www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 12 December 2014, Page No. 9587-9590

Cyber-bullying

Er. Anup Lal Yadav, Er. Sahil Verma, Er. Kavita

M-Tech Student
Asst. Prof. in C.S.E. Deptt.
EMGOI , Badhauli.
sahilkv4010@yahoo.co.in
Asst. Prof. in C.S.E. Deptt.
EMGOI , Badhauli.

INTRODUCTION:

"Internet crime is crime committed on the Internet, using the Internet and by means of the Internet".Since the introduction of the Internet in the 1950's, the world has been introduced to innovative technology that has seemingly enhanced our lives. It has brought convenience to the busy lifestyle. However, this continuum of boundless information has become a portal for Internet criminals to breach the barriers of online privacy and protection. Internet crimes (also termed as '*computer*' or 'web' *or* 'cyber' *crimes*) are being viewed as one of the greatest challenges of the 21st century. From child pornography and sex crimes to Internet theft and computer fraud, prosecutors and investigators are aggressively confronting all types of computer and web crime. The United States is home base for 78% of Internet-related crimes committed in the world. Of late, Thailand and seven other Asian and South Pacific countries have been discussing ways of combating criminals using the Internet and other information technology to commit crimes. *Most importantly*, some of the crimes are real-world based, and can have serious repercussions. *They could even result in death in some cases where a bomb is sold over the internet.*

In order to put a check on ever increasing Internet crime, many national governments have set up cyber crime units (which work to prosecute all types of computer crimes, including Internet pornography, cyber crimes against children, Internet sex crimes, identity theft, Internet fraud, computer hacking, etc.), but *'not with much success'* due to technical reasons. The fact is that Internet law is still not universal and this slows it down in respect to fighting internet crime, which knows no boundaries and can attack various countries at once. This paper investigates prominent criminal methods for Internet crime and assesses the capabilities of the current online security systems. It also discusses the impact of cyber crime on the society.

According to an estimate, of the 1.09 billion people accessing the Internet each day, 500 million can be affected by the emergence of crime each day. If calculated, that comes out to 1 out of every 2 people at risk. People everywhere rely on the Internet for communication, research, and transactions. It can virtually be used for anything. The interconnectivity of the Internet paved the way for future advancements, but it also widened access for criminal advancement. Because of this, there are many implications involved.

The Internet is of high importance; however it brings into question the ethics of society. People have transformed this enlightening tool to a destructive device. People can now gain unauthorized access to resources, destroy the integrity of information, and jeopardize the physical safety of the public. Unauthorized access can be obtained when criminals breach the security system. Integrity of information is destroyed when criminals hack into the system and alters files- even government files can be broken into. Worst of all, public safety can be at risk because criminals can utilize the Internet as a method of luring and kidnapping children- thereby transforming the Internet with potential of social disaster.

Box – 1: Online Fraud: Phishing and Pharming

The explosive growth of online fraud has made 'phishing', and to a lesser extent 'pharming' part of nearly every Internet user's vocabulary during 2005. Phishing and pharming are two popular forms of fraud that aim to dupe victims into believing they are at a trusted Web site such as their bank, when in fact they have been enticed to a bogus Web site that intends to steal their identity and drain their financial resources.

As Internet crime spreads in the world, there are many financial implications. Not only do criminals target users on the individual level, but they can also cause massive destruction that will cause the government millions of dollars in damages. This, in turn, forces the government to reallocate funds in dealing with the damages.

3. CRIME METHODS:

Internet Crime has become increasingly popular because it is a global means of perpetration. It allows for wider access through less bodily kinesthetic action. The evolution of Internet access has allowed for a revolutionary surge of new criminals. There are various ways to penetrate the networking system, the most prominent are the following methods:

- **Hacking v. Cracking**: Hacking is the act in which a person penetrates a computer system. However, hacking can also be the manner in which a person makes the system more convenient and feasible for use. Therefore, the term *'Cracking'* would be politically correct for referring to gaining unauthorized access of another's computer system. Hackers can monitor every action. They can write new files, access old files, and edit/delete existing files on else's computer. If a Hacker is not able to penetrate system entirely, they can install programs that will enable them to steal personal information such as passwords and credit card numbers.

- **Fraud:** Internet fraud usually occurs when credit card holders are tricked into releasing personal information for false payment of goods/services they will not really be receiving. Types of credit card frauds are:

  (a) **Stolen Card Fraud:** This happens when someone steals a credit card and makes unauthorized purchases.

  (b) **Credit Card Mail Order Fraud:** This is the case of use of a stolen or made up credit card number to ship goods to an address, in which the cardholder will later call for a chargeback. In this case, the company will be in a loss for the transaction.

  (c) **Mail Non-receipt Fraud:** This is interception of a replacement credit card by an outsider other than the card holder.

  (d) **Chargeback Fraud:** This is a method implemented by the cardholder, in which they claim to never have received the good, service, or perform the transaction.

  (e) **Carding:** This is a process used by the Criminals to verify the validity of stolen cards.

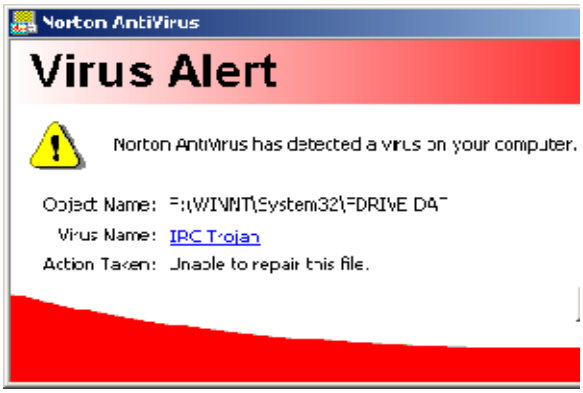
- **Phishing:** Phishing is exactly what it sounds like- fishing out private information. Phishers utilize social engineering techniques such as emails, phone contact, or instant messaging to acquire passwords and personal information. Phishing also includes the use of JavaScript commands to alter the web address. Phishers "SPOOF" innocent victims- meaning they hoax them with misleading information about people, organizations, and intent of the website.

- **Spam and Viruses:** Once Criminals break into someone else's computer, they can steal files or leave bugs and unwanted malicious codes to attack the security system. The image, as shown right, or one that is similar to it, pops up when the security system detects unfamiliarity in the computer. Following is the difference between Spam and Viruses:

  (a) Spam: This is the abuse of electronic message. Criminals utilize spam as a filter for planting viruses. Spam are messages sent in an undesired bulk manner. Various types of spamming

methods are: (1) Email Spam (Because emails do not require permission from the receivers to be sent, this method is most prominent amongst criminals); (2) Instant Messaging Spam (Instant Messaging spam occurs because the Instant Message System provides a 'User Directory' that enables Spammers to retrieve demographic and other private information); and (3) Mobile Phone Spam (As Instant Messaging became popularized, mobile companies installed the program on mobile phones. Beginning in 2003, spammers targeted phones with unsolicited messages and viruses. Not only does this increase phone bill, but it also affects the efficiency of phone).

(b) Viruses: Viruses are the malicious bugs that criminals embed into the heart of security system to destroy data, files, and hard drive.



Viruses can be induced in home-computer use or corporate businesses. Viruses not only harm files but they harm the economy because when injected into the networking system it can cause millions of dollars of damage.

4. SECURITY METHODS:

Electronic Security is any tool, technique or process used to protects a system's information assets. Online Security is the means in which a force protects and adds value to networks and infrastructures. It is protection of information from inside and outside organizations. This is a risk management tool that filters out malicious mediums to increase services and functionality. Since the Internet creation in the 1960's, the many governments have implemented rules & regulations to prevent cyber crime. However, despite all the government can do, it is still vital that users maintain their own security system. Users should take precaution in protecting the information, privacy, and self from any unwanted security breach. Following is the list of tips and advice for the purpose of user protection:

4.1 Tips – Update Frequently:

- Keep the system updated
- Try to scan the system daily for malicious interupters
- Check for software updates, because software continually improves with each occurring problem

Box – 2: Protecting Personal Information

- **Keep an eye out for phony email messages**: Things that indicate a message may be fraudulent are misspellings, poor grammar, odd phrasings, Web site addresses with strange extensions, Web site addresses that are entirely numbers where there are normally words, and anything else out of the ordinary.
- **Don't respond to email messages that ask for personal information**: Legitimate companies will not use email messages to ask for personal information. When in doubt, one can contact the company by phone or by typing in the company Web address into Web browser.
- **Pay attention to privacy policies on Web sites and in software.** It is important to understand how an organization might collect and use personal information.
- **Guard your email address.** Spammers and phishers sometimes send millions of messages to email addresses that may or may not exist in hopes of finding a potential victim. Responding to these messages or even downloading images ensures that one will be added to their lists. Also, there is need to be careful when posting email address online in newsgroups, or online communities.

4.2 Protect while Logging in:

- User ID should have at least 7 characters and some alphanumeric characters (these are more secure than #'s).
- Passwords should be 6-16 characters.
- Passwords should be changed every 90 days.

4.3 Never be too careful:

- *Never* open an email unless you know who it's from and what it is.
- *Never* give out personal information or credit card information online unless you can verify that it is secure.
- *Never* download files from untrusted sources – they are infected with spyware and adware. If you do choose to download, do so first on your hard drive and scan it for viruses.

5. FINAL WORDS:

Internet crime is defined as any illegal activity involving one or more components of the Internet, such as websites, chat rooms, and/or email. Internet crime involves the use of the Internet to communicate false or fraudulent representations to consumers. Today, there is meed to promote, maintain and enhance an effective and proportionate working relationship between industry, government and law enforcement to tackle crime and foster confidence in the use of the Internet.

To sum up, law enforcement must seek ways to keep the drawbacks from overshadowing the great promise of the computer age. Cyber crime is a menace that has to be tackled effectively not only by the official but also by the users by co-operating with the law. *"The founding fathers of internet wanted it to be a boon to the whole world and it is upon us to keep this tool of modernization as a boon and not make it a bane to the society".*

REFERENCES: (Note: The websites listed below were accessed on July 16-17, 08)

1. Bridis, Ted."Government Warns Banks ABout Virus-Like Infections". June 2003. Association Press.
2. Caplan, Jeff., Donnell, Richard.(2006) All About the Internet: Legal Guide, *Guide to Internet Law*.
3. http://en.wikipedia.org/wiki/Internet_crime
4. http://www.crime-research.org/news/02.08.2008/3184/
5. http://www.homeoffice.gov.uk/crime-victims/reducing-crime/internet-crime/
6. http://www.internetcrimes-attorney.com/
7. http://www.accessmylibrary.com/coms2/summary_0286-18262560_ITM
8. http://inisc.org/crime/index.htm
9. Boswell, Wendy.(2006) New York Times Company, "*Black Hat Search Engine Optimization".*
10. http://websearch.about.com/od/seononos/a/spamseo.htm
11. http://www.cert.org/other_sources/viruses.html
12. http://www.fbi.gov/homepage.htm
13. Fiorina, M., Johnson, B., Peterson, P., Voss, D.S. (2005) Civil Liberties, *The New American Democracy* (p. 458). New York: Pearson Education Inc.
14. Glaessner, Thomas C., Tom kellermann, Valerie McNevin. (2004). *Electronic Safety and Soundness.* Washington D.C.: The World Bank.
15. http://www.techweb.com/wire/security/186701001
16. http://www.mttlr.org/volfour/menthe_art.html
17. Smith, R. G., Holmes, M. N. &Kaufmann, P. (1999): Nigerian Advance Fee Fraud., Trends and Issues in Crime and Criminal Justice, No. 121, Australian Institute of Criminology, Canberra.
18. http://www.crime-research.org/analytics/702/2
19. http://www.symantec.com/norton/cybercrime/prevention.jsp
20. http://www.usdoj.gov/criminal/cybercrime/reporting.htm