

Cyber has been misused. a wide range

[Business](#), [E-Commerce](#)



Cyber security is the activity of protecting information and information systems (networks, computers, data bases, data centres and applications) with appropriate procedural and technological security measures. Firewalls, antivirus software, and other technological solutions for safeguarding personal data and computer networks are essential but not sufficient to ensure security. As our nation rapidly building its Cyber Infrastructure, it is equally important that we educate our population to work properly with this infrastructure.

Cyber-Ethics, Cyber-Safety, and Cyber-Security issues need to be integrated in the educational process beginning at an early age. Security counter measures help ensure the confidentiality, availability, and integrity of information systems by preventing or mitigating asset losses from Cyber security attacks. Recently cybersecurity has emerged as an established discipline for computer systems and infrastructures with a focus on protection of valuable information stored on those systems from adversaries who want to obtain, corrupt, damage, destroy or prohibit access to it. An Intrusion Detection System (IDS) is a program that analyses what happens or has happened during an execution and tries to find indications that the computer has been misused.

A wide range of metaphors was considered, including those relating to: military and other types of conflict, biological, health care, markets, three-dimensional space, and physical asset protection. These in turn led to consideration of a variety of possible approaches for improving cyber security in the future. These approaches were labelled “ Heterogeneity” , “ Motivating Secure Behaviour” and “ Cyber Wellness” . Cyber Security plays

<https://assignbuster.com/cyber-has-been-misused-a-wide-range/>

an important role in the development of information technology as well as Internet services.

Our attention is usually drawn on “ Cyber Security” when we hear about “ Cyber Crimes”. Our first thought on “ National Cyber Security” therefore starts on how good is our infrastructure for handling” Cyber Crimes”. This paper focus on cyber security emerging trends while adopting new technologies such as mobile computing, cloud computing, e-commerce, and social networking. The paper also describes the challenges due to lack of coordination between Security agencies and the Critical IT Infrastructure