

Cyberdeviance is a fascinating mix of old crime and new opportunity....
—Jeffrey Arbaugh

Cybercrime

Chapter

12

Objectives

- Define and understand digital piracy.
- Define cybercrime and understand the importance of this behavior.
- Understand the importance of cybercrime markets.
- Recognize the extent of pornography as a cybercriminal behavior.
- Define identity theft and identity fraud.
- Understand the ease with which identity theft and fraud can occur as part of cybercriminal behavior.
- Know the steps to help minimize the likelihood of becoming a cybercriminal.
- Define and understand cybercrime communities.

Features

Theory in Action: What Would You Do to Get the CD?

Theory in Action: How Do You Explain This Much Identity Theft?

Wrap up

Chapter Spotlight

Putting It All Together

Key Terms

Notes

introduction

Computer crime has been an issue in criminal justice and criminology since the 1970s. In this venue, the types of computer crimes fall within two categories: computer theft or using computers to commit crimes. First, a prevalent activity is criminals stealing computers. For example, during final exams at a university, a student who is studying leaves his or her computer to use the restroom. When the student returns, the computer is missing. Second, criminals use computers to commit crimes.

Technological development in the 1980s allowed many individuals to be able to own and use a personal computer. Before this period, computers were large, bulky, and expensive. In the early 1960s, J.C.R. Licklider dreamt of a global communication system. His idea was to internationally connect a set of computers that would allow for easy access to information. Licklider named his idea “Galactic Network.” This “Galactic Network” is now known as the Internet. As the Internet has grown in development, use, and popularity, it has provided criminals another place to commit their crimes. Taken as a whole, the development of the personal computer and the Internet has provided the tools for an emerging area of criminal behavior called cybercrime.

Cybercrime is a criminal act that occurs over the Internet using a computer. The Internet has become the source for multiple types of crimes and different ways to perform these crimes. The types of crime may be loosely grouped into three categories of cybercrimes: (1) fraudulent behavior (i.e., cyberfraud), (2) the creation and maintenance of cybercrime markets, and (3) the development of cybercriminal communities. The purpose of this chapter is to outline and exemplify these different forms of digital communities. The chapter then shifts into policy approaches to reduce some types of cybercrime.

Cybercrime markets

The Internet allows for illicit markets to be created and maintained. Users can hide their identities and be in remote locations to create and be part of illicit markets. For instance, cybercriminals can use different Websites to trade (i.e., buy or sell)

merchandise illegally through legitimate sources (e.g., eBay) or through illegal sites while they are in a different neighborhood, city, state, or country. Some of these Websites and users are not traceable back to their original sources. While a host of illicit markets exist (e.g., illegal adoptions, surrogate mothers, egg donors, banned substances, organ donors, forbidden animals, endangered species, and illegal gambling), the discussion in this chapter will focus on digital piracy, cyberpornography, cyberfraud, and cybercrime communities.

Digital Piracy

An important form of cybercrime is digital piracy. **Digital piracy** is defined as the illegal act of copying digital goods, such as software, documents, audio (including music and voice), and video, for any reason other than to back up (i.e., save a copy) without explicit permission from and compensation to the copyright holder.¹ **table 12-1** presents different behaviors that may be deemed digital piracy.

The Internet has facilitated an increase in digital piracy in recent years. Four characteristics of the Internet that have enabled individuals to easily commit criminal activity include the Internet’s transnational nature, the ease of anonymous communication, a shift in thinking from the ownership of physical property to the ownership of ideas, and the fact that piracy does not require a lot of skill.² Additionally, some contend that the Internet facilitates piracy because it allows the offense to take

TABLE 12-1

summary of Forms of Digital piracy

type of Digital piracy	example
Software piracy	Downloading or using software without properly securing the copyrights to the software.
Music (i.e., audio)	Downloading or sharing music without the express written consent of the copyright holder. In other words, the individual does not pay for the music that he or she has obtained.
Voice	Obtaining someone else’s voice for use from the Internet.
Video	Downloading or sharing video without the express written consent of the copyright holder. In other words, the individual does not pay for the video that he or she has obtained.

TABLE 12-2

summary of teenage perpetration of Digital piracy

year	percentage
2004	60
2006	43
2007	36

Source: Business Software Alliance—*Fact Sheet: Youth and Downloading Behavior* (2007); see also <http://www.bsa.org/country/Research%20and%20Statistics/~media/5D4CE35FE06A4AE394059943D1B3B28E.ashx>

place detached from the copyright holder, which provides the offender with the perception that the act is victimless.³ Recent percentages of teenage perpetration of these acts are summarized in table 12-2.

Several researchers have acknowledged sub-forms of digital piracy (e.g., audio and video piracy) as being increasingly pervasive.^{4, 5} Audio and video piracy has been defined as the “illegal act of uploading or downloading digital sound or video without explicit permission from and compensation to the copyright holder.”⁶ Higgins, Fell, and Wilson analyzed data from a study of college students to examine the roles of self-control and learning in understanding digital piracy. Their results indicated that those with low self-control are likely to learn the techniques necessary to perform digital piracy and that once the techniques are learned, the individual is likely to develop

intentions to perform digital piracy.⁷ Beyond an individual’s level of self-control and learning the techniques to perform digital piracy, technological advancements are partly responsible for the increased ease of and accessibility to digital piracy. Industry monitors have estimated that one in three music discs purchased around the world are an illegal copy.⁸ The International Federation of the Phonographic Institute (IFPI) further estimates that 37% of all CDs purchased in 2005 were pirated, resulting in 1.2 billion illegal copies purchased worldwide.⁹ By these estimates, pirate CD sales outnumbered legitimate CD sales in 30 markets across the world and resulted in a loss of \$4.5 billion from the music industry.¹⁰ See **Theory in Action: What Would You Do to Get the CD?** for more on this topic.

Similar issues exist in the context of the movie industry. Industry figures indicate that the costs of unauthorized copying and redistribution of movies via physical media (e.g., video cassettes, DVDs, VCDs, etc.) exceed several billion dollars annually. In 2005, over 90% of the movies that were initially pirated were camcord recorded in movie theaters.¹¹ The Internet has allowed for movie pirates to be able to illegally download movies.¹² In 2005, the MPAA reported that \$2.3 billion were lost due to Internet piracy.¹³

THEORY IN ACTION

What Would you Do to get the CD?

Chris heard that a popular CD has just been released to music stores nationwide. All of Chris’ friends have heard the CD and said that it is great and that he has to get it. Unfortunately, every time that Chris tries to buy the CD, he cannot because it is always sold out, and Chris cannot buy the CD online. However, a friend tells him about a Website that has posted an underground copy of the entire CD. The site will only allow members to download the CD. Chris really wants the CD, so he thinks about it for two days and then becomes a member and downloads the CD.

Use two criminological theories to explain Chris’s decision to join the Website and download the CD. Contrast how the different theories influence the explanations.

Source: Higgins, G. E., Fell, B. D., & Wilson, A. L. (2006). Digital piracy: Assessing the contributions of an integrated self-control theory and social learning theory. *Criminal Justice Studies: A Critical Journal of Crime, Law, and Society*, 19, 3–22.

Several have argued that college students are likely to pirate almost all forms of digital media. For instance, Hinduja used a sample of college students to show that piracy is a prevalent behavior. From the sample, a piracy profile emerged: male, Asian, between the ages of 17 and 20, and a member of the freshman class.¹² According to the Business Software Alliance, the trend of piracy among college students fell slightly in 2007 compared to 2003 and 2005 rates.¹³ **table 12-3** summarizes these trends.

Importantly, two-thirds of students still believe that it is OK to swap or illegally download software without paying for these items. This is an example of a technique of neutralization. Techniques of neutralization allow an individual to take a moral holiday to perform a deviant or criminal act. **table 12-4** summarizes this issue.

Since the Copyright Act of 1976, digital piracy has been considered a criminal act.¹⁴ Mass copyright violations of movies and music were made a felony offense in 1982 by The Piracy and Counterfeiting Amendments Act. The No Electronic Theft Act amended the 1982 act to include the distribution of copyrighted materials over the Internet.¹⁵ That is, when an individual proceeds to burn an extra copy of a music CD, download music from the Internet without paying, or use a peer-to-peer network to download music information, they are pirating music. This is especially true for digital music piracy that is committed through a multitude of modus operandi such as CD burning, peer-to-peer networks, LAN file sharing, digital stream ripping, and mobile piracy (see www.IFPI.org for a discussion of these techniques). The penalties for these acts and legislation may be civil (e.g., \$10,000 per pirated copy) and criminal (e.g., possible jail sentences).¹⁶

TABLE 12-3
summary of College student piracy rates

year	percentage
2003	68
2005	61
2007	55

Source: Business Software Alliance—*Fact Sheet: Higher Education Unlicensed Software Experience—Student and Academics* (2007); see also <http://www.bsa.org/country/Research%20and%20Statistics/~media/F3F0E9C1C2AB4B308D5D6D0E3042A5A7.ashx>

Several criminologists have applied criminological theories to explain digital piracy. For instance, Gottfredson and Hirschi's version of self-control theory links with digital piracy.¹⁷ Individuals will weigh the pleasure of digital piracy against the potential pain of digital piracy.¹⁸ When the pleasure outweighs the pain, the individual is inclined to perform the act. Self-control is also a deciding factor. Impulsive individuals are not likely to wait to purchase the digital media (e.g., songs or movies) so that they properly own the copyrights.¹⁹ That is, individuals who have low self-control are less likely to consider the consequences of their digital piracy. Others have found similar results that self-control is correlated to digital piracy.^{20, 21}

Social learning theory may help to explain software piracy.²² Applying social learning theory, individuals who associate with others that perform digital piracy (i.e., differential association), are likely to acquire attitudes (i.e., definitions) that are favorable to performing digital piracy. In addition, the individual will find digital piracy rewarding from their friends, and they will learn the techniques for digital piracy through imitation of the behavior. Researchers have found social learning theory has a link with software piracy and an expanded definition of digital piracy.^{23, 24}

Rational choice/deterrence theory is a means to understand how to reduce instances of digital piracy. Specifically, deterrence theory can be applied to software piracy.²⁵ Higgins, Wilson, and Fell used a sample of college students to examine the role of deterrence. They used a factorial design (i.e., an experimental design) to determine whether different factors for certainty that piracy would be discovered and severity of punishment once piracy was discovered would deter the students from performing software piracy. In addition, Higgins et al.

TABLE 12-4
summary of College student beliefs: it's OK to swap

year	percentage
2003	23
2005	32
2007	33

Source: Business Software Alliance—*Fact Sheet: Higher Education Unlicensed Software Experience—Student and Academics* (2007); see also <http://www.bsa.org/country/Research%20and%20Statistics/~media/F3F0E9C1C2AB4B308D5D6D0E3042A5A7.ashx>

applied some concepts from contemporary deterrence theory (e.g., shame and family discovery). The results indicated that certainty of discovery, shame, and family discovery were the most relevant factors to deter an individual from performing software piracy. Specifically, they argued that rational individuals are less likely to perform software piracy when the chances of being detected increase and the likelihood of punishment is certain and severe.

Cyberpornography

Cybercrime includes the promotion and distribution of unwanted pornography. This is known as **cyberpornography**. The promotion of pornography is the unwanted emails or solicitations to view pornography. The distribution occurs when emails are provided that include the pornography attached or within the message. While pornography may not be criminal for those of age, the Internet does not discriminate access based on age. That is, teenagers' sexual fantasies are replaced by hardcore pornographic images of every conceivable sexual activity easily found on the Internet.

In the academic literature, some researchers have shown that cyberpornography is an emerging issue. For instance, researchers used data from kids and young adults to examine their exposure to cyberpornography.²⁶ They showed that individuals who sought out cyberpornography were likely to be male, 14 years old and older, and more depressed than older females. Individuals who were younger than 14 were more likely to be exposed to pornography through traditional mediums—movies and magazines.²⁶

Stack, Wasserman, and Kern used the General Social Science Survey to examine who viewed pornography using the Internet and their reasons why.²⁷ This study included several thousand responses from individuals in the United States. Data showed that individuals with weak religious ties, unhappy marriages, and past sexual deviance were more likely to view pornography via the Internet.²⁸ The study also showed that when employment status increased, technology did assist in the access to cyberpornography.

The Internet allows cybercriminals to participate in underage liaisons. One form of this particular type of cybercrime is the online solicitation of children for sex. This is exploitation that

involves an adult who engages in discussion with a child online and uses his or her manipulation skills to coerce to meet the child in person for sexual purposes.

The anonymity of the Internet allows cybercriminals to have the ability to disguise their postings, responses, and identities. This affords the cybercriminals the opportunity to disappear at a moment's notice. In short, the Internet allows cybercrimes to be performed easily and simply while making their detection, apprehension, and prosecution difficult. Therefore, the Internet makes cybercrimes through illicit markets more difficult to examine.

Cyberfraud

Cyberfraud includes behaviors that are committed with guile and deceit. An example of this behavior is identity theft that may lead to identity fraud. Definitions for identity theft vary. For instance, one definition of **identity theft** is, "the unlawful use of another's personal identifying information."²⁹ Others have defined identity theft as "involv[ing] financial or other personal information stolen with intent of establishing another person's identity as the thief's own . . ."³⁰ The FTC sees identity theft as "occur[ring] when someone uses your personally identifying information, like your name, Social Security number, or credit card number without your permission to commit fraud or other crimes."³¹ This chapter adopts the FTC's definition of identity theft, although, some may regard this definition as identity fraud. In one sense, identity fraud involves financial or other private information stolen, or totally invented, to make purchases or gain access to financial accounts.³² See **Theory in Action: How Do You Explain This Much Identity Theft?** for an example of this type of fraud.

The FTC's definition clarifies some of the potential forms of personal information that may be used in identity theft. Other forms of personal information include address, date of birth, alien registration number, and government passport. While these forms of personal information and the definition of identity theft provide some context, identity theft can be summed up as constituting the unauthorized use of someone else's personal information for criminal activity.

how Do you explain this much identity theft?

In October 2002, an FBI team searched a house in New Rochelle, New York. The team thought that they had completed their search, but one officer was unconvinced and was not about to let months of investigation go for nothing. The officer returned to a bedroom that seemed to have oversized furniture. The officer pulled the draping back from an oversized canopy over a bed and discovered hundreds of individuals' identities that had been used in an intricate scheme that netted nearly \$50 million.

At the time, this case was described as the biggest identity theft ever uncovered in the United States. Two perpetrators committed this crime; one had contacts with a ring of Nigerian street criminals and the other

was a help-desk clerk at a software company. They used several means of obtaining the identities that included Internet access. Their crimes victimized at least 30,000 people nationwide. Some of their activities included taking out as much as \$65,000 in loans.

Is this identity theft or identity fraud? What theory may be used to explain the activities of the perpetrators?

Source: (2004, October 24). Identity theft is epidemic. Can it be stopped? *New York Times*, Retrieved March 18, 2009, from <http://www.nytimes.com/2004/10/24/business/yourmoney/24theft.html>

Federal Statutes

The crime of identity theft has received substantial coverage from a wide variety of legal mechanisms. A substantial number of federal and state statutes relate to the criminality of identity theft and those who suffer its victimization. In the federal arena, the laws relating to identity theft are convoluted. They can, however, be divided into statutes that relate to criminality and penalties and statutes that provide consumers with information or rights. The primary criminal statute in the federal system is the Identity Theft and Assumption Deterrence Act of 1998. Specifically, this statute makes it a federal crime when anyone “knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.”³³ In 2004, the Identity Theft Penalty Enhancement Act was enacted.³⁴ This act provides for enhanced punishments for identity thieves. For example, the act requires an additional two years of punishment for those violators using another’s identity in the commission of a crime and five-year sentences for the use of a false identity in the commission of a terror offense.³⁵ Sentencing discretion is also restricted in

that sentences may not run concurrently for offenses, and probation is prohibited for those convicted under the statute.

Other federal statutes provide some aid for victims of identity theft.³⁶ The Fair Credit Reporting Act establishes procedures for persons seeking to correct mistakes on their credit record and ensures that credit histories are only provided for legitimate business needs.³⁷ The Fair and Accurate Credit Transactions Act allows consumers to obtain free copies of their credit reports as well as restricts what information can be placed on a sales receipt. Similarly, the Fair Credit Billing Act establishes procedures for resolving billing errors on credit card accounts and establishes limits on a consumer’s liability for fraudulent credit card charges.³⁸ And, the Electronic Fund Transfer Act focuses on transactions using debit cards or electronic means to debit or credit an account and limits the liability for unauthorized electronic fund transfers.³⁹

State Laws

Since the majority of all criminal prosecutions occur in state court systems, state legal schemes are critically important. All 50 states and the District of Columbia have criminal laws relating to identity theft.⁴⁰ Thirty-one states have created freeze laws

for persons fearing identity theft. These laws generally lock access to credit reports, scores, and limits. While these laws vary greatly, there is generally no charge for the creation, temporary lifting, or complete termination of a freeze (a so-called credit thaw) for the victim of identity theft. Others wishing to limit their risks may have to pay between \$5 and \$20. While these freezes will not completely shield a consumer from victimization, they will stop the creation of any new victimization where the issuer relies upon a credit report to provide credit. A few states have statutes that require the credit reporting agencies to block false information from consumer victims' credit reports within a certain time frame or upon the receipt of a police report.

California was the first state to pass a mandatory disclosure law for persons whose information has been compromised. Currently, at least 35 states have some form of breach notification statute. These laws vary greatly by state. The threshold for notification may be mandatory upon a security breach. For example, Massachusetts recently passed a mandatory notification law similar to California's. Other states have a risk-based analysis requiring notification only in cases of substantial risk of harm. These laws are based on three rationales. First, with timely notice consumers can take preventive measures to limit or reduce the potential for identity theft. Second, reporting provides an ability to accurately measure the true number of breaches and thus aids in research on identity theft. Lastly, the social and pecuniary costs associated with notification provide substantial motivation to protect consumer information.⁴¹ Notification laws differ from fraud alert protections. An alert requirement forces notification if a person's credit file receives an inquiry. A breach notification law requires that a consumer be informed when his or her information has been compromised.

Forms and Costs of Identity Theft

Identity theft or identity fraud creates a large number of issues around the theft of information. Identity thieves commit fraudulent acts to obtain identities of other individuals. For instance, identity thieves may "hack" (i.e., break into network databases) via the Internet to obtain personal information. Another form of fraudulent activity is the use of "phishing." Phishing is when an identity criminal goes online and poses as a corporation (e.g., requesting information from Western Union, Amazon, eBay, or PayPal) or an individual in need (e.g., travel scams, stock frauds, financial transfers, nondelivery of merchandise, Internet auction fraud, credit card fraud) and requests personal information. An emerging form of identity theft is "pharming." Pharming is when a hacker redirects an individual from a legitimate site to a fraudulent site without the user's knowledge.

These forms of identity theft over the Internet are costly to the economy and the victim. For instance, it has been shown that the U.S. economy was particularly susceptible to identity theft, and over a span of three years (1995 to 1997), identity theft resulted in actual losses ranging from \$442 million to \$745 million.⁴² Others have estimated that identity theft costs total between \$53 to \$73.8 billion annually.⁴³ While this gives some perspective, the true extent of identity theft is unknown. Identity theft also can have profound individual costs. For instance, a victim can expect to pay up to \$3000 and spend a substantial amount of time restoring his or her identity.⁴⁴

table 12-5 presents the different types of identity theft. The most common complaint is credit card fraud, followed by phone, utility, employment, and bank fraud.⁴⁵

TABLE 12-5

summary of Forms of identity Fraud

type of identity theft	example
Credit card fraud	Using someone else's credit card identity without their knowledge
Phone or utilities fraud	Establishing phone or utility services in someone else's identity without their knowledge
Employment-related fraud	Gaining employment-related benefits using someone else's identity
Other identity theft	Bank fraud Government benefits fraud Loan fraud Attempted identity theft



Some weeks, 20,000 people contact the Federal Trade Commission about recovering from identity theft.

Source: FBI.

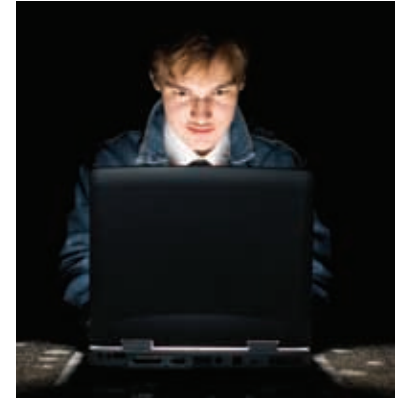
It took the Senate almost five years to ratify the Council of Europe Convention on Cybercrime, the major international treaty that allows governments to work together to combat cybercrime. Suspected cybercrime havens such as Lithuania and Romania ratified it years before the United States did.

Source: Council of Europe.



Cybersecurity research accounted for 1% of the Department of Homeland Security's science and technology research budget. The research funding for biological attack countermeasures was roughly 22 times as large.

Source: Department of Homeland Security, American Association for the Advancement of Science.



There were 326 data breaches during 2006. Only five thieves were successfully prosecuted for data breaches throughout the year.

Source: Privacy Rights Clearinghouse.

What to Do to minimize risk of identity theft or Fraud

1. Check your credit reports once a year from all three of the credit reporting agencies (Experian, Transunion, and Equifax).
2. Guard your Social Security number. When possible, don't carry your Social Security card with you.
3. Don't put your Social Security number or driver's license number on your checks.
4. Guard your personal information. You should never give your Social Security number to anyone unless you can verify that they are required to collect it.
5. Carefully destroy papers you discard, especially those with sensitive or identifying information such as bank account and credit card statements.
6. Be suspicious of telephone solicitors. Never provide information unless you have initiated the call.
7. Delete any suspicious email requests without replying. Remember: If your bank or credit card company needs you to contact them, they have telephone numbers and Website information on your statement. You do not have to click on unsolicited emails to contact them.

steps to take if victimized

1. Contact the fraud departments of each of the three major credit bureaus and report that your identity has been stolen.
2. Get a "fraud alert" placed on your file so that no new credit will be granted without your approval.
3. Contact the security departments of the appropriate creditors and/or financial institutions for any accounts that may have been fraudulently accessed. Close these accounts. Create new passwords on any new accounts that you open.
4. File a report with your local police and/or the police where the identity theft took place.
5. Retain a copy of the police report because it may be needed by the bank, credit card company, or other businesses as evidence that your identity was stolen.

Source: National White Collar Crime Center (2007).

Cybercrime Communities

The Internet provides a place for cybercriminal communities to exist and flourish. The communities may be seen as subcultures. Subcultures are cohesive cultural systems that vary in form and substance from the dominant culture. A subculture maintains values, beliefs, and traditions that differ from the dominant culture. Thus, individual behaviors are consistent with those of the subculture, but differ from the dominant culture. Examples of subcultures include ethnic groups, delinquent gangs, and religious sects. Others may form or primarily exist on the Internet.

Cybercriminal subcultures may utilize individuals who understand and can infiltrate computer operating systems (i.e., hackers). About 75% of companies reported that hacking is likely from employees, and 45% of companies have reported unauthorized access by insiders.⁴⁶

Others deviants or criminals also may be part of an online subculture (e.g., pedophiles). Cybercrime communities are important to cybercriminals because they are the venue where their criminal activities are reinforced and encouraged. These communities create more effective criminals by transmitting knowledge and legitimizing criminal behavior. In short, the individuals participating in these deviant subcultures learn new techniques for

performing their behavior and how to handle potential issues (e.g., outsiders, legal or medical services). For instance, an individual may learn how to hide his or her pedophilia behavior in one of these communities. Cybercrime communities provide a level playing field; in these communities, individuals are not alienated, rebuked, or ostracized based on age, race, sex, marital status, ethnicity, or socioeconomic status. All that is required is a computer, an Internet connection, and an individual with criminal intent who is able to learn from the community.

Conclusion

Cyberspace is a relatively new venue for criminal activity. Some criminal behaviors that previously took place on the streets are now perpetrated on the Internet and with greater ease. Additionally, the characteristics of the Internet encourage new forms of criminal behavior. For instance, the Internet has created new venues to pirate digital media, to view and transmit pornography, and to commit fraudulent behavior. As the Internet grows, so too do the opportunities for criminal activity. This growth requires a greater understanding of these crimes and those who commit them, as well as policies that protect against cybercrime.

WRAP UP

Chapter spotlight

- Cybercrime is an emerging area of study for criminologists.
- Digital piracy (e.g., stealing music, movies, and software) is a cybercrime with many markets both on and off the Internet.
- Pornography is a form of cybercrime when individuals younger than 18 are participants. Participation includes the making, viewing, or marketing of pornography. Each method of participation is a criminal act.
- Cyberfraud encompasses identity theft and identity fraud. Identity theft and identity fraud are fast-growing criminal behaviors. These activities cost the United States billions of dollars each year.
- Cybercrime communities are important because they provide havens for cybercrime and deviance on the Internet. For instance, these communities may help hackers become better at their work.

putting it all together

1. Define cybercrime and provide examples of this behavior.
2. What are the main categories for thinking of cybercrime?
3. What is a subculture and how do they work with cybercrimes? Use two theories to help guide your response.
4. Discuss the importance of cyberfraud to individuals and to countries as a whole.

Key terms

cybercrime A criminal act that occurs over the Internet using a computer.

digital piracy The illegal act of copying digital goods such as software, documents, audio (including music and voice), and video for a reason other than to back up (i.e., saving the media) without explicit permission from and compensation to the copyright holder.

cyberpornography The promotion and distribution of unwanted pornography using the computer or Internet.

identity theft When someone uses your personally identifying information, like your name, Social Security number, or credit card number without permission in order to commit fraud or other crimes.

NOTES

1. Higgins, G. E., Fell, B. D., & Wilson, A. L. (2006). Digital piracy: Assessing the contributions of an integrated self-control theory and social learning theory. *Criminal Justice Studies: A Critical Journal of Crime, Law, and Society*, 19, 3–22.
2. Wall, David S. (2005). The Internet as a conduit for criminal activity. In Pattavina, A. (ed). *Information Technology and the Criminal Justice System*. Thousand Oaks, CA: Sage, pp. 78–94
3. Leiner, B., Cerf, V., Clark, D., Kahn, R., Kleinrock, L., Lynch, D., Postel, J., Roberts, L., & Wolff, S. (2003). A brief history of the Internet. *Internet Society*. From <http://www.isoc.org/internet/history/brief.html>
4. Gopal, R., Sanders, G. L., Bhattacharjee, S., Agrawal, M., & Wagner, S. (2004). A behavioral model of digital music piracy. *Journal of Organizational Computing and Electronic Commerce*, 14, 89–105.
5. Hinduja, S. (2003). Trends and patterns among online software pirates. *Ethics and Information Technology*, 5, 49–61.
6. Note 3, p. 4.
7. Note 1.
8. International Federation of Phonographic Industries (IFPI). (2004). *The recording industry 2004 piracy report: Protecting creativity in music*. Retrieved December 7, 2004, from www.ifpi.org/content/section_news/20041007d.html
9. Note 8.
10. Note 8.
11. Motion Picture Association of America (MPAA). (2005). *U.S. piracy fact sheet*. Retrieved December 10, 2006, from www.mpa.org/USPIRACYFactSheet.PDF
12. Motion Picture Association of America (MPAA). (2004). *U.S. piracy fact sheet*. Retrieved December 10, 2004, from www.mpa.org/anti-piracy/content.htm
13. Note 11.
12. Hinduja, S. (2003). Trends and patterns among online software pirates. *Ethics and Information Technology*, 5, 49–61.
13. Business software alliance. *Fact sheet: Youth and downloading behavior*. Retrieved January 27, 2011, from <http://www.bsa.org/country/Research%20and%20Statistics/~media/5D4CE35FE06A4AE394059943D1B3B28E.ashx>
14. Note 1.
15. Koen, C. M., & Im, J. H. (1997). Software piracy and its legal implications. *Security Journal*, 31, 265–272.
16. Note 15.
17. Higgins, G. E. (2005.) Can low self-control help with the understanding of the software piracy problem. *Deviant Behavior*, 26, 1–24.
18. Note 17.
19. Note 17.
20. Higgins, G. E., & Makin, D. A. (2004.) Does social learning theory condition the effects of low self-control on college students' software piracy? *Journal of Economic Crime Management*, 2, 1–22. Retrieved on March 5, 2007, from www.jecm.org
21. Note 1.
22. Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency*, 34, 495–518.
23. Note 20.
24. Note 1.
25. Higgins, G. E., Wilson, A. L., & Fell, B. D. (2005). An application of deterrence theory to software piracy. *Journal of Criminal Justice and Popular Culture*, 12, 166–194.
26. Ybarra, M. L., & Mitchell, K. J. (2005). Exposure to Internet pornography among children and adolescents: A national survey. *Cyberpsychology & Behavior*, 8, 473–486.
27. Stack, S., Wasserman, I., & Kern, R. (2004). Adult social bonds and use of Internet pornography. *Social Science Quarterly*, 85, 75–88.
28. Buzell, T. (2005). Demographic characteristics of persons using pornography in three technological contexts. *Sexuality and Culture*, 9, 28–48.
29. Bellah, J. (2001). Training: Identity theft. *Law & Order*, 49(10), pp. 222–226.
30. Identity Theft. (2004, December 15). Confusion between fraud, identity theft frustrates industry. *LRP Publications*, 8, 12.
31. Federal Trade Commission. (2004). *About identity theft*. Retrieved January 27, 2011, from www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html
32. Higgins, G. E., Hughes, T., Ricketts, M. L., & Fell, B. D. (2005). Student perception and understanding identity theft: “We’re just dancing in the dark.” *Law Enforcement Executive Forum*, 5(5), pp. 163–178.
33. Aggravated Identity Theft, 18 U.S.C. § 1028A (2004).
34. Note 33.
35. Acts of Terrorism transcending national boundaries. (2004). Section 2332b(g)(5)(B).
36. The Fair Debt Collection Practices Act.
37. Fair Credit Reporting Act, 15 U.S.C. § 1681 to 1681u. (2004).
38. Fair Credit Billing Act, 15 U.S.C. § 1666i. (2004).
39. Consumer Credit Protections: Electronic Funds Transfer, 15 U.S.C. § 41, 1693. (2004).
40. Federal Trade Commission. (2007). *National and state trends in fraud & identity theft: January–December 2005*. Retrieved September 13, 2007, from <http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/national-data.html>

41. Schneier, B. (2006). *The anti-ID-theft bill that isn't*. Wired.com. Retrieved November 1, 2007, from <http://www.wired.com/politics/security/commentary/securitymatters/2006/04/70690>
42. Allison, S. F. H., Schuck, A. M., & Lersch, K. M. (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice*, 33(1), 19–29.
43. Weingart, J. (2003). Identity theft. *The Metropolitan Corporate Counsel, Northeast Edition*.
44. Federal Trade Commission. (2006). *National and state trends in fraud & identity theft: January–December 2005*. Retrieved January 27, 2011, from <http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/national-data.html>
45. Federal Trade Commission. (2007). *National and state trends in fraud & identity theft: January–December 2005*. Retrieved January 27, 2011, from <http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/national-data.html>
46. Computer Security Institute (CSI). (2010). *CSI: Computer crime and security survey*. Retrieved January 27, 2011, from <http://gocsi.com/members/reports>