

# Impact of Cyber Crimes and Education

<sup>[1]</sup> A.Simon, <sup>[2]</sup> Dr.A.Veliappan<sup>[1]</sup> M.Ed Scholar, <sup>[2]</sup> Assistant professor<sup>[1][2]</sup> Department of Education, Manonmaniam Sundaranar University,  
Tirunelveli, Tamilnadu

---

**Abstract:-** Cyber Crimes as any crime that is committed by means of special knowledge use of computer technology. The threat of cybercrime is an ever-present and increasing reality in both the private and professional sectors. With the advent of the internet, old crimes have taken on a new appearance. Theft and fraud can now be received directly into a personal home through online means. The financial loss and personal pain caused by hacking and other internet-related crimes cannot always be measured, but statistics are reported each year. Though these crimes span many aspects of life, the most prolific boil down to hacking and digital piracy. Hackers are able to gain access to financial assets and information, while other criminals are able to illegally download entertainment products, causing a decline in sales and loss of revenue. Cybercrime highlights the centrality of networked computers in our lives and the fragility of such seemingly solid facts as individual identity.

**Keywords:** Cyber Crimes, Technology, Internet, Computer.

---

## INTRODUCTION

Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. It is very difficult to classify crimes in general into distinct groups as many crimes evolve on a daily basis. Even in the real world, crimes like rape, murder or theft need not necessarily be separate. However, all cybercrimes involve both the computer and the person behind it as victims, it just depends on which of the two is the main target. Hence, the computer will be looked at as either a target or tool for simplicity's sake.

Education is the process through which the experiences of generations, comprising knowledge, skills and attitudes are transmitted to individuals, who are members of the community. Concepts change, attitudes and skills undergo alterations, interests and values face revisions and life itself undergoes a continuous modification of experience. In this context, education is the process of assisting the learner to adjust to the ever-changing world.

New technologies create new criminal opportunities as well as new types of crime. With the modernization and availability of technology at affordable prices it has led to wide spread use of technology for development as well as destructive. Cyber crime highlights the centrality of networked computers in our lives and the fragility of such seemingly solid facts as individual identity. For example, hacking involves attacking the computer's information and other resources.

## Social Impacts of Cyber Crime

Computer -related crime dates to the origins of computing, though the greater connectivity between computers through the Internet has brought the concept of cyber crime into the public consciousness of our information society.

In 1995, when the World Wide Web was in its early stages of development, futurist Dr. Gene Stephens wrote about the present and future reality of cyber crime and made several predictions: "Billions of dollars in losses have already been discovered. Billions more have gone undetected. Trillions will be stolen, most without detection, by the emerging master criminal of the twenty-first century—the cyberspace offender" (Stephens, 1995).

## Definition of Cyber Crime

Cyber crime, as distinguished from computer crime, is an umbrella term for the various crimes committed using the World Wide Web, such as:

- The theft of one's personal identity (identity theft) or financial resources;
- The spread of malicious software code such as computer viruses;
- The use of others' computers to send spam email messages (botnets);
- Denial of Service (DoS) attacks on computer networks or websites by the hacker
- Cyber stalking, by which sexual predators use Internet chat rooms, social networking sites, and other online venues to find and harass their victims;
- Cyber bullying, where individuals are harassed by others, causing severe mental anguish;
- Cyber pornography, the use of the Internet to spread child and adult pornography;

- Internet gambling and software piracy; and
- Cyber terrorism, the use of the Internet to stage intentional, wide-spread attacks that disrupt computer networks; using the Internet to spread violent messages, recruit terrorists, and plan attacks.

Cyber crime can be divided into four sub-categories:

- Cyber-trespass (hactivism, viruses, Denial of Service attacks)
- Cyber-deceptions (identity theft, fraud, piracy)
- Cyber-pornography
- Cyber-violence (cyber bullying, cyber stalking)

Several of these activities have a long history that predates the Internet, and they also have technological antecedents. "Some of the nineteenth-century wire frauds perpetrated by tapping into the early electric telegraph systems, for example, bear an uncanny resemblance to modern day hacks.

Media reports since the 1990s have documented the many methods by which criminals have used the Internet to commit crimes. Cyber thieves have become skilled at using the anonymity and secrecy of the Internet to defraud their victims of their money, their peace of mind, and indeed even their lives. When victims let their guard down by muting a healthy scepticism and caution, Cyber-crime takes place. As one FBI spokeswoman noted, "The scammer tries to prey on victims who are kind of in tune with what's going on in the world. The scam changes, but ultimately they're preying on the good will of people" (Simmons, 2008).

#### **Computer as a tool**

When the individual is the main target of cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise. Human weaknesses are generally exploited. The damage dealt is largely psychological and intangible, making legal action against the variants more difficult. These are the crimes which have existed for centuries in the offline world. Scams, theft, and the likes have existed even before the development in high-tech equipment. The same criminal has simply been given a tool which increases his potential pool of victims and makes him all the harder to trace and apprehend.

#### **The Scope of Cyber Crime**

Law enforcement officials have struggled to identify, arrest, and prosecute these tech-savvy offenders, even as sociologists have sought to get to the root of cyber crime. The Federal Bureau of Investigation (FBI) created a special cyber division in 2002 to "address cyber crime in a coordinated and cohesive manner (Federal Bureau of Investigation, 2013) with cyber squads in each of its fifty-six field offices, "cyber action teams" that travel worldwide to address cyber attacks, and nationwide computer task forces.

The field of cyber crime has spawned the field of cyber criminology, defined as "the study of causation of crimes that occur in the cyberspace and its impact in the physical space" As more and more people have used the Internet to do their shopping, communicating, banking, and bill paying, they have become targets for cyber criminals. There are common-sense steps that can prevent or reduce having one's financial information stolen online, as well as to avoid other scams and threats, but cyber crime in these areas persists largely due to a lack of consumer education.

Some varieties of cyber crime, such as hactivism, are ostensibly motivated by noble intentions, such as protest against perceived abuses by governments and corporations. Often these attacks involve posting comments on official government websites and are not motivated by a desire for monetary gain. However, other forms of cyber crime have a much more violent intent. These include cyber stalking, cyber bullying, and cyber terrorism. It attacks the very foundations of modern, technological societies, bound up as they are with the rapid flow of computer data facilitated by the Internet. At the most basic level, cyber criminals often take advantage of technologically unsophisticated individuals who nonetheless find themselves in a world where the Internet plays an increasingly central role in both community and private life. It depends, at this level, on the ability of those who are more technologically sophisticated to use that knowledge to trick others into surrendering vital information, such as their bank account information or Social Security number. While it is possible in some situations for the victim of cyber crime to restore stolen money or even their personal online identity, the event often leaves the victim traumatized and deeply suspicious of the Internet and other trappings of modern life.

#### **Diffusion of cybercrime**

The broad diffusion of cybercriminal activities is an issue in computer crimes detection and prosecution. Hacking is much less complex than it was a few years ago, as hacking communities have greatly diffused their knowledge through the Internet. Blogs and communities have hugely contributed to information sharing: beginners could benefit from older hackers' knowledge and advice. Furthermore, Hacking is cheaper than ever: before the cloud computing era, in order to spam or scam one needed a dedicated server, skills in server management, network configuration, and maintenance, knowledge of Internet service provider standards, etc.

#### **CONCLUSION**

Cyber crime encompasses any criminal act dealing with computers and networks and also includes traditional crimes conducted through the Internet.

**REFERENCES**

- [1] Hester, S & Eglin, P (1992). A Sociology of Crime. London. Roulledge Publications.
- [2] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
- [3] Padhy, P (2006). Crime and Criminology, Principles of Criminology. New Delhi: Mehra Press Ltd.
- [4] Rebecca & Jeanne, M.(2011) Criminology. Encyclopedia of the Social and cultural Foundation of Education. New Delhi: SAGE Publications.
- [5] Tanner, R.E.S (2007).Social Impact of Cyber Crimes. New Delhi. Concept Publishing Company.

