Ethical Hacking

Ethical hacking is an authorized activity to recognize the potential data breaches and threats in a network. It involves an authorized attempt to gain unauthorized access to a device's system, application, or data. The people who do ethical hacking are called ethical hackers or white hats. Ethical hackers are security professionals who test the security, recognize loopholes, create reports and analyses, and work with authorized and proper permissions. They mainly work to help an organization improve its security posture. The process of ethical hacking is done with prior approval from the owner of the organization, which is opposite to malicious hacking. Sometimes it is performed to search for any weak points that malicious hackers could exploit. When ethical hackers find any weak point, they provide the information to the organization's owner, and the organization then uses the information to improve the system security. That is why it can be found safer in cyberspace as it looks like for ethical hackers.

Cyber Security

Cyber security is an activity of protecting networks, data, programs, and other information from unauthorized access or destruction. It refers to the body of technologies, processes, and practices designed to protect these essentials. It works to secure information and protect essentials from virus attacks. Nowadays, cyber threats are hazardous to a country's security. The pathway of cybercrimes has also increased with the development of technology and the internet's availability to people. Hackers gain access to someone's device quickly if the user of that device clicks on infected web links or unintentionally downloads malicious websites. That is why cyber security has become a significant concern in the era where communication devices have become ordinary for everyone. It plays a vital role in preventing heinous crimes like blackmailing, fraud transactions through another account, leakage of personal information. People and governments have to spread awareness among everyone to keep their system and network security updated to prevent cyber-attacks from happening worldwide.