**About Cyber Crime**

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.

Cybercrime may also be referred to as computer crime.

Cybercrimealso called computer crime, the use of a [computer](https://www.britannica.com/technology/computer) as an instrument to further illegal ends, such as committing [fraud](https://www.britannica.com/topic/fraud), trafficking in child pornography and [intellectual](https://www.merriam-webster.com/dictionary/intellectual) property, [stealing identities](https://www.britannica.com/topic/identity-theft), or violating privacy. Cybercrime, especially through the [Internet](https://www.britannica.com/technology/Internet), has grown in importance as the computer has become central to commerce, entertainment, and government.

Because of the early and widespread adoption of computers and the Internet in the United States, most of the earliest victims and villains of cybercrime were Americans. By the 21st century, though, hardly a hamlet remained anywhere in the world that had not been touched by cybercrime of one sort or another.

**Defining Cybercrime**

New technologies create new criminal opportunities but few new types of [crime](https://www.britannica.com/topic/crime-civil-law). What distinguishes cybercrime from traditional criminal activity? Obviously, one difference is the use of the [digital computer](https://www.britannica.com/technology/digital-computer), but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Criminals do not need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone’s privacy. All those activities existed before the “cyber” prefix became [ubiquitous](https://www.merriam-webster.com/dictionary/ubiquitous). Cybercrime, especially involving the Internet, represents an extension of existing criminal behaviour alongside some novel illegal activities.

Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age our virtual identities are essential elements of everyday life: we are a bundle of numbers and identifiers in multiple computer [databases](https://www.britannica.com/technology/database) owned by governments and corporations. Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity.

An important aspect of cybercrime is its nonlocal character: actions can occur in jurisdictions separated by vast distances. This poses severe problems for law enforcement since previously local or even national crimes now require international cooperation. For example, if a person accesses child pornography located on a computer in a country that does not ban child pornography, is that individual committing a crime in a nation where such materials are illegal? Where exactly does cybercrime take place? Cyberspace is simply a richer version of the space where a telephone conversation takes place, somewhere between the two people having the conversation. As a planet-spanning network, the Internet offers criminals multiple hiding places in the real world as well as in the network itself. However, just as individuals walking on the ground leave marks that a skilled tracker can follow, cybercriminals leave clues as to their identity and location, despite their best efforts to cover their tracks. In order to follow such clues across national boundaries, though, international cybercrime treaties must be ratified.

In 1996 the [Council of Europe](https://www.britannica.com/topic/Council-of-Europe), together with government representatives from the United States, Canada, and Japan, drafted a preliminary international treaty covering computer crime. Around the world, civil libertarian groups immediately protested provisions in the treaty requiring [Internet service providers](https://www.britannica.com/topic/Internet-service-provider) (ISPs) to store information on their customers’ transactions and to turn this information over on demand. Work on the treaty proceeded nevertheless, and on November 23, 2001, the Council of Europe Convention on Cybercrime was signed by 30 states. The convention came into effect in 2004. Additional [protocols](https://www.merriam-webster.com/dictionary/protocols), covering [terrorist](https://www.britannica.com/topic/terrorism) activities and [racist](https://www.britannica.com/topic/racism) and xenophobic cybercrimes, were proposed in 2002 and came into effect in 2006. In addition, various national laws, such as the [USA PATRIOT Act](https://www.britannica.com/topic/USA-PATRIOT-Act) of 2001, have expanded law enforcement’s power to monitor and protect [computer networks](https://www.britannica.com/technology/computer-network).

**Types Of Cybercrime**

Cybercrime ranges across a spectrum of activities. At one end are crimes that involve fundamental [breaches](https://www.merriam-webster.com/dictionary/breaches) of personal or corporate privacy, such as assaults on the [integrity](https://www.merriam-webster.com/dictionary/integrity) of information held in digital depositories and the use of illegally obtained digital information to [blackmail](https://www.britannica.com/topic/extortion) a firm or individual. Also at this end of the spectrum is the growing crime of identity theft. Midway along the spectrum lie transaction-based crimes such as [fraud](https://www.britannica.com/topic/fraud), trafficking in child [pornography](https://www.britannica.com/topic/pornography), digital piracy, [money laundering](https://www.britannica.com/topic/money-laundering), and [counterfeiting](https://www.britannica.com/topic/counterfeiting). These are specific crimes with specific victims, but the criminal hides in the relative anonymity provided by the [Internet](https://www.britannica.com/technology/Internet). Another part of this type of crime involves individuals within corporations or government [bureaucracies](https://www.merriam-webster.com/dictionary/bureaucracies) deliberately altering data for either profit or political objectives. At the other end of the spectrum are those crimes that involve attempts to disrupt the actual workings of the Internet. These range from [spam](https://www.britannica.com/topic/spam), hacking, and [denial of service attacks](https://www.britannica.com/topic/denial-of-service-attack) against specific sites to acts of cyber terrorism—that is, the use of the Internet to cause public disturbances and even death. Cyber terrorism focuses upon the use of the Internet by non state actors to affect a nation’s economic and technological [infrastructure](https://www.merriam-webster.com/dictionary/infrastructure). Since the [September 11 attacks](https://www.britannica.com/event/September-11-attacks) of 2001, public awareness of the threat of cyber terrorism has grown dramatically.

**Identity theft and invasion of privacy**

Cybercrime affects both a virtual and a real body, but the effects upon each are different. This phenomenon is clearest in the case of identity theft. In the United States, for example, individuals do not have an official identity card but a Social Security number that has long served as a de facto identification number. Taxes are collected on the basis of each citizen’s Social Security number, and many private institutions use the number to keep track of their employees, students, and patients. Access to an individual’s Social Security number affords the opportunity to gather all the documents related to that person’s citizenship—i.e., to steal his identity. Even stolen [credit card](https://www.britannica.com/topic/credit-card) information can be used to reconstruct an individual’s identity. When criminals steal a firm’s credit card records, they produce two distinct effects. First, they make off with digital information about individuals that is useful in many ways. For example, they might use the credit card information to run up huge bills, forcing the credit card firms to suffer large losses, or they might sell the information to others who can use it in a similar fashion. Second, they might use individual credit card names and numbers to create new identities for other criminals. For example, a criminal might contact the issuing bank of a stolen credit card and change the mailing address on the account. Next, the criminal may get a passport or driver’s license with his own picture but with the victim’s name. With a driver’s license, the criminal can easily acquire a new Social Security card; it is then possible to open bank accounts and receive loans—all with the victim’s credit record and background. The original cardholder might remain unaware of this until the debt is so great that the bank contacts the account holder. Only then does the identity theft become visible. Although identity theft takes places in many countries, researchers and law-enforcement officials are plagued by a lack of information and statistics about the crime worldwide. Cybercrime is clearly, however, an international problem.

In 2015 the U.S. Bureau of [Justice](https://www.merriam-webster.com/dictionary/Justice) Statistics (BJS) released a report on identity theft; in the previous year almost 1.1 million [Americans](https://www.britannica.com/place/United-States) had their identities fraudulently used to open bank, credit card, or utility accounts. The report also stated that another 16.4 million Americans were victimized by account [theft](https://www.britannica.com/topic/theft), such as use of stolen credit cards and automatic teller machine (ATM) cards. The BJS report showed that while the total number of identity theft victims in the United States had grown by about 1 million since 2012, the total loss incurred by individuals had declined since 2012 by about $10 billion to $15.4 billion. Most of that decline was from a sharp drop in the number of people losing more than $2,000. Most identity theft involved small sums, with losses less than $300 accounting for 54 percent of the total.

**Internet fraud**

Schemes to defraud consumers abound on the Internet. Among the most famous is the Nigerian, or “419,” scam; the number is a reference to the section of Nigerian law that the scam violates. Although this con has been used with both [fax](https://www.britannica.com/technology/fax) and traditional mail, it has been given new life by the [Internet](https://www.britannica.com/technology/Internet). In the scheme, an individual receives an [e-mail](https://www.britannica.com/technology/e-mail) asserting that the sender requires help in transferring a large sum of money out of Nigeria or another distant country. Usually, this money is in the form of an asset that is going to be sold, such as [oil](https://www.britannica.com/topic/oil-chemical-compound), or a large amount of cash that requires “laundering” to conceal its source; the variations are endless, and new specifics are constantly being developed. The message asks the recipient to cover some cost of moving the funds out of the country in return for receiving a much larger sum of money in the near future. Should the recipient respond with a check or [money order](https://www.britannica.com/topic/money-order), he is told that complications have developed; more money is required. Over time, victims can lose thousands of dollars that are utterly unrecoverable.

In 2002 the newly formed U.S. Internet Crime Complaint Center (IC3) reported that more than $54 million dollars had been lost through a variety of fraud schemes; this represented a threefold increase over estimated losses of $17 million in 2001. The annual losses grew in subsequent years, reaching $125 million in 2003, about $200 million in 2006, close to $250 million in 2008, and over $1 billion in 2015. In the United States the largest source of fraud is what IC3 calls “non-payment/non-delivery,” in which goods and services either are delivered but not paid for or are paid for but not delivered. Unlike identity theft, where the theft occurs without the victim’s knowledge, these more traditional forms of fraud occur in plain sight. The victim willingly provides private information that enables the crime; hence, these are transactional crimes. Few people would believe someone who walked up to them on the street and promised them easy riches; however, receiving an unsolicited e-mail or visiting a random Web page is sufficiently different that many people easily open their wallets. Despite a vast amount of consumer education, Internet fraud remains a growth industry for criminals and prosecutors. Europe and the United States are far from the only sites of cybercrime. [South Korea](https://www.britannica.com/place/South-Korea) is among the most wired countries in the world, and its cybercrime fraud statistics are growing at an alarming rate. [Japan](https://www.britannica.com/place/Japan) has also experienced a rapid growth in similar crimes.

**ATM Fraud**

Computers also make more [mundane](https://www.merriam-webster.com/dictionary/mundane) types of fraud possible. Take the automated teller machine (ATM) through which many people now get cash. In order to access an account, a user supplies a card and personal identification number (PIN). Criminals have developed means to intercept both the data on the card’s magnetic strip as well as the user’s PIN. In turn, the information is used to create fake cards that are then used to withdraw funds from the unsuspecting individual’s account. For example, in 2002 the New York Times reported that more than 21,000 American bank accounts had been skimmed by a single group engaged in acquiring ATM information illegally. A particularly effective form of fraud has involved the use of ATMs in shopping centres and convenience stores. These machines are free-standing and not physically part of a bank. Criminals can easily set up a machine that looks like a [legitimate](https://www.merriam-webster.com/dictionary/legitimate) machine; instead of dispensing money, however, the machine gathers information on users and only tells them that the machine is out of order after they have typed in their PINs. Given that ATMs are the preferred method for dispensing currency all over the world, ATM fraud has become an international problem.

## Wire fraud

The international nature of cybercrime is particularly evident with wire fraud. One of the largest and best-organized wire fraud schemes was orchestrated by Vladimir Levin, a Russian programmer with a computer software firm in [St. Petersburg](https://www.britannica.com/place/St-Petersburg-Russia). In 1994, with the aid of dozens of confederates, Levin began transferring some $10 million from subsidiaries of [Citibank, N.A.](https://www.britannica.com/topic/Citibank-NA), in Argentina and Indonesia to bank accounts in San Francisco, [Tel Aviv](https://www.britannica.com/place/Tel-Aviv-Yafo), Amsterdam, Germany, and Finland. According to Citibank, all but $400,000 was eventually recovered as Levin’s accomplices attempted to withdraw the funds. Levin himself was arrested in 1995 while in transit through London’s Heathrow Airport (at the time, Russia had no extradition treaty for cybercrime). In 1998 Levin was finally extradited to the United States, where he was sentenced to three years in jail and ordered to reimburse Citibank $240,015. Exactly how Levin obtained the necessary account names and passwords has never been disclosed, but no Citibank employee has ever been charged in connection with the case. Because a sense of security and privacy are paramount to financial institutions, the exact extent of wire fraud is difficult to [ascertain](https://www.merriam-webster.com/dictionary/ascertain). In the early 21st century, wire fraud remained a worldwide problem.

**File sharing and piracy**

Through the 1990s, sales of [compact discs](https://www.britannica.com/technology/compact-disc) (CDs) were the major source of revenue for recording companies. Although piracy—that is, the illegal duplication of [copyrighted](https://www.britannica.com/topic/copyright) materials—had always been a problem, especially in the Far East, the proliferation on college campuses of inexpensive personal computers capable of capturing music off CDs and sharing them over high-speed (“broadband”) Internet connections became the recording industry’s greatest nightmare. In the United States, the recording industry, represented by the [Recording Industry Association of America](https://www.britannica.com/topic/Recording-Industry-Association-of-America) (RIAA), attacked a single file-sharing service, [Napster](https://www.britannica.com/topic/Napster), which from 1999 to 2001 allowed users across the Internet access to music files, stored in the [data-compression](https://www.britannica.com/technology/data-compression) format known as [MP3](https://www.britannica.com/technology/MP3), on other users’ computers by way of Napster’s central computer. According to the RIAA, Napster users regularly violated the copyright of recording artists, and the service had to stop. For users, the issues were not so clear-cut. At the core of the Napster case was the issue of [fair use](https://www.britannica.com/topic/fair-use-doctrine). Individuals who had purchased a CD were clearly allowed to listen to the music, whether in their home stereo, automobile sound system, or personal computer. What they did not have the right to do, argued the RIAA, was to make the CD available to thousands of others who could make a perfect digital copy of the music and create their own CDs. Users rejoined that sharing their files was a fair use of copyrighted material for which they had paid a fair price. In the end, the RIAA argued that a whole new class of cybercriminal had been born—the digital pirate—that included just about anyone who had ever shared or downloaded an MP3 file. Although the RIAA successfully shuttered Napster, a new type of file-sharing service, known as [peer-to-peer](https://www.britannica.com/technology/P2P) (P2P) networks, sprang up. These decentralized systems do not rely on a central [facilitating](https://www.merriam-webster.com/dictionary/facilitating) computer; instead, they consist of millions of users who voluntarily open their own computers to others for file sharing.

The RIAA continued to battle these file-sharing networks, demanding that ISPs turn over records of their customers who move large quantities of data over their networks, but the effects were minimal. The RIAA’s other tactic has been to push for the development of technologies to enforce the digital rights of copyright holders. So-called [digital rights management (DRM) technology](https://www.britannica.com/topic/digital-rights-management) is an attempt to forestall piracy through technologies that will not allow consumers to share files or possess “too many” copies of a copyrighted work.

At the start of the 21st century, copyright owners began accommodating themselves with the idea of commercial digital distribution. Examples include the online sales by the iTunes Store (run by [Apple Inc.](https://www.britannica.com/topic/Apple-Inc)) and [Amazon.com](https://www.britannica.com/topic/Amazoncom) of music, television shows, and movies in downloadable formats, with and without DRM restrictions. In addition, several cable and satellite television providers, many [electronic game](https://www.britannica.com/topic/electronic-game) systems ([Sony Corporation](https://www.britannica.com/topic/Sony)’s [PlayStation 3](https://www.britannica.com/topic/PlayStation) and [Microsoft Corporation](https://www.britannica.com/topic/Microsoft-Corporation)’s [Xbox 360](https://www.britannica.com/topic/Xbox)), and streaming services like [Netflix](https://www.britannica.com/topic/Netflix-Inc) developed “[video-on-demand](https://www.britannica.com/technology/video-on-demand)” services that allow customers to download movies and shows for immediate (streaming) or later playback.

File sharing brought about a fundamental reconstruction of the relationship between producers, distributors, and consumers of artistic material. In America, CD sales dropped from a high of nearly 800 million albums in 2000 to less than 150 million albums in 2014. Although the music industry sold more albums digitally than it had CDs at its peak, revenue declined by more than half since 2000. As broadband Internet connections proliferate, the motion-picture industry faces a similar problem, although the digital videodisc ([DVD](https://www.britannica.com/topic/DVD)) came to market with encryption and various built-in attempts to avoid the problems of a video Napster. However, sites such as [The Pirate Bay](https://www.britannica.com/topic/The-Pirate-Bay) emerged that specialized in sharing such large files as those of movies and [electronic games](https://www.britannica.com/topic/electronic-game).

**Counterfeiting and forgery**

File sharing of intellectual property is only one aspect of the problem with copies. Another more mundane aspect lies in the ability of digital devices to render nearly perfect copies of material [artifacts](https://www.merriam-webster.com/dictionary/artifacts). Take the traditional crime of [counterfeiting](https://www.britannica.com/topic/counterfeiting). Until recently, creating passable currency required a significant amount of skill and access to technologies that individuals usually do not own, such as printing presses, engraving plates, and special inks. The advent of inexpensive, high-quality colour copiers and printers has brought counterfeiting to the masses. [Ink-jet printers](https://www.britannica.com/technology/ink-jet-printer) now account for a growing percentage of the counterfeit [currency](https://www.britannica.com/topic/currency)confiscated by the [U.S. Secret Service](https://www.britannica.com/topic/US-Secret-Service). In 1995 ink-jet currency accounted for 0.5 percent of counterfeit U.S. currency; in 1997 ink-jet printers produced 19 percent of the illegal cash. By 2014 almost 60 percent of the counterfeit money recovered in the U.S. came from ink-jet printers. The widespread development and use of computer technology prompted the U.S. Treasury to redesign U.S. paper currency to include a variety of anticounterfeiting technologies. The [European Union](https://www.britannica.com/topic/European-Union)currency, or [euro](https://www.britannica.com/topic/euro), had security designed into it from the start. Special features, such as embossed foil holograms and special ribbons and paper, were designed to make counterfeiting difficult. Indeed, the switch to the euro presented an unprecedented opportunity for counterfeiters of preexisting national currencies. The great fear was that counterfeit currency would be laundered into legal euros. Fortunately, it was not the problem that some believed it would be.

Nor is currency the only document being copied. Immigration documents are among the most valuable, and they are much easier to duplicate than currency. In the wake of the [September 11 attacks](https://www.britannica.com/event/September-11-attacks), this problem came under increasing scrutiny in the United States. In particular, the U.S. General Accounting Office (GAO) issued several reports during the late 1990s and early 2000s concerning the extent of document fraud that had been missed by the [Immigration and Naturalization Service](https://www.britannica.com/topic/Immigration-and-Naturalization-Service) (INS). Finally, a 2002 report by the GAO reported that more than 90 percent of certain types of benefit claims were fraudulent and further stated that immigration fraud was “out of control.” Partially in response to these revelations, the INS was disbanded and its functions assumed by the newly [constituted](https://www.merriam-webster.com/dictionary/constituted) U.S. [Department of Homeland Security](https://www.britannica.com/topic/United-States-Department-of-Homeland-Security) in 2003.

**Child Pornography**

With the advent of almost every new media technology, [pornography](https://www.britannica.com/topic/pornography) has been its “killer app,” or the application that drove early deployment of technical [innovations](https://www.merriam-webster.com/dictionary/innovations) in search of profit. The Internet was no exception, but there is a criminal element to this business bonanza—child pornography, which is unrelated to the lucrative business of legal adult-oriented pornography. The possession of child pornography, defined here as images of children under age 18 engaged in sexual behavior, is illegal in the United States, the European Union, and many other countries, but it remains a problem that has no easy solution. The problem is [compounded](https://www.merriam-webster.com/dictionary/compounded) by the ability of “kiddie porn” Web sites to [disseminate](https://www.merriam-webster.com/dictionary/disseminate) their material from locations, such as states of the former [Soviet Union](https://www.britannica.com/place/Soviet-Union) as well as [Southeast Asia](https://www.britannica.com/place/Southeast-Asia), that lack cybercrime laws. Some law-enforcement organizations believe that child pornography represents a $3-billion-a-year industry and that more than 10,000 Internet locations provide access to these materials.

The Internet also provides [pedophiles](https://www.britannica.com/topic/pedophilia) with an unprecedented opportunity to commit criminal acts through the use of “[chat rooms](https://www.britannica.com/topic/chat-room)” to identify and lure victims. Here the virtual and the material worlds intersect in a particularly dangerous fashion. In many countries, state authorities now pose as children in chat rooms; despite the widespread knowledge of this practice, pedophiles continue to make contact with these “children” in order to meet them “off-line.” That such a meeting invites a high risk of immediate arrest does not seem to deter pedophiles. Interestingly enough, it is because the Internet allows individual privacy to be [breached](https://www.merriam-webster.com/dictionary/breached) that the authorities are able to capture pedophiles.

**Hacking**

While [breaching](https://www.merriam-webster.com/dictionary/breaching) privacy to detect cybercrime works well when the crimes involve the theft and misuse of information, ranging from credit card numbers and personal data to file sharing of various commodities—music, video, or child pornography—what of crimes that attempt to wreak havoc on the very workings of the machines that make up the network? The story of hacking actually goes back to the 1950s, when a group of phreaks (short for “phone freaks”) began to hijack portions of the world’s [telephone networks](https://www.britannica.com/technology/telecommunications-network), making unauthorized long-distance calls and setting up special “party lines” for fellow phreaks. With the proliferation of computer [bulletin board systems](https://www.britannica.com/technology/bulletin-board-system) (BBSs) in the late 1970s, the informal [phreaking](https://www.britannica.com/topic/phreaking)[culture](https://www.merriam-webster.com/dictionary/culture) began to coalesce into quasi-organized groups of individuals who graduated from the telephone network to “hacking” corporate and government [computer network](https://www.britannica.com/technology/computer-network) systems.

Although the term hacker predates computers and was used as early as the mid-1950s in connection with electronic hobbyists, the first recorded instance of its use in connection with computer programmers who were adept at writing, or “hacking,” computer code seems to have been in a 1963 article in a student newspaper at the [Massachusetts Institute of Technology](https://www.britannica.com/topic/Massachusetts-Institute-of-Technology) (MIT). After the first computer systems were linked to multiple users through telephone lines in the early 1960s, hacker came to refer to individuals who gained unauthorized access to computer networks, whether from another computer network or, as [personal computers](https://www.britannica.com/technology/personal-computer) became available, from their own computer systems. Although it is outside the scope of this article to discuss hacker culture, most hackers have not been criminals in the sense of being vandals or of seeking illicit financial rewards. Instead, most have been young people driven by intellectual curiosity; many of these people have gone on to become [computer security](https://www.britannica.com/technology/computer-security) architects. However, as some hackers sought notoriety among their peers, their exploits led to clear-cut crimes. In particular, hackers began breaking into computer systems and then bragging to one another about their exploits, sharing pilfered documents as trophies to prove their boasts. These exploits grew as hackers not only broke into but sometimes took control of government and corporate computer networks.

One such criminal was Kevin Mitnick, the first hacker to make the “most wanted list” of the U.S. [Federal Bureau of Investigation](https://www.britannica.com/topic/Federal-Bureau-of-Investigation) (FBI). He allegedly broke into the [North American Aerospace Defense Command](https://www.britannica.com/topic/North-American-Air-Defense-Command) (NORAD) computer in 1981, when he was 17 years old, a feat that brought to the fore the gravity of the threat posed by such security breaches. Concern with hacking contributed first to an overhaul of federal sentencing in the United States, with the 1984 [Comprehensive](https://www.merriam-webster.com/dictionary/Comprehensive) Crime Control Act and then with the Computer Fraud and Abuse Act of 1986.

The scale of hacking crimes is among the most difficult to assess because the victims often prefer not to report the crimes—sometimes out of embarrassment or fear of further security breaches. Officials estimate, however, that hacking costs the world economy billions of dollars annually. Hacking is not always an outside job—a related criminal endeavour involves individuals within corporations or government bureaucracies deliberately altering [database](https://www.britannica.com/technology/database) records for either profit or political objectives. The greatest losses stem from the theft of [proprietary](https://www.merriam-webster.com/dictionary/proprietary) information, sometimes followed up by the extortion of money from the original owner for the data’s return. In this sense, hacking is old-fashioned [industrial espionage](https://www.britannica.com/topic/industrial-espionage) by other means.

One of the largest known case of computer hacking was discovered in late March 2009. It involved government and private computers in at least 103 countries. The worldwide spy network known as GhostNet was discovered by researchers at the [University of Toronto](https://www.britannica.com/topic/University-of-Toronto), who had been asked by representatives of the [Dalai Lama](https://www.britannica.com/biography/Dalai-Lama-XIV) to investigate the exiled Tibetan leader’s computers for possible [malware](https://www.britannica.com/technology/malware). In addition to finding out that the [Dalai Lama’s](https://www.britannica.com/topic/Dalai-Lama) computers were compromised, the researchers discovered that GhostNet had infiltrated more than a thousand computers around the world. The highest concentration of compromised systems were within embassies and foreign affairs bureaus of or located in South Asian and Southeast Asian countries. Reportedly, the computers were infected by users who opened e-mail attachments or clicked on Web page links. Once infected with the GhostNet malware, the computers began “phishing” for files throughout the local network—even turning on cameras and video-recording devices for remote monitoring. Three control servers that ran the malware were located in [Hainan](https://www.britannica.com/place/Hainan), [Guangdong](https://www.britannica.com/place/Guangdong), and [Sichuan](https://www.britannica.com/place/Sichuan) provinces in China, and a fourth server was located in California.

**Computer Viruses**

The deliberate release of damaging [computer viruses](https://www.britannica.com/technology/computer-virus) is yet another type of cybercrime. In fact, this was the crime of choice of the first person to be convicted in the United States under the Computer Fraud and Abuse Act of 1986. On November 2, 1988, a [computer science](https://www.britannica.com/topic/computer-science) student at [Cornell University](https://www.britannica.com/topic/Cornell-University) named Robert Morris released a software “[worm](https://www.britannica.com/technology/computer-worm)” onto the [Internet](https://www.britannica.com/technology/Internet) from MIT (as a guest on the campus, he hoped to remain anonymous). The worm was an experimental self-propagating and replicating [computer program](https://www.britannica.com/technology/computer-program) that took advantage of flaws in certain [e-mail](https://www.britannica.com/technology/e-mail) protocols. Due to a mistake in its programming, rather than just sending copies of itself to other computers, this software kept replicating itself on each infected system, filling all the available [computer memory](https://www.britannica.com/technology/computer-memory). Before a fix was found, the worm had brought some 6,000 computers (one-tenth of the Internet) to a halt. Although Morris’s worm cost time and millions of dollars to fix, the event had few commercial consequences, for the Internet had not yet become a fixture of economic affairs. That Morris’s father was the head of computer security for the U.S. [National Security Agency](https://www.britannica.com/topic/National-Security-Agency) led the press to treat the event more as a high-tech Oedipal drama than as a foreshadowing of things to come. Since then, ever more harmful viruses have been cooked up by anarchists and misfits from locations as [diverse](https://www.merriam-webster.com/dictionary/diverse) as the United States, Bulgaria, Pakistan, and the Philippines.

Compare the Morris worm with the events of the week of February 7, 2000, when “mafia boy,” a 15-year-old Canadian hacker, orchestrated a series of [denial of service attacks](https://www.britannica.com/topic/denial-of-service-attack) (DoS) against several [e-commerce](https://www.britannica.com/topic/e-commerce) sites, including [Amazon.com](https://www.britannica.com/topic/Amazoncom) and [eBay.com](https://www.britannica.com/topic/eBay). These attacks used computers at multiple locations to overwhelm the vendors’ computers and shut down their [World Wide Web](https://www.britannica.com/topic/World-Wide-Web) (WWW) sites to legitimate commercial traffic. The attacks crippled Internet commerce, with the FBI estimating that the affected sites suffered $1.7 billion in damages. In 1988 the Internet played a role only in the lives of researchers and academics; by 2000 it had become essential to the workings of the U.S. government and economy. Cybercrime had moved from being an issue of individual wrongdoing to being a matter of national security.

Distributed DoS attacks are a special kind of hacking. A criminal salts an array of computers with computer programs that can be triggered by an external computer user. These programs are known as [Trojan horses](https://www.britannica.com/topic/Trojan-horse) since they enter the unknowing users’ computers as something [benign](https://www.merriam-webster.com/dictionary/benign), such as a photo or document attached to an e-mail. At a predesignated time, this Trojan horse program begins to send messages to a predetermined site. If enough computers have been compromised, it is likely that the selected site can be tied up so effectively that little if any legitimate traffic can reach it. One important insight offered by these events has been that much software is insecure, making it easy for even an unskilled hacker to compromise a vast number of machines. Although software companies regularly offer patches to fix software vulnerabilities, not all users [implement](https://www.merriam-webster.com/dictionary/implement) the updates, and their computers remain [vulnerable](https://www.merriam-webster.com/dictionary/vulnerable) to criminals wanting to launch DoS attacks. In 2003 the Internet service provider PSINet Europe connected an unprotected server to the Internet. Within 24 hours the server had been attacked 467 times, and after three weeks more than 600 attacks had been recorded. Only vigorous security regimes can protect against such an [environment](https://www.merriam-webster.com/dictionary/environment). Despite the claims about the pacific nature of the Internet, it is best to think of it as a modern example of the Wild West of American lore—with the sheriff far away.

**Spam, steganography, and e-mail hacking**

E-mail has spawned one of the most significant forms of cybercrime—[spam](https://www.britannica.com/topic/spam), or unsolicited advertisements for products and services, which experts estimate to [comprise](https://www.merriam-webster.com/dictionary/comprise) roughly 50 percent of the e-mail circulating on the Internet. Spam is a crime against all users of the Internet since it wastes both the storage and network capacities of ISPs, as well as often simply being offensive. Yet, despite various attempts to legislate it out of existence, it remains unclear how spam can be eliminated without violating the [freedom of speech](https://www.britannica.com/topic/freedom-of-speech) in a liberal democratic polity. Unlike junk mail, which has a postage cost associated with it, spam is nearly free for perpetrators—it typically costs the same to send 10 messages as it does to send 10 million.

One of the most significant problems in shutting down spammers involves their use of other individuals’ personal computers. Typically, numerous machines connected to the Internet are first infected with a virus or Trojan horse that gives the spammer secret control. Such machines are known as [zombie computers](https://www.britannica.com/technology/zombie-computer), and networks of them, often involving thousands of infected computers, can be activated to flood the Internet with spam or to institute DoS attacks. While the former may be almost benign, including solicitations to purchase legitimate goods, DoS attacks have been [deployed](https://www.merriam-webster.com/dictionary/deployed) in efforts to blackmail Web sites by threatening to shut them down. Cyberexperts estimate that the United States accounts for about one-fourth of the 4–8 million zombie computers in the world and is the origin of nearly one-third of all spam.

E-mail also serves as an instrument for both traditional criminals and terrorists. While libertarians laud the use of [cryptography](https://www.britannica.com/topic/cryptography) to ensure privacy in communications, criminals and terrorists may also use cryptographic means to conceal their plans. Law-enforcement officials report that some terrorist groups embed instructions and information in images via a process known as steganography, a sophisticated method of hiding information in plain sight. Even recognizing that something is concealed in this fashion often requires considerable amounts of computing power; actually decoding the information is nearly impossible if one does not have the key to separate the hidden data.

In a type of scam called business e-mail compromise (BEC), an e-mail sent to a business appears to be from an executive at another company with which the business is working. In the e-mail, the “executive” asks for money to be transferred into a certain account. The FBI has estimated that BEC scams have cost American businesses about $750 million.

Sometimes e-mail that an organization would wish to keep secret is obtained and released. In 2014 hackers calling themselves “Guardians of Peace” released e-mail from executives at the [motion picture](https://www.britannica.com/art/motion-picture) company Sony Pictures Entertainment, as well as other [confidential](https://www.merriam-webster.com/dictionary/confidential) company information. The hackers demanded that Sony Pictures not release The Interview, a comedy about a CIA plot to assassinate North Korean leader [Kim Jong-Eun](https://www.britannica.com/biography/Kim-Jong-Eun), and threatened to attack theatres that showed the movie. After American movie theatre chains canceled screenings, Sony released the movie online and in limited theatrical release. E-mail hacking has even affected politics. In 2016, e-mail at the Democratic National Committee (DNC) was obtained by hackers believed to be in Russia. Just before the Democratic National Convention, the media organization WikiLeaks released the e-mail, which showed a marked preference of DNC officials for the presidential campaign of [Hillary Clinton](https://www.britannica.com/biography/Hillary-Rodham-Clinton) over that of her challenger [Bernie Sanders](https://www.britannica.com/biography/Bernie-Sanders). DNC chairperson Debbie Wasserman Schultz resigned, and some American commentators speculated that the release of the e-mail showed the preference of the Russian government for Republican nominee [Donald Trump](https://www.britannica.com/biography/Donald-Trump).

**Sabotage**

Another type of hacking involves the [hijacking](https://www.britannica.com/topic/hijacking) of a government or corporation [Web site](https://www.britannica.com/topic/Web-site). Sometimes these crimes have been committed in protest over the incarceration of other hackers; in 1996 the Web site of the U.S. [Central Intelligence Agency](https://www.britannica.com/topic/Central-Intelligence-Agency) (CIA) was altered by Swedish hackers to gain international support for their protest of the Swedish government’s prosecution of local hackers, and in 1998 the New York Times’s Web site was hacked by supporters of the incarcerated hacker Kevin Mitnick. Still other hackers have used their skills to engage in political protests: in 1998 a group calling itself the Legion of the Underground declared “cyberwar” on China and Iraq in protest of [alleged](https://www.merriam-webster.com/dictionary/alleged) [human rights](https://www.britannica.com/topic/human-rights) abuses and a program to build weapons of mass destruction, respectively. In 2007, Estonian government Web sites, as well as those for banks and the media, were attacked. Russian hackers were suspected because [Estonia](https://www.britannica.com/place/Estonia) was then in a dispute with Russia over the removal of a Soviet war memorial in Tallinn.

Sometimes a user’s or organization’s computer system is attacked and encrypted until a ransom is paid. The software used in such attacks has been dubbed ransom ware. The ransom usually demanded is payment in a form of virtual currency, such as [Bitcoin](https://www.britannica.com/topic/Bitcoin). When data are of vital importance to an organization, sometimes the ransom is paid. In 2016 several American hospitals were hit with ransom ware attacks, and one hospital paid over $17,000 for its systems to be released.

Defacing Web sites is a minor matter, though, when compared with the specter of cyber terrorists using the Internet to attack the infrastructure of a nation, by rerouting airline traffic, contaminating the [water supply](https://www.britannica.com/science/water-supply), or disabling nuclear plant safeguards. One consequence of the [September 11 attacks](https://www.britannica.com/event/September-11-attacks) on [New York City](https://www.britannica.com/place/New-York-City) was the destruction of a major telephone and Internet switching centre. Lower Manhattan was effectively cut off from the rest of the world, save for radios and cellular telephones. Since that day, there has been no other attempt to destroy the infrastructure that produces what has been called that “consensual hallucination,” [cyberspace](https://www.britannica.com/topic/cyberspace). Large-scale [cyber war](https://www.britannica.com/topic/cyberwar) (or “information warfare”) has yet to take place, whether initiated by rogue states or terrorist organizations, although both writers and policy makers have imagined it in all too great detail.

In late March 2007 the Idaho National Laboratory released a video demonstrating what catastrophic damage could result from utility systems being compromised by hackers. Several utilities responded by giving the U.S. government permission to run an audit on their systems. In March 2009 the results began to leak out with a report in The Wall Street Journal. In particular, the report indicated that hackers had installed software in some computers that would have enabled them to disrupt electrical services. Homeland Security spokeswoman Amy Kudwa affirmed that no disruptions had occurred, though further audits of electric, water, sewage, and other utilities would continue.