**Cybercrime**

**Cybercrime, or computer crime, is crime that involves a** [**computer**](https://en.wikipedia.org/wiki/Computer) **and a** [**network**](https://en.wikipedia.org/wiki/Computer_network)**.**[**[1]**](https://en.wikipedia.org/wiki/Cybercrime#cite_note-moore-1) **The computer may have been used in the commission of a crime, or it may be the target.**[**[2]**](https://en.wikipedia.org/wiki/Cybercrime#cite_note-kruse-2) **Debarati Halder and K. Jaishankar define cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)".**[**[3]**](https://en.wikipedia.org/wiki/Cybercrime#cite_note-igiglobal.com-3) **Such crimes may threaten a nation's security and financial health.**[**[4]**](https://en.wikipedia.org/wiki/Cybercrime#cite_note-4) **Issues surrounding these types of crimes have become high-profile, particularly those surrounding** [**hacking**](https://en.wikipedia.org/wiki/Hacker_%28computer_security%29)**,** [**copyright infringement**](https://en.wikipedia.org/wiki/Copyright_infringement)**,** [**child pornography**](https://en.wikipedia.org/wiki/Child_pornography)**, and** [**child grooming**](https://en.wikipedia.org/wiki/Child_grooming)**. There are also problems of** [**privacy**](https://en.wikipedia.org/wiki/Privacy) **when** [**confidential**](https://en.wikipedia.org/wiki/Confidential) **information is intercepted or disclosed, lawfully or otherwise. Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones".**[**[3]**](https://en.wikipedia.org/wiki/Cybercrime#cite_note-igiglobal.com-3) **Internationally, both governmental and non-state actors engage in cybercrimes, including** [**espionage**](https://en.wikipedia.org/wiki/Espionage)**,** [**financial theft**](https://en.wikipedia.org/wiki/Theft)**, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as** [**cyberwarfare**](https://en.wikipedia.org/wiki/Cyberwarfare)**. The international legal system is attempting to hold actors accountable for their actions through the** [**International Criminal Court**](https://en.wikipedia.org/wiki/International_Criminal_Court)**.**[**[5]**](https://en.wikipedia.org/wiki/Cybercrime#cite_note-5)

**Classification**

**Computer crime encompasses a broad range of activities.**

**Fraud and financial crimes**

[**Computer fraud**](https://en.wikipedia.org/wiki/Computer_fraud) **is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. In this context, the fraud will result in obtaining a benefit by:**

* **Altering in an unauthorized way. This requires little technical expertise and is common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes;**
* **Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. This is difficult to detect;**
* **Altering or deleting stored data;**

**Other forms of fraud may be facilitated using computer systems, including** [**bank fraud**](https://en.wikipedia.org/wiki/Bank_fraud)**,** [**carding**](https://en.wikipedia.org/wiki/Carding_%28fraud%29)**,** [**identity theft**](https://en.wikipedia.org/wiki/Identity_theft)**,** [**extortion**](https://en.wikipedia.org/wiki/Extortion)**, and** [**theft of classified information**](https://en.wikipedia.org/wiki/Classified_information)**.**

**A variety of** [**internet scams**](https://en.wikipedia.org/wiki/Internet_fraud)**, many based on** [**phishing**](https://en.wikipedia.org/wiki/Phishing) **and** [**social engineering**](https://en.wikipedia.org/wiki/Social_engineering_%28security%29)**, target consumers and businesses.**

**Cyber terrorism**

**Government officials and** [**information technology**](https://en.wikipedia.org/wiki/Information_technology) **security specialists have documented a significant increase in Internet problems and server scans since early 2001. But there is a growing concern among federal officials[**[***who?***](https://en.wikipedia.org/wiki/Wikipedia:Manual_of_Style/Words_to_watch#Unsupported_attributions)**] that such intrusions are part of an organized effort by** [**cyberterrorists**](https://en.wikipedia.org/wiki/Cyberterrorist)**, foreign intelligence services, or other groups to map potential security holes in critical systems. A cyberterrorist is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching a computer-based attack against computers, networks, or the information stored on them.**

**Cyberterrorism in general, can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983). As such, a simple propaganda in the Internet, that there will be bomb attacks during the holidays can be considered cyberterrorism. There are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.[**[***citation needed***](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)**]**

**Cyberextortion**

**Cyberextortion occurs when a website, e-mail server, or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand money in return for promising to stop the attacks and to offer "protection". According to the Federal Bureau of Investigation, cyberextortionists are increasingly attacking corporate websites and networks, crippling their ability to operate and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. Perpetrators typically use a** [**distributed denial-of-service attack**](https://en.wikipedia.org/wiki/Distributed_denial-of-service_attack)**.**[**[11]**](https://en.wikipedia.org/wiki/Cybercrime#cite_note-11)

**Computer as a target**

**These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. As such, as technology evolves, so too does the nature of the crime. These crimes are relatively new, having been in existence for only as long as computers have—which explains how unprepared society and the world in general is towards combating these crimes. There are numerous crimes of this nature committed daily on the internet:**

**Crimes that primarily target computer networks or devices include:**

* [**Computer viruses**](https://en.wikipedia.org/wiki/Computer_viruses)
* [**Denial-of-service attacks**](https://en.wikipedia.org/wiki/Denial-of-service_attacks)
* [**Malware**](https://en.wikipedia.org/wiki/Malware) **(malicious code)**

**Computer as a tool**

**When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline world. Scams, theft, and the likes have existed even before the development in high-tech equipment. The same criminal has simply been given a tool which increases his potential pool of victims and makes him all the harder to trace and apprehend.**[**[14]**](https://en.wikipedia.org/wiki/Cybercrime#cite_note-14)

**Crimes that use computer networks or devices to advance other ends include:**

* [**Fraud**](https://en.wikipedia.org/wiki/Fraud) **and** [**identity theft**](https://en.wikipedia.org/wiki/Identity_theft) **(although this increasingly uses malware, hacking and/or phishing, making it an example of both "computer as target" and "computer as tool" crime)**
* [**Information warfare**](https://en.wikipedia.org/wiki/Information_warfare)
* [**Phishing scams**](https://en.wikipedia.org/wiki/Phishing)
* [**Spam**](https://en.wikipedia.org/wiki/E-mail_spam)
* **Propagation of illegal obscene or offensive content, including harassment and threats**

**Obscene or offensive content**

**The content of websites and other electronic communications may be distasteful,** [**obscene**](https://en.wikipedia.org/wiki/Obscene) **or offensive for a variety of reasons. In some instances these communications may be legal.**

**The extent to which these communications are unlawful varies greatly between countries, and even within nations. It is a sensitive area in which the courts can become involved in arbitrating between groups with strong beliefs.**

|  |  |
| --- | --- |
| **Combating computer crime** |  |

**Diffusion of cybercrime**

**The broad diffusion of cybercriminal activities is an issue in computer crimes detection and prosecution. According to Jean-Loup Richet (Research Fellow at ESSEC ISIS), technical expertise and accessibility no longer act as barriers to entry into cybercrime.**[**[32]**](https://en.wikipedia.org/wiki/Cybercrime#cite_note-32) **Indeed, hacking is much less complex than it was a few years ago, as hacking communities have greatly diffused their knowledge through the Internet. Blogs and communities have hugely contributed to information sharing: beginners could benefit from older hackers' knowledge and advice. Furthermore, Hacking is cheaper than ever: before the** [**cloud computing**](https://en.wikipedia.org/wiki/Cloud_computing) **era, in order to spam or scam one needed a dedicated server, skills in server management, network configuration and maintenance, knowledge of Internet service provider standards, etc. By comparison, a mail** [**software-as-a-service**](https://en.wikipedia.org/wiki/Software-as-a-service) **is a scalable, inexpensive, bulk, and transactional e-mail-sending service for marketing purposes and could be easily set up for** [**spam**](https://en.wikipedia.org/wiki/Email_spam)**.**[**[33]**](https://en.wikipedia.org/wiki/Cybercrime#cite_note-33) **Jean-Loup Richet explains that cloud computing could be helpful for a cybercriminal as a way to leverage his attack – brute-forcing a password, improve the reach of a** [**botnet**](https://en.wikipedia.org/wiki/Botnet)**, or facilitating a spamming campaign.**[**[34]**](https://en.wikipedia.org/wiki/Cybercrime#cite_note-34)

**Investigation**

**A computer can be a source of** [**evidence**](https://en.wikipedia.org/wiki/Evidence) **(see** [**digital forensics**](https://en.wikipedia.org/wiki/Digital_forensics)**). Even where a computer is not directly used for criminal purposes, it may contain records of value to criminal investigators in the form of a** [**logfile**](https://en.wikipedia.org/wiki/Logfile)**. In most countries[**[***citation needed***](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)**]** [**Internet Service Providers**](https://en.wikipedia.org/wiki/Internet_Service_Providers) **are required, by law, to keep their logfiles for a predetermined amount of time. For example; a European wide** [**Data Retention Directive**](https://en.wikipedia.org/wiki/Data_Retention_Directive) **(applicable to all** [**EU**](https://en.wikipedia.org/wiki/European_Union)[**member states**](https://en.wikipedia.org/wiki/Member_states)**) states that all** [**E-mail**](https://en.wikipedia.org/wiki/E-mail) **traffic should be retained for a minimum of 12 months.**

**Legislation**

**Due to easily exploitable laws, cybercriminals use developing countries in order to evade detection and prosecution from law enforcement. In developing countries, such as the Philippines, laws against cybercrime are weak or sometimes nonexistent. These weak laws allow cybercriminals to strike from international borders and remain undetected. Even when identified, these criminals avoid being punished or extradited to a country, such as the United States, that has developed laws that allow for prosecution. While this proves difficult in some cases, agencies, such as the FBI, have used deception and subterfuge to catch criminals. For example, two Russian hackers had been evading the FBI for some time. The FBI set up a fake computing company based in Seattle, Washington. They proceeded to lure the two Russian men into the United States by offering them work with this company. Upon completion of the interview, the suspects were arrested outside of the building. Clever tricks like this are sometimes a necessary part of catching cybercriminals when weak legislation makes it impossible otherwise.**[**[35]**](https://en.wikipedia.org/wiki/Cybercrime#cite_note-35)

**President Barack Obama released in an executive order in April 2015 to combat cybercrime. The executive order allows the United States to freeze assets of convicted cybercriminals and block their economic activity within the United States. This is some of the first solid legislation that combats cybercrime in this way.**[**[36]**](https://en.wikipedia.org/wiki/Cybercrime#cite_note-36)

**The European Union adopted** [**directive 2013/40/EU**](https://en.wikipedia.org/w/index.php?title=Directive_2013/40/EU&action=edit&redlink=1)**. All offences of the directive, and other definitions and procedural institutions are also in the** [**Council of Europe**](https://en.wikipedia.org/wiki/Council_of_Europe)**'s** [**Convention on Cybercrime**](https://en.wikipedia.org/wiki/Convention_on_Cybercrime).[[37]](https://en.wikipedia.org/wiki/Cybercrime#cite_note-37)

**Penalties**

**Penalties for computer related crimes in New York State can range from a fine and a short period of jail time for a Class A misdemeanor such as unauthorized use of a computer up to computer tampering in the first degree which is a Class C felony and can carry 3 to 15 years in prison.[**[***citation needed***](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)**]**

**However, some** [**hackers**](https://en.wikipedia.org/wiki/Hacker_%28computer_security%29) **have been hired as** [**information security**](https://en.wikipedia.org/wiki/Information_security) **experts by private companies due to their inside knowledge of computer crime, a phenomenon which theoretically could create** [**perverse incentives**](https://en.wikipedia.org/wiki/Moral_hazard)**. A possible counter to this is for courts to ban convicted hackers from using the Internet or computers, even after they have been released from prison – though as computers and the Internet become more and more central to everyday life, this type of punishment may be viewed as more and more harsh and draconian. However, nuanced approaches have been developed that manage cyberoffender behavior without resorting to total computer and/or Internet bans.**[**[38]**](https://en.wikipedia.org/wiki/Cybercrime#cite_note-38) **These approaches involve restricting individuals to specific devices which are subject to computer monitoring and/or computer searches by probation and/or parole officers.**[**[39]**](https://en.wikipedia.org/wiki/Cybercrime#cite_note-39)

**Awareness**

**As technology advances and more people rely on the internet to store sensitive information such as banking or credit card information, criminals are going to attempt to steal that information. Cyber-crime is becoming more of a threat to people across the world. Raising awareness about how information is being protected and the tactics criminals use to steal that information is important in today's world. According to the FBI's Internet Crime Complaint Center in 2014 there were 269,422 complaints filed. With all the claims combined there was a reported total loss of $800,492,073. But yet cyber-crime doesn't seem to be on the average person's radar. There are 1.5 million cyber-attacks annually, that means that there are over 4,000 attacks a day, 170 attacks every hour, or nearly three attacks every minute. Anybody who uses the internet for any reason can be a victim, which is why it is important to be aware of how one is being protected while online.**