Contents

Cybercrime

Cybercrime

Cybercrime encompasses a wide range of criminal activities that are carried out using *digital devices* and/or *networks*. It has been variously defined as "a crime committed on a computer network, especially the *Internet*"; Cybercriminals may exploit vulnerabilities in computer systems and networks to gain unauthorized access, steal sensitive information, disrupt services, and cause financial or reputational harm to individuals, organizations, and governments.[1]

In 2000, the tenth *United Nations Congress on the Prevention of Crime and the Treatment of Offenders* classified cyber crimes into five categories: unauthorized access, damage to computer data or programs, sabotage to hinder the functioning of a computer system or network, unauthorized interception of data within a system or network, and computer espionage.[1]

Internationally, both state and non-state actors engage in cybercrimes, including *espionage*, financial *theft*, and other cross-border crimes. Cybercrimes crossing international borders and involving the actions of at least one nation-state are sometimes referred to as *cyberwarfare*. *Warren Buffett* has stated that cybercrime is the "number one problem with mankind",[2] and that it "poses real risks to humanity".[3]

The *World Economic Forum's* (WEF) 2020 *Global Risks Report* highlighted that organized cybercrime groups are joining forces to commit criminal activities online, while estimating the likelihood of their detection and prosecution to be less than 1 percent in the US.[4] There are also many *privacy* concerns surrounding cybercrime when confidential information is intercepted or disclosed, legally or otherwise.

The World Economic Forum's 2023 Global Risks Report ranked cybercrime as one of the top 10 risks facing the world today and for the next 10 years.[5] If viewed as a nation state, cybercrime would count as the third largest economy in the world.[6] In numbers, cybercrime is predicted to cause over 9 trillion US dollars in damages worldwide in 2024.[6]

Classification

Computer crime encompasses a broad range of activities, including computer fraud, financial crimes, scams, cybersex trafficking, and ad-fraud.[7][8]

A proposed taxonomy classifies cybercrime into two top-level groups: *pure-technology cybercrime* and *cyber-advanced crime*. Pure-technology cybercrime "targets or victimizes the computer technology ecosystem" to "disrupt the confidentiality, integrity, or availability of a computer-technology ecosystem", while cyber-advanced crime "uses computer

Cybercrime

technology to target or victimize natural persons, governments, business entities, or property" in order to "deprive, disrupt or damage entities or assets."[9]

Computer fraud

Main article: *Computer fraud*

Computer fraud is the act of using a computer to take or alter electronic data, or to gain unlawful access to a computer or system.[10][*failed verification*] Computer fraud that involves the use of the Internet is also called internet fraud. The legal definition of computer fraud varies by jurisdiction, but typically involves accessing a computer without permission or authorization.

Forms of computer fraud include hacking into computers to alter information, distributing malicious code such as computer worms or viruses, installing malware or spyware to steal data, phishing, and advance-fee scams.[11]

Other forms of fraud may be committed using computer systems, including bank fraud, carding, identity theft, extortion, and theft of classified information. These types of crimes often result in the loss of personal or financial information.

Digital arrest

Digital arrest is a form of online fraud where perpetrators impersonate law enforcement officials to deceive victims. This scam typically involves contacting individuals via phone, falsely claiming they are implicated in criminal activity related to a parcel containing illegal goods, drugs, counterfeit documents, or other contraband. In some variations, scammers target the victim's relatives or friends, falsely stating the victim is in custody due to criminal involvement or an accident. Victims are then coerced into remaining on camera and isolating themselves, while the fraudsters extract personal and financial information under the guise of an official investigation, ultimately transferring the victim's assets to money mule accounts.[12]

To detect and prevent the fraud, be wary of unsolicited calls from supposed law enforcement demanding immediate payment or personal information. Legitimate law enforcement agencies rarely conduct investigations in this manner. Verify the identity of the caller independently by contacting the relevant agency directly through official channels. Remember, the government agencies never put anyone under digital arrest, it's not permissible.[12]

Cybercrime

Fraud factories

Main article: *Fraud factory*

A fraud factory is a collection of large fraud organizations, usually involving cyber fraud and human trafficking operations.

IP address

An **Internet Protocol address** (**IP address**) is a numerical label such as *192.0.2.1* that is assigned to a device connected to a computer network that uses the Internet Protocol for communication.[1][2] IP addresses serve two main functions: network interface identification, and location addressing.

Internet Protocol version 4 (IPv4) was the first standalone specification for the IP address, and has been in use since 1983.[2] IPv4 addresses are defined as a 32-bit number, which became too small to provide enough addresses as the internet grew, leading to IPv4 address exhaustion over the 2010s. Its designated successor, IPv6, uses 128 bits for the IP address, giving it a larger address space.[3][4][5] Although IPv6 deployment has been ongoing since the mid-2000s, both IPv4 and IPv6 are still used side-by-side as of 2025.

IP addresses are usually displayed in a human-readable notation, but systems may use them in various different computer number formats. CIDR notation can also be used to designate how much of the address should be treated as a routing prefix. For example, *192.0.2.1/24* indicates that 24 significant bits of the address are the prefix, with the remaining 8 bits used for host addressing. This is equivalent to the historically used subnet mask (in this case, *255.255.255.0*).

The IP address space is managed globally by the Internet Assigned Numbers Authority (IANA) and the five regional Internet registries (RIRs). IANA assigns blocks of IP addresses to the RIRs, which are responsible for distributing them to local Internet registries in their region such as internet service providers (ISPs) and large institutions. Some addresses are reserved for private networks and are not globally unique.

Within a network, the network administrator assigns an IP address to each device. Such assignments may be on a *static* (fixed or permanent) or *dynamic* basis, depending on network practices and software features. Some jurisdictions consider IP addresses to be personal data.

Function

An IP address serves two principal functions: it identifies the host, or more specifically, its network interface, and it provides the location of the host in the network, and thus, the capability of establishing a path to that host. Its role has been characterized as follows: "A name indicates what we seek. An address indicates where it is. A route indicates how to get there."[2] The header of each IP packet contains the IP address of the sending host and that of the destination host.

IP versions

IP

Two versions of the Internet Protocol are in common use on the Internet today. The original version of the Internet Protocol that was first deployed in 1983 in the ARPANET, the predecessor of the Internet, is Internet Protocol version 4 (IPv4).

By the early 1990s, the rapid exhaustion of IPv4 address space available for assignment to Internet service providers and end-user organizations prompted the Internet Engineering Task Force (IETF) to explore new technologies to expand addressing capability on the Internet. The result was a redesign of the Internet Protocol which became eventually known as Internet Protocol Version 6 (IPv6) in 1995.[3][4][5] IPv6 technology was in various testing stages until the mid-2000s when commercial production deployment commenced.

Today, these two versions of the Internet Protocol are in simultaneous use. Among other technical changes, each version defines the format of addresses differently. Because of the historical prevalence of IPv4, the generic term *IP address* typically still refers to the addresses defined by IPv4. The gap in version sequence between IPv4 and IPv6 resulted from the assignment of version 5 to the experimental Internet Stream Protocol in 1979, which however was never referred to as IPv5.

Other versions v1 to v9 were defined, but only v4 and v6 ever gained widespread use. v1 and v2 were names for TCP protocols in 1974 and 1977, as there was no separate IP specification at the time. v3 was defined in 1978, and v3.1 is the first version where TCP is separated from IP. v6 is a synthesis of several suggested versions, v6 *Simple Internet Protocol*, v7 *TP/IX: The Next Internet*, v8 *PIP — The P Internet Protocol*, and v9 *TUBA — Tcp & Udp with Big Addresses*.[6]

IP

Subnetworks

IP networks may be divided into subnetworks in both IPv4 and IPv6. For this purpose, an IP address is recognized as consisting of two parts: the *network prefix* in the high-order bits and the remaining bits called the *rest field*, *host identifier*, or *interface identifier* (IPv6), used for host numbering within a network.[1] The subnet mask or CIDR notation determines how the IP address is divided into network and host parts.

The term *subnet mask* is only used within IPv4. Both IP versions however use the CIDR concept and notation. In this, the IP address is followed by a slash and the number (in decimal) of bits used for the network part, also called the *routing prefix*. For example, an IPv4 address and its subnet mask may be *192.0.2.1* and *255.255.255.0*, respectively. The CIDR notation for the same IP address and subnet is *192.0.2.1/24*, because the first 24 bits of the IP address indicate the network and subnet.

Index