9

Juveniles and Cybercrime
After reading this chapter you should be able to

1. Explain the emergence of cybercrime
2. Define digital piracy and discuss the perception of many juveniles that it is an acceptable form of behavior
3. Define cyberbullying and describe its categories
4. Define cyberstalking and cyberharassment
5. Identify various forms of online sexual exploitation
6. Describe the behaviors and values of the hacking community

Key Terms in Chapter 9

black hats
cyberbullying
cybercrime
cyberstalking
digital piracy
hackers
hacking
Internet
revenge porn
sexting
sextortion
white hats

INTRODUCTION

In 2008, Jonathan Joseph James shot himself in the head in the shower of his home. He was 24 years old. James, however, will always hold a not-so-enviable record: He was the first juvenile incarcerated for cybercrime in the United States. Born in South Florida, James was 15 when he committed his first offense—a hack of the Miami-Dade school system’s computers. After that, he became a prolific hacker. He was brought down a year later when he attacked computers of the federal Defense Threat Reduction Agency, a part of the U.S. Defense Department (DOD). In the attack, James obtained mission-critical NASA files, including software used to control the living habitat inside the International Space Station. The news caused NASA to disconnect its computers from the Internet for 3 weeks while an investigation was underway. Federal agents were able to identify James as the source of the DOD attacks, and his house was raided in January of 2000. A few months later, he entered into a plea agreement under which he admitted to two counts of juvenile delinquency. He was sentenced to 7 months of house arrest and placed on probation until his 18th birthday. Under the terms of the agreement, he was banned from the recreational use of computers. He soon violated the probationary terms when he tested positive for drugs. Following the failed drug test James was arrested and sent to a federal correctional facility, where he served a 6-month sentence.

The prison experience appeared to have a huge impact on James, and he vowed never to return. Not long after his release, however, some of his cyber associates carried out a massive data breach of numerous department stores’ computers, and authorities began to investigate James’s possible involvement in the scheme. While credible evidence linking James to the crimes was never found, he apparently
believed that he would soon be arrested again—a belief that led to his suicide. He left a note in which he wrote: “I honestly, honestly had nothing to do with [these crimes, but] I have no faith in the ‘justice’ system.”

THE INTERNET

**LO 9.1** Explain the emergence of cybercrime.

The Internet has dramatically changed the lives of many youths, but it has also opened up a variety of new possibilities for crime—much of it involving young people. The Internet can be traced back to the early 1960s, when J. C. R. Licklider of the Massachusetts Institute of Technology (MIT) proposed the idea of an internationally connected set of computers, known as the Intergalactic Computer Network. Working with MIT colleagues, Licklider pressed for improvements in networking capabilities and efficiency. Licklider and colleagues eventually created a set of interconnected computers called the ARPANET, which evolved into the Internet. While large corporations were active in the early days of Internet, using computer systems that took up entire rooms, Internet did not become popular in homes and businesses until the 1990s.

The Internet we know today is a global network of interconnected networks using standardized protocols, allowing people to share information, pictures, and other data. We have become dependent on it for shopping, paying bills, researching, maintaining relationships, and even getting an education. Because the Internet contributes to many different types of activities, it has also provided a new nexus for criminality—and it often does not take a degree from MIT to commit crime online, known as cybercrime. **Cybercrime** is the “destruction, theft, or unauthorized or illegal use, modification or copy of information, programs, services, equipment or communication networks.” In other words, cybercrime is any crime that uses technology, including computers, smartphones, and the Internet itself.

Cybercrime can range from the smallest online credit card theft to the biggest Ponzi scheme. Someone can request a mail-order bride and get scammed out of a lot of money or become the victim of a nasty malware infection. Similarly, terrorist groups can recruit and raise funds online. This chapter will review common forms of cybercrime, especially those often committed or experienced by juveniles.

**DIGITAL PIRACY**

**LO 9.2** Define digital piracy and discuss the perception of many juveniles that it is an acceptable form of behavior.

For years, a popular target for young shoplifters was cassette tapes, and later music CDs. Today, music and other digital materials are often stolen on the Internet. This material can be downloaded onto smartphones, iPods, and other electronic devices. **Digital piracy** is the act of illegally copying music, movies, software, and other digital materials without permission from or payment to the copyright holder. Piracy behaviors are quite simple to carry out, possibly explaining why a great many such pirates are under age 21. Youths enjoy listening to music and watching movies, and the temptation to access them for free (albeit illegally) can be extremely alluring. Juveniles generally pirate movies or music for convenience and not for the thrill of stealing. Several studies have estimated that digital music worth $14 billion has been stolen over the past decade or so. According to the Recording Industry Association of America, only 37% of music owned in the United States was
legally purchased, and legitimate music sales have dropped by 50% since 1999, when file sharing was introduced. Even with all the free music available on apps and Internet radio, about 70% of Internet users admit to supporting the idea of digital piracy.4

The question is, how can someone justify stealing this material? Many people who would find it unfathomable to walk into a music store and steal a CD think nothing of illegally downloading music online. One potential explanation comes from social learning theory (discussed in Chapter 3), which asserts that criminal behavior is learned, much like tying your shoes or using a fork. Offenders learn these behaviors from people close to them. According to this theory, if your friends are illegally downloading online material and find it completely acceptable, you will mimic that behavior. After all, everyone is doing it!

Another view is found in Sykes and Matza’s techniques of neutralization (see Chapter 3), under which offenders rationalize behaviors. They justify their behavior by denying that it causes any injury, or by telling themselves that everyone does it. For instance, offenders can justify that illegally downloading Beyoncé’s newest song and not paying the $1.49 charge (on iTunes or Amazon Music) won’t affect Beyoncé or her record company. However, if 100,000 Internet users steal the song, that’s a loss of $149,000.5

Digital piracy is often overlooked by the juvenile court system because the system is overloaded with more serious cases, such as burglary, auto theft, and sexual assault. While legislation such as the Copyright Felony Act and the No Electronic Theft Act introduces higher fines and even prison sentences for adults who commit digital piracy, courts have generally taken a milder stance with juveniles. Antipiracy advertising campaigns on TV are often directed at juveniles, and if digital piracy is committed in a school, it could result in loss of computer privileges for the whole school.

CYBERBULLYING

» **LO 9.3** Define cyberbullying and describe its categories.

Bullying is repeated, intentional, and aggressive behavior that is intended to establish dominance and intimidate.6 The Internet version of bullying is called cyberbullying, which is the “willful and repeated harm inflicted through the use of computers, cell phones, and electronic devices.”7 Unlike physical bullying, just one act of cyberbullying can be repeated again and again virtually when one nasty and untrue post is passed on to others.

Cyberbullying can occur in many ways via electronic means, as described in Table 9.1.

<table>
<thead>
<tr>
<th>TABLE 9.1</th>
<th>Categories of Cyberbullying</th>
</tr>
</thead>
<tbody>
<tr>
<td>CATEGORY OF CYBERBULLYING</td>
<td>DEFINITION</td>
</tr>
<tr>
<td>Harassment</td>
<td>Insulting or taunting the victim through repetitive messages, such as e-mails, instant messages, or texts</td>
</tr>
<tr>
<td>Outing</td>
<td>Sharing of the victim’s personal information with others without permission, such as telling others that a person who has not “come out” publicly is gay</td>
</tr>
<tr>
<td>Flaming</td>
<td>Hostile and insulting interaction in a chat room or on a discussion board, often involving the use of profanity</td>
</tr>
<tr>
<td>Denigration</td>
<td>Posting untrue and insulting information</td>
</tr>
<tr>
<td>Exclusion</td>
<td>Ostracizing a person</td>
</tr>
</tbody>
</table>
PART III  JUVENILE BEHAVIORS

In many cases, cyberbullies have dominant personalities and short tempers. Many youths who say their friends are cyberbullies are also cyberbullies themselves. And cyberbullies are less likely to be caught than are bullies on the playground, because they can act anonymously on the Internet.

Victims of cyberbullying, especially juveniles, often have a difficult time coping with the harassment, gossip, and humiliation that results from cyberbullying. They may not be physically abused, but they face many of the same outcomes as victims of physical bullying, such as dropping out of school, drug use, and even displaying aggression toward others. They may experience anxiety, depression, loneliness, and suicidal thoughts, and may even attempt suicide.

The Cyberbullying Research Center surveyed middle school and high school students in the United States regarding what would help block or reduce the impact of cyberbullying. More than 30% of these students reported that blocking a cyberbully online stopped the behavior, and 18.9% ignored the behavior. While 16.5% informed the cyberbully’s parent, only 7.6% reported the perpetrator to the website, but those students who did said this was an effective strategy. Faced with losing privileges on Twitter, Facebook, or other social media, cyberbullies often end their behavior. However, victims may also refrain from reporting cyberbullying for fear that their parents or guardians will take away their cell phones, laptops, or social media, not as a punishment but as a protective measure.

CYBERSTALKING

LO 9.4 Define cyberstalking and cyberharrassment.

Most stalkers in physical space are familiar to their victims, such as would be the case with past romantic partners or shunned acquaintances. But online stalkers, known as cyberstalkers, may victimize complete strangers. Cyberstalking is the monitoring or harassment of another person on the Internet. Cyberstalkers may access their victims’ e-mail and social networking accounts without permission. They may then pretend to be the victim in posts and other communication. For instance, a female high school student (Girl 1) could log into the Instagram page of another student (Girl 2) and post nasty remarks about a male friend, making it seem as though Girl 2 was the writer. Cyberstalkers may also threaten to release personal information about their victims, continually send them unwanted instant messages, or post humiliating photographs of them.

Cyberstalking can be a part of cyber dating abuse. Current or former romantic partners, many of whom are juveniles or young adults, monitor the online behaviors, locations, and other activities of their victims. This is called “low-tech” cyberstalking. Cyberstalkers are often very open about their activities, location, and helpers, so their movements can usually be tracked by officials. In addition, there are “high-tech” methods, such as computer spyware apps, listening devices and bugs, and video or digital cameras, that allow some to stalk victims online without their knowledge. GPS locators can be downloaded on a person’s cell phone without their knowledge so the victim’s movements can be tracked. Since most young people depend on the Internet to form and maintain relationships, they often find these forms of cyberstalking more acceptable as a way of checking up on what partners are doing.

Cyberstalking is becoming a growing trend among young people as a way to monitor romantic partners. New federal and state laws are addressing cyberstalking as a serious criminal offense and have designated appropriate punishments. The National Conference of State Legislatures (NCSL) reports that many states
have passed laws against cyberstalking or cyberharassment, often by adding new language to existing antistalking laws. The NCSL defines these two activities this way:

**Cyberstalking** is the use of the Internet, email or other electronic communications to stalk, and [it] generally refers to a pattern of threatening or malicious behaviors. Cyberstalking may be considered the most dangerous of the types of Internet harassment, based on posing a credible threat of harm. Sanctions range from misdemeanors to felonies.

**Cyberharassment** differs from cyberstalking in that it is generally defined as not involving a credible threat. This behavior usually pertains to threatening or harassing email messages, instant messages, or blog entries or websites dedicated solely to tormenting an individual. Some states approach cyberharassment by including language addressing electronic communications in general harassment statutes, while others have created stand-alone cyberharassment statutes.

### ONLINE SEXUAL OFFENSES BETWEEN ROMANTIC PARTNERS

Based on the [NCSL](https://www.ncsl.org) definition, here are brief descriptions for the terms used:

**Cyberstalking** is the use of the Internet, email, or other electronic communications to stalk, and it generally refers to a pattern of threatening or malicious behaviors. Cyberstalking may be considered the most dangerous of the types of Internet harassment, based on posing a credible threat of harm. Sanctions range from misdemeanors to felonies.

**Cyberharassment** differs from cyberstalking in that it is generally defined as not involving a credible threat. This behavior usually pertains to threatening or harassing email messages, instant messages, or blog entries or websites dedicated solely to tormenting an individual. Some states approach cyberharassment by including language addressing electronic communications in general harassment statutes, while others have created stand-alone cyberharassment statutes.

### Child Pornography and Sexting

A Florida news outlet reported that Phillip Alpert, age 18, and Jane Doe, age 16, had been dating for 2 years when Jane sent Alpert a nude picture of herself. Afterward the couple had an argument. As revenge, Alpert forwarded the picture to Jane’s family and friends. Alpert was subsequently charged with possession and distribution of child pornography, as well as lewd and lascivious battery. He pled no contest and was sentenced to a year of probation. Under Florida law, Alpert also had to register as a sex offender and will remain on the list for at least 25 years. Being listed as a sex offender harmed his reputation, destroyed employment opportunities, and led to his expulsion from community college.

**Putting It Into Action**

To complete this active learning assignment, you should pair up with a friend (whether a classmate or not) and discuss the following questions:

- How do you both feel about Alpert’s punishment? Was it appropriate for his crime? Should Jane have also been punished (if so, how)? Should sexting offenders be required to register as sex offenders? Why should age matter?
- Summarize the conclusions that you and your friend arrive at, and describe any differences in opinion.
- Submit your work to your instructor when asked to do so.


In December 1965, Mary Beth Tinker was 13 years old when she and a group of friends wore black armbands to protest the Vietnam War. The school board heard about the protest and passed a preemptive ban. Four other students were suspended, including Mary Beth’s brother, John, and his friend Chris Eckhardt. They were not allowed to return to school until the armbands were removed. The suspended students returned after Christmas break without the armbands but wore black the rest of the year in protest.

Via their parents, the students sued the school district for violating their right to expression, claiming that the students should not have been disciplined. The district court dismissed the case, and the U.S. Court of Appeals of the Eighth Circuit confirmed that ruling. In February 1969, the U.S. Supreme Court ruled in favor of the students, stating they do not “shed their constitutional rights to freedom of speech or expression at the schoolhouse gate.” In the ruling, written by Justice Abe Fortas, the court held that wearing the armbands was freedom of speech and if schools wished to suppress the speech of the students, they must verify that it would “materially and substantially interfere” with the school’s operation.

1. Do you agree with the ruling?
2. How does a juvenile’s right to freedom of speech apply to what can be posted online?
3. In your opinion, would this ruling be the same today?

**Online Case Opinion**

---

**Sexting**

Sexting is the use of a cell phone, tablet, or other electronic device to share sexually explicit content. Pictures or videos often show at least one person nude or partially nude, and sometimes performing sexual acts. Sexting may also include sexually suggestive or aggressive text. Past research shows that 5% to 35% of young people participate in sexting. Females are often more likely to admit to creating and sending the material than are males.

Although the activity is socially discouraged, sexting is permissible between two consenting adults, but not when it is unwanted, harmful, or involves an adult and a minor. Sexual material can easily be forwarded to other parties without the permission of the victim. Let’s say John, age 17, and Hailey, age 16, are high school students consensually dating. Hailey sends a topless picture of herself to John. Rather than keeping it to himself, John sends the picture to a few friends, and they post it on social media sites, where it can be viewed by thousands of people within a few hours, potentially traumatizing Hailey and destroying her reputation.

While most sexting is a protected form of free speech under the First Amendment, the age of the people sending and receiving the material can lead to serious federal and state criminal offenses. In our example, if John sent the photo of Hailey to Henry, a high school senior who is 18 years old and thus legally an adult, Henry could be criminally prosecuted for possession of child pornography, because Hailey is a minor. And if Henry forwarded the photo to his friends, he could also be charged with distribution of...
child pornography.\textsuperscript{21} Child pornography statutes protect individuals under the age of 18 from violation and abuse.\textsuperscript{22} Although Hailey originally sent the picture of her own volition, child pornography statutes protect her from what transpired after that point.

**Revenge Porn and Sextortion**

Angry ex-lovers can seek revenge against their ex-partners on thousands of websites by posting \textit{revenge porn}, which is sexually explicit material posted without the consent of the subject.\textsuperscript{23} Some argue that this is a form of sexual assault, because it is demeaning to the subject. Many of these photos are selfies taken by the subject, usually a woman, and only meant for her partner. The subject did not give permission to share the photo with others.

Victims of revenge porn are sometimes harassed or stalked by strangers who saw the pornographic material online. Laws against this behavior are slowly going on the books. As of May 2017, 35 states and the District of Columbia had passed bills criminalizing revenge porn.\textsuperscript{24} However, penalties vary. For instance, while California considers revenge porn a misdemeanor disorderly conduct, North Carolina considers it a Class H felony for adults over age 18. Initiatives to pass legislation in more states are gaining prominence, such as EndRevengePorn.org, headed by Dr. Holly Jacobs, a victim of revenge porn.

A fairly new online crime, often linked with revenge porn, is sextortion. \textit{Sextortion} is the acquisition of sexually explicit photographs or videos that are then used to blackmail the victim.\textsuperscript{25} The material is often obtained by hacking into the victim’s computer or cell phone, but the victim may also have provided it willingly. Offenders may use the photographs to get money from the victim in exchange for not posting the sexually explicit material online, or even request more photographs or videos of sexual acts as a kind of ransom.

The Crimes Against Children Research Center at the University of New Hampshire found that about 60% of sextortion victims knew the offenders in some way and 40% met them online.\textsuperscript{26} Most offenders were male and most victims were female, and almost half of victims were under the age of 18.

The Federal Bureau of Investigation has warned Internet users about the dangers of extortion, citing fake identities and other schemes to prey on users of social networks. Predators also use instant messaging and other apps to lure victims. For example, Christopher Gunn, an adult, created fake Facebook pages that cast him as a boy moving into the neighborhood or the singer Justin Bieber. Gunn befriended 9- to 16-year-old girls and obtained sexually explicit photographs from them, and then acquired more photographs and videos by threatening to inform parents or school officials. After his arrest, he was sentenced to 35 years in prison for creating child pornography.\textsuperscript{27}

Since sextortion is still not illegal in some states, criminal courts in many states handle these offenses using current laws against bribery, extortion, corruption, child pornography, computer hacking, and sexual exploitation or assault. State and federal law enforcement agencies have been proactively combatting these crimes with sting operations and other targeting methods.

**HACKING**

**LO 9.6** Describe the behaviors and values of the hacking community.

While some delinquents commit burglary or larceny to gain access to physical property without permission, the analogous activity in the cyberworld is hacking. \textit{Hacking} is usually seen as unauthorized intrusion into a computer or network for illegal purposes.\textsuperscript{28} Some \textit{hackers} argue that hacking requires a great deal of skill and knowledge of the technology.\textsuperscript{29} Hackers also argue that information on the Internet should be freely available. Furthermore, not all hacking is malicious. Some hackers are hired by legitimate parties to try to break into government or corporate computer systems to check security.
The following activities are categorized as illegal computer hacking:

1. Accessing a computer system without permission
2. Development or use of viruses
3. Destruction or alteration of a computer file without permission
4. Theft of services
5. Fraudulent use of credit cards
6. Infiltration of software

Hackers as a group pride themselves on mastering technology. They communicate in online forums and on discussion boards, as well as on social media. Hackers who overcome challenging security win high respect from their colleagues. Hackers are distinguished as white hats or black hats (see Figure 9.1). **White hats** are ethical hackers who try to improve security systems by successfully hacking them, while being careful not to harm anyone. The goal of **black hats**, however, is to exploit and destroy, sometimes for revenge.

Research on juvenile hackers is still rare. Hackers tend to be male and white or Asian. They also tend to be highly intelligent and are often college age. Youths with high academic achievement are more likely to be involved in hacking. Researchers have found that 5% to 15% of high school students admitted gaining unauthorized access to a website, e-mail address, or social networking page.

**FIGURE 9.1**

White Hats Versus Black Hats

<table>
<thead>
<tr>
<th>Black Hat Categories</th>
<th>White Hat Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crackers—Hackers who break through security, steal data, and use it in improper ways</td>
<td>Elites—Skilled hackers who have training to access computer systems but avoid causing destruction</td>
</tr>
<tr>
<td>Destructive hacktivists—Hackers who access the websites of political foes to cause havoc</td>
<td>CyberAngels—Hackers who uphold online safety</td>
</tr>
<tr>
<td>Cyberstalkers—Hackers who engage in unauthorized monitoring and even make death threats</td>
<td>Hacktivists—Hackers who want to enact social change in ways that are not destructive</td>
</tr>
<tr>
<td>Cyberterrorists—Hackers who want to intimidate governments and societies</td>
<td>Samurais—Hackers hired to investigate corporate computer crimes</td>
</tr>
</tbody>
</table>
Federal and state legislation to combat hacking started in the late 1970s and continues today. The Federal Computer System Protection Act of 1977 defined hacking behaviors as a federal crime and was adopted as model legislation by almost all states by 1986. The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 identifies certain behaviors as hacking. The Identity Theft Enforcement and Restitution Act of 2008 revised previous legislation and identified malware and denial-of-service attacks as hacking crimes.

**District of Columbia v. Cleveland (2014)**

In September 2014, Washington, D.C., Superior Court judge Juliet McKenna dismissed all criminal charges against Christopher Cleveland. Cleveland had been arrested in 2013 for taking pictures up the skirts of women sitting on the steps of the Lincoln Memorial, an activity known as “upskirting.” McKenna ruled that women have no reasonable expectation of privacy when “clothed and positioned” in a public place, regardless of the posture they assume. Upskirting, downblousing, and other forms of similar activity are deemed “nonconsensual pornography” and are handled differently by each state.

**Putting It Into Action**

Use the web to determine how your state classifies and handles nonconsensual pornography. Include a description of your state’s laws in a written file, and add to it whether or not you agree with the law. Submit your paper to your instructor when requested to do so.

**SUMMARY**

**LO 9.1 Explain the emergence of cybercrime.**

Although the average college student cannot remember a world without the Internet, many people still remember a time when they did not rely on computers or use the Internet. The Internet was introduced in the 1960s and became a prominent feature in most people’s lives in the 1990s, when a new form of criminality—cybercrime—began to develop and grow. While cybercrime can occur in many ways, there are a few main categories that involve juvenile offenders and victims.

**Key Terms**

cybercrime 142  
Internet 142

**LO 9.2 Define digital piracy and discuss the perception of many juveniles that it is an acceptable form of behavior.**

Digital piracy is the act of illegally copying music, movies, software, and other digital materials without the permission of or compensation to the copyright holder. Pirating behaviors can be extremely simple to perform, possibly explaining why a large amount of such pirates are under the age of 21. Music piracy is a common crime among juveniles, often perceived as a victimless one that doesn’t really affect a wealthy music artist. The perception that “everyone does it” diminishes deterrence.
Key Terms

digital piracy 142

**LO 9.3** Define cyberbullying and describe its categories.

Cyberbullying is purposeful and repeated harm inflicted through the use of technology, and can be performed in multiple ways. Cyberstalking is monitoring or harassing another person through the Internet. Some cyberbullying behaviors are also considered cyberstalking. State legislatures have enacted new statutes that criminalize the offenses or have added language on them to existing statutes.

Key Terms
cyberbullying 143 cyberstalking 144

**LO 9.4** Define cyberstalking and cyberharassment.

**LO 9.5** Identify various forms of online sexual exploitation.

The Internet can easily be used for sexting, which involves consensually sharing sexual material, such as nude or partially nude photographs. But it can also be used to share this material for revenge and humiliation, without the consent of the subject. Revenge porn is sexually explicit material that is posted online, often by a former sex partner, as a form of revenge for perceived wrongdoing. Sextortion, often used in conjunction with revenge porn, is a form of blackmail with the intention of gaining more sexually explicit material, money, or other demands.

Key Terms
revenge porn 147 sexting 145 sextortion 147

**LO 9.6** Describe the behaviors and values of the hacking community.

Hackers are often intelligent and proud of their work. They think free access to information is a basic right. Hackers have different levels of expertise and different intentions. Hacking usually involves unauthorized access to computer systems and files, but it can sometimes be altruistic. White hat hackers try to improve security, while black hat hackers have malicious intent.

Key Terms
black hats 148 hacking 147
hackers 147 white hats 148

**DISCUSSION QUESTIONS**

1. Why do so many juveniles commit some forms of cybercrime?

2. What types of punitive measures should the juvenile court system take to combat this type of criminality?

3. How should public and private school systems address juvenile cybercriminality?
1. Investigate and outline the legal ramifications in your state of origin for a juvenile who participates in the distribution of child pornography. Do you believe the sanctions are too harsh or too lenient?

2. Interview a law enforcement officer in your area, and ask him or her about the jurisdiction's experience with juvenile cybercrimes, as well as his or her perception of the jurisdiction's preparedness for investigation of these crimes.

SAGE edge™

Give your students the SAGE edge!

SAGE edge offers a robust online environment featuring an impressive array of free tools and resources for review, study, and further exploration, keeping both instructors and students on the cutting edge of teaching and learning. Learn more at edge.sagepub.com/schmallegerk.