extortion, investment fraud, lotteries, Nigerian letter or "419," phishing/spoofing, Ponzi/pyramid, reshipping, spam, third party receiver of funds.[319] Property crimes involve cracking and hacking, drive by download, a logic bomb, malware, password sniffers, piggybacking, pod slurping, and wardriving.

6.3 Crimes Against a Person/Business

Auction fraud involves an online auction in which the goods described are not what the customer receives. Or, auction fraud could involve a buyer who transfers funds to a seller and the seller never receives the product. Online auction sites, such as eBay®, are very sensitive to this type of issue, and eBay has instituted a "money back guarantee" for customers who purchase an item from a fraudulent seller.[320]

Auction fraud from Romania is in its own category because it is often a part of fraudulent selling issues. In Romanian fraud, the seller appears to be from the United States, and creates a scenario that asks the buyer to send the money to a business associate or family member in Europe. The money is sent through Western Union® or a Moneygram®, which can be picked up anywhere in the world.

Credit card fraud is simply the unauthorized and fraudulent use of someone's credit card over the Internet.

Debt elimination involves a situation in which a website advertises elimination of a person's debt. The borrower fills out an application providing all their personal information and is asked by the debt elimination company to send a large deposit such as $3000 or $4000 with the borrower's application. In return, the debtor receives a "loan" document to present to their bank or mortgage company. Unfortunately, the document will be a fake, so the consumer will not only owe their original debt, but they will also have been cheated out of their deposit.

Counterfeit cashier's checks involve a situation in which an individual posts an item for sale on the Internet, and a prospective purchaser outside the U.S. contacts the seller expressing an interest in acquiring the item. The purchaser tells the seller he would like to buy the seller's item. However, the buyer tells the seller that someone owes him money that is more than the purchase price. The seller has his "phantom" borrower send a check to the seller to pay for the product. The amount of the check is more than the cost of the product, so the seller is asked to send the overpayment to the purchaser. Unfortunately, the check the seller receives in counterfeit. Figure 6-1 presents an example of this type of fraud.

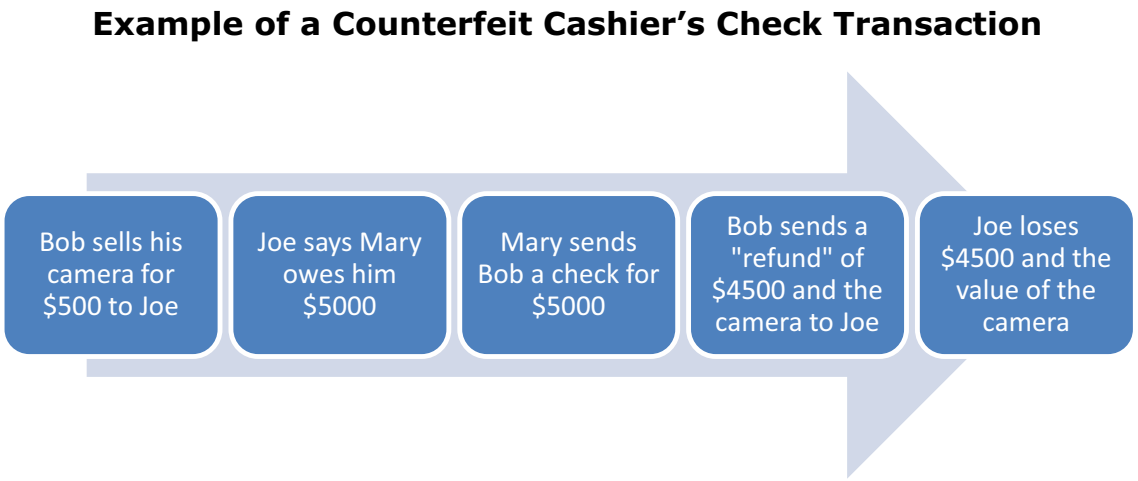

Figure 6-1

Another way that the counterfeit cashier's check has been used is with the "secret shopper" scam. A person receives a "cashier check" in the mail for roughly $3,000. Enclosed with the check is an official looking letter that says that "you have been selected to be a secret shopper to test the quality of service for Western Union." Also enclosed will be a survey form. The cashier's check will look very legitimate. The letter would include instructions to cash the check at a local bank, take $2800.00 of the $3,000.00 to Western Union, and send the $2800 to an address in California. Those caught by this fraud would be out $2800, instead of receiving the promised $200.

Email spoofing is the forgery of an email header so that a message appears to come from someone other than the true sender (who would be called the **spammer**). The recipient thinks that the email is legitimate and from the true sender. Spoofing is illegal under the CAN-AM SPAM Act[321]. Often times, the email will include a virus or link to a pornographic site when opened.

In **employment/business opportunities fraud,** typically there is an international company supposedly soliciting people for work at home opportunities. Similar to auction fraud, the potential employee is told that the company has U.S. based creditors and one of those will be paying the employee. However, when the person receives their paycheck, it is higher than what was owed and the employee is told to cash the check and then wire the difference back to the international company. The check is fraudulent, and the "employee" is out the entire amount of the check.

Escrow services fraud also involves Internet auctions. In this type of scam, the seller creates a payment look alike service such as PayPal®, which is actually a fake site. The victim sends money to the site to pay for their purchase, bus instead loses their funds.

Identity theft is the fastest growing Internet crime in the United States.[322] This is an instance in which the criminal takes someone's personal information, such as a Social Security number or a person's mother's maiden name, and impersonates that person to make purchases using the stolen credentials. Many times credit card purchases are also charged to the person whose credentials were stolen.

Tips for Preventing Identity Theft

Identity thieves steal your personal information to commit fraud. They can damage your credit status and cost you time and money restoring your good name. To reduce your risk of becoming a victim, follow the tips below:

- **Don't carry your Social Security card** in your wallet or write it on your checks. Only give out your SSN when absolutely necessary.
- **Protect your PIN**. Never write a PIN on a credit/debit card or on a slip of paper kept in your wallet.
- **Watch out for "shoulder surfers"**. Use your free hand to shield the keypad when using pay phones and ATMs.
- **Collect mail promptly**. Ask the post office to put your mail on hold when you are away from home for more than a day or two.
- **Pay attention to your billing cycles**. If bills or financial statements are late, contact the sender.
- **Keep your receipts**. Ask for carbons and incorrect charge slips as well. Promptly compare receipts with account statements. Watch for unauthorized transactions.
- **Tear up or shred** unwanted receipts, credit offers, account statements, expired cards, etc., to prevent dumpster divers getting your personal information.
- **Store personal information in a safe place** at home and at work. Don't leave it lying around.
- **Don't respond to unsolicited requests** for personal information in the mail, over the phone or online.
- **Install firewalls** and virus-detection software on your home computer.
- **Check your credit report** once a year. Check it more frequently if you suspect someone has gotten access to your account information.

Figure 6-2[313]

International lottery type frauds usually begin with an unsolicited email with a message a person has won or has been selected to receive money from an international lottery. The consumer is often asked to provide a variety of personal information to collect the promised funds.

Example of an International Lottery Scam[324]

"Congratulations! You may receive a certified check for up to $400,000,000 U.S. CASH!
One Lump sum! Tax free! Your odds to WIN are 1-6."

"Hundreds of U.S. citizens win every week using our secret system!
You can win as much as you want!"

Figure 6-3

Internet extortion has many twists and turns. The most common is a case in which someone hacks into a company's website or mainframe, and then refuses to give control back to the company unless a payment is made.

Investment fraud is defined as "an offer using false or fraudulent claims to solicit investments or loans, or providing for the purchase, use, or trade of forged or counterfeit securities."[325] The well-known billions of fraud[326] committed by Bernie Madoff[327] would fit in this category.

The **Nigerian letter** is a take-off from the lottery fraud, often called 419's, which is a section of the Nigerian civil code these schemes violate. With this scam, the perpetrator will send an email asking for the reader's help to transfer money to the United States. This is one of the oldest frauds on the net. The FTC provides more details in Figure 6-4 below.

The "Nigerian" Email Scam[328]
The Bait: These messages are the butt of late night jokes, but people still respond to them. The people behind these messages claim to be officials, businesspeople, or the surviving spouses of former government honchos in Nigeria or another country whose money is tied up temporarily. They offer to transfer lots of money into your bank account if you will pay the fees or "taxes" they need to get their money. If you respond to the initial offer, you may receive documents that look "official." They may even encourage you to travel to the country in question, or a neighboring country to complete the transaction. Some fraudsters have produced trunks of dyed or stamped money to try to verify their claims. **The Catch:** The emails are from crooks trying to steal your money or your identity. Inevitably, emergencies come up, requiring more of your money and delaying the "transfer" of funds to your account. In the end, there aren't any profits for you, and your money is gone along with the thief who stole it. According to State Department reports, people who have responded to their emails have been beaten, subjected to threats and extortions, and in some cases, murdered.

Figure 6-4

Online **phishing** (pronounced like the word fishing) is a way to trick computer users into revealing personal or financial information through a fraudulent email message or website. A common online phishing scam starts with an email message that looks like an official notice from a trusted source, such as a bank, credit card company, or reputable online merchant. In the email message, recipients are directed to a fraudulent website at which they are asked to provide personal information, such as an account number or password. This information is then used to steal a person's identity. As an aside, text messaging can also be used for phishing.

In a **Ponzi scheme,** an investment person promises what to most people appears to be an unreasonable rate of return on an investment. This is actually a fraudulent investment and the operator usually pockets the money. Similar to a Ponzi, is a **pyramid scheme**. This is an operation in which the operator takes money from one investor and uses a part of the proceeds to pay dividends to other investors, and keeps the remainder for his or her own use. Pyramid schemes also are perpetrated through email. Figure 6-5 below explains the process behind a pyramid scam.

How Pyramid Schemes Operate[329]

Let's look at how a pyramid scheme operates from three points of view: the potential investor, the promoter or con artist, and the victim Many pyramid schemes will present a payout formula or matrix much like this one:

	# Payment of $500		
Level 1 $150 x 3 = $450	#	#	#
Level 2 $30 x 9 = $270	###	###	###
Level 3 $30 x 27 = $810	#########	#########	#########
Level 4 $30 x 81 = $2430	etc. #########	#########	########etc.
-------- $3960			

This example illustrates what is known as a three by four matrix. Each investor pays $500 to the promoter and is told to build a "downline" by recruiting three new members, who then each should recruit three more members. The investor is told that he will be paid $150 for each of the three members whom he enlists at the first level. The investor is also promised a $30 commission for each recruit at the next three levels. Thus, the investor should receive commission for four levels of recruits below him, each of whom must recruit three more members, hence the name – a three by four matrix.

Figure 6-5

Skimmers are devices that attach to point of sale (POS) devices. They are used to capture credit card and bankcard information. In addition to devices at the point of sale, skimmers can be placed on ATM machines. These devices are essentially elaborate, genuine looking face plates placed over real ATMs. When a customer inserts his or her card, the skimmer reads the card just before the card enters the ATM machine. Typically, a small hidden camera has also been placed in close proximity to capture the customer's PIN number. Less frequently, a fake ATM will be in place, which receives a card, asks for the PIN, and then simply gives an "out of service" or other error message. The customer's card is then returned after recording the card information and PIN number. In addition, certain credit cards using RFID tags (radio frequency identification) can be electronically scanned with a skimmer from a few feet away. Note that enhanced drivers licenses and passports now have RFID tags embedded within them as well, and users of these cards should exercise caution particularly when traveling overseas.

Reshipping is similar to employment and business fraud, and occurs when a person is offered employment and their job is to package and ship products to the "employer" overseas. Unknown to the supposed employee, the goods he or she is packaging and shipping were purchased with fraudulent credit cards, so they are participating in shipping "stolen" merchandise.

Spam is the sending of unsolicited email to bulk email. However, spam can also be used to provoke attacks on company and government computers with viruses or botnets.

Third party receiver of funds has common elements with reshipping. The scammer posts availability of work at home job opportunities and the person's job is to post payments for the company. The business has its supposed client send the employee payment for his or her work. The checks are made out to the employee who is directed to deposit the checks in his or her personal bank account less commission (such as 10%) and then send the remainder (90%) via Western Union to the scammer located overseas. It is common that the person picking up the funds from Western Union will have fake ID, making tracking much more difficult.

6.4 Crimes Against Property

A **cracker** is someone who hacks, and uses his or her skills for illegal and personal gain. Crackers have an illegal intent in mind.

Drive by download occurs when an Internet user visits a website, or views an html email message, and a program is automatically downloaded to the user's computer. Most of the time, the user does not know the program is being installed.

Hacking is the unauthorized use and entry into a network by either a person or some sort of equipment.

A **logic bomb** is like a **Trojan horse** (see malware), but the program is activated upon some event or date.

Malware involves programming developed for doing harm. This could include computer **viruses** and **worms**, or Trojan horses. A virus is a computer program that, when downloaded, causes harm to a computer. A worm it is a self-replicating virus that resides in the computer and duplicates itself but it does not alter files. A Trojan horse is a program with harmful or malicious code that is found inside what the user believes is harmless data or a program. The Trojan horse's goal is to gain control of the user's computer or to harm its programs and data.

A **password sniffer** is a computer program that goes through a network to capture user passwords. It can be used for both legal and illegal means.

Pod slurping involves a person setting up a portable media player, such as an iPod®, to a business network to steal data and information. A keyboard is not needed to pod slurp, and to the casual observer, the person is simply listening to music.

Piggybacking is using an unsecured wireless connections to surf the Internet. This is actually theft of Internet bandwidth and it is communications theft.

Wardriving is driving around with a WIFI laptop and then mapping the houses, apartments and businesses that have unsecured, wireless access points. The driving part is not illegal.

There are many, many more types of crimes against property, but these are just a few.

6.5 Case Study One

This is a Nigerian 419 example.

Ann Marie Poet had worked for Michigan attorney Jules Olsman for nine years. One fall day in 2002, Olsman came back to the office from a business trip to find that paychecks he had just signed were being bounced by his bank. Upon investigation, he quickly learned that Poet, described as a meticulous and religious woman, had written checks over $2.2 million from the firm's account and were sent to Africa in a Nigerian scam. The woman only had $200 signature authority that the firm's financial institution, Bank One, had ignored.[330] The Bank One manager approved these transfers knowing she had limited signature authority. [331]

Since the embezzlement also involved client funds, Olsman eventually had to pump in one-half million in personal funds to cover the loss. He was particularly concerned because he could have been subject to discipline because of the loss of client funds.

Poet made 13 wire transfers between February and August of 2001 that encompassed the $2.2 million loss.[322] She was eventually indicted by a federal grand jury in Detroit, Michigan on 13 counts of wire fraud. Each count carried a maximum penalty of five years in prison and a $250,000 fine.[333]

6.6 Case Study Two

This is a Ponzi example.

P. Scott Scherrer was a smart and dashing attorney formerly from Michigan who later settled in New Hampshire. According to the federal court documents, "Scherrer induced or attempted to induce over 40 individuals or couples – some of them his friends – to "invest" over $3 million, primarily through sales of stock in a software company. False statements concerning the value of the stock and other particulars facilitated the sales and attempted sales. Scherrer did not buy the stock, but used the money to maintain a luxurious lifestyle, including membership in a country club, expensive cars, gambling, frequent vacations, and lavish entertaining,"[334] similar to the fraud perpetrated by Bernie Madoff.

It is interesting to note that Scherrer moved from Michigan to North Carolina to New Hampshire, while committing Ponzi and Pyramid schemes in each state. He was imprisoned in Michigan for a short period of time. It was not until the federal government charged Scherrer with a federal crime that he ended up in prison with a nine-year sentence.[335]

6.7 Case Study Three

Figure 6-6 below represents an example of an Internet employment fraud with ScottsMoneyBlog.com.[336] Frauds of this type should be reported to the Federal Trade Commission.[337]

Employment Fraud from ScottsMoneyBlog.com

Figure 6-6 Used with permission

6.8 Case Study Four

This case study is an example of hacking.

In December 2013, Target Corporation announced to its customers that its computing systems had been hacked between November 2013 to December 2013. Hackers were able to access customer debit and credit card information including names, addresses, email addresses, and phone numbers. At the time of the attack, this was described as the largest computer breach of customer information in US history.[328] Below is a customer letter received by your author, as one of Target's customers.

Target Guest Breach Notification Letter

Dear Target Guest,

As you may have heard or read, Target learned in mid-December that criminals forced their way into our systems and took guest information, including debit and credit card data. Late last week, as part of our ongoing investigation, we learned that additional information, including name, mailing address, phone number or email address, was also taken. I am writing to make you aware that your name, mailing address, phone number or email address may have been taken during the intrusion.

I am truly sorry this incident occurred and sincerely regret any inconvenience it may cause you. Because we value you as a guest and your trust is important to us, Target is offering one year of free credit monitoring to all Target guests who shopped in U.S. stores, through Experian's® ProtectMyID® product which includes identity theft insurance where available. To receive your unique activation code for this service, please go to creditmonitoring.target.com and register before April 23, 2014. Activation codes must be redeemed by April 30, 2014.

In addition, to guard against possible scams, always be cautious about sharing personal information, such as Social Security numbers, passwords, user IDs and financial account information. Here are some tips that will help protect you:

- Never share information with anyone over the phone, email or text, even if they claim to be someone you know or do business with. Instead, ask for a call-back number.
- Delete texts immediately from numbers or names you don't recognize.
- Be wary of emails that ask for money or send you to suspicious websites. Don't click links within emails you don't recognize.

Target's email communication regarding this incident will never ask you to provide personal or sensitive information.

Thank you for your patience and loyalty to Target. You can find additional information and FAQs about this incident at our Target.com/databreach website. If you have further questions, you may call us at 866-852-8680.

Gregg Steinhafel

Gregg Steinhafel

Chairman, President and CEO

Figure 6-7 Used with permission

6.9 Federal Legislation

This last section will review major federal legislation that controls many of the cybercrimes previously discussed. Laws to be covered include:

1. Computer Fraud and Abuse Act (18 U.S.C. § 1030)
2. Electronic Communications Privacy Act (18 U.S.C. § 2510)
3. Electronic Funds Transfer Act (15 U.S.C. § 1601)
4. Fair Housing Act (42 U.S.C. § 3601)
5. Identify Theft Penalty Enhancement Act (18 U.S.C. § 1001)
6. Mail and Wire Fraud Act (18 U.S.C. § 1343)
7. National Stolen Property Act (18 U.S.C. § 2314)
8. Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1961)
9. Securities Act of 1933 (15 U.S.C. § 77a) and the Securities and Exchange Act of 1934 (15 U.S.C. 78a–78kk)
10. USA Patriot Act (various)
11. Wire Wager Act (18 U.S.C. § 1084)

6.9.1 Computer Fraud and Abuse Act[339]

This law was enacted in 1984 and revised in 1994. It makes illegal the intentional and unauthorized access of a "federal interest computer." A federal interest computer may be:

- used by a financial institution,
- government computers,
- financial systems,
- medical systems,
- interstate commerce, and
- any computer on the Internet.[340]

The concept "federal interest" is interpreted broadly, and covers any area over which the federal government has jurisdiction (such as financial, medical, and government computers and computers relating to national security).

An interesting case based on a violation of the statute was decided by the United States District Court, Western District of Washington State in Seattle, in which a Michigan plaintiff, Justin Gawronski and California plaintiff, A. Bruguier, sued Amazon.com, after a copy of George Orwell's *1984* was deleted from their Kindle electronic reading devices. Amazon had remotely deleted the content from the devices without asking or telling the users, although Amazon did refund the payment amounts. The book was deleted because Amazon developed concerns over possession of the proper copyright permissions to have made the initial sale. Plaintiff's alleged Amazon committed a violation of the Computer Fraud and Abuse Act of 1986. Ultimately the case was settled in September, 2009, for $150,000. Additionally Amazon agreed not to delete or remove content in the future from Kindle devices, absent a few exceptions.[341]

6.9.2 Electronic Communications Act[342]

The Electronic Communications Act (ECPA) was signed into law in 1986. This key law provides rules for the access, use, disclosure, interception, and privacy protections of electronic communications. According to the law, electronic communications are defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce."[343]

This law protects computer networks and communication systems from tampering and eavesdropping. This law often also forms the basis for the prosecution of crackers.

6.9.3 Electronic Funds Transfer Act[344]

This law "establishes the basic rights, liabilities, and responsibilities of consumers who use electronic fund transfer services and of financial institutions that offer these services. The primary objective of the act and this part is the protection of individual consumers engaging in electronic fund transfers."[345] It outlines the legal rights of a consumer when confronted with a bank mistake or error on an ATM or banking statement, as well as the rights a consumer in case an ATM card is lost or stolen. This law also covers any Internet fraud involving a patron's bank account.

6.9.4 Fair Housing Act[346]

This law is the combination of traditional law with an Internet twist. The Fair Housing Act prohibits discrimination in the sale and rental of housing. The "twist" is that in 2004 the U.S. Department of Justice filed the first federal lawsuit against a website for violation of the law. Specifically, Spyder Web Enterprises was sued over an allegation of publishing notices and online ads on the Internet in violation of the Fair Housing Act,[347] and that Spyder Web discriminated based on race, gender, family status, religion, and national origin.

The law also applies to mortgage or home improvement loans discrimination on the web.

6.9.5 The Identify Theft Penalty Enhancement Act[348]

The Identity Theft Penalty Enhancement Act (ITPEA) is a 2004 law that provides penalties for aggravated identity theft, which is identify theft in conjunction with a felony, such as the use of a stolen identity to commit a crime. A person convicted of aggravated identity theft must serve an additional mandatory two-year prison term beyond the punishment for identity theft.[349]

More recently, Congress passed the Identity Theft Enforcement and Restitution Act of 2008.[350] The Act allows restitution to identity theft victims for time spent recovering from the harm caused by the actual or intended identity theft.

6.9.6 Mail and Wire Fraud Act[351]

This law goes back to the nineteenth century to 1872. Under the Mail and Wire Fraud Act, a person commits mail or wire fraud if he or she has "a) perpetuated a scheme to defraud that includes a material deception; b) with the intent to defraud; c) while using the mails in furtherance of the scheme."[352]

Fraudulent actions on the Internet, fall under this statute. Keep in mind that intent is a key element of this crime and intent must be evident from the facts the perpetrator intended to commit the crime. Punishment for a conviction under the mail fraud statute is a fine or imprisonment for not more than five years, or both. If the violation affects a financial institution, the punishment is increased and "the person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both."[353]

6.9.7 The National Stolen Property Act[354]

The National Stolen Property Act (NSPA) criminalizes the "*interstate* transportation, transmittal, transfer, receipt, possession, concealment, storage, barter, sale, or disposal of any goods, wares, merchandise, securities, money or articles used in counterfeiting valued at $5,000 or more."[355] It requires evidence of actual knowledge that the goods were stolen or that the perpetrator should have known they were stolen.[356] Presenting proof that the person receiving goods was unaware the goods were stolen can be admitted as a defense.

6.9.8 Racketeer Influenced and Corrupt Organizations Act[357]

The Racketeer Influenced and Corrupt Organizations Act, known as RICO, is a law originally passed to curb organized crime. However, courts have broadly interpreted the law to also cover criminal enterprises[358] that take place over the Internet. RICO has been used to combat rogue Internet pharmacies and some Internet gambling, along with many other more traditional crimes that are not web based.

Under RICO, certain acts are prohibited, including:

- Investment of income derived from racketeering activities in an enterprise engaged in interstate commerce;
- Acquisition or maintenance of interest in an enterprise that effects commerce *through racketeering activities*;
- Conduct or participation in an *enterprise's affairs* **through** *a pattern of racketeering activities*; or
- Engaging in a conspiracy to do any of the above.[359]

The maximum penalties for racketeering include a fine of up to $25,000 and up to 20 years in prison plus forfeiture of monetary gains and profits.[360]

6.9.9 Securities Act of 1933[361] and the Securities and Exchange Act of 1934[362]

Securities fraud is a crime that has matured from a friend-to-friend interaction to online interaction. In securities fraud, a criminal will use blogs, message boards, and chat rooms that focus on the stock market to make posts that are intended to manipulate stock prices. In other words, the criminal posts lies about the value of a company's stock. This is called "pumping up" the price of the stock, or a pump and dump scheme.[363]

"Pump-and-Dumps" and Market Manipulations[364]

"Pump-and-dump" schemes involve the touting of a company's stock (typically small, so-called "microcap" companies) through false and misleading statements to the marketplace. These false claims could be made on social media such as Facebook and Twitter, as well as on bulletin boards and chat rooms. Pump-and-dump schemes often occur on the Internet where it is common to see messages posted that urge readers to buy a stock quickly or to sell before the price goes down, or a telemarketer will call using the same sort of pitch. Often the promoters will claim to have "inside" information about an impending development or to use an "infallible" combination of economic and stock market data to pick stocks. In reality, they may be company insiders or paid promoters who stand to gain by selling their shares after the stock price is "pumped" up by the buying frenzy they create. ***Once these fraudsters "dump" their shares and stop hyping the stock, the price typically falls, and investors lose their money.***

Figure 6-8

Often times, the criminal in a pump and dump might have a false online identity, which is referred to as a "sock puppet." One example of pumping up involved the former CEO of Whole Foods Market. The CEO, John Mackey used a "sock puppet" and posted messages on Yahoo stock message boards for about seven years to push his company's stock and to criticize the business efforts of his competitors.[365]

6.9.10 USA Patriot Act[366]

The Patriot Act's full name is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. It has been controversial from its inception, primarily because many of the traditional constitutional safeguards were changed by its inaction. The law was passed in response to the terrorist attacks of 9/11.

The Patriot Act amended many federal statutes. One key provision is that the federal government may intercept electronic messages that are "relevant to an ongoing criminal investigation".[367] In the past, the law required that a crime first had to have been committed before messages could be intercepted. This law applies to all types of surveillance cases and it is not limited to those that appear to be related to suspected terrorists.

One criticism of the law is the lowering of the bar that the government can use to intercept Internet routing information. The law also allows ISP's to disclose voluntarily to the government customer records and content of electronic transmissions.[368]

Another controversial area of the law is that it allows, "sneak and peek warrants".[369] Such warrants allow federal law enforcement agencies, such as the FBI, to search a home or business without immediately notifying the person or company that they are the target of an investigation. In other words, this section allows for "delayed notice" of search warrants. This is a contentious provision because law enforcement can use these warrants for minor crimes and not only terror and espionage cases.

6.9.11 Wire Wager Act[370]

The U.S. Wire Wager Act makes illegal the use of an electronic wire method (i.e. the Internet) to transmit bets to places where gambling is not allowed. Therefore, a casino set up in the Bahamas is breaking U.S. law if a player in the U.S. plays their games. However, the U.S. does not really have the legal authority to prosecute someone in another country. The federal government relies primarily on the Wire Wager Act (WWA) to prosecute online casino operators.

This law states:

> Whoever being engaged in the business of betting or wagering knowingly uses a wire communication facility for the transmission in interstate or foreign commerce of bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest, or for the transmission of a wire communication which entitles the recipient to receive money or credit as a result of bets or wagers, or for information assisting in the placing of bets or wagers, shall be fined under this title or imprisoned not more than two years, or both.[371]

There is some controversy application of the law to the Internet; yet attempts to amend the law or enact a specific law on Internet gaming have not been successful. If this law is challenged in court, changes may take effect. Note that many credit card companies decline credit card transactions from online casinos based on pressure from the U.S. DOJ.

6.10 Summary

In this chapter, you learned that the U.S. DOJ classifies computer crimes as a target, as a weapon or tool, and as an accessory or incidental to a crime. Computer crimes can be against a person or business, or against property. Several key federal laws were discussed; however, the list was not intended to be exhaustive. Instead, it was meant to provide an overview of the key crimes that take place on the Internet. It should be noted that most of these laws were not written to address Internet crimes, and courts have been forced to take existing laws and *make them work*.

6.11 Key Terms

Auction fraud	Escrow services fraud	Password sniffer
Auction fraud from Romania	Fair Housing Act	Pod slurping
Computer Fraud and Abuse Act	Hacking	Piggybacking
Conspiracy/RICO	Identity theft	Ponzi/Pyramid
Cracking	Identity Theft Penalty	Racketeer Influenced and Corrupt
Credit card fraud	Enforcement Act	Organizations Act
Counterfeit cashier's checks	Internet extortion	Reshipping
Debt elimination	Investment fraud	Securities Act of 1933
Drive by download	Logic bomb	Securities and Exchange Act of 1934
Email spoofing	Lottery type frauds	Spam
Electronic Communications Privacy Act	Mail and Wire Fraud Act	Third party receiver of funds
Electronic Funds Transfer Act	Malware	USA Patriot Act
Employment/business opportunities fraud	National Stolen Property Act	Wardriving
	Nigerian letter	Wire Wager Act
	Online phishing	

6.12 Chapter Discussion Questions

1. How does the U.S. DOJ describe computer crime?
2. What is a Nigerian letter or "419"?
3. Provide an example of identity theft.
4. What is the difference between hacking and cracking?
5. Who is a third party receiver of funds?
6. What is wardriving?
7. The Mail and Wire Fraud Act goes back to 1872. How can such an old law be relevant to the Internet?
8. Under RICO, what is a criminal enterprise?
9. What is the NSPA?
10. List three key elements of the USA Patriot Act.

6.13 Additional Learning Opportunities

For more information on cybercrime look at the following sources for more ideas:

Department of Justice Computer Crime & Intellectual Property Section's website at http://www.cybercrime.gov;

The Computer Emergency Response Team (CERT) at http://www.cert.org;

The National Infrastructure Protection Center at the FBI at http://www.infragard.net provides regularly updated information and descriptions of cybercrimes;

The Federal Trade Commission at http://www.ftc.gov; and

The Internet Crime Complaint Center at http://www.ic3.gov.

The primary federal law enforcement agencies that investigate domestic crime on the Internet include the Federal Bureau of Investigation (FBI), the United States Secret Service, the United States Immigration and Customs Enforcement (ICE), the United States Postal Inspection Service, and the Bureau of Alcohol, Tobacco and Firearms (ATF).

For more information on identity theft, you can visit the Federal Trade Commission website http://www.ftc.gov in which they have an entire section on this crime and what to do if you become a victim.

6.14 Test Your Learning

1. Drive by download is an example of using a computer
   A. as a target
   B. as a weapon or tool
   C. as an accessory
   D. incidental to a crime

2. Auction fraud is an example of a
   A. crime against a person/business
   B. crime against property
   C. crime against the government
   D. crime against a person/business and property
   E. crime against property and the government

3. Charlie Criminal uses a skimmer to take a person's credit card information from a credit card reader at a gas station. This is an example of
   A. debt elimination
   B. counterfeit cashier's checks
   C. escrow services fraud
   D. identity theft
   E. Ponzi/pyramid

4. A computer program is set to be activated on September 11, 2016, and act as a virus to shut down the system. This is an example of
   A. cracking
   B. logic bomb
   C. pod slurping
   D. piggybacking
   E. wardriving

5. This law provides privacy protection for electronic communications.
   A. Electronic Communications Act
   B. Electronic Funds Transfer Act
   C. Mail and Wire Fraud Act
   D. National Stolen Property Act
   E. RICO

6. This law is used to combat rogue Internet pharmacies.
   A. Electronic Communications Act
   B. Electronic Funds Transfer Act
   C. Mail and Wire Fraud Act
   D. National Stolen Property Act
   E. RICO

7. Pump and dump violates which of the following laws?
   A. Electronic Communications Act
   B. Electronic Funds Transfer Act
   C. National Stolen Property Act
   D. RICO
   E. Securities Act of 1933/Exchange Act of 1934

8. This law allows for sneak and peak warrants.
   A. National Stolen Property Act
   B. RICO
   C. USA Patriot Act
   D. Wire Wager Act
   E. None of the above

9. This law was enacted as a response to the 9/11 attacks in the United States.
   A. National Stolen Property Act
   B. RICO
   C. USA Patriot Act
   D. Wire Wager Act
   E. None of the above

10. In debt elimination fraud
    A. a website advertises it will eliminate a person's debt
    B. the consumer is asked to send a large money deposit with their application
    C. documents from the "loan" company are fake
    D. all of the above
    E. none of the above

Test Your Learning answers are located in the Appendix.