Abstract

Offences those are committed against an individual or a group with a criminal motive to intentionally harm the reputation or cause physical or mental harm to the victim using modern telecommunication networks such as the Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS) are termed as cyber-crimes. Cyber-crime is any illegal activity that uses a computer as its primary means. There are two main categories that define the make-up of cyber-crimes. Firstly viruses, malware, or denial of service attacks that target computer networks or devices. The second category relate to crimes that are facilitated by computer networks or devices like cyber-stalking, fraud, identity-theft, extortion, phishing (spam) and theft of classified information. It is widely known that victims of Internet crimes are often reluctant to report an offence to authorities or in some cases the individual may not even be aware a crime has been committed. Even though facilities for reporting incidents of cyber-crime have improved in recent years many victims remain reluctant to do so due to embarrassment. International cooperation is essential if a good response is to be found against global cyber-crime. No nation can effectively combat the issue alone in an easy way. Many computer based crimes are initiated off-shore; and this presents enormous challenges to
any nations agencies of law enforcement. It is crucial that agencies from around the world formulate actionable plans to detect, follow, arrest and prosecute criminals of cyber-crime. Computers and the Internet have been a boon to our society; unfortunately criminals now make use of these technologies to detriment our society.

References

- Cyber Crime Today & Tomorrow, Thiru Dayanithi Maran.

Index Terms

Computer Science
Security

Keywords

Cyber Stalking  Hacking  Phishing  Cross Site Scripting  Vulnerability