

## CYBER CRIME EDUCATION



**Prin. Dr. Shrinivas V. Joshi.**



**Dr. Mrs. Pallavi K. Kulkarni Deshpande**

Cyber Crime is not new for the readers, Electronic gadgets (either wireless or wired), whenever are used to harm public and business organization are called cyber crimes. It may be done in the form of a virus attack, Phishing attack, Spoofing, Identify Theft or any of the tricks to misguide the victim. There is significant and worth investigation by criminologists because victims of Cyber-Crimes are increasing more quickly than cyber police can detect, arrest and prosecute. With the advent of the Internet, people have changed the way in which they communicate or interact with others, shop. These changes in organization's have increased the probability of being any kind of cyber threat.

That Consumer awareness of Phishing, a burning cyber crime is high, and most consumers take appropriate action upon receiving suspicious email. More than half of consumers immediately delete email purporting to be from their banks asking for personal information.

Willox N.A., Regan T.M. (2002) studied identity theft, a type of cyber crime, which violates the individual victim and wreaks huge financial losses on the commercial victim. However, the crime of using false identifiers and false identification documents transcends identity theft, as it includes not only the identity thief, but also the drug trafficker, the alien smuggler and the terrorist. One who commits this crime of identity fraud needs to be culled out and prevented innovative and effective solutions.

It is investigated that computer related crime is growing rapidly, but we are unable to measure with any precision its incidence and impact. More accurate measurements would be instructive to government and the private sector, to properly size prevention and investigation efforts. The study recommended in this paper established terms of reference and a metrics measurement process that would facilitate allocation of appropriate resources to preventing and responding to computer-related crime.

Conway M. investigated that cyber crime may be used to support terrorism and such activities ought not to be classed as cyber terrorism. Although hackers have demonstrated that they are willing to crash computer networks to cause functional paralysis and even significant financial loss, this propensity for expensive mischief is not sufficient evidence that they would be willing to jeopardize lives or even kill for a political cause. Organized crime groups view the Net as a tool, not a target because

many such organizations employ the Internet – and the public telecommunications network generally – as a vehicle for intelligence gathering, fraud, extortion, and theft.

#### **Need for Cyber Crime Education (CCE) :**

With the advancement in Information Technology and growing need of MISs, there is a tremendous growth in the facilities endowed with banks, insurance companies; FMCG and e-commerce companies. Cyber Crime awareness has to be addressed at all levels, from the individual user to an organization. Mobile life, covering maximum of the dealings accessible online has granted the probability of being victimized by hackers, intruders and phishers. Of course, network administrators are coming with advanced technology and generating secure channels for data transmission. In spite of these security measures (either at software or hardware end), credit card frauds. ATM frauds have become common now a days. Why so ?

Many studies have been carried out on cyber crime issues viz., Identify Theft, Hacking, Phishing, Vishing, Pharming etc., but no any study suggests a specific measure to get rid of these threats. The researches recommend taking precautions while using computer networks (either internet ) to overcome cyber attacks. Education has always been supposed to enlighten the people's mind and aware the masses, whenever the problems viz. environment's threat and like come across.

#### **Mobile Lift :**

The emergence of the Internet has brought dramatic changes in the living patterns of the masses all over the globe. The traditional payment, where the clumsy and expensive way to handle coins and notes is being replaced by efficient electronic payments initiated by various types of plastic cards, a tantalizing prospect for the twenty-first century. These business activities include electronic fund transfer (EFT), supply chain management (SCM), e-Marketing, online marketing, online transaction processing, electronic data interchange (EDI) and automated data management among others. Everybody is in hurry due to sky-scraping competition in every sphere of life causing people to use payment technologies, which are more convenient and less time consuming.

#### **Active Cyber Criminals :**

Due to unexpected growth in cyber crimes in society, information system security has become the greatest challenge for MIS experts. Security is the main concern of the organizations in the present scenario of information and data, where every transaction is on transmission lines visible to cyber criminals directly or indirectly. It is more dangerous when the data is about the money and the financial information. For so many companies and even individuals, the secrecy of information about the financial and their accounts and so many things like this, is highly important. If they lose a small amount of data, they may lose their all things. The growth of the Internet as a medium of transaction has made

possible an economic transformation in which commerce is becoming electronic. Engineers and technocrats are endeavoring to block up the loopholes through an assortment of software and hardware practices, viz., SSL Certificates, SET Protocols, Pretty Good Privacy, Kerberos, Digital Signatures, Electronic Wallets, MeChip and so on. In spite of implementing such potential security tools and techniques, cyber criminals trap the security measures and create vulnerabilities for the organization and its stakeholders due to some weak spots within the system using some tricks viz.,

1. Impersonation
2. Hoaxing
3. Cyber Defamation
4. Cyber stalking
5. Identify Theft
6. Denial of Service Attack

#### **Online Transactions :**

In the current age of information and Communication Technology every job has become online from banks to restaurants and education to crime. Sky-scraping competition in corporate world compelled every business organization to become technology savvy as people have needed for hi-tech services at their doorsteps within moments. Every moment, managers are trying to facilitate their customers in an effective way to live their business. Financial Institutions cover not only banking sector as Central Bank (Reserve Bank of India), Commercial Banks, Credit Rating Agencies, Credit Reporting and Debt Collection, Financial authorities, Insurance Companies, Merchant Banks and Venture Capitalists but also cover insurance sector with some companies, viz., NSDL, BSE, NSE, IRDA, NEDFI, UTI, NABARD etc. Banks and insurance companies are facilitating their customers with electronic services at their portals and outlets to retain their customers.

- E-Ticketing to facilitate the customers to book the bus, air and railway tickets online.
- E-Tax enables customers to pay TDS, Income tax, Indirect tax, Corporation tax, wealth tax, Estate Duty and Fringe Benefits tax online through NSDL site where customer can select an online challan based on the tax s/he wishes to pay.
- E-Donation facilitates the customers to donate money to charitable and religious institutions online through their bank account.
- Gone are the days the customer had to depend on long queues to shop goods. Shopping malls are now available online and bills are paid through E-Payment by either Credit or Debit Cards. Telephone Bills, Electricity Bills, Recharge of Cell Phones can be paid online through E-Payment within moments.

- Fund Transfer enable the customers to relocate the money within your account in the same name. Transaction rights would play a major role.
- Third Party transfer to transfer the funds with third parties with secure identity.
- New Account Opening to open new accounts on internet.
- Demat / Account Statement to catch the daily transactions as well as account status.
- Share trading has become the business for investors, which has only become possible through corporate IT networks via E-Auctions.

#### Lack of Technical Control

Newsrooms are full with ATM frauds, Credit Card frauds and many such accidents, due to loopholes existing in the system. Why do most people still like to do their businesses in traditional form as before ? These people prefer to touch the documents and money in hand and doing the process manually to electronically. They believe in every dealing and business, physically rather than virtually. There are many people even in this digital era, who are not agreed and accept the all new technologies. The job is very hard to pursue and to make these people eager to do in this way and accept the technologies. People are always not certain and assured to the technologies because of poor technical control causing malfunctions, frauds and unavailability of devices in the time of need.

This live case shows mind set of a cyber criminal that s/he might target any citizen either an IT professional or Non IT Professional. People usually make use of internet without taking precautions as they do not know that a single click of mouse might be dangerous if destination like having some Malware or Spyware. Most of the internet users not having the knowledge of-

1. Cyber criminals and their ideology
2. Cyber threats
3. Web browser's security policy and its usage
4. Pop up windows and its mechanism
5. Firewall and Antivirus software usage
6. E-Mail mechanism
7. Security toolbars
8. Password policy and Virtual Keyboards
9. SSL Certificates
10. Universal Resource Locators

In broad terms, the functions of the higher education institutes in the modern world may be said to be:

- To seek and cultivate new knowledge, to engage vigorously and fearlessly in the pursuit of truth, and to interpret old knowledge and beliefs in the light of new needs and discoveries.
- To provide society with competent men and women trained in agriculture, arts, medicine, science and technology and various other professions, who will also be cultivated individuals imbued with a sense of social purpose.
- To strive to promote equality and social justice and to reduce social and cultural differences through diffusion of education.
- To foster in the students and through them in society generally, the attitudes and values needed for developing the good life in individuals and society.

Cyber Crime Education can make an appropriate contribution to modernization of the traditional curriculum especially in Professional Programs in the field of Information Technology, Management, Pharmacy, Law, Engineering, Education, Agriculture and various like fields. It will create awareness among the students who are supposed as nation builders to serve the nation in various walks of life. In such environments, education gets top priority so as to have a richer and fuller life in material terms by its progressive utilization as well as to cultivate a practical approach in the individuals for solving social and economic problems in an ideal way. Knowledge is power by which things are done said Socrates.

#### REFERENCES :

1. Taneja VR (2018), Socio Philosophical approach to Education, Atlantic Publishers, p. 38, 23, 24, 93, 94.
2. The Hindu (2019, Aug 16), Cyber Crime in Law Curricula
3. Vladimir Z. (2018), Electronic Commerce: Structures and Issues, International Journal of Electronic Commerce.
4. Vladimir Z. (2018), Electronic Commerce and Organizational Innovation: Aspects and Opportunities, International Journal of Electronic Commerce.
5. Willox N.A. Regan T.M. (2017), Identity Fraud: Providing a solution, Journal of Economic Crime Management.

