alarming their customers if such a scam is detected. Recommended action steps for institutions and organizations include the following:

- Companies should educate their customers about the dangers of phishing, smishing, and vishing through letters, recorded messages for those calling into the company's call center, and articles on the company's Web site.
- Call center service employees should be trained to detect customer complaints that indicate a scam is being perpetrated. They should attempt to capture key pieces of information, such as the callback number the customer was directed to use, details of the phone message or text message, and the type of information requested.
- Customers should be notified immediately if a scam occurs. This can be done via a recorded message for customers phoning the call center, working with local media to place a news article in papers serving the area of the attack, placing a banner on the institution's Web page, and even displaying posters in bank drive-through and lobby areas.
- If it is determined that the calls are originating from within the United States, companies should report the scam to the Federal Bureau of Investigation (FBI).
- Institutions can also try to notify the telecommunications carrier for the particular phone number that victims are requested to call, to request that they shut down that number.[27]

Types of Perpetrators

The people who launch these kinds of computer attacks include thrill seekers wanting a challenge, common criminals looking for financial gain, industrial spies trying to gain a competitive advantage, and terrorists seeking to cause destruction to further their cause. Each type of perpetrator has different objectives and access to varying resources, and each is willing to accept different levels of risk to accomplish his or her objective. Each perpetrator makes a decision to act in an unethical manner to achieve his or her own personal objectives. Knowing the profile of each set of likely attackers, as shown in Table 3-5, is the first step toward establishing effective countermeasures.

TABLE 3-5 Classifying perpetrators of computer crime

Type of perpetrator	Typical motives
Hackers	Test limits of system and/or gain publicity
Crackers	Cause problems, steal data, and corrupt systems
Malicious insiders	Gain financially and/or disrupt company's information systems and business operations
Industrial spies	Capture trade secrets and gain competitive advantage
Cybercriminals	Gain financially
Hacktivists	Promote political ideology
Cyberterrorists	Destroy infrastructure components of financial institutions, utilities, and emergency response units

Source Line: Course Technology/Cengage Learning.

Hackers and Crackers

Hackers test the limitations of information systems out of intellectual curiosity—to see whether they can gain access and how far they can go. They have at least a basic understanding of information systems and security features, and much of their motivation comes from a desire to learn even more. The term *hacker* has evolved over the years, leading to its negative connotation today rather than the positive one it used to have. While there is still a vocal minority who believe that hackers perform a service by identifying security weaknesses, most people now believe that a hacker does not have the right to explore public or private networks.

Some hackers are smart and talented, but many are technically inept and are referred to as **lamers** or **script kiddies** by more skilled hackers. Surprisingly, hackers have a wealth of available resources to hone their skills—online chat groups, Web sites, downloadable hacker tools, and even hacker conventions (such as DEFCON, an annual gathering in Las Vegas).

Malicious Insiders

A major security concern for companies is the **malicious insider**—an ever-present and extremely dangerous adversary. Companies are exposed to a wide range of fraud risks, including diversion of company funds, theft of assets, fraud connected with bidding processes, invoice and payment fraud, computer fraud, and credit card fraud. Not surprisingly, fraud that occurs within an organization is usually due to weaknesses in its internal control procedures. As a result, many frauds are discovered by chance and by outsiders—via tips, through resolving payment issues with contractors or suppliers, or during a change of management—rather than through control procedures. Often, frauds involve some form of **collusion**, or cooperation, between an employee and an outsider. For example, an employee in Accounts Payable might engage in collusion with a company supplier. Each time the supplier submits an invoice, the Accounts Payable employee adds $1,000 to the amount approved for payment. The inflated payment is received by the supplier, and the two split the extra money.

Insiders are not necessarily employees; they can also be consultants and contractors. The risk tolerance of insiders depends on whether they are motivated by financial gain, revenge on their employers, or publicity.

Malicious insiders are extremely difficult to detect or stop because they are often authorized to access the very systems they abuse. Although insiders are less likely to attack systems than outside hackers or crackers are, the company's systems are far more vulnerable to them. Most computer security measures are designed to stop external attackers but are nearly powerless against insiders. Insiders have knowledge of individual systems, which often includes the procedures to gain access to login IDs and passwords. Insiders know how the systems work and where the weak points are. Their knowledge of organizational structure and security procedures helps them avoid detection of their actions.

The Saudi Arabian Oil Company (Aramco) is the state-owned oil company of Saudi Arabia. It owns approximately one-fifth of the world's oil reserves and employs more than 55,000 workers in 77 countries.[28] In 2012, the firm was a victim of a cyberattack that erased data on about 30,000 of its personal computers. Security experts believe that the attack was led by a company insider who had privileged access to Aramco's network.[29]

There are several steps organizations can take to reduce the potential for attacks from insiders, including the following:

- Perform a thorough background check as well as psychological and drug testing of candidates for sensitive positions.
- Establish an expectation of regular and ongoing psychological and drug testing as a normal routine for people in sensitive positions.
- Carefully limit the number of people who can perform sensitive operations, and grant only the minimum rights and privileges necessary to perform essential duties.
- Define job roles and procedures so it is not possible for the same person to both initiate and approve an action.
- Periodically rotate employees in sensitive positions so that any unusual procedures can be detected by the replacement.
- Immediately revoke all rights and privileges required to perform old job responsibilities when someone in a sensitive position moves to a new position.
- Implement an ongoing audit process to review key actions and procedures.

Organizations must also be concerned about **negligent insiders**, poorly trained and inadequately managed employees who mean well but have the potential to cause much damage by accident.

Industrial Spies

Industrial spies use illegal means to obtain trade secrets from competitors. In the United States, trade secrets are protected by the Economic Espionage Act of 1996, which makes it a federal crime to use a trade secret for one's own benefit or another's benefit. Trade secrets are most often stolen by insiders, such as disgruntled employees and exemployees.

Competitive intelligence is legally obtained information gathered using sources available to the public. Information is gathered from financial reports, trade journals, public filings, and printed interviews with company officials. **Industrial espionage** involves using illegal means to obtain information that is not available to the public. Participants might place a wiretap on the phones of key company officials, bug a conference room, or break into a research and development facility to steal confidential test results. An unethical firm may spend a few thousand dollars to hire an industrial spy to steal trade secrets that can be worth a thousand times that amount. The industrial spy avoids taking risks that would expose his employer, as the employer's reputation (an intangible but valuable item) would be considerably damaged if the espionage were discovered. Industrial espionage can involve the theft of new product designs, production data, marketing information, or new software source code. For example, a virus called "ACAD/Medre.A" was used to steal thousands of blueprints from companies based mainly in Peru and secretly email them to two Chinese firms. The virus targets AutoCAD software used by engineers and industrial designers to create drawings of new products, equipment, and plant layouts. It is suspected that the virus was initially distributed via an innocent looking AutoCAD template emailed to Peruvian companies. The virus sends a copy of every new design to the virus owners, giving them full "access to the designs even before they go into production."[30]

Cybercriminals

Information technology provides a new and highly profitable venue for **cybercriminals**, who are attracted to the use of information technology for its ease in reaching millions of potential victims. Cybercriminals are motivated by the potential for monetary gain and hack into computers to steal, often by transferring money from one account to another to another—leaving a hopelessly complicated trail for law enforcement officers to follow. Cybercriminals also engage in all forms of computer fraud—stealing and reselling credit card numbers, personal identities, and cell phone IDs. Because the potential for monetary gain is high, they can afford to spend large sums of money to buy the technical expertise and access they need from unethical insiders.

The use of stolen credit card information is a favorite ploy of computer criminals. Fraud rates are highest for merchants who sell downloadable software or expensive items such as electronics and jewelry (because of their high resale value). Credit card companies are so concerned about making consumers feel safe while shopping online that many are marketing new and exclusive zero-liability programs, although the Fair Credit Billing Act limits consumer liability to only $50 of unauthorized charges. When a charge is made fraudulently in a retail store, the bank that issued the credit card must pay the fraudulent charges. For fraudulent credit card transactions over the Internet, the Web merchant absorbs the cost.

A high rate of disputed transactions, known as charge-backs, can greatly reduce a Web merchant's profit margin. However, the permanent loss of revenue caused by lost customer trust has far more impact than the costs of fraudulent purchases and bolstering security. Most companies are afraid to admit publicly that they have been hit by online fraud or hackers because they don't want to hurt their reputations.

In a major case of identity theft, MasterCard recently notified financial institutions that a data breach had occurred at one of its third-party payment processors that could enable the thieves to duplicate the cards of millions of its cardholders. (A **data breach** is the unintended release of sensitive data or the access of sensitive data by unauthorized individuals.) It is likely that data of Visa card holders was also stolen. The total number of card holders that might be affected and the banks notified were not revealed.[31]

To reduce the potential for online credit card fraud, most e-commerce Web sites use some form of encryption technology to protect information as it comes in from the consumer. Some also verify the address submitted online against the one the issuing bank has on file, although the merchant may inadvertently throw out legitimate orders as a result—for example, a consumer might place a legitimate order but request shipment to a different address because it is a gift. Another security technique is to ask for a card verification value (CVV), the three-digit number above the signature panel on the back of a credit card. This technique makes it impossible to make purchases with a credit card number stolen online. An additional security option is transaction-risk scoring software, which keeps track of a customer's historical shopping patterns and notes deviations from the norm. For example, say that you have never been to a casino and your credit card information is being used at Caesar's Palace at 2:00 a.m. The transaction-risk score would go up dramatically, so much so that the transaction might be declined.

Some card issuers are issuing debit and credit cards in the form of **smart cards**, which contain a memory chip that is updated with encrypted data every time the card is used.

This encrypted data might include the user's account identification and the amount of credit remaining. To use a smart card for online transactions, consumers must purchase a card reader that attaches to their personal computers and enter a personal identification number to gain access to the account. Although smart cards are used widely in Europe, they are not as popular in the United States because of the changeover costs for merchants.

Hacktivists and Cyberterrorists

Hacktivism, a combination of the words *hacking* and *activism*, is hacking to achieve a political or social goal. A **cyberterrorist** launches computer-based attacks against other computers or networks in an attempt to intimidate or coerce an organization in order to advance certain political or social objectives. Cyberterrorists are more extreme in their goals than hacktivists, although there is no clear demarcation line. Because of the Internet, cyberattacks can easily originate from foreign countries, making detection and retaliation much more difficult. Cyberterrorists seek to cause harm rather than gather information, and they use techniques that destroy or disrupt services. They are extremely dangerous, consider themselves to be at war, have a very high acceptance of risk, and seek maximum impact.

In late 2012, the hacktivist group Parastoo hacked into the International Atomic Energy Agency (IAEA) network and stole the email addresses of 167 experts working with the agency. The group then posted an online statement demanding that the experts petition the IAEA to investigate what it considered to be "beyond-harmful operations" at Israel's Negev Nuclear Research Center. Parastoo threatened to expose the whereabouts of these experts, as well as other personal information, if they failed to act.[32]

Federal Laws for Prosecuting Computer Attacks

Computers came into use in the 1950s. Initially, there were no laws that pertained strictly to computer-related crimes. For example, if a group of criminals entered a bank and stole money at gunpoint, they could be captured and charged with robbery—the crime of seizing property through violence or intimidation. However, by the mid-1970s, it was possible to access a bank's computer remotely using a terminal (a keyboard and monitor), modem, and telephone line. A knowledgeable person could then transfer money (in the form of computer bits) from accounts in that bank to an account in another bank. This act did not fit the definition of robbery, and the traditional laws were no longer adequate to punish criminals who used computer modems.

Over the years, several laws have been enacted to help prosecute those responsible for computer-related crime; these are summarized in Table 3-6. For example, the USA Patriot Act defines cyberterrorism as hacking attempts that cause $5,000 in aggregate damage in one year to medical equipment, or that cause injury to any person. Those convicted of cyberterrorism are subject to a prison term of 5 to 20 years. (The $5,000 threshold is quite easy to exceed, and, as a result, many young people who have been involved in what they consider to be minor computer pranks have found themselves meeting the criteria to be tried as cyberterrorists.)

Now that we have discussed various types of computer exploits, the people who perpetrate these exploits, and the laws under which they can be prosecuted, we will discuss how organizations can take steps to implement a trustworthy computing environment to defend against such attacks.

TABLE 3-6 Federal laws that address computer crime

Federal law	Subject area
USA Patriot Act	Defines cyberterrorism and associated penalties
Identity Theft and Assumption Deterrence Act (U.S. Code Title 18, Section 1028)	Makes identity theft a federal crime with penalties up to 15 years imprisonment and a maximum fine of $250,000
Fraud and Related Activity in Connection with Access Devices Statute (U.S. Code Title 18, Section 1029)	False claims regarding unauthorized use of credit cards
Computer Fraud and Abuse Act (U.S. Code Title 18, Section 1030)	Fraud and related activities in association with computers: • Accessing a computer without authorization or exceeding authorized access • Transmitting a program, code, or command that causes harm to a computer • Trafficking of computer passwords • Threatening to cause damage to a protected computer
Stored Wire and Electronic Communications and Transactional Records Access Statutes (U.S. Code Title 18, Chapter 121)	Unlawful access to stored communications to obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage

Source Line: Course Technology/Cengage Learning.

IMPLEMENTING TRUSTWORTHY COMPUTING

Trustworthy computing is a method of computing that delivers secure, private, and reliable computing experiences based on sound business practices—which is what organizations worldwide are demanding today. Software and hardware manufacturers, consultants, and programmers all understand that this is a priority for their customers. For example, Microsoft has pledged to deliver on a trustworthy computing initiative designed to improve trust in its software products, as summarized in Figure 3-4 and Table 3-7.[33]

The security of any system or network is a combination of technology, policy, and people and requires a wide range of activities to be effective. As the Committee on Improving Cybersecurity Research in the United States wrote in a report for the National Academy of Sciences, "Society ultimately expects computer systems to be trustworthy—that is, that they do what is required and expected of them despite environmental disruption, human user and operator errors, and attacks by hostile parties, and that they not do other things."[34] A strong security program begins by assessing threats to the organization's computers and network, identifying actions that address the most serious vulnerabilities, and educating end users about the risks involved and the actions they must take to prevent a security incident. An organization's IT security group must lead the effort to prevent security breaches by implementing security policies and procedures, as well as effectively employing available hardware and software tools. However, no security system

lawsuits argue that perpetrators should not be able to hide behind anonymity to avoid responsibility for their actions.

Anonymity on the Internet is not guaranteed. By filing a lawsuit, companies gain immediate subpoena power, and many message board hosts release information as soon as it is requested, often without notifying the poster. Everyone who posts comments in a public place on the Web should consider the consequences if their identities were to be exposed. Furthermore, everyone who reads anonymous postings online should think twice about believing what they read.

The California State Court in *Pre-Paid Legal v. Sturtz et al*[34] set a legal precedent that refined the criteria the courts apply when deciding whether or not to approve subpoenas requesting the identity of anonymous Web posters. The case involved a subpoena issued by Pre-Paid Legal Services (PPLS), which requested the identity of eight anonymous posters on Yahoo!'s Pre-Paid message board. Attorneys for PPLS argued that it needed the posters' identities to determine whether they were subject to a voluntary injunction that prevented former sales associates from revealing PPLS's trade secrets.

The Electronic Frontier Foundation (EFF) represented two of the John Does whose identities were subpoenaed. EFF attorneys argued that the message board postings cited by PPLS revealed no company secrets but were merely disparaging the company and its treatment of sales associates. They argued further that requiring the John Does to reveal their identities would let the company punish them for speaking out and set a dangerous precedent that would discourage other Internet users from voicing criticism. Without proper safeguards on John Doe subpoenas, a company could use the courts to uncover its critics.

EFF attorneys urged the court to apply the four-part test adopted by the federal courts in the *Doe v. 2TheMart.com, Inc*.[35] case to determine whether a subpoena for the identity of the Web posters should be upheld. In that case, the federal court ruled that a subpoena should be enforced only when the following occurs:

- The subpoena was issued in good faith and not for any improper purpose.
- The information sought related to a core claim or defense.
- The identifying information was directly and materially relevant to that claim or defense.
- Adequate information was unavailable from any other source.

In August 2001, a judge in Santa Clara County Superior Court invalidated the subpoena to Yahoo! requesting the posters' identities. He ruled that the messages were not obvious violations of the injunctions invoked by PPLS and that the First Amendment protection of anonymous speech outweighed PPLS's interest in learning the identity of the speakers.

Hate Speech

In the United States, speech that is merely annoying, critical, demeaning, or offensive enjoys protection under the First Amendment. Legal recourse is possible only when hate speech turns into clear threats and intimidation against *specific* citizens. Persistent or malicious harassment aimed at a specific person is **hate speech**, which can be prosecuted under the law, but general, broad statements expressing hatred of an ethnic, racial, or religious group cannot. A threatening private message sent over the Internet to a person, a public message displayed on a Web site describing intent to commit acts of hate-motivated

violence against specific individuals, and libel directed at a particular person are all actions that can be prosecuted.

Although ISPs do not have the resources to prescreen content (and they do not assume any responsibility for content provided by others), many ISPs do reserve the right to remove content that, in their judgment, does not meet their standards. The speed at which content may be removed depends on how quickly such content is called to the attention of the ISP, how egregious the content is, and the general availability of ISP resources to handle such issues.

To post videos on YouTube, you must first create a YouTube or a Google account (Google is the owner of YouTube) and agree to abide by the site's published guidelines.[36] The YouTube guidelines prohibit the posting of videos showing such things as pornography, animal abuse, graphic violence, predatory behavior, and drug use. The guidelines also prohibit the posting of copyrighted material—such as music, television programs, or movies—that is owned by a third party. YouTube staff members review user-posted videos on a regular basis to find any that violate the site's community guidelines. Those that violate the guidelines are removed. Certain other videos are age-restricted because of their content. Users are penalized for serious or repeated violations of the guidelines and can have their account terminated.[37]

Because such prohibitions are included in the service contracts between a private ISP and its subscribers, and do not involve the federal government, they do not violate the subscribers' First Amendment rights. Of course, ISP subscribers who lose an account for violating the ISP's regulations may resume their hate speech by simply opening a new account with some other, more permissive ISP.

Although they may implement a speech code, public schools and universities are legally considered agents of the government and therefore must follow the First Amendment's prohibition against speech restrictions based on content or viewpoint. Corporations, private schools, and private universities, on the other hand, are not considered part of state or federal government. As a result, they may prohibit students, instructors, and other employees from engaging in offensive speech using corporate-, school-, or university-owned computers, networks, or email services.

Most other countries do not provide constitutional protection for hate speech. For example, promoting Nazi ideology is a crime in Germany, and denying the occurrence of the Holocaust is illegal in many European countries. Authorities in Britain, Canada, Denmark, France, and Germany have charged people for crimes involving hate speech on the Web.

A U.S. citizen who posts material on the Web that is illegal in a foreign country can be prosecuted if he subjects himself to the jurisdiction of that country—for example, by visiting there. As long as the person remains in the United States, he is safe from prosecution because U.S. laws do not allow a person to be extradited for engaging in an activity protected by the U.S. Constitution, even if the activity violates the criminal laws of another country.

Pornography

Many people, including some free-speech advocates, believe that there is nothing illegal or wrong about purchasing adult pornographic material made by and for consenting adults. They argue that the First Amendment protects such material. On the other hand, most

parents, educators, and other child advocates are concerned that children might be exposed to pornography. They are deeply troubled by its potential impact on children and fear that increasingly easy access to pornography encourages pedophiles and sexual predators.

Clearly, the Internet has been a boon to the pornography industry by providing fast, cheap, and convenient access to a huge array of pornography Web sites—some estimates are as high as 24 million pornography sites worldwide.[38] Access via the Internet enables pornography consumers to avoid offending others or being embarrassed by others observing their purchases. There is no question that online adult pornography is big business (however, revenue estimates vary widely between $1 billion and $97 billion)[39] and generates a lot of traffic; it is estimated that there are over 72 million visitors to pornographic Web sites monthly.[40]

Pornography purveyors are free to produce and publish whatever they want; however, if what they distribute or exhibit is judged obscene, they are subject to prosecution under the obscenity laws. The precedent-setting *Miller v. California* ruling on obscenity discussed earlier in the chapter predates the Internet. The judges in that case ruled that contemporary community standards should be used to judge what is obscene. The judges allowed that different communities could have different norms.

The key question in deciding what Internet material is obscene is: "Whose community standards are used?" Because Internet content publishers cannot easily direct their content into or away from a particular geographic area, one answer to this question is that the Internet content publisher must conform to the norms of the most restrictive community. However, this line of reasoning was challenged by the Third Circuit Court of Appeals in the *Ashcroft v. American Civil Liberties Union* case, which involved a challenge to the 1998 Child Online Protection Act (COPA). The Supreme Court reversed the circuit court's ruling in this case—but with five different opinions and no clear consensus on the use of local or national community standards.[41] In *United States v. Kilbride,* the Ninth Circuit Court of Appeals ruled that "a national community standard must be applied in regulating obscene speech on the Internet, including obscenity disseminated via email."[42] In *United States v. Little,* the Eleventh Circuit Court of Appeals rejected the national community standard and adopted the older, local community standard. Currently there is no clear agreement within the courts on whether local or national community standards are to be used to judge obscenity.

U.S. organizations must be very careful when dealing with issues relating to pornography in the workplace. By providing computers, Internet access, and training in how to use those computers and the Internet, companies could be seen by the law as purveyors of pornography because they have enabled employees to store pornographic material and retrieve it on demand. A Nielsen survey on the viewing of pornography in the workplace revealed that 21 million Americans accessed porn from their work computers in March 2010—29 percent of the workforce.[43] In addition, if an employee sees a coworker viewing porn on a workplace computer, that employee may be able to claim that the company has created a hostile work environment. Such a claim opens the organization to a sexual harassment lawsuit that can cost hundreds of thousands of dollars and tie up managers and executives in endless depositions and court appearances.

Many companies believe that they have a duty to stop the viewing of pornography in the workplace. As long as they can show that they took reasonable steps and determined

actions to prevent it, they have a valid defense if they become the subject of a sexual harassment lawsuit. If it can be shown that a company made only a half-hearted attempt to stop the viewing of pornography in the workplace, then the company could have trouble defending itself in court. Reasonable steps include establishing and communicating an acceptable use policy that prohibits access to pornography sites, identifying those who violate the policy, and taking disciplinary action against those who violate the policy, up to and including termination.

A few companies take the opposite viewpoint—that they cannot be held liable if they don't know employees are viewing, downloading, and distributing pornography. Therefore, they believe the best approach is to ignore the problem by never investigating it, thereby ensuring that they can claim that they never knew it was happening. Many people would consider such an approach unethical and would view management as shirking an important responsibility to provide a work environment free of sexual harassment. Employees unwillingly exposed to pornography would have a strong case for sexual harassment because they could claim that pornographic material was available in the workplace and that the company took inadequate measures to control the situation.

There are numerous federal laws addressing issues relating to child pornography—including laws concerning the possession, production, distribution, or sale of pornographic images or videos that exploit or display children. Possession of child pornography is a federal offense punishable by up to five years in prison. The production and distribution of such materials carry harsher penalties; decades or even life in prison is not an unusual sentence. In addition to these federal statutes, all states have enacted laws against the production and distribution of child pornography, and all but a few states have outlawed the possession of child pornography. At least seven states have passed laws that require computer technicians who discover child pornography on clients' computers to report it to law enforcement officials.

Sexting—sending sexual messages, nude or seminude photos, or sexually explicit videos over a cell phone—is a fast-growing trend among teens and young adults. According to a survey by the National Campaign to Prevent Teen and Unplanned Pregnancy, one in five teenagers has sent or posted nude or seminude photos of himself/herself, including 22 percent of teen girls, 18 percent of teen boys, and 11 percent of young teen girls aged 13 to 16.[44] Now there is even a smartphone app, Snapchat, that enables users to send messages and share videos or images that disappear after a few seconds. However, users should be aware that recipients can take screenshots of a Snapchat on their phone, and an apparent security flaw enables recipients to retrieve deleted videos sent via Snapchat.[45]

Increasingly, sexters are suffering the consequences of this fad. Once an image or video is sent, there is no taking it back and no telling to whom it might be forwarded. And it is not just teenagers who participate in sexting. Consider quarterback Bret Favre and U.S. Representative Anthony Weiner who were both parties to embarrassing sexting episodes. Sexters can also face prosecution for child pornography leading to possible years in jail and decades of registration as a sex offender.

Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act

The **Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act** (2003) specifies requirements that commercial emailers must follow when sending

messages that have a primary purpose to advertise or promote a commercial product or service. The key requirements of the law include:

- The *From* and *To* fields in the email, as well as the originating domain name and email address, must be accurate and identify the person who initiated the email.
- The subject line of the email cannot mislead the recipient as to the contents or subject matter of the message. In addition, if the message contains sexually-oriented material, the phrase "SEXUALLY-EXPLICIT" must appear in capital letters as the first characters in the subject line.
- The email must be identified as an advertisement and include a valid physical postal address for the sender.
- The emailer must provide a return email address or some other Internet-based response procedure to enable the recipient to request no future emails, and the emailer must honor such requests to opt out.
- The emailer has 10 days to honor the opt-out request.
- Additional rules prohibit the harvesting of email addresses from Web sites, using automated methods to register for multiple email accounts, or relaying email through another computer without the owner's permission.

Messages whose primary purpose is to communicate information about a specific transaction or relationship between the sender and recipient are not subject to the CAN-SPAM Act. Thus, a message regarding an attempt to deliver a legitimately placed online order or information about a product recall would be exempt.

Each violation of the provisions of the CAN-SPAM Act can result in a fine of up to $250 for each unsolicited email, and fines can be tripled in certain cases. A Canadian spammer was ordered to pay $873 million in fines for allegedly spamming Facebook accounts with over 4 million posts. Of course, the spammer was unable to pay the fine and instead declared bankruptcy.[46]

The Federal Trade Commission (FTC) is charged with enforcing the CAN-SPAM Act, and the agency maintains a consumer complaint database relating to the law. Consumers can submit complaints online at *www.ftc.gov* or forward email to the FTC at *spam@use.gov*. Other countries have their own version of the CAN-SPAM Act. The United Kingdom recently fined two people £440,000 (about $700,000 USD) for sending out as many as 800,000 spam text messages per day to cell phone users on behalf of claims management companies looking for accident victims to pass on to lawyers.[47]

The CAN-SPAM Act can also be used in the fight against the dissemination of pornography. For example, two men were indicted by an Arizona grand jury for violating the CAN-SPAM Act by sending massive amounts of unsolicited email advertising pornographic Web sites. They had amassed an email database of 43 million people and used it to send emails containing pornographic images. AOL stated it received over 660,000 complaints from people who received spam from the two, whose operation was highly profitable—enabling the two men to earn over $1.4 million in 2003. The defendants ran afoul of the CAN-SPAM Act by sending messages with false return addresses and for using domain names registered using false information. They were convicted of multiple counts of spamming and criminal conspiracy, which carry a maximum sentence of five years each