Nizami e*t al.LGU (IJECI)* 2017

LGU (IJECI)
ISSN: 2522-3429

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol.1 issue1 Oct-Dec 2017

Electronic Crimes and Prevention

Syeda Marrium Nizami[1] and Gulfraz Naqvi[2]
Lahore Garrison University
mariyum002@yahoo.com[1], gulfraz.naqvi@gmail.com[2]

Abstract:

The basic purpose of this article is to make provision for provision of electronic crimes where as it is expedient to prevent unauthorized acts with respect to information systems, and accommodate related offenses, as well as mechanisms for their investigation, prosecution, trail and international cooperation.

Keywords: Electronic crime, Internet, Hacker, Victim

1. Introduction

"Our pursuit of cyber security will not – I repeat, will not – include monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish." [1] .

Internet and World Wide Web works as a backbone for all online services and activities These online services can be accessed anytime from any place where internet service can reach. Internet provides opportunities of significant social benefits but also opens door of crimes for criminals. Websites and emailing in present era are preferred as medium of sharing data and communication as well This communication is not only restricted to personal data but it also includes sensitive data of organizations for whom information security is very important.

Now days, the technology rests with the devices like mobile phones tablets computers, MP3 players' smart watches and other electronic gadgets that can be used to track daily activities of users Most of these devices share internet via wireless devices or share data through Bluetooth to the devices that enable internet. These changes have dramatically changed the affect of nature of crime in the modern world.

A man is linked with crime and criminality since his failure. Crime remains puzzling and ever scrambles to hide itself in the face of advancement. Depending on the nature and extent of crime different democracies have adopted different plans to pact dispute with crime. This one thing is obvious; it is that a nation with high percentage of crime rate cannot benefit , that is so because crime is directionally proportional to the development. This increase in crime rate will leave an adverse social and economic effect on the

environment. Electronic crime is defined as crimes committed (on the) using electronic devices or internet utilizing the personal computers as either a device to accomplish criminal targets or to target a victim. It is very difficult to classify crimes in general, into distinct groups as many crimes evolve on a daily basis. The crimes like rape, murder or theft need not necessarily be separate, in the real world today. However, the computer and the individual behind it as casualties both are similarly involved in electronic or cyber crime; it all depends on the main target and the criminal. Hence, the computer will be looked at as either a target or tool for creating loss.

The term 'cyber crime' is a misnomer.. The concept of cyber crime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law and counterbalanced by the sanction of the state. Before evaluating the concept of cyber crime it is obvious that the concept of conventional crime be discussed and the points of similarity and deviance between both these forms may be discussed.

2. Cyber Crime Includes

Following are the few examples of cyber crime:

2.1 Cyber Stalking

Stalking is a termed used to define online harassments and abuses of all soughts.It includes acts like unwanted attention of someone, harassment or intimidation, unauthorized monitoring of someone's activities. Mostly the stalker is motivated by a desire to control his victims.

2.2 Bot Network

A Bot Network is a cyber-crime where a hacker remotely overtakes computer by using malware. The botnet's originator can command and control the system remotely. Systems can be co-opted into a botnet when they execute malicious software.

2.3 Hacking

The wall street journal has reported that computer hackers have accessed the imagined systems containing designs for a new Air force Fighter jet and have stolen huge amount of information [2]

The journal has also reported that spies have infiltrated imagined the electric power grid and left behind malicious computer code. [3]

U.S intelligence agencies, which have developed capabilities to launch cyber attacks on adversary's information system, have made a move to sounded cautions about a determined adversary could do to critical information system in the United States [4]

In general words hacking means seeking and exploiting weakness and security of a computer system or a computer network by gaining unauthorized access. The person who does hacking is known as hacker. Hacker use computer expertise and some tool or scripts to hack any computer system.

2.4 Cracking

It is indeed very unpleasant feeling if the user come to know that a stranger has broken into his computer system without his knowledge or consent and has tampered precious confidential data and information. If

someone has done it to you, it means you have been targeted by a cracker.

Crackers are different from hackers because hackers may be hired to audit network security or test softwares but on the other hand, crackers do same for their own profit or to harm others

2.5 Phishing

Phishing is defined as the act of acquiring data or information such as user name password financial account details through electronic communication. Phishing is done by producing fake links, messages that possess nothing but address of infection/malware contaminated fake website. The website then lure user to enter their personal data and eventually the user will share his/her data once he enters his info on such websites.

2.6 Voice Phishing

Voice phishing is use to gain access of private, personal and financial information from the public. The term is a combination of "voice" and phishing that uses a landline telephone call to get information.

2.7 Carding

Carding is the act of stealing money using debit/credit card information of victim's bank account.

2.8 E-Mail/SMS Spoofing

A spoofed E-mail/ SMS may be said to be one that fakes its origin. It shows different origin from which actually it was originated. Attacker through that email or sms steals identity of another in the form of email address, mobile phone number etc. and via internet sends message.

2.9 Cross site scripting

Cross-site scripting (XSS) is a type of computer security vulnerability. By cross-site scripting attacker can bypass the predefine access permissions of website. Reflected XSS is the most frequent type of XSS attack. Reflected XSS attack is also known as non-persistent XSS. Scripting languages like java script, VBScript etc are use for Reflected XSS attack.

3 Cyber Squatting

Squatting is gaining possession of unused abandoned or unoccupied domain. Cyber squatting is the act of registering a famous domain name and then selling it to someone who may need that domain at high cost.

3.1 Cyber Crime & Social Networking

Social media is frequently used by cyber criminals to commit online crimes, not only that but it also serve as a platform for carrying out real world crime owing to "over sharing" of these online networking stages. The risk associated with information related to our identity is also high because of social networking sites. Identity information theft can strike anyone who is posting personal information without configuring proper privacy settings. It is estimated that approximately 39-45% of social network users have been victims of profile hacking scam.

3.2 Reasons for Electronic or Cyber Crime

According to "The Concept of Law" 'people are accessible so proper rules are necessary to provide safeguard to them'. Applying this to the cyberspace, we can say

computers are accessible so implementation of proper rules is necessary to provide security to the general population against cybercrime. Following are the reasons for the accessibility of computer:

3.2.1 Data Storage in Small Space

A computer is such a machine, in which very small space to store large amount of data. This makes easy to input or retrieve data or information.

3.2.2 Convenient Access

The reason for digital Terrorism is to assault basic framework, including sites, organizes, and to take data from these Critical Infrastructures to pressurize the legislature and its kin to accomplish political, social or money related goals.

3.2.3 Complicated

The operating systems are made up of millions of codes and the computers work on operating systems. Human personality is broken and it isn't possible that there viability not be a bungle at any progression. Since Human have outlined and composed these codes they are conceivable outcomes that there are some glitches inside the framework. The cyber criminals take benefit of these gaps and cracks into the computer system.

3.2.4 Carelessness

Carelessness is associated with human behaviour the same behaviour of humans serve as a tool to gain control of computer system.

3.2.5 Loss of Witness

Loss of witness is a very accepted & frequent issues as all the data are consistently ruined. Advance collection of information outside the sectional degree additionally crashes the entire course of action of wrongdoing examination.

4. Best Practices for Prevention of Cyber Crime

In an effort to improve security, the Government has developed and is deploying a new intrusion detection system called “Einstein 2.” [5] Einstein 2 will be deployed at participating Federal agency Internet access points. [6] The first full implementation was at the Department of Homeland Security (DHS). [7]

Below mentioned security guidelines and good practices may be followed to minimize the security risk of Cyber crime:

4.1 By updating the Computer

The cyber-attacks can be avoided by keeping operating systems and antiviruses updated because updated computer will be able to deal with latest viruses. However, it will not be enough to protect user from all attacks but it will make information framework security much secure and for hackers it will not be easy to access computer systems.

4.2 By choosing strong passwords

Choosing strong and unique password can ensure data security. Password is like a key to your account and the rule is simple that if your key is strong and secure your account is not an easy meal for any hacker. The user should avoid easy words like names of person city etc. while setting passwords. The password should be combination of upper lower case and alphanumeric letters in a way that no one could be able to guess.

4.3 By protecting computer with security software

Security software commonly includes firewall and antivirus programs. What can be communicated with computer online is controlled by firewall Anti-virus is a software that counters viruses to invade in to systems. A good antivirus software monitor all online activities and warns as soon as it detects any threat to system.

4.4 Online offers are not always too good

Free tool and softwares are also used at times to penetrate viruses into your system. The user must examine the credibility of website and software. Reviews and comments also can help to know the quality before downloading.

4.5 Regular review of bank and credit card statements

The online crimes can be controlled through educating people so they may recognize it after their data is stolen or tried to be hacked. Whenever user observes irregular activities. In such case, one should regularly check banks and credit card's statements.

4.6 Be Social-Media Savvy

Social networking sites like Facebook twitter etc. are prime source of getting information. The user should focus on security setting and it must be ensured that no sensitive data is posted on your profile.

4.7 Secure Mobile Devices

Mobile devices are soft target for hackers, as different application are required to be installed in mobiles for convenience. While downloading applications, always use trusted platform otherwise there is a fair chance of data theft as application could also contain hidden malware.

4.8 Secure wireless network

Wi-Fi networks are vulnerable to intrusion if security concerns are not addressed properly. Public Wi-Fi spots are also used by hackers to trap users by inviting them to free connection.

4.9 Call the Right Person for Help

If computer crime is suspected by a way of identity theft or a commercial scam then immediately report this to local police. If help is needed for maintenance or software installations on computer then consult with authenticated service provider or a certified computer technician.

5. Conclusion

At present criminals have changed their method and have started using advanced technology. In order to deal with cybercrimes all the stakeholders of the society especially the legal and law enforcement authorities will have to take responsibility. Maximum cybercrimes are due to the lack of awareness. This is a duty of Government, print media to educate its public about the dangerous areas of the cyberworld because prevention is better than cure. Cyber Space Security Management has already become an important component of National Security Management, Military Secu- rity Management, Scientific Security Management and Intelligence Management all over the world. However, some countries like India has found a way to stop digital wrongdoings yet (No association with the procedure or past proclamation) the cyber law cannot afford to be

static, it has to change with the changing time.

Cybercrime cannot be fully eradicated from cyber space however; check on cyber irregularities can be kept. It is evident that no law is effective until enforced properly. The fear of being caught works as a barrier to get involved in such unethical activities. In short, prevention of cyber-crimes can be ensured through two steps. First is effective legislation so law enforcement agencies can act accordingly. Second is awareness of public that will not only stop the cyber-crimes in its very start but will also discourage the offenders to trap people.

6. Reference

1 President Barack Obama, Remarks at Release of White House Cyberspace Policy Review (May 29, 2009), available at https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

2 See Siobhan Gorman et al., Computer Spies Breach Fighter-Jet Project, WALL ST. J., Apr. 21, 2009, at A1.

3 See Siobhan Gorman, Electricity Grid in U.S. Penetrated by Spies, WALL ST. J.,Apr. 8, 2009, at A1.

4 See generally NATIONAL RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009).

5 Stephen. G. Bradbury, Principal Deputy Assistant Attorney General, Legal Issues Relating to the Testing, Use and Deployment of an Intrusion-Detection System (Einstein 2.0) To Protect Unclassified Computer Networks in the Executive Branch, Jan. 9, 2009, available at http://www.justice.gov/olc/2009/ e2-issues.pdf. The memo concludes that operation of Einstein 2 does not violate the Constitution or surveillance statutes, and an opinion from the Justice Department's Office of Legal Counsel affirms that conclusion. Legality of Intrusion-Detection System To Protect Unclassified Computer Networks in the Executive Branch, Aug. 14, 2009, available at http://www.justice.gov/olc/ 2009/legality-of-e2.pdf.

6 It is unclear whether this means that Einstein 2 operates on privately owned and Operated equipment or on government equipment. More importantly, it is unclear whether The network points at which Einstein is deployed handle only government traffic or could Carry both government and private-to-private traffic.

7 See Hearing Before the Subcomm. on Tech. and Innovation of the H. Comm. on Sci. and Tech., 111th Cong., at 1, 5 (June 16, 2009) (statement of Dr. Peter Fonash, Acting Dir., Nat'l Cybersecurity Div., DHS), available at http://democrats.science.house.gov/Media/file/ Commdocs/hearings/2009/Tech/16jun/Fonash_Testimony.pdf.