Cybercrime

Cybercrime is also called computer crime – it is the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.

Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.

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 owned by governments and corporations. 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.

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.

Types of cybercrime

The 5 of the top cybercrimes affecting businesses and individuals in 2022 are: phishing Scams, website Spoofing, ransomware, malware, IOT Hacking.

Cybercrime ranges across a spectrum of activities. At one end are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories and the use of illegally obtained digital information to blackmail 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, trafficking in child pornography, digital piracy, money laundering, and counterfeiting. These are specific crimes with specific victims, but the criminal hides in the relative anonymity provided by the Internet. Another part of this type of crime involves individuals within corporations or government 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, hacking, and denial of service attacks against specific sites to acts of cyberterrorism—that is, the use of the Internet to cause public disturbances and even death. Cyberterrorism focuses upon the use of the Internet by nonstate actors to affect a nation's economic and technological infrastructure.

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, covering terrorist activities and racist and xenophobic cybercrimes, were proposed in

2002 and came into effect in 2006. The Council of Europe's Cybercrime Treaty uses the term "Cybercrime" to refer to offences ranging from criminal activity against data to content and copyright infringement.

The United Nations Manual on the Prevention and Control of Computer Related Crime includes fraud, forgery, and unauthorized access in its cybercrime definition.