

Next Generation Cybercrime: A Review

Neelinderjeet Kaur Sandhu

The Director Principal, the S. D. Vidya School, India

Yamini Bansal

Abstract

WWW, Cyberspace, Internet, ARPANET, the much engaging tools, the tools without which one's life becomes fragmented...but for whom? Millions of potential victims, including the BIPOC community, are most likely to be financially impacted by cybercrimes. Any criminal activity that involves a networked computer device to generate profit for the cybercriminals can be considered a cybercrime. These activities occur in a virtual world, an electronic medium to facilitate online communications known as Cyberspace. Internal reports show that millions of cases attempt to illegally access and interfere with other people's files.

The IT technologists and government officials have documented a sharp increase in such crimes since early 2001. Cybercrime bodies link to penetrating criminal activities online while estimating the likelihood of their destination and prosecution. Even the global communities witness the sporadic growth in cybercrime. Computer-based crimes encompass various activities, including financial crime scams and cyber trafficking through Ad frauds. Cybercrimes have led to significant damage not only to individuals but also to various businesses causing employment disruption and reduced trust in a company's online services.

The paper revolves around cybercrimes, famous cybercrimes acts, Cyberspace, different types of crimes, their importance, prevention, detection, and investigation, and also outlines various aspects of the Cybercrime Prevention Act of 2012(10175).

Keywords: Cybercrimes, Cyber Defamation, Dark web, Password-sniffing, Prevention Act