Security protection

Security in information technology is the defense of digital information and IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services. Weak security can result in compromised systems or data, either by a malicious threat actor or an unintentional internal threat.

A distinction is made between physical and informational security.

Physical security.

Physical security is a protection of personnel, hardware, software, networks and data from physical actions, intrusions and other events that could damage an organization. This includes natural disasters, fire, theft and terrorism, among others.

Information security.

Information security, also called infosec, is a broad set of strategies that prevent, detect and respond to threats to both digital and nondigital information assets. Infosec includes application security – the protections of applications. These protections use software, hardware and policies, and are sometimes called countermeasures. Common countermeasures include application firewalls, encryption programs, patch management and biometric authentication systems.

Hackers are computer criminals who use technology to perform a variety of crimes: virus propagation, fraud, intellectual property theft and so on. Hackers differentiate themselves into 3 groups:

White hat hackers.

A white hat hacker, upon finding some flaw in a system, will report the flaw to the vendor of that system. They are often hired specifically by companies to do penetration tests.

Black hat hackers.

Their goal is to cause some type of harm. They might steal data, erase files, or deface websites. Black hat hackers are sometimes referred to as crackers.

Grey hat hackers.

A gray hat hacker is normally a law-abiding citizen, but in some cases will venture into illegal activities.

Internet-based crimes include scam, email fraud to obtain money or valuables and phishing, bank fraud, to get banking information such as password of Internet bank account or credit card details. The Internet also provides the right environment for cyber stalking, online harassment or abuse, mainly in chat rooms or newsgroups. Piracy, the illegal copying and distribution of copyrighted software, information, music and video files, is widespread.

Malware or malicious software is software created to damage or alter the computer data or its operations. These are main types:

Viruses are programs that spread by attaching themselves to executable files or documents. When the infected program is run, the virus propagates to other files or programs on the computer.

Worms are self-copying programs that have the capacity to move from one computer to another without human help, by exploiting security flaws in computer networks.

Trojan horses are malicious programs disguised as innocent-looking files or embedded within legitimate software. They don’t copy themselves or reproduce by infecting other files.

Spyware, software designed to collect information from computers for commercial or criminal purposes, is another example of malicious software.

In the context of cyber security, social engineering (SE) is a deceptive practice that exploits human psychology by inducing victims to interact with a digital device in a way that is not in their best interest. Social engineer is a judgment-neutral term for a person who devises and carries out a scam in order to accomplish a goal, such as financial gain, unauthorized access, or service disruption. The target of a social engineering exploit is an individual or organization that may be tricked into participating in the scam.

SE attacks can be carried out using a variety of technologies, such as email, malware, fraudulent Web sites, SMS, and IRC. For each of these technologies, social engineers have developed a variety of effective techniques for tricking victims, including phishing, pretexting, and pharming.