5

Crime

5.1 Introduction

Nineteenth-century bank robbers fled the scenes of their crimes on horseback. In the 20th century, they drove getaway cars. In the 21st, they work from a computer. For generations, teenagers have committed pranks and minor crimes. Hacking into school, corporate, and government computer systems was a natural step. Employees embezzled funds from employers by "doctoring" the books. Now they modify or misuse company software. Computing technology and the Internet provide new environments for fraud, stock manipulation, theft, forgery, industrial espionage, and many old and new scams. Hacking—intentional, unauthorized access to computer systems—includes a wide range of activities from minor pranks to huge thefts and shutdowns of services on which lives and livelihoods depend.

Crimes committed with computing technology are more devastating and harder to detect than similar crimes committed without it. A robber who enters a bank and uses a gun gets $2,500–$5000 on average. The average loss from a computer fraud is more than $100,000.[1] A thief who steals a credit card (or a credit card number) gains access to a much larger amount of money than the thief of the past who stole a wallet containing only cash. A hacker who breaks into a retailer's or bank's computer might steal not one or a dozen but thousands or millions of credit card numbers. Identity theft affects millions of people. It can disrupt a victim's life for years. Computer vandalism by teenagers brings business operations of major companies to a halt. Terrorists could sabotage power and communications systems and other critical infrastructure. Global business networks and the Web extend the criminal's reach and make arrests and prosecutions more difficult. With so much sensitive information and infrastructure online, why is security weak enough to allow repeated significant breaches?

Activities that are legal in some countries are illegal in others. But the Web is global. Businesses and individuals are sued and arrested for violating laws of countries that their online business or writing reaches. How serious is this problem, and how can we deal with it?

In this chapter, we examine many of these problems and a variety of approaches for addressing them. The examples we include are representative of dozens or hundreds more.

5.2 Hacking

5.2.1 What is "Hacking"?

The term "hacker," to many people, means an irresponsible, destructive criminal. Hackers break into computer systems. They intentionally release computer viruses. They steal sensitive personal, business, and government information. They steal money, crash websites, destroy files, and disrupt businesses. But other people who call themselves hackers

do none of these things. So our first problem is to figure out what "hacker" means and what hackers do.

To organize the discussion, we describe three phases of hacking:

Phase 1—the early years (1960s and 1970s), when hacking was a positive term
Phase 2—from the 1970s to the 1990s, when hacking took on its more negative meanings
Phase 3—beginning in the mid-1990s, with the growth of the Web and of e-commerce and the participation of a large portion of the general public online

The boundaries are not sharp, and each phase includes the kinds of hacking common in the earlier phases. In Sections 5.2.2, 5.2.3, and 5.2.4, we consider hacking for special purposes (political activism, hacking to expose security flaws, and government hacking for military purposes).

Phase 1: The joy of programming

In the early days of computing, a "hacker" was a creative programmer who wrote very elegant or clever programs. A "good hack" was an especially clever piece of code. Hackers were "computer virtuosos." They created many of the first computer games and operating systems. They tended to be outside the social mainstream. Many were high school and college students—or drop-outs. Although they sometimes found ways into systems where they were not authorized users, the early hackers mostly sought knowledge and intellectual challenges—and, sometimes, the thrill of going where they did not belong. Most had no intention of disrupting services; they frowned on doing damage. The *New Hacker's Dictionary* describes a hacker as a person "who enjoys exploring the details of programmable systems and how to stretch their capabilities; . . . one who programs enthusiastically (even obsessively)."[2] Jude Milhon described hacking as "clever circumvention of imposed limits."[3] The limits can be the technical limits of the system one is using, the limits that someone else's security techniques impose, legal limits, or the limits of one's own skills. Her definition is a good one in that it encompasses many of the uses of the term.

"Hacking" still sometimes has the early meaning of clever programming that reflects a high level of skill and that circumvents limits. Fans of Nintendo's Wii videogame console reprogrammed its remote controller to perform tasks Nintendo never imagined. Soon after Apple released the iPhone, hackers found ways to make it operate in ways Apple had tried to prevent. Hundreds of people gather for day-long "hackathons," to work intensely at developing innovative new software products. Another example, of course, is software to circumvent the limits of protection schemes for digital intellectual property (discussed in Section 4.2.2). Hacking often has a whiff, at least, of challenge to powerful institutions.

Phase 2: From the 1970s to the mid-1990s

The meaning, and especially the connotations, of the word "hacker" changed as more people began using computers and more people began abusing them. The word eventually

took on its most common meaning today: breaking into computers for which the hacker does not have authorized access. By the 1980s, hacking also included spreading computer viruses, then mostly in software traded on floppy disks. Hacking behavior included pranks, thefts (of information, software, and sometimes money), and *phone phreaking* (manipulating the telephone system). Hackers obtained passwords by sophisticated techniques and by *social engineering*: fooling people into disclosing them.

Hacking a computer at a big research center, corporation, or government agency was a challenge that brought a sense of accomplishment, a lot of files to explore, and respect from one's peers. This "trophy" hacking was often associated with young hackers. Young hackers were especially fond of breaking into Defense Department computers, and they were very successful at it. Clifford Stoll described a more serious case in his book *The Cuckoo's Egg*: a German hacker broke into dozens of U.S. computers, including military systems, in the 1980s, looking for information to sell to the Soviet Union.

A program known as the Internet Worm demonstrated the vulnerability of the Internet as a whole in 1988. A graduate student at Cornell University wrote the worm and released it onto the Internet.* The worm did not destroy files or steal passwords, and there was disagreement about whether its author intended or expected it to cause the degree of disruption that it did. However, it spread quickly to computers running particular versions of the UNIX operating system, jamming them up and preventing normal processing. The worm affected a few thousand computers (a large portion of the Internet at the time). It took a few days for systems programmers to discover, decode, and rid their systems of the worm. The worm disrupted work and inconvenienced a large number of people. This incident raised concern about the potential to disrupt critical computer services and cause social disruption.[4]

Adult criminals began to recognize the possibilities of hacking. Thus, business espionage and significant thefts and frauds joined the list of hacking activities in the 1980s and 1990s. For example, a Russian man, with accomplices in several countries, used stolen passwords to steal $400,000 from Citicorp. He transferred another $11 million to bank accounts in other countries. This incident illustrates the international nature of computer crimes and some of the difficulties it creates for law enforcement. Extraditing the Russian man from London, where he was arrested, to the United States for trial took more than two years.

Phase 3: The growth of the Web and mobile devices

Beginning roughly in the mid-1990s, the intricate interconnectedness of the Web and the increased use of the Internet for email and other communications, for sensitive information, and for economic transactions made hacking more dangerous and damaging—and more attractive to criminal gangs. The kind of accessible information expanded to include

* A worm is a program that copies itself to other computers. The concept was developed to make use of idle resources, but it was adopted by people using it maliciously. A worm might destroy files or just waste resources.

credit reports, consumer profiles, medical records, tax records, confidential business information, and other types of information we described in Chapter 2 when we discussed threats to privacy. With basic infrastructure systems (for example, water and power, hospitals, transportation, emergency services, in addition to the telephone system) accessible on the Net, the risk increased. Hacking for political motives increased. As the Web spread globally, so did hacking. We describe examples ranging from new pranks to serious disruptions.

Pranksters modified the U.S. Department of Justice Web page to read "Department of Injustice" in protest of the Communications Decency Act. They changed the CIA's site to read "Central Stupidity Agency" and added links to pornography sites.[5]

A teenager crippled a computer system that handled communications between the airport tower and incoming planes at a small airport. Hackers in England impersonated air traffic controllers and gave false instructions to pilots. Hackers took over Federal Aviation Administration (FAA) computers in Alaska, resulting in a shutdown of part of the system. The hackers also appeared to have access to thousands of FAA passwords.

More than a decade after the Internet Worm, numerous viruses showed that the Internet, by then much bigger, was still vulnerable. The Melissa virus of 1999 infected approximately a million computers worldwide. In 2000, the "Love Bug," or "ILOVEYOU" virus, spread around the world in a few hours. It destroyed image and music files, modified a computer's operating system and Internet browser, and collected passwords. This virus infected major corporations like Ford and Siemens and 80% of U.S. federal agencies, including the State Department and the Pentagon, along with members of the British Parliament and the U.S. Congress. Many businesses and government agencies had to shut down their email servers. The virus hit tens of millions of computers worldwide and did an estimated $10 billion in damage.[6⋆] Viruses and worms such as Code Red, Zotob, Sasser, and MyDoom caused hundreds of millions or billions of dollars in damage. Some viruses set up a "back door" on infected computers that allowed later access to sensitive information such as credit card numbers.

Within about one week, *denial-of-service attacks* shut down almost a dozen major websites, some for several hours. Victims included Yahoo, eBay, Amazon, E∗Trade, Buy.com, CNN, and others. In this kind of attack, hackers overload the target site with hundreds of thousands of requests for Web pages and other information. Programs planted on numerous other systems (many at universities), to disguise their origin, generate the requests. Investigators traced the attack to a 15-year-old Canadian who used the name mafiaboy; he pleaded guilty to a long list of charges. The U.S. government estimated the cost of this incident at $1.7 billion. One disturbing aspect of this case is that mafiaboy apparently did not write the destructive programs himself. He found them on the Net, where other 15-year-olds can find them too.[7]

⋆ Damages from such virus attacks are difficult to value precisely; estimates may be rough.

The purposes and techniques of hacking have shifted as the Web and the amount of stored data of all kinds have grown. Hackers steal millions of credit card numbers from large retailers, restaurant chains, banks, and so on. Some are members of organized crime groups; others sell the numbers to organized crime groups. Some demand extortion payments. Such incidents signaled the beginning of the huge problem of credit card fraud and identity theft that we discuss in Section 5.3.

A new type of virus became popular. The virus gives the person who distributed it the power to remotely control the infected computers. Tens of thousands of infected computers (called *zombies*) send spam, contribute to denial-of-service attacks, participate in various kinds of online advertising fraud, and so on. The actual owners of the zombie computers are usually unaware of what their computers are doing. A 21-year-old California man pleaded guilty and was sentenced to almost five years in prison (the longest hacking sentence at that time, 2006) for a collection of offenses related to such a virus. He, according to prosecutors, took over hundreds of thousands of computers (some at military sites), used the infected computers to commit fraud, and "rented" them to others for sending spam and for criminal schemes. In the same year, an antispam expert reported a sophisticated international scam. It involved 20 billion spam messages sent within a two-week period from more than 100,000 computers in more than 100 countries. The messages directed people to e-commerce websites where the unwary ordered products with their credit cards and received nothing. Credit card charges went to a company in Russia. This scam illustrates the growing complexity of crime on the Web combining hacking, spam, phony websites, and international fraud.[8]

As computer systems replaced human ticket sellers for transportation and other services, hackers found more opportunities for theft. For example, New York City accused several people of stealing $800,000 from the city's subway system by taking advantage of an error in the software in the machines that sell fare cards.

Hackers continue to execute pranks and revenge attacks—some quite expensive. Hackers modified the programming at an online gambling site so that everyone won. The site lost $1.9 million. After police raided a popular pirate music site in Sweden, an apparent retaliation attack by hackers shut down the main websites of the Swedish government and police. After Sony sued George Hotz in 2011 for showing how to run unauthorized applications and games on Sony's PlayStation 3, a hacker group launched a denial-of-service attack on Sony and accessed names, birthdates, and credit card information of millions of users of Sony's gaming systems.[9] Hackers attacked companies that criticized or withdrew services from WikiLeaks.

As social networks grew, they became targets of hackers. In 2011, hackers gained access to Facebook member profile pages and posted pornographic and violent images. The hackers had tricked members into running malware. It is a common tactic for hackers to create fake offers of discounts, freebies, or just something funny or interesting. Clicking on it initiates the malware. In this particular attack the purpose might have been to express

criticism of a company whose policies the hackers disapprove. Similar attacks encourage a social media friend to view a video. The video site indicates that the user must install software to view the clip; that software is malware. Social networks offer a huge pool of potential victims who are used to sharing.[10]

Hacking of mobile devices (other than stolen laptops) has not yet been a major problem (while I am writing this), but I expect it to become one. With smartphones acting as electronic wallets and tablets synching to all one's data in clouds, they will be attractive targets.

Is "harmless hacking" harmless?

In many cases, it is the excitement and challenge of breaking in that motivates young hackers. Some claim that such hacking is harmless. Is it?

When a system administrator for a computer system at a university, a website, a business, or the military detects an intruder, he or she cannot immediately distinguish a nonmalicious hacker from a thief, terrorist, or spy. The administrator must stop the intrusion. The administrator's responsibility is to protect the system and its data. Thus, at a minimum, the organization will expend time and effort to track down the intruder and shut off his or her means of access. Companies sometimes shut down their Internet connection, at great inconvenience, while investigating and defending against an intruder. Responding to nonmalicious or prank hacking uses resources that might be needed to respond to serious threats.

Uncertainty about the intruder's intent and activities has additional costs for systems that contain sensitive data. According to the head of the computer crime unit at the Department of Justice, after a hacker accessed a Boeing Corporation computer, apparently just to hop to another system, Boeing spent a large sum to verify that the intruder changed no files. Would we be comfortable flying a new Boeing airplane if they had *not* done this? A group of young Danes broke into National Weather Service computers and computers of numerous other government agencies, businesses, and universities in the United States, Japan, Brazil, Israel, and Denmark. Eventually, police caught them. It appeared they had done little damage. But consider the risks. Their activities caused the Weather Service computers to slow down. There was the potential that serious conditions, such as tornadoes, could have gone undetected and unreported.[11] Similarly, if system administrators detect unauthorized access in a medical records system, a credit database, or payroll data, they must stop the intruders and determine whether they copied or changed any records. Uncertainty causes harm, or expense, even if hackers have no destructive intent.

Another problem, of course, is that a hacker with good intentions could make a mistake and do significant damage accidentally. Almost all hacking is a form of trespass. Hackers with nonmalicious intentions should not be surprised that others will often not view them kindly.

5.2.2 Hacktivism, or Political Hacking

Hacktivism is the use of hacking to promote a political cause. Is there ethical justification for such hacking? Should penalties for hacktivists differ from penalties for other hackers? Just as hacking in general ranges from mild to highly destructive activities, so can political hacking. We consider some examples.

Someone posted a pro-drug message on a police department antidrug website. Earlier we mentioned incidents of defacement of U.S. government websites; many make implicit political statements. Three teenagers hacked into the network of an atomic research center in India and downloaded files to protest India's tests of nuclear weapons. Hacktivists targeted the governments of Indonesia and China for their antidemocratic policies. A hacker group hacked into the Bay Area Rapid Transit (BART) system and released emails, passwords, and personal information about a few thousand BART customers. They did this to protest BART's controversial shutdown of wireless communication in several BART stations to thwart a planned protest demonstration.

A fundamental problem with evaluating political hacking is that it can be hard to identify. People who agree with the political or social position of the hackers will tend to see an act as "activism," while those who disagree will tend to see it as ordinary crime (or worse). Is posting a pro-drug message on a police website a political statement against the futility, dishonesty, expense, and international intrusions of U.S. drug policy, or is it the act of a kid showing off? To some political activists, any act that shuts down or steals from a large corporation is a political act. To the customers and owners, it is vandalism and theft.

Suppose we know that a political cause motivates the hackers. How can we begin to evaluate the ethics of their hacktivism? Suppose a religious group, to protest homosexuality, disables a website for gay people. Suppose an environmentalist group, to protest a new housing development, disables a website of a real estate developer. Many of the people who might argue that one of these acts is justifiable hacktivism would argue that the other is not. Yet it would be extremely difficult to develop a sound ethical basis for distinguishing them.

Some academic writers and political groups argue that hacktivism is ethical, that it is a modern form of civil disobedience.[12] Others argue that the political motive is irrelevant, or at the other extreme, that political hacking is a form of cyberterrorism. Civil disobedience has a respected, nonviolent tradition. Henry David Thoreau, Mahatma Gandhi, and Martin Luther King Jr. refused to cooperate with rules they saw as unjust. Peaceful protestors have marched, rallied, and boycotted to promote their goals. Burning down ski resorts (because one would prefer to see the land undeveloped) or abortion clinics (because one opposes abortion) is quite another category of activity. To evaluate incidents of hacktivism, it is helpful to fit them into a scale from peaceful resistance to destruction of other people's property and actions that risk serious harm to innocent people.

Are hacktivists merely exercising their freedom of speech? Freedom of speech does not include the right to hang a political sign in a neighbor's window or paint one's slogans on someone else's fence, even if that "someone else" is a group of people organized as a business or corporation. We have the freedom to speak, but not the right to compel others to listen. Crashing a website or defacing a Web page is comparable to shouting down a speaker with whom one disagrees. Those who believe that the specific content or cause is more important than the principle of freedom of speech defend such actions. It is common for people involved in political causes to see their side as unquestionably morally right, and anyone on the other side as morally evil, not simply someone with a different point of view. This often leads to the view that the freedom of speech, freedom of choice, and property rights of the other side deserve no respect. Peace, freedom, and civil society require that we respect such basic rights and not impose our views on those we disagree with.

Another factor to consider when evaluating hactivism is the political system under which the hacktivists live. From both an ethical and social perspective, in free countries where almost anyone can tweet or post their words and video on the Web for free, it is hard to justify hacking someone else's site to promote a political cause. Activists use the Internet to organize opposition to oil exploration in Alaska that they fear will harm a caribou herd. Activists use free social media to organize mass demonstrations against international meetings of government leaders. Human rights organizations effectively use the Web, Twitter, and Facebook. Groups supporting all kinds of nonmainstream causes, from animal rights to anarchism to odd religions, promote their views in cyberspace. None of this activism requires hacktivism. On the other hand, countries with oppressive governments control the means of communications and prohibit open political discussion, have secret police who kill dissenters, ban some religions, and jail people who express opposition views. In such countries, where openly communicating one's views is impossible or dangerous, there might be good arguments to justify political hacking to get one's message out to the public and, in some cases, to sabotage government activities. The nations in which hacktivism is likely to have the most ethical justification are those least likely to respect acts of civil disobedience.

5.2.3 Hackers as Security Researchers

Since well before the advent of the Web there has been a subculture of hackers who probe computer systems, most often without permission, to find security flaws as an intellectual exercise and, for some, as a public service. They sometimes call themselves "security researchers" to avoid the now negative connotation of the term hacker. In old cowboy movies, the good guys wore white hats and the bad guys wore black hats. So some people use the terms "white hat hacker" and "black hat hacker" for the cowboys of the computer frontier. White hat hackers, for the most part, use their skills to demonstrate system vulnerabilities and improve security. Those who use methods of questionable legality or

who publicize vulnerabilities before informing the system owners are sometimes called "gray hats." Many are computer security professionals. Some spent time in jail or on probation for hacking when in their teens. The security researcher who found that some smartphones sent location and ID data to Google and Apple is one example.

Security researcher hackers face ethical dilemmas. The most obvious is: Is it ethical to break into a system without permission, even with good intentions? We discussed this to some degree in the discussion of whether harmless hacking is truly harmless (in Section 5.2.1). Another dilemma is: How can people responsibly inform potential victims of security vulnerabilities without informing malicious hackers who would exploit them? Some post details about security weaknesses on the Internet. Some work quietly with software companies. Most computer professionals are very critical of the first approach. Responsible security professionals do not announce security flaws to the public as soon as they discover them. They inform the software company or system manager responsible for the software and allow time for them to prepare patches (corrections) or close security holes before making a public announcement. They believe that when a security researcher hacker discovers a security weakness in a system, he or she should do the same.

Although the topics are somewhat different, the discussion of the ethics of publishing sensitive leaked material in Section 3.3 has relevance here. In particular, two critical aspects to consider are how important the information is to the public and how much harm might be done by publishing it.

Many security researcher hackers are very scornful of big software companies both because of the large number of security flaws in their products and because they are slow to plug leaks even when they know of them. The hackers argue that these businesses do not behave responsibly toward the public. Publicizing security problems spurs the companies to take action. This argument has some truth to it. Hackers and security consultants say they repeatedly warn companies of flaws that allow access by hackers, but the companies do not respond until malicious hackers exploit the flaws and cause significant problems. Some businesses and government agencies have so much confidence in their systems that they refuse to believe anyone can break in. A man who copied patient files from a medical center said he did it to publicize the system's vulnerability, not to use the information. He disclosed portions of the files to a journalist after the medical center said that no one had copied patient files.[13] Should we view him as a whistleblower or a criminal? Members of a group called Goatse Security collected the email addresses of more than 100,000 iPad owners from an AT&T website. The site displayed the email address of an iPad owner to anyone who entered the iPad ID number; it did not require a password. A spokesperson for Goatse Security said they notified the media about the security flaw after AT&T fixed it. Did they act responsibly or irresponsibly and criminally?[14] A security researcher discovered a major flaw in the Internet's domain name server system (the system that translates Web addresses, say, www.yourbank.com

to IP addresses*) that could have allowed hackers to redirect and steal any information transmitted on the Net. He kept the problem secret while working with several companies to develop a patch, and then announced the patch and said he would make details of the problem—and how to exploit it—public in 30 days. The 30-day limit, he said, encouraged companies to install the patch and encouraged others who knew of the flaw not to disclose it sooner.

Exposing security flaws is not a legitimate justification for most hacking, but, as a side effect, it does sometimes speed up security improvements. As software companies, financial companies, and online retailers began taking security more seriously, some began treating well-intentioned hackers as allies rather than enemies.

5.2.4 Hacking as Foreign Policy

> *[K]eystrokes originating in one country can impact the other side of the globe in the blink of an eye. In the 21st century, bits and bytes can be as threatening as bullets and bombs.*
>
> —William J. Lynn III, Deputy Defense Secretary[15]

Hacking by governments—for economic and military espionage and to disable enemies (or future enemies)—has increased dramatically in the past few years. The first cyber attack apparently coordinated with a military attack occurred in 2008 when the Russian military moved into Georgia (the former Soviet republic). Georgian government websites were attacked and some disabled. Internet security experts and the Georgian government thought it very likely that the Russian government was responsible. The source of the attack could not be definitely determined, a frequent problem with cyberattacks. In 2011, the government of Iran attempted to hack into the computers and phones of United Nations nuclear inspectors who were attempting to learn whether Iran's nuclear facilities are for military purposes. Whether Iran's intelligence agency was able to extract sensitive information (what the inspectors found, who assisted the inspectors, and so on) was uncertain.

Many cyber attacks come from China, and once again, it is difficult to prove that the government is behind them. However, the nature and sophistication of the attacks, as well as the type of targets lead security researchers to believe that they are the work of government agencies, not civilian hackers. For example, a Chinese government-owned company sent false messages to the Internet routing system to reroute a large amount of Internet traffic through servers in China. The intended (and eventual) destinations of the rerouted traffic included U.S. military agencies and Congress. Clearly, someone (or a government) that does this could spy on, tamper with, or disrupt communications.

---

* That is, the Internet Protocol address, a string of numbers that identifies a website.

Hackers stole several terabytes of information about the design of one of the Pentagon's new and extremely expensive fighter jets. The computer attack appeared to originate in China. Hackers, apparently in China, had high-level and widespread access to the computer system of a large U.S. telecommunications company for almost 10 years. They stole technical documents, research reports, business plans, and email. Security experts report that Russian and Chinese hackers broke into computer networks that control the U.S. electric power grid. They left behind code that could disrupt the system if activated. Hackers intruded on U.S. satellites to the point where they could control, damage, or destroy them (but did not do so). Hackers, apparently in China, systematically hacked oil and gas companies worldwide.[16]

A 2011 attack on the Gmail accounts of White House staffers, China policy experts, military officials, human rights activists, and others originated in a Chinese city where a major Chinese national security division is located. This attack used email carefully written in government jargon about State Department reports to fool the recipients into thinking the email was authentic. High-level government officials (and other people targeted) disclosed their passwords, allowing the hackers to read their email for months.[17]

If the attacks we described are the work of foreign governments, they pose a huge threat to safety and national security. Even if not, they demonstrate the potential for hackers with ill intent to cause significant damage to communication, financial, military, and power systems.

The Pentagon announced that it would consider and treat some cyber attacks as acts of war, and the United States might respond with military force. Countries targeted with cyber attacks must determine whether a foreign government or terrorist organization

Stuxnet

Stuxnet is an extremely sophisticated worm program that targets a particular type of control system and, beginning in 2008, damaged equipment in a uranium enrichment plant in Iran. The focus on Iran's nuclear program and the sophistication of Stuxnet led to speculation that the Israeli and/or U.S. government created it. In 2012, journalist David Sanger published extensive research indicating that the two governments did indeed produce Stuxnet.

Is such cyber sabotage against Iran justified? (Is it better than a military attack by Israel on Iran's nuclear facilities?) Will China, Russia, or other governments cite Stuxnet as an excuse for their own cyber intrusions into the United States and other countries?

Stuxnet eventually spread from Iran and infected equipment in other countries. Wars regularly include deaths of civilians and incidents where military units accidentally kill fighters on their own side. How common and how serious will analogous side effects of cyber attacks be?[18]

(or teenager) organized the attack. What level of certainty should there be before a counterattack? When is a cyber attack an act of war? What responses are appropriate? Perhaps more importantly, how can we make critical systems safer from attacks?

5.2.5 Security

> *The fact that I could get into the system amazed me.*
>
> —Frank Darden, a member of the Legion of Doom, which hacked the BellSouth telephone system[19]

Hacking and the spread of viruses are as much a comment on the security of computers, telecommunication systems, and the Web as they are on the skills and ethics of the hackers. Hacking is a problem; so is poor security. We talked about responsibility for security of personal data when we discussed privacy in Chapter 2, and we say more when we discuss identity theft in Section 5.3. It is hard to overemphasize the importance of responsible, effective security.

A variety of factors contribute to security weaknesses. They come from the history of the Internet and the Web, from the inherent complexity of computer systems (especially the software and communications systems that run phones, the Web, industrial systems, and the many interconnected devices we use), from the speed at which new applications develop, from economic and business factors, and from human nature. We will describe and illustrate some of these influences.

In its early years, the Internet was primarily a communications medium for researchers. The focus was on open access, ease of use, and ease of sharing information. The Internet was not designed for security against malicious intruders, teenage explorers, or organized criminals. Many early systems did not have passwords. Few early systems connected to telephone networks, so protection against intruders was not a concern. Security depended primarily on trust. The World Wide Web developed as a communications tool for physics researchers. Again, security was not a primary design concern. Security on the early Web was extremely weak. When businesses and government agencies began to set up websites, Internet security expert Dan Farmer ran a program to probe the websites of banks, newspapers, government agencies, and pornography sellers for software loopholes that made it easy for hackers to invade and disable or damage the sites. Of the 1700 sites he examined, he found that about two-thirds had security weaknesses—and only four sites apparently noticed that someone was probing their security. Farmer's warnings had little effect.

Attitudes about security in businesses, organizations, and government agencies were slow to catch up with the risks. Gradually, computer scientists responded to increased security threats with improved security technology, and entrepreneurs and the market responded with the development of many security firms and consultants offering a

variety of software products and services. Security techniques and practices improved dramatically. Many government agencies, businesses, and organizations have up-to-date, high-quality security, but there are still serious weaknesses. News reports of major break-ins and security lapses appear almost weekly. Numerous government studies warn of vulnerabilities and the potential for sophisticated attacks on critical infrasturcture.

It might not be surprising that, initially, computer security at universities and businesses was weak. It is unsettling, however, that it has been so easy to hack into military systems, other government agencies, and defense contractors. In 1998, the U.S. deputy defense secretary described a series of attacks on numerous U.S. military computers as "the most organized and systematic attack the Pentagon has seen to date."[20] Two boys, aged 16 and 17, had carried them out. A security expert described one hacking attack on Defense Department computers that did not contain classified information as the modern equivalent of a kid sneaking into a Pentagon cafeteria. Maybe. On the other hand, we should expect Pentagon security to be good enough to keep a kid out of its cafeteria. As we noted in Section 5.2.4, foreign governments are replacing teenagers as the major threat to defense systems. Their resources and expertise far surpass those of teenagers. In 2011, the deputy defense secretary said that in the previous decade, intruders stole plans (from the government and defense industry firms) for aircraft avionics, satellite communications systems, network security protocols, missile tracking systems, satellite navigation devices, surveillance drones, and jet fighters. The *New York Times* described a theft (by a foreign intelligence service) of 24,000 Defense Department documents as "one of its worst digital attacks in history"—a description that reappears in hacking reports repeatedly as hackers steal more and more sensitive information.[21]

Security in other government agencies is weaker than in the Defense Department. For example, the Government Accountability Office (GAO) reported that computer security at NASA was so weak that hackers could easily disrupt such functions as the tracking of spacecraft. The same report described Environmental Protection Agency (EPA) computers as "riddled with security weaknesses." Hackers were able to use the EPA's system to launch hacking attacks on other agencies. The U.S. Transportation Department warned of numerous vulnerabilities in the air traffic control system and the potential for sophisticated attacks on air traffic control by foreign governments. Its report said that almost all ATC facilities had insufficient controls for detecting intrusions. A review in 2011 recommended that users be required to enter an ID and password—a requirement that should have long been in place by then.[22]

Encryption is a particularly valuable security tool. It is often not used sufficiently and appropriately, by both governments and businesses, because it can be inconvenient and expensive. For example, the video feeds on U.S. predator drones (unmanned aricraft used in Iraq) were not encrypted. Insurgents in Iraq used $26 software, available on the Internet, to intercept the feeds. Access to the video feeds gave them valuable information about surveillance and attacks. It also might give them the potential to modify the feeds.

U.S. military officials had known the feeds were unprotected since the 1990s (when they used drones in Bosnia). They reconsidered the issue in 2004, but they assumed adversaries would not know how to exploit this security hole. Adding encryption to the system is expensive, but even if omitting it in the 1990s was a reasonable trade-off, they clearly should have updated the decision.[23] Underestimating the skills of opponents and unwillingness to pay for stronger security are frequent underlying causes of vulnerabilities in both government and business systems.

In several major thefts of consumers' personal data from retailers, the databases included unencrypted credit card numbers and other security numbers read from the magnetic strips on the cards. Hacking attacks on major security firms show that even such firms often leave sensitive data (including credit card numbers) on their systems unencrypted. Retailer TJX used a vulnerable, out-of-date encryption system to protect data transmitted between cash registers and store computers on its wireless network. Investigators believe hackers used high-power antennas to intercept data, decoded employee passwords, and then hacked into the company's central database. Over a period of about 18 months, the hackers stole millions of credit and debit card numbers and critical identification information for hundreds of thousands of people. (Stolen numbers were used fraudulently in at least eight countries.) The investigation revealed other security problems. The problems included transmission of debit card transaction information to banks without encryption and failure to install appropriate software patches and firewalls.[24]

In addition to technical security tools such as encryption, there are numerous market pheonomena that can help improve security. For example, just as some home insurance companies give discounts for deadbolt door locks and fire extinguishers in a home, insurance companies that offer insurance for hacker attacks require that their customers use high-quality computer security technology. Some software and security companies hire hackers to attack and find flaws in systems they are developing. Some pay consulting fees to teams of students and faculty at universities to find security weaknesses in their products so that they can fix the flaws before destructive hackers exploit them.

Another factor leading to weak security for systems that affect the general public is the speed of innovation and people's desire for new things fast. Hackers and security professionals regularly find gaping holes each time a new product, application, or cyberspace phenomenon appears. Competitive pressure spurs companies to develop products with insufficient thought or budget devoted to analyzing potential security risks and protecting against them. The culture of sharing and the phenomenon of users developing applications and games for social networks and smartphones come with vulnerabilities as well as all the wonderful benefits. Consumers buy the new products and services and download the apps with far more interest in convenience and dazzling new features than in risks and security.

Many incidents of stolen sensitive data (including some we described in Section 2.1.2) involve stolen portable devices such as laptops and phones. This is one example where

individuals, organizations, government agencies, and businesses embraced an advance in technology (portable devices with huge data storage) with little thought to the risks and when few security measures were available. Laptop security is now a booming business. There are systems that track stolen or lost laptops and allow the owner to erase files remotely. Fingerprint readers can control access to a device. Companies learned to use more physical protections, such as cables to secure laptops to heavy furniture in offices or hotels, and to train employees to be more careful with portable devices.

More and more appliances and machinery—from microwave ovens to cars to factory machinery to heart monitors—are going online. Doctors access and control medical devices over the Net. Automated fleets of cars will communicate with each other to drive safely on highways. These appliances and machines are vulnerable. Already, security researchers have manipulated the security system in a car by sending messages to the system over a cellular communication network, unlocking the car and starting its engine. Others used simple off-the-shelf hardware to send fake traffic and weather information to navigation systems in cars.[25] The focus in developing new applications is on making them work. Often, there is insufficient thought to protecting against malicious interference. We have seen (in Section 5.2.1) that some hackers think misdirecting airplane pilots is fun and that satellites and critical infrastructure such as power grids are vulnerable. The potentially dangerous and destructive consequences of malicious hacking of such systems impose a strong degree of responsibility for security on those who design the systems.

Responsibility for security

There are many parallels between security issues for preventing crime and security issues for protecting privacy. There are also similarities with the safety issues we discuss in Chapter 8. Principles and techniques for developing good systems exist, and responsible software designers must learn and use them. The field of computer security is robust and fascinating. System designers can make security from intrusion a major design goal. When a computer system contains valuable or sensitive data, or if many people depend on its smooth operation, the system administrators have a professional and ethical obligation, and in many cases a legal obligation as well, to take reasonable security precautions to protect the system. They must anticipate risks and prepare for them. System developers and administrators must stay up to date about new risks and new security measures. This is often not an easy task, but it is an essential goal and a professional responsibility. No matter how well designed security software and procedures are, the complexity of computer systems means that there will be unexpected security failures. We cannot expect perfection, but we should expect professionalism.

Most people who use smartphones, tablets, and computers have no technical training. Many do not use firewalls or antivirus software, because they do not understand the risks or because they find the security tools too confusing. It does not occur to consumers to ask when buying a new cellphone if their calls are encrypted or easily interceptable. Sellers of any widely used consumer product have an ethical obligation to build in a level of safety

appropriate for the general population. Software companies have an ethical obligation to design and implement their products so that they do not expose users to severe security threats.

The security vulnerabilities with the most profound potential threats to the lives and well-being of millions of people are in major infrastructure systems and defense systems. The companies and government agencies that operate these systems have, therefore, a profound responsibility for improving security.

5.2.6 The Law: Catching and Punishing Hackers

The law

When teenagers started hacking for the challenge of getting into off-limits computers, there was disagreement not only about whether the activity was a crime under existing law but also about whether it should be. Gradually, state governments passed laws that specifically addressed computer crimes. Congress passed the main federal computer-crime law, the Computer Fraud and Abuse Act (CFAA), in 1984.[26] As a federal law, the CFAA covers areas over which the federal government has jurisdiction: government computers, financial systems, and computers used in interstate or international commerce or communication. That, of course, includes computers connected to the Internet, cellphone systems, and so on. Under the CFAA, it is illegal to access a computer without authorization or to exceed one's authorization (in most cases). Sections of the law address altering, damaging, or destroying information and interference with authorized use of a computer. These cover denial-of-service attacks and the launching of computer viruses and other malicious programs. The CFAA is the main antihacking law, but prosecutors also use other federal laws to prosecute people for crimes related to computer and telecommunications systems. Illegal actions include access to commit fraud, disclosing passwords or other access codes to unauthorized people, and interrupting or impairing government operation, public communication, transportation, or other public utilities. State and federal antihacking laws provide for strong penalties, including prison sentences and fines.

The USA PATRIOT Act includes amendments to the Computer Fraud and Abuse Act. The PATRIOT Act expanded the definition of loss to include the cost of responding to a hacking attack, assessing damage, and restoring systems. It raised the maximum penalty in the CFAA for a first offense to 10 years. It increased penalties for hacking computers used by the criminal justice system or the military. It allows the government to monitor online activity of suspected hackers without a court order. We have observed that hacking covers a wide range of activity—some deserving serious punishment, some comparable to minor offenses kids of all generations commit, and some intended to demonstrate security weaknesses and encourage fixing them. Definitions of the actions to which the PATRIOT Act's antiterrorism provisions apply are broad and include activity few would consider terrorism.

Catching hackers

The people responsible for almost all the hacking incidents we described have been caught. It took only one week to catch the author of the Melissa virus. The FBI traced the denial-of-service attacks in 2000 to mafiaboy and had his real name within a week. Investigators identified four Israeli teenagers who wrote and launched the Goner worm in about the same time. How do hacker trackers do their job?

Initially, the response of law enforcement agencies was ill-informed and embarrassing. John Perry Barlow, a founder of the Electronic Frontier Foundation, colorfully described how he spent two hours explaining the basics of computing and computer networks to an FBI agent who came to question him in 1990. Law enforcement agencies now employ people who are well informed about technical aspects of hacking and the hacker culture. They and security professionals read hacker newsletters and participate in online discussions of hacking, sometimes undercover. Law enforcement agents, some undercover, attend hacker conferences. Security specialists maintain logs of Chat channels used by hackers. Security professionals set up *honey pots*—websites that look attractive to hackers—so that they can record and study everything a hacker does at the site. Law enforcement agents use wiretaps to collect evidence and build their cases against hacking suspects. Investigators identified a number of hackers because they bragged about their exploits.

The field of collecting evidence from computer files and disks is *computer forensics*. (Some use the term *digital forensics*). Computer forensics specialists can recover deleted files, often even if the user has erased and wiped the disks. In Chapter 2, we saw how easy it is to collect and save information about everything we do in cyberspace and to search and match records to build consumer profiles. The same tools that threaten privacy aid in catching criminals. Investigators trace viruses and hacking attacks by using ISP records and the logs of routers, the machines that route messages through the Internet. For example, David Smith, the man who released the Melissa virus, used someone else's AOL account, but AOL's logs contained enough information to enable authorities to trace the session to Smith's telephone line. After a series of high-profile hacking incidents by members of Anonymous, LulzSec, and related groups, police in several countries arrested dozens of members in 2011 and 2012 (though other members continued hacking exploits).

Most people are unaware that word processors and other programs include a lot of "invisible information" in files—in some cases, unique identifying numbers and the author's name. Security experts use such information to trace viruses. The hidden identifying information in files worries privacy advocates—another reminder of the tension between privacy and crime fighting.

Many of the techniques we just described worked because hackers did not know about them. When such methods receive publicity in big cases, hackers learn what mistakes to avoid. Hackers, as well as people seeking privacy, learn how to remove identifying numbers from documents. Hackers learn how to forge such numbers to throw suspicion elsewhere. Thus, the particular methods described here will be less effective when you read this. Law enforcement and security personnel update their skills and tools as hackers change theirs.

Penalties for young hackers

Many young hackers are the modern analogue of other generations of young people who snooped where they did not belong or carried out clever pranks, sometimes breaking a law. In his book *The Hacker Crackdown*, Bruce Sterling describes the phone phreakers of 1878. That is not a typo. The new American Bell Telephone company initially hired teenage boys as operators, some of whom disconnected calls and crossed lines on the switchboard, connecting people to strangers. The boys were also, like many teenage hackers, rude.[27] The phone company learned its lesson and replaced teenage boys with woman operators.

We want young hackers to mature, to learn the risks of their actions, and to use their skills in better ways. Most of them do grow up and go on to successful, productive careers. We do not want to turn them into resentful, hardened criminals or wreck their chances of getting a good job by putting them in jail. This does not mean that we should not punish young hackers if they trespass or cause damage. Kids do not mature and become responsible without good direction or if we reward their irresponsibility. The point is that we should not overreact and overpunish. Some young hackers will become the great innovators of the next generation. Steve Wozniak created the Apple computer, co-founded the Apple company, and, after Apple's success, donated large amounts of money to medical research and other valuable efforts. But before he was building Apples, Wozniak was building blue boxes, devices that enabled people to make long-distance phone calls without paying for them. Nobel Prize winner Richard Feynman used "hacker" techniques when he was a young physicist working on the highly secret atomic bomb project at Los Alamos National Laboratory in the 1940s. He hacked safes (not computers) containing classified work on the bomb. He found or guessed the combinations and delighted in opening the safes at night and leaving messages for the authorized users informing them that security was not as good as they thought.[28]

Many exploits of young hackers are pranks, trespass, and vandalism. They usually do not include financial gain for the hacker (though, as we observed in Section 4.1.5 in the context of copyright infringement, lack of financial gain is often not significant in determining whether actions are wrong). Difficult penalty issues arise for hackers who are young, hackers who do not intend to do damage, and hackers who, through accident, ignorance, or immature irresponsibility, do vastly more damage than they can pay for. How can we distinguish between young hackers who are malicious and likely to commit more crimes and those who are likely to become honest and productive professionals? What penalties are appropriate? Clearly, offenses related to unauthorized access vary in degree, and penalties should likewise vary, as they do for trespass, vandalism, invasion of privacy, fraud, theft, and sabotage.

In many hacking cases, especially those involving young people, the hacker pleads guilty. The evidence is clear, and the hacker and prosecutor work out a plea bargain. At first, most hackers younger than 18 received relatively light sentences including two or three years probation, community service, and sometimes a fine or order to pay restitution. The 15-year-old who disabled an airport radio system got probation even though his

exploits could have endangered people. In 2000, a 16-year-old was sentenced to six months in a juvenile detention facility. He was the first juvenile incarcerated for hacking. He had broken into NASA and Defense Department computers and was a member of a hacker group that vandalized government websites. As more young people caused more disruption, the severity of penalties increased.

One of the purposes of criminal penalties is to discourage people from committing crimes. Some people advocate heavy penalties for minor hacking to "send a signal" to others who might be thinking of trying something similar. There is a temptation to do this with hacking because of the costs to the victims and the potential risks to the public. On the other hand, justice requires that punishments fit the specific crime and not be increased dramatically because of the potential of what someone else might do.

Sometimes the company whose computers a hacker invaded gives him a job after catching him. Give a hacker a job instead of a jail sentence? Some computer professionals and law enforcement officials are very critical of this practice of "rewarding" hackers with security jobs. We do not reduce hacking by encouraging young people to think breaking into a computer system is an acceptable alternative to sending a résumé. But, in some cases, the job, the responsibility and respect that go with it, and the threat of punishment for future offenses are enough to turn the hacker's energy and skills toward productive uses. With any criminal law, there is a trade-off between having fixed penalties (for fairness, to avoid favoritism) and flexibility (to consider the particular circumstances). With young people, flexibility is probably more important. Penalties can focus on using the hacker's computer skills in a productive way and on paying victims for damage done (if possible). Deciding on what is appropriate for a particular person is delicate, one of the difficulties prosecutors and judges face with juvenile crime.

How can we dissuade young teens from breaking into computer systems, launching viruses, and shutting down websites? We need a combination of appropriate penalties, education about ethics and risks, and parental responsibility. Parents of many young hackers have no idea what their children are doing. Just as parents have responsibility for teaching their children to avoid unsafe behavior in cyberspace, they also have some responsibility for preventing their children from engaging in malicious, destructive hacking.

Criminalize virus writing and hacker tools?

You can find hacking scripts and computer code for thousands of computer viruses on the Internet. Intentionally or recklessly making such programs available in a context that encourages their destructive use is irresponsible. Should the software itself be illegal? Some law enforcement personnel and security professionals propose making it a crime to write or post computer viruses and other hacking software. A law against writing or publishing viruses and hacking software could keep them from casual hackers. Criminal penalties might dissuade potential teenage hackers, but probably not serious criminals. Such a law could make security work and research more difficult. Security personnel and researchers must be able to possess security and hacker software to effectively do their job.

A law against distributing virus and hacking code would raise issues similar to some we discussed in Chapters 2 and 4 about restricting or banning strong encryption and technologies to circumvent copyright protections. We saw in Chapter 3 that writing about how to make illegal or destructive devices, such as bombs, is not (in most cases) illegal. On the other hand, as a security professional commented, "With a computer virus, the words are the bomb."[29] A federal court ruled that software is a form of speech (see Section 2.5.1), so a law against hacking software or virus software might conflict with the First Amendment. The First Amendment does not protect some kinds of speech, such as inciting a riot. However, encouraging people to commit destructive or illegal actions is generally protected by the First Amendment in situations where the listener has time to reflect and make a decision about whether to act. A person who reads virus code has the opportunity to decide whether to activate the virus.

How do *you* think the law should treat virus code and hacking scripts?

Expansion of the Computer Fraud and Abuse Act

The CFAA predates social networks, smartphones, and sophisticated invisible information collection about our activities in cyberspace. It was intended for malicious and prank hacking. Later applications of the law illustrate how the impact of a law can change and grow with new technology. Some of the new applications can help protect privacy. Some might criminalize common activities of millions of people. We consider the latter first.

Is violating the terms of use of a website a crime under the CFAA's provision about exceeding one's authorized access for the purpose of committing fraud and obtaining something of value?* This question is both a legal and a social one: Does it make sense for violation of terms of use to be a crime? The first major case involved a woman who pretended to be a 16-year-old boy on MySpace, began an online flirting relationship with a 13-year-old girl in her neighborhood (a former friend of the woman's daughter), then broke off the relationship and sent cruel messages. The girl killed herself. The woman's behavior was nasty and unethical. People wanted to see her punished, but it was not clear that she had broken any law. Prosecutors charged her with illegal hacking under the CFAA. They said she exceeded authorized access because she violated MySpace's terms of use requiring that profile information be truthful. A jury convicted the woman, but the judge reversed the conviction. He said in effect that this application of the law was too broad. Normally, a breach of contract is not a criminal offence, and the CFAA does not state or suggest that it has become one. An ordinary, reasonable person does not expect that violating the terms of use of a website is a criminal offense.[30] The decision of one judge, though, does not settle the legal situation. Prosecutions and lawsuits continue to treat violation of terms of use as a crime under the CFAA. Some businesses state in their websites' terms of use that competitors may not use the site for any purpose. Under the broad interpretation of exceeding authorized access, such a business may sue any

* This is a simplification of the legal language.

competitor who visits the site. Could someone be prosecuted for lying about his or her age (or attractiveness) on a dating site if the site says members may not provide false or misleading information? Could a high school student be prosecuted for setting up a Gmail account? Gmail's terms of service require that the user be of legal age to form a binding contract; that generally leaves out minors. Who knew?

There are more sensible approaches to handling violations of terms of use. A social network, dating service, or other membership service can terminate the membership of anyone who violates the terms of use to an extent that the organization considers a serious problem. A business can attempt to block access to its website by people (or companies) it wants to exclude—or just accept the fact that if it makes the site public and chooses not to require membership or passwords, then anyone in the public might visit it. If someone violates terms of use and actually commits fraud, theft, or vandalism, appropriate laws against those acts apply.

Another unintended application of the CFAA might help protect privacy. As we discussed in Chapter 2, hidden software on websites or in smartphone apps tracks our online or phone activity. Such software collects information from our phone or other device. When we install an app or visit a website, we implicitly authorize it to interact with our phone or device, using the data necessary to perform its stated purpose. We can interpret going beyond that purpose (if the app or site does not disclose that it does so) as exceeding authorized access. Some prosecutors use the CFAA to bring charges against people or businesses that do unauthorized data collection. The definition of "authorized" is important when prosecutors use the CFAA in this way. The bounds of authorization are often unstated and can be fuzzy. If the line is drawn well, this will be an innovative way of using the CFAA to protect us against surreptitious information collection. If applied too broadly, it could criminalize practices that many consumers accept or like. These cases are new, so it is as yet unclear what the results will be.

The CFAA and personal use of an employer's computer: Section 6.3.2

5.3 Identity Theft and Credit Card Fraud

Con artists and crooks of many sorts have found ample opportunity to cheat unsuspecting people in cyberspace. Some scams are almost unchanged from their pre-Web forms: pyramid schemes, chain letters, sales of counterfeit luxury goods, sales of food-stamp cards, phony business investment opportunities, and so forth. Each generation of people, whatever level of technology they use, needs a reminder that if an investment or bargain looks too good to be true, it probably is. Other scams are new or have evolved to take advantage of characteristics of the Web. In online dating scams, crooks use profiles and photos lifted from social media sites to develop online relationships and convince the unwary to send money for a family emergency or some other false reason. In a particularly offensive scam, people set up websites after disasters such as terrorist attacks and hurricanes

to fraudulently collect credit card donations from people who think they are contributing to the Red Cross or funds for victims.

In this section, we examine identity theft and credit card fraud at some length. We look at the thieves' methods and some countermeasures that have emerged. The point is not the particular details but the patterns: insufficient security, big losses, then gradual improvement. People learn the risks. Businesses and individuals respond with new protection mechanisms, and law enforcement agencies acquire skills to catch and convict the crooks and discourage their activity.

5.3.1 Stealing Identities

We buy products and services from strangers in stores and on the Web. We do our banking and investing online without seeing or knowing the physical location of the company we deal with. We can travel with only a passport and a credit or debit card. We can qualify for a mortgage or a car loan in minutes. As part of providing this convenience and efficiency, our identity has become a series of numbers (credit and debit card numbers, Social Security number, driver's license number, phone number, account numbers) and computer files (credit history, Web activity profile, work history, driving record). The convenience and efficiency engender risks. Remote transactions are fertile ground for many kinds of crime, especially identity theft and its most common result, credit and debit fraud.

Identity theft describes various crimes in which a criminal (or large, well-organized criminal group) uses the identity of an unknowing innocent person. If the thieves get credit (or debit) card numbers, they buy expensive items or sell the numbers to others who use them. If they do not have card numbers, they use other personal information (Social Security number, for example) to open new accounts in the victim's name. In one scam, thieves used names and Social Security numbers of almost 2000 people and applied for their tax refunds. Identity thieves take out loans, buy groceries, raid the victim's bank account, pass bad checks, or use the victim's identity in various other ways for financial gain. A security company executive says a complete identity sells for less than $20.[31]

The Federal Trade Commission receives hundreds of thousands of complaints of identity theft each year. Losses from identity theft amount to billions of dollars per year in the United States, with several million victims. A single incident can affect thousands of people. For example, two U.S. grocery chains reported that data thieves planted malware in the computer systems of their stores and gained access to more than four million credit and debit card numbers. The malware sent the data to a server outside the United States; almost 2000 cases of fraud resulted. Credit card companies and other businesses bear the direct cost of most credit card fraud, but the losses lead to higher charges to consumers. In addition, individual victims might lose a good credit rating, be prevented from borrowing money or cashing checks, be unable to get a job, or be unable to rent an apartment. Creditors might sue the victim for money the criminal borrowed.

The many tactics used for identity theft and credit and debit card fraud, and the many solutions developed in response, illustrate the continual leapfrogging between increased sophistication of security strategies and increased sophistication of criminal strategies. They also illustrate the value of the mix of technology, innovative business policies, consumer awareness, and law to solve the problems. We describe a variety of tactics for identity theft, then consider many approaches to reducing identity theft and reducing its impact on its victims. A few of the methods we describe are no longer used because the other side defeated them or consumers found them too cumbersome. Technology evolves and clever people on both sides of the law develop new ideas. For the general public and for anyone working with sensitive personal data, it is necessary to remain aware and flexible.

Have you received email or a text message from PayPal, Amazon, or a bank asking you to confirm information about your account? Have you received email from the IRS telling you the agency has a tax refund for you? These are examples of fraudulent spam called *phishing* (in the case of email) and *smishing* (in the case of text messaging)*: sending millions of messages fishing for information to use to impersonate someone and steal money and goods. The message tells the victim to click on a link to what purports to be the website of a well-known bank or online company. The phony site asks for account numbers, passwords, and other identifying information. Identity thieves take advantage of our knowledge that there is a lot of online fraud: Several pretexts that appear frequently in phishing scams warn that there has been a breach in the security of your bank or PayPal account and you need to respond to determine whether someone else is misusing your account. Some messages tell the recipient they just made a very big purchase and if the purchase was not really theirs, they should click a link to cancel the order. In a panic, people do—and enter their identifying information when asked for it.

The first defense against phishing is to be extremely wary of clicking on a link in an unsolicited message, especially if the message is about account information. The standard antifraud advice is: If you are uncertain whether the message is authentic but you want to respond, ignore the link and check your account in the usual way. As more people learned to be wary of clicking on links in messages that appear to be from a legitimate company, thieves modified their phishing scams; the message provides a telephone number to call. Those who call hear a request for their account number and other identifying information. This variation is sometimes called *vishing*, for voice phishing. Of course, a phone number provided by phishers is as fake as the links they provide.

Pharming is another technique to lure people to fake websites where thieves collect personal data. Normally when we indicate a website we want to visit, our browser looks up the IP address of the site on one of many Domain Name Servers (DNS), special computers on the Internet for this purpose. Pharming involves planting false Internet addresses in the tables on a DNS that lead the browser to a counterfeit site set up by identity thieves.

* SMS is the abbreviation for Short Message Service, the method used for texting on cellphones.

Corrupting a DNS is more difficult than sending a huge number of phishing emails, so it is much less common.

Figure 2.1 lists incidents of loss or theft of large databases containing personal information. In several of those incidents, identity theft and fraud were the goals. Sophisticated criminal rings hack into corporate and government computer networks, steal computers and disks, or pose as legitimate businesses and buy credit records and personal dossiers to obtain information to use in identity theft.

Identity thieves love the millions of résumés that people post on job-hunting sites. They collect addresses, Social Security numbers, birth dates, work histories, and all the other details that help them convincingly adopt the identity of the job seeker. Some identity thieves pose as employers and post fake job announcements; some respond to job hunters and ask for more information, perhaps for a background check. Of course, job-hunting sites are very popular and useful. Now that identity thieves misuse them, people must adapt and be more cautious. That means omitting sensitive data from a posted résumé, not providing sensitive information until you have an actual interview, or finding other ways to determine that the potential employer is authentic. Job sites, once aware of the threat, began to offer services to keep sensitive information private.

Although we focus on criminal groups who use hacking and other technical means to commit identity theft, family members and acquaintances of the victim are responsible for a significant percentage of identity theft. And many identity theft cases result from lost or stolen wallets and checkbooks. We still must use care in protecting our own passwords, documents, Social Security numbers, and so on, in low-tech environments as well as in cyberspace.

5.3.2 Responses to Identity Theft

Authenticating websites

Email programs, Web browsers, search engines, and add-on software (some free) can alert users to likely fraud. Spammers and hackers fake the apparent return address on email, but some mail programs let users check the actual return address. (I find that email claiming to be from PayPal has come from hotmail.com, yahoo.com, Denmark, Germany, and a variety of other unlikely places.) Some mail programs will alert the user if the actual Web address that a link will take you to is different from the one displayed in the text of a message.

Whether someone reaches a website from a link in an email or by browsing or searching, various tools can help determine if the site is safe. Sometimes fake websites are easy to spot because of poor grammar and generally low quality. Software can determine the geographic location of a site reasonably well. If it claims to be a U.S. bank but is located in Romania, it is wise to leave.

Some browsers (and add-on software used with browsers and search engines) will flag websites they consider safe or show alerts for sites known to collect and misuse personal

Tactics and countertactics in credit card and debit card fraud

Credit card fraud began with simple crimes, say, an individual on a shopping spree with a lost or stolen card. At first, the main method was to steal and use (or sell) the actual credit card. Both well-organized theft rings and individual purse snatchers stole credit cards. (They still do.) Several dozen people were convicted in one case where airline employees stole new cards from the mail transported on the airline's airplanes. Charges on the stolen cards ran to an estimated $7.5 million.[32]

Procedural changes helped protect against theft of new cards from the mail. To verify that the legitimate owner received the card, credit card issuers require the customer to call in and provide identifying information to activate a card. This procedure is only as good as the security of the identifying information. At first, credit card companies commonly used the person's Social Security number and mother's maiden name. Several Social Security Administration employees provided the Social Security numbers and mothers' maiden names of thousands of people to a credit card fraud ring so that they could activate stolen cards, according to federal prosecutors.[33] Now credit card companies use caller ID to verify that the authorization call comes from the customer's telephone. Similarly, if you send a change-of-address notification to your credit card company, the company will probably send a confirmation to both your old and new addresses. Why? Thieves who plan to use a stolen credit card number for a long time do not want the owner of the card to see fraudulent charges on the bill and close the account. Thus, they send a change-of-address notice (using a fake address for the new one). A confirmation letter sent to the old address alerts the real card owner.

E-commerce made it easier both to steal card numbers (not cards) and to use the numbers without the physical cards. When retail sales began on the Web, technically trained thieves used software to intercept credit card numbers in transmission from a personal computer to a website. Encryption and secure servers solved much of that problem; without such security, e-commerce could not have thrived.

A simple change in a business policy helped to thwart thieves who searched the trash near stores or banks for receipts with card numbers. Large stores and banks began printing only the last four digits on the receipts. Later, a law required this practice.

Thieves surreptitiously install recording devices, called *skimmers*, inside the card readers in stores, gas stations, and restaurants. They collect debit card numbers and PINs, make counterfeit cards, and raid people's bank accounts through ATM machines.

Credit card companies run sophisticated artificial intelligence software to detect unusual spending activity. When the system finds something suspicious, a merchant can ask a customer for additional identification or the credit card company can call a cardholder to verify purchases. The vast amount of data that businesses store about our purchases and other activities—the data that can threaten privacy—enables the credit card company software to make fairly accurate conclusions about whether a charge on our credit card is likely to be fraudulent.

Services like PayPal provide a trusted third party to increase confidence (and convenience) in online commerce and reduce credit fraud. A customer can buy from strangers online without giving them a credit card number. PayPal handles the payment for a small fee. PayPal and other companies that provide online payment services initially lost millions of dollars to fraud. Gradually, PayPal developed clever solutions and sophisticated security expertise.