Henson, B., Reyns, B., & Fisher, B. (2011). Internet crime. In W. Chambliss (Ed.), Key Issues in Crime and Punishment: Crime and criminal behavior. (pp. 155-168). Thousand Oaks, CA: SAGE Publications, Inc. doi: 10.4135/9781412994118.n12

Crime and Criminal Behavior

Internet Crime

Contributors: William J. Chambliss
Print Pub. Date: 2011
Online Pub. Date: June 24, 2011
Print ISBN: 9781412978552
Online ISBN: 9781412994118
DOI: 10.4135/9781412994118
Print pages: 155-168

10.4135/9781412994118.n12

[p. 155 ↓]

Chapter 12: Internet Crime

The birth of the information age brought with it changes far beyond the scope of human imagination. Technological developments such as video cameras, cellular phones, and computers have changed the way people think and act. One of the most monumental technological advances in the history of humankind was the development of the Internet. The Internet is a series of interconnected networks that allow for electronic communication and information sharing all over the world with the use of capable electronic devices. The Internet is the name given to the main system of networks; however, there are numerous Internet systems. Also, the term *Internet* is often mistakenly used interchangeably with the term *World Wide Web.* Internet refers to the actual network, while World Wide Web refers to a series of interconnected electronic documents that can be searched for and shared on the Internet. Unfortunately, while the Internet has revolutionized communication, business, academia, retail, and almost every other industry, it has also created opportunities for crime.

The advancement of technology such as the Internet has provided individuals and organizations with a means to both commit new types of crimes and adopt new methods of committing traditional street crimes. From online identity theft to cyberstalking to viruses, millions of people worldwide **[p. 156 ↓]** are affected by online deviant behavior every day. Internet crime is quickly becoming one of the biggest and most threatening problems for both law enforcement and the public at large.

Legal approaches have been developed throughout the history of the Internet to address the different types of Internet crime. Various arguments, both pro and con, have arisen surrounding this complex issue.

Defining Internet Crime

The birth of Internet crime brought with it a slew of terms—including *technology crime, information crime, intellectual crime,* and *online crime.* As a result, there is often confusion as to the exact definition of Internet crime. To understand what Internet crime is, it is necessary to understand what it isn't. Internet crime is often incorrectly referred to as *computer crime.* Computer crime is any illegal activity that is perpetrated through the use of a computer. Internet crime, on the other hand, is any illegal activity perpetrated on an information network, such as the Internet. Though the two may overlap, they are not the same. For example, making illegal copies of a CD would be considered a computer crime, as a computer is necessary to perform the action. However, if one were to illegally download music from the Internet, this act would be considered an Internet crime, as use of the Internet or other information network is necessary to perform the download. While a computer crime may involve the Internet, the Internet is not necessary; while an Internet crime may involve a computer, a computer is not necessary.

Often, during the examination of online deviance, the term *cybercrime* is used. Cybercrime refers to any illegal activity that occurs in the virtual world of cyberspace. Most researchers use it interchangeably with Internet crime. Internet crime can be divided into two main categories: Internet-assisted crime and Internet-based crime. An Internet-assisted crime is one in which the Internet or other information network was used, but not required, to commit the crime. Internet-assisted crimes can be committed offline, such as during identity theft or fraud, but are ever more frequently being committed online. In fact, according to the Federal Bureau of Investigation, online identity theft and fraud are quickly becoming two of the most prolific crimes in the world.

Internet-based crimes are those that exist and proliferate solely due to the presence of the Internet. Hacking and pharming are common examples of Internet-based crimes. Hacking is most often considered the act of breaking **[p. 157 ↓]** through or surpassing a Website or network's online security systems. This process could be performed to steal or alter information, or even simply to show off an individual's computer skills. While hacking has noncriminal meanings, it is the negative connotations that are most frequently used. The term *pharming* refers to a process through which the programming

code or entire files are altered on a computer or network server to redirect users from legitimate Websites to unauthorized cloned versions. In many cases, this process is used to steal a user's personal information, such as passwords or usernames.

There are certain crimes that fall into both categories of Internet crime. For example, cyberstalking can be either an Internet-assisted crime or an Internet-based crime, depending on the offender's actions. If an individual is following, contacting, and/or harassing someone offline, in addition to online contact, then his/her actions could be considered Internet-assisted stalking. However, if the pursuit behavior originated and is limited to online activities, then his/her actions could be considered Internet-based stalking. While the two versions of cyberstalking are legally considered the same by law enforcement, the need and ability to differentiate between the two has become a topic of debate among criminologists, as effectively understanding the difference allows prevention efforts to be tailored to address specific aspects of each form.

History of Internet Crime

The origins of the Internet can be traced back well over several decades to the early 1960s. Originally developed for military and educational applications, interlinked computer networks were designed to allow individuals and working groups to store and share information quickly and efficiently. The Internet and World Wide Web became accessible for public-wide use in the late 1980s. The first semblance of the modern Website appeared around 1990. Since that point, the number and size of files, networks, and Websites have grown exponentially. By 2009, several sources placed the estimated number of Websites at almost 200 million and the number of Internet users at well over 1.5 billion. The ambiguous nature and lax security measures of early information network systems make it nearly impossible to know when the first Internet crime actually occurred. As a result, the only method of examining the history of Internet crime is to focus on case studies. Given the numerous types of Internet crime, however, a review of all the major cases would not be possible in a compressed discussion. However, a few **[p. 158 ↓]** of the first, more well-known incidents can provide a snapshot of early Internet crime.

One of the first documented Internet crimes occurred in the late 1970s. A teenaged boy named Kevin Mitnick was caught by police after hacking into a phone company's digital network. Though the Internet as it is known today did not exist at that time, it was possible to use a modem to dial into information networks through phone lines. By remotely accessing the phone company's network, Mitnick was able to make free calls, as well as eavesdrop on others' calls. Though this may not be considered an Internet crime in the traditional sense, it would only be the first of Mitnick's illegal online activities, leading him to become one of the most famous hackers of all time. Hackers remained the central target of Internet crime prosecution for the last two decades of the 20th century.

In the early 1990s, it became evident to law enforcement that hackers were not the only people using the Internet for criminal activities. While working on cases of missing and abducted children, FBI agents found one of the first online child pornography rings. It was discovered that pedophiles were using the Internet to share sexually explicit images of children. Further, pedophiles were also using electronic bulletin boards (early precursors to chat rooms) to contact underage individuals in an effort to solicit sexual activity. With this discovery, the FBI began the Innocent Images National Initiative. Since 1995, FBI agents have been going undercover on Websites, blogs (a Website where users can journal their thoughts), and chat rooms in an effort to catch child predators. Their efforts have resulted in the arrest and conviction of almost 7,000 offenders in the United States.

Although email programs technically existed before the Internet, they were not used with any widespread regularity until the mid to late 1990s. During that time, programs like Microsoft Outlook were developed, and new companies, such as America Online, began offering free email accounts. As a result, the number of email users grew exponentially to an estimated 100 million by 2000. With the explosion in email use came another explosion—email spam, which is any unsolicited, bulk email sent out to a large number of email users. Spam emails may be advertisements, special offers or, most often, some type of scam. Though they were used somewhat during the early 1980s, the Nigerian solicitation scam, or 419 scam, became notorious during the 1990s. These fraudulent emails most often claim to be from a Nigerian prince or businessman who needs assistance transferring a large amount of money out of the country. Email users are asked to provide either their bank account information or a fee in exchange for a

portion of the **[p. 159 ↓]** money. After a series of communications and interactions in which participants are strung along, the victims end up losing their money and receiving nothing in return. According to the Internet Crime Complaint Center (IC3), in 2002, the median amount lost as a result of these scams was $5,575 per reported victim.

In January 1999, one of the first cases of cyberstalking was prosecuted in California. Gary Dellapenta spent the better part of 1998 terrorizing a woman who rejected his advances. Posing as the woman, Dellapenta placed ads and messages on several different Websites and online bulletin boards describing “her” rape fantasies. He also posted her address and directions on disabling her home alarm system. Dellapenta's actions led to at least six men visiting the woman's home, with the intent of fulfilling her purported rape fantasies. The situation became dire when Dellapenta began posting ads stating that the woman's negative responses to visitors were simply part of her fantasy. Dellapenta was arrested and charged with using the Internet to stalk and solicit rape, and was sentenced to six years in California state prison.

Cyberbullying

In October 2006, the world was introduced to a new type of crime known as *cyberbullying.* Similar to cyberstalking, cyberbullying is typically described as continued harassment and torment with the use of an electronic communications device, most often via the Internet. The main difference is that cyberbullying most often involves adolescents as victims and/or offenders. While cyberbullying had been discussed long before October 2006, it was the case of Megan Meier that really brought it to the attention of the American public. Earlier that year, 13-year-old Megan Meier befriended whom she thought was a teenage boy named Josh on MySpace. For a while, the correspondence was mutually friendly, as the two exchanged flirtatious messages. However, events suddenly took a turn for the worse when Josh, along with several other teenagers, began posting very derogatory comments about Megan. One night, the insults pushed Megan's already fragile self-esteem to the breaking point, and she took her own life. The case took another strange turn when it was discovered that “Josh” didn't actually exist. Instead, the account was created by Lori Drew, the mother of one of Megan's friends and one of her coworkers. Her reason for creating the profile and initiating contact was because Megan and her daughter had gotten into a fight, and

she wanted to unearth what Megan was saying about her daughter. Though Megan's parents demanded that Drew be prosecuted, **[p. 160 ↓]** there were no statutes in their home state that prohibited cyberbullying. Drew was eventually convicted of three misdemeanor charges of computer fraud under the Computer Fraud and Abuse Act, but the case was later overturned because the statute was deemed too vague. As a result of that case, cyberbullying is a topic of interest among researchers, reporters, and lawmakers. In fact, numerous states have modified their harassment laws to include harassment via the Internet. In those states, cyberbullying is now being prosecuted under the harassment statutes.

Types of Internet Crime

There is no universally accepted typology of Internet crimes. At a basic level, these types of crimes can be divided into four general categories: online assault, online fraud, online theft, and online intrusion. Several specific types of Internet crime exist within each of these basic categories. While published estimates on the extent of each type of Internet crime are few, and change daily, available information suggests that each of these crimes are growing in scope (in terms of number of victims, number of offenders, and cost). These four categories of Internet crime and some of the more common types of Internet crimes within these categories are defined.

Online Assault

Online assault involves violence perpetrated via the Internet, such as threats or unwanted sexual advances that result in an emotional response on the part of the victim (e.g., feelings of worry or fear). Types of online assault include: cyberbullying, cyberstalking, and online sexual exploitation of children.

Online Fraud

Online fraud is the use of deceit or a breach of confidence online in an effort to profit financially. Among the more common types of online fraud are such crimes as auction

fraud, lottery/inheritance scams, Nigerian letter schemes, phishing (posing as a legitimate business in an effort to convince victims to divulge valuable information such as bank account numbers and passwords), and others.

Online Theft

Online theft involves using the Internet to steal information, property, or money from its rightful owner. Identity theft and piracy fall into this category of Internet crime.

Online Intrusion

Online intrusion involves the use of the Internet to invade, harm, or otherwise infect another individual's online space, computer programs, or computer systems. The most common examples of this type of online crime are hacking and sending out viruses or worms.

The Legal System's Approach to Internet Crime

Internet crime poses a special problem for both law enforcement and the judicial system. The Internet and the number and type of Internet users have grown much quicker than anyone could have imagined. Likewise, Internet crime is progressing with great momentum, as new methods of accessing targets are surfacing almost daily. As a result, local police departments are constantly playing catch-up in their efforts to prevent and control Internet crime. Beginning in the 1990s, many police departments had begun developing cybercrime units in an effort to combat Internet crime. These units have been created at the federal, state, and local levels. They are specialized units comprised of both law enforcement officers and civilian personnel with a certain level of computer expertise.

While their main concern is to educate the public about the dangers of Internet crime, cybercrime units also attempt to detect, investigate, and apprehend online offenders. In an effort to reach the general public, most cybercrime units have their own Website. A study performed by Sameer Hinduja and Joseph Schafer in 2009 found that there were 88 different U.S. police department cybercrime-unit Websites in 2007. While several states had multiple Websites, about a third of states had no cybercrime unit Websites. Given the impact of Internet crime already wreaked on law enforcement and the general public, it is very possible that every major city police department will have a cybercrime unit in the future.

The judicial and legislative branches of the government are also striving to stay ahead of Internet criminals. State and federal statutes focused on Internet crime are relatively new to the legal system. Laws are created in one of two ways. Legislators either propose new bills, some of which are eventually passed and made into law, or existing laws are amended to include new **[p. 164 ↓]** criminal behaviors. Both processes have been used in the establishment of laws against Internet crime. For example, hacking is a crime that is relatively unique to computer systems and the Internet. As a result, most hacking laws had no previous legal precedent, and their content had to be originally drafted. Other crimes, however, such as cyberstalking and cyberbullying, have an offline counterpart. In many states, previous stalking and harassment laws were simply amended to include use of electronic communication devices. All U.S. states and the District of Columbia have established laws forbidding some type of Internet crime. There are also several federal statutes forbidding a wide range of online activities. By 2010, there were laws focusing on almost every known facet of Internet crime, including hacking, password cracking, viruses, cyberfraud, cyberstalking, cyberbullying, cyberterrorism, theft of intellectual property, identity theft, inappropriate communication with minors, and online child pornography. While not every U.S. state currently has laws forbidding every type of Internet crime, legislators pass new statutes every year to address the growing number and different types of online criminal behavior.

Pro: The Ability to Prosecute Internet Crime

While they do share some similarities, Internet and traditional criminal behaviors are very different. This is most evident in the attempts by law enforcement to prevent

and control crime. Valid and reliable evidence plays a significant role in securing a conviction, and criminal cases of all types are either made or broken based on one key element—physical evidence. Conversely, in many situations, evidence is fundamental to proving the innocence of the accused. With many traditional street crimes, however, evidence can easily be contaminated or destroyed. Blood or DNA can be destroyed with bleach, fingerprints can be wiped away, and weapons can be altered or destroyed. Research has shown that eyewitness testimony is not very reliable and can be altered by time, stress, and/or fear. However, it is not so easy to corrupt evidence in the cyber world.

The expression “once something is put on the Internet, it can never be removed,” is a commonly repeated phrase. To a certain extent, this is true. While truly expert computer users may be able to remove some items that have been posted or sent on the Internet, the average person is simply unable to delete information from the Internet. With so many computers on the network, information is stored in so many different places that it is practically impossible to completely erase or destroy it. Although one can remove **[p. 165 ↓]** a picture or video from his/her social networking site, it is still stored on the site's servers. The IT staff at any office can retrieve deleted emails, find hidden files, and in many cases recover corrupted documents. While this may be disheartening for many people, it is invaluable for law enforcement to perform an investigation and gather evidence. With the exception of the few true computer geniuses, individuals who commit Internet crime will leave a digital trail. As a result, with enough expertise and persistence, the police are often able to build strong evidence-based cases against Internet criminals.

Con: Lack of Awareness and Internet Crime Challenges

For most of the general public, there appears to be a strong disparity between the perceived severity of street crime versus Internet crime. Simply put, individuals are not as afraid of becoming victims of Internet crime as they are being victims of street crime. This occurs because most people do not have a clear understanding of the dangers of Internet crime. In many instances, a victim of Internet crime rarely comes

into direct, face-to-face contact with the offender, and often does not even realize they have been victimized until after the crime occurs. When individuals are not afraid of being victimized, they let their guard down, making them vulnerable targets to offenders. This is especially problematic for groups or demographics that do not routinely adopt crime prevention and security measures and are already vulnerable to victimization, such as children.

While U.S. and international police departments are beginning to utilize cybercrime units in an effort to prevent and control Internet crime, it has not come without difficulties. Internet crime is a completely new arena for law enforcement, and most departments need to make numerous organizational changes to effectively combat it. Among the primary issues is obtaining adequate resources to fund a cybercrime unit. For most departments, it is necessary to hire new personnel with training in computer science and/or information systems, as the average officer does not have substantial experience or training with computer systems. It may also be necessary to buy new equipment annually to meet any technological demands. Police departments are constantly struggling with budgetary problems in an effort to meet the demands of crime control, and simply aren't able to afford the appropriate tools necessary for cybercrime units.

The evidence points to Internet crime becoming increasingly problematic in the future. To date, there are very few large-scale studies examining the extent of Internet crime, in the United States or any other country.

[p. 166 ↓] While there appears to be a substantial number of Internet crime victims, based on reports produced by organizations such as the Internet Crime Complaint Center (IC3), in reality, there is very little information on how many victims have experienced which types of Internet crime, and more importantly in terms of prevention, an understanding of why the victimization occurred. Most studies performed by independent researchers have utilized small convenience samples and are thus not representative of larger populations of Internet users. As a result, it is difficult to determine the full scope and nature of Internet crime. Without knowing the true extent of Internet crime, it becomes extremely difficult to estimate the effectiveness of prevention efforts. The lack of appropriate empirical evidence creates a daunting challenge to accurately determine the trajectory of Internet crime rates, and the physical, psychological, and financial consequences on Internet crime victims.

Billy Henson Bradford W. Reyns Bonnie S. Fisher University of Cincinnati

Further Readings

See Also: Corporate Crime Intellectual Property Rights.

Alshalan, Abdullah. Cyber-Crime Fear and Victimization: An Analysis of a National Survey . Saarbruecken, Germany: VDM Verlag, 2008.

Bocij, Paul. Cyberstalking: Harassment in the Internet Age and How to Protect Your Family . Westport, CT: Praeger Publishers, 2006.

Brenner, Susan W. “U.S. Cybercrime Law: Defining Offenses.” Information Systems Frontiers , v.6/2 (2004).

Carr, Indira. Computer Crime . Burlington, VT: Ashgate Publishing, 2009.

Choi, Kyung-shick . “Computer Crime Victimization and Integrated Theory: An Empirical Assessment.” International Journal of Cyber Criminology , v.2/1 (2008).

Clarke, Ronald V. “Technology, Criminology and Crime Science.” European Journal on Criminal Policy and Research , v.10/1 (2004).

Franklin, Carl J. The Investigator's Guide to Computer Crime . Springfield, IL: Charles C Thomas, 2006.

Grabosky, Peter N. Electronic Crime . Upper Saddle River, NJ: Pearson, 2007.

Grabosky, Peter N. “Virtual Criminology: Old Wine in New Bottles?” Social and Legal Studies , v.10 (2001).

Hallam-Baker, Phillip . The dotCrime Manifesto: How to Stop Internet Crime . Boston: Pearson Education, 2008.

Henson, Billy. “Cyberstalking.” In Encyclopedia of Victimology and Crime Prevention , edited by Bonnie S. Fisher and Steven, P. Lab. Thousand Oaks, CA: Sage, 2010.http://dx.doi.org/10.4135/9781412979993

Hinduja, Sameer Justin, W. Patchin. Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying . Thousand Oaks, CA: Corwin Press, 2008.

Hinduja, Sameer Joseph, A. Schafer. “U.S. Cybercrime Units on the World Wide Web.” Policing , v.32/2 (2009).

Internet Crime Complaint Center (IC3) . http://www.ic3.gov (Accessed August 2010).

Marcum, Catherine D. Adolescent Online Victimization: A Test of Routine Activities Theory . El Paso, TX: LFB Scholarly Publishing, 2009.

McQuade, Samuel C. “Cyber and Internet Offenses.” In Encyclopedia of Victimology and Crime Prevention , edited by Bonnie S. Fisher and Steven, P. Lab. Thousand Oaks, CA: Sage, 2010.http://dx.doi.org/10.4135/9781412979993

McQuade, Samuel C. Encyclopedia of Cybercrime . Westport, CT: Greenwood Publishing Group, 2009.

McQuade, Samuel C. Understanding and Managing Cyber Crime . Boston: Pearson Education, 2006.

Newman, Graeme R. Ronald, V. Clarke. Superhighway Robbery: Preventing E-Commerce Crime . Portland, OR: Willan Publishing, 2003.

Reyns, B. W. “A Situational Crime Prevention Approach to Cyberstalking Victimization: Preventive Tactics for Internet Users and Online Place Managers.” Crime Prevention & Community Safety , in press.

Schmalleger, Frank Michael, Pittaro. Crimes of the Internet . Upper Saddle River, NJ: Prentice Hall, 2008.

Stadler, William A. “Internet Fraud.” In Encyclopedia of Victimology and Crime Prevention , edited by Bonnie S. Fisher and Steven, P. Lab. Thousand Oaks, CA: Sage, 2010.http://dx.doi.org/10.4135/9781412979993

Wall, David S. Cybercrime: The Transformation of Crime in the Information Age . Cambridge: Polity Press, 2007.

Yar, Majid. Cybercrime and Society . Thousand Oaks, CA: Sage, 2006.http://dx.doi.org/10.4135/9781446212196

Yar, Majid. “The Novelty of ‘Cybercrime:’ An Assessment in Light of Routine Activity Theory.” European Journal of Criminology , v.2/4 (2005).http://dx.doi.org/10.1177/147737080556056

10.4135/9781412994118.n12