Knowledge of Cybercrime among Elderly

Nabat Arfi , Shalini Agarwal

Abstract

Cybercrime is a kind of crime that happens in "cyberspace", that is, happens in the world of computer and the Internet. Although many people have a limited knowledge of "cybercrime", this kind of crime has the serious potential for severe impact on our lives and society, because our society is becoming an information society, full of information exchange happening in "cyberspace". There studies indicating cybercrime in present scenario, cybercrime and their laws and cybercrime during adolescent. As the Internet, mobile phones, and other computer technologies have flourished, criminals have found ways to use them for old-fashioned goals such as theft, fraud, intimidation, and harassment that's why cybercrime is becoming even more serious. Elderly is that vulnerable group who has been deprieved from any information regarding latest technologies and innovation especially in the world of computers and internet . The purpose of the present study is to assess the knowledge of cybercrime among elderly.

Keywords: Cybercrime, Internet, Knowledge, Elderly.

1. Introduction

The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite to serve billions of users worldwide. Computers are used to commit crime and users become the target of crime every day. Besides the magnitude and scope of the threat, one of the greatest challenges in fighting computer crime resides in the fundamental nature of the computing world. A lot of us have a limited knowledge of crime occurring in "cyberspace", known as cybercrime, which happens on computer and the Internet, however, cybercrime has a severe potential for remarkable impact on the lives of individuals and our society. Cybercrime is a kind of crime that happens in "cyberspace", that is, happens in the world of computer and the Internet. Although many people have a limited knowledge of "cybercrime", this kind of crime has the serious potential for severe impact on our lives and society, because our society is becoming an information society, full of information exchange happening in "cyberspace".**[1]**

- *Author name is currently pursuing masters degree program in Department of Human Development & Family Studies in Baba Saheb Bhimrao Ambedkar University Lucknow,U.P., India ,Mobile-919044890612. E-mail: nabat.arfi@gmail.com*
- *Co-Author name is Assistant Professor in Department of Human Development & Family Studies in Baba Saheb Bhimrao Ambedkar University Lucknow,U.P., India.*

2. Types of Cybercrime

Crimes committed through the use of computer, internet in the mobile systems are known as cybercrimes. Here are some common cybercrimes to look out for.

2.1. Child pornography – the use of computer networks to create, distribute, or access materials that sexually exploit underage children.

2.2. Cyber laundering – electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.

2.3. Cyber stalking – express or implied physical threats that creates fear through the use of computer technology such as email, phones, text messages, webcams, websites or videos.

2.4. Cyber terrorism – premeditated, usually politically-motivated violence committed against civilians through the use of, or with the help of, computer technology.

2.5. Cyber theft is using a computer to steal. This includes activities related to: breaking and entering, DNS cache poisoning, embezzlement and unlawful appropriation, espionage, identity theft, fraud, malicious hacking, plagiarism, and piracy.

2.6. Spam - Unsolicited mass e-mail, known colloquially as "spam", is more than annoying: spam messages can be used to trick people into giving up sensitive personal information (known as "phishing"), or as carriers for computer worms and viruses**. [2]**

3. Types of cybercrime against elderly

3.1. Health Care Fraud or Health Insurance Fraud-Medical Equipment Fraud: Equipment manufacturers offer "free" products to individuals. Insurers are then charged for products that were not needed and/or may not have been delivered."Rolling Lab" Schemes: Unnecessary and sometimes fake tests are given to individuals at health clubs, retirement homes, or shopping malls and billed to insurance companies or Medicare.Services Not Performed: Customers or providers bill insurers for services never rendered by changing bills or submitting fake ones.

3.2. Telemarketing Fraud-
If one is of age 60 or older—and especially an older woman living alone—one may be a special target of people who sell bogus products and services by telephone. Telemarketing scams often involve offers of free prizes, low-cost vitamins and health care products, and inexpensive vacations**.[3]**

4. Reason of Cybercrime

Hart in his work " The Concept of Law" has said 'human beings are vulnerable so rule of law is required to protect them'. Applying this to the cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them against cyber crime. The reasons for the vulnerability of computers may be said to be:

4.1. Easy to access- The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

4.2.Complex- The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

4.3.Negligence- Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal to gain access and control over the computer system**.[4]**

5. Problem of Cybercrime against Elderly

5.1. Fraud Committed by Strangers-

5.1.1. Investments- Because many seniors live on fixed incomes, they often want to increase the value of their estate and ensure they have sufficient funds to meet basic needs. In investment scams, offenders persuade the elderly to invest in precious gems, real estate, annuities, or stocks and bonds by promising unrealistically high rates of return. The investments often consist of fake gemstones, uninhabitable property, or shares in a nonexistent or unprofitable company.

5.1.2. Charity contributions- Playing on some seniors' desire to help others, offenders solicit donations to nonexistent charities or religious organizations, often using sweepstakes or raffles to do so.

5.1.3.Loans and mortgages- Seniors may experience cash flow shortages in the face of needed medical care or home repairs. Predatory lenders may provide loans with exorbitant interest rates, hidden fees, and repayment schedules far exceeding the elderly's means, often at the risk of their home, which has been used as collateral.

5.2.Financial Exploitation by Relatives and Caregivers-

Unlike strangers, relatives and caregivers often have a position of trust and an ongoing relationship with the elderly. Financial exploitation occurs when the offender steals, withholds, or otherwise misuses their elderly victims' money, property, or valuables for personal advantage or profit, to the disadvantage of the elder. Their methods can include the following:

- simply taking the elder's money, property, or valuables;
- borrowing money (sometimes repeatedly) and not paying it back;
- signing or cashing pension or social security checks without permission;
- misusing ATM or credit cards, or using them without permission;
- doling out the elder's money to family or friends; and
- forcing the elder to part with resources or to sign over property. **[3][4]**

6.Factors contributing to financial crimes against Elderly

Understanding the factors that contribute to your problem will help you frame your own local analysis questions, determine good effectiveness measures, recognize key intervention points, and select appropriate responses.

6.1. Underreporting-

Researchers agree that elder fraud is dramatically underreported, which is problematic for several reasons. First, the failure to report means that the assistance of police, adult protective services, family members and others is not mobilized to stop the abuse. Second, even if intervention is not necessary, the underreporting of these crimes makes it very difficult for problem-oriented efforts to proceed because of a lack of information on the targets, methods and perpetrators. Finally, the lack of reporting may encourage the offenders to victimize others. Many elderly victims do not report fraud because they feel ashamed, or they fear others will think they cannot care for themselves, which may trigger placement in a nursing home or long-term care facility. Significantly, many victims are not aware of support resources or do not know how to access them. In the case of financial exploitation, many victims have close ties to the offender and may feel protective. They may want to stop the exploitation and recover their assets, but not want the offender punished. In addition, many victims believe they are at least partially to blame.

6.2. Victim Facilitation-

In contrast to victims of most other forms of crime, consumer fraud victims have a participatory role that is critical to a successful transaction. Victim compliance can fall along a continuum. At one end is the completely uninvolved victim, as in the case of identity theft or credit card fraud. Toward the middle is the victim who makes a purchase or financial arrangement that is not well-informed or well-researched. At the far end is the repeat victim. Even after victimization, many people repeat high-risk behaviors.

The following are key moments that put the victim at risk in the typical fraud transaction. They have clear relevance to points of intervention:

- The victim makes the initial contact, or takes steps that lead to the initial contact, indicating receptivity to the pitch.
- The victim provides information about him- or herself that helps the offender to carry out the fraud.
- The victim allows the conversion of a business relationship to one of trust, and waives customary safeguards**. [4]**

7. Mode and manner of committing cybercrime

Unauthorized access to computer systems or networks / Hacking- This kind of offence is normally referred as hacking in the generic sense. However the framers of the information technology act 2000 have no where used this term

so to avoid any confusion we would not interchangeably use the word hacking for 'unauthorized access' as the latter has wide connotation.

7.1. Email bombing- This kind of activity refers to sending large numbers of mail to the victim, which may be an individual or a company or even mail servers there by ultimately resulting into crashing.

7.2. Data diddling- This kind of an attack involves altering raw data just before a computer processes it and then changing it back after the processing is completed. The *electricity board* faced similar problem of data diddling while the department was being computerised.

7.3. Salami attacks- This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. e.g. the *Ziegler case* wherein a logic bomb was introduced in the bank's system, which deducted 10 cents from every account and deposited it in a particular account.**[1]**

8. Factors that contribute to increased risk of Elderly

8.1. Lack of computer skills- Though many seniors are very computer savvy, many more are not. Often their computers are not properly secured. Even when you have installed security software, it is critical that you set up automatic updates, turn on a firewall, use secure password, and so on.If one feel that he/she is unble to set up your computer security, it may be well worth hiring a computer technician from a reputable company to review the settings for security and fix any problems one may have. Make sure that one have checked the company through the Better Business Bureau and that whoever comes to your home is fully licensed and bonded.

8.2.Lack of Internet skills- Though many seniors are cutting edge users of Internet services, most of them are beginners when it comes to computer technology.Just spending more time online will help you feel more comfortable with the ins and outs of navigating online and interacting on Web sites. Once you familiarized yourself with the tricks scammers and some less reputable companies use, one can simply avoid them. There are many Web sites, books, and courses offered for every level of user. Many of these courses are offered at low cost through colleges across the state.

8.3.More Trusting- Elderly have a wealth of experience in judging the character of people you meet in person, but have probably developed fewer skills for assessing the character of the people and companies you meet online. Elderly are typically more trusting and respectful of official looking material than younger generations, so are more apt to fall for scams. And you are more worried about notices that claim there is a problem with your information that might somehow sully your good name.**[3]**

9. Cybercrime laws and Agencies

Important Sections Related to Cyber Crimes:-

Information Technology (Amendment) Act 2008-

Sections under IT Act (2008)-

Sec 65. Tampering with Computer Source Documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Sec 66. Computer Related Offences

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

66C Punishment for identity theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

66E Punishment for violation of privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees.

66F. Punishment for cyber terrorism

(1) Whoever with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by-

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or

(iii) introducing or causing to introduce any Computer Contaminant.

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

Section 383. Extortion

Whoever intentionally puts any person in fear of any injury to that person, or to any other, and thereby dishonestly induces the person so put in fear to deliver to any property or valuable security, or anything signed or sealed which may be converted into a valuable security, commits "extortion". **[7]**

HELP CENTRES:

1.INDIA-

Centre for Cyber Victim Counseling: The mission of the CCVC is to: Help you to understand the nature of the crime that has been committed against you; help you take action against the offender; to provide counseling for the trauma you have gone through, and to help you to understand the present legal scenario and to connect you with the appropriate police service, if needed.

2. INTERNATIONAL-

Cyber Law Enforcement.org**:** This organization has four goals: (1) To unite police officers worldwide and educate them on cybercrime, cyber law, investigative techniques and how they interact. (2) To provide investigative assistance to police departments when requested. (3) To provide online help and education for victims of cyber stalking, cyber harassment, pedophile, hacking, and virus attacks as well as access to support groups and online counseling. (4) To standardize relations and communications between police departments, Internet Service Providers, Legal system contacts and victim advocacy groups worldwide**.[6]**

11. Prevention from Cybercrime

1.to prevent cyber stalking avoid disclosing any information pertaining to oneself. This is as good as disclosing your identity to strangers in public place.

2.always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.

3.always use latest and up date anti virus software to guard against virus attacks.

4.always keep back up volumes so that one may not suffer data loss in case of virus contamination

5.never send your credit card number to any site that is not secured, to guard against frauds.

6.always keep a watch on the sites that your children are accessing to prevent any

kind of harassment or depravation in children.

7.it is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal. **[9]**

12. References

[1] Bowen, Mace (2009), Computer Crime, Available at: http://www.guru.net/, Visited: 07/09/12.

[2] Mali P. (2010), " Types of cybercrime and cyber laws in India", *Journal of Law*, 10(1):1.

[3] Bick B.J. (2011), "Internet crime and the Elderly", *New Jersey Law*, 2(4):1-2.

[4] Campbell R.J. & Wabby J. (2003), "The Elderly and the Internet: A case study", *The Internet Journal of Health*, Vol.3, Issue.1.

[5] Knowledge of internet. http://www.internetworld.com. Accessed on September 2012.

[6] Cyber report index. http://www.cyber index:cyber reporting organization.com.html. Accessed on October 2012.

[7] Cyber laws. http://delhicourts.nic.in/ejournals/CYBER%20LAW.html. Accessed on October 2012.

[8] Cyberlawtimes (2009), Available at http://www.cyberlawtimes.com/forums/index.php?board =52.0, Visited: 10/11/12.

[9] Cyber Trust and Crime Prevention, Mid-Term Review, November 2005 – January 2009, Available at: http://www.bis.gov.uk/assets/bispartners/foresight/docs/cyber/ctcp_midterm_ review.pdf, Visited: 10/11/2012.