ISSN 2278-3083

International Journal of Science and Applied Information Technology, Vol.7. No.1, Pages : 23-29 (2017)
Special Issue of ICSIC 2017 - Held during 23-24 September 2017 in Amman Arab University, Amman-Jordan
http://www.warse.org/IJSAIT/static/pdf/Issue/icsic2017sp04.pdf

Cybercrimes, Real or Meth?

Prof. Khalid Kaabneh
Department of Computer Science,
College of Computer Science and
Informatics.
Amman Arab University
kaabneh@aau.edu.jo

Dr. Hassan Tarawneh
Dept. of Mobile Computing,
College of Computer Science and
Informatics. Amman Arab
University
hassan@aau.edu.jo

Dr. Issam Al-Hadid
Dept. of Business Information
Technology, College of Information
Technology. Jordan University
i.hadid@ju.edu.jo

***Abstract* - Cybercrimes are responsible for the interruption of normal computer functions and has been known to cause the downfall of many companies and personal entities. This research paper aims to discuss following aspects of Cybercrimes: the definition, why they occur, laws governing them, methods of committing cybercrimes, who they affect, and cybercrime prevention procedures. More specifically, this paper will delve into one main example of cybercrime "hacking". The report will show the usage and progression of technology has amplified different types of crimes such as theft crimes and terrorism. Also, this report will display statistical data which will give an idea of how far cybercrimes has increase over the period of ten years or more.**

Keywords—Hacking, Cybercrimes, Risk, Threat, Data Integrity, vulnerability, User Authentication.

I. INTRODUCTION

In our modern technology-driven age, keeping our personal information private is becoming more difficult. The truth is, highly classified details are becoming more available to public databases, because we are more interconnected than ever. Our data is available for almost anyone to sift through due to this interconnectivity. This creates a negative stigma that the use of technology is dangerous because practically anyone can access one's private information for a price. Technology continues to promise to ease our daily lives; however, there are dangers of using technology. One of the main dangers of using technology is the threat of cybercrimes.

Common internet users may be unaware of cybercrimes, let alone what to do if they fall victim of cyber attacks. Many innocent individuals fall victim to cybercrimes around the world, especially since technology is evolving at a rapid pace. Cybercrimes are any crimes that cause harm to another individual using a computer and a network. Cybercrimes can occur by issues surrounding penetration of privacy and confidentiality. When privacy and confidential information is lost or interrupted by unlawfully individuals, it gives way to high profile crimes such as hacking, cyber terrorism, espionage, financial theft, copyright infringement, spamming, cyber warfare and many more crimes which occur across borders. Cybercrimes can happen to anyone once their information is breach by an unlawful user. (webopedia.com)

According to Norton, "over the last 18 months, an ominous change has swept across the internet. The threat landscape once dominated by the worms and viruses unleashed by irresponsible hackers is now ruled by a new breed of cybercriminals. Cybercrime is motivated by fraud, typified by the bogus emails sent by "phishers" that aim to steal personal information" (Cybercrime 2011) Cybercrimes are responsible for the success of their respective criminal assets and the downfall of many companies and personal entities.

Cybercrimes create an overwhelming task for law enforcement bureaus since they are extremely technological crimes. Law enforcement organizations must have individuals trained in computer disciplines and computer forensics in order to accurately investigate computer crimes or cybercrimes that have been committed. Additionally, many states must modernize and generate legislation, which disallows cybercrimes and outlines suitable penalties for those crimes. Cybercrimes will likely become more frequent with the arrival of advance technologies. It is important that civilians, law officials, and other associates of the justice system are well-informed about cybercrimes in order to diminish the threat that they cause.

The purpose of this paper is to educate individuals who don't know what are cybercrimes and its importance in growing technological advance throughout society. Understanding the threat of cybercrimes is a very pertinent issue because technology holds a great impact on our society as a whole. Cybercrime is growing every day because since technological advancing in computers makes it very easy for anyone to steal without physically harming anyone because of the lack of knowledge to the general public of how cybercrimes are committed and how they can protect themselves against such threats that cybercrimes poses. This paper will discuss several aspects of Cybercrimes including: defining the term, why cybercrimes occur, laws governing them, methods of committing cybercrimes, who is affected, and prevention procedures and many more.

II. DEFINING THE PROBLEM

Currently, when individual talk about cybercrime, they may not understand the extent of these crimes. Many questions arise when the term cybercrime is brought into question. Some questions that arise are, “Does cybercrimes only done via the internet?”, “Cybercrimes are done via computers only?” and so on, however, traditional crimes such as theft and fraud that have been done via physical ways are now been converted into digital resources and are now considered as cybercrimes. But what are cybercrimes?

A commonly accepted definition of this term is that a cybercrime is a “crime committed using a computer and the internet to steal a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs” (Definition of Cybercrimes).However, other definitions have constraints to an expansive meaning to more closely describe the word “cybercrime”. Some of these definitions as follow:

- New World Encyclopedia defines it as “is a term used broadly to describe activity in which computers or computer networks are the tool, target, or place of criminal activity. These categories are not exclusive and many activities can be characterized as falling in one or more categories.” www.newworldencyclopedia.org/entry/Cybercrime.
- Bukisa defines it as “It is this access to the technical specifications of how the Internet and Internet technologies are implemented that allows an attacker to subvert systems, networks and the Internet for their own ends.”www.bukisa.com/articles/206_internet-security-concepts.
- Webopedia defines it as “Cybercrime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cybercrime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cybercrimes when the illegal activities are committed through the use of a computer and the Internet. ”http://www.webopedia.com/TERM/C/cyber_crime.html.

While there are many different definitions of cybercrime they all have a few key concepts throughout. These key concepts are criminal activity and the use or abuse of computers. With these concepts in mind cyber crime can be easily defined as using a computer to commit a criminal act.

III. LAWS OF CYBERCIMES

In this section of this paper we’ll discusses Laws and legislation that governs cybercrime in the United State and within other countries worldwide. This section will highlight some laws and let people know some of the laws that are out there to protect them and some of the amendments to these laws to keep up with the different advancement in technology.

- In the United States

  In the United States, the legislation concerning cybercrimes differs from state to states. In other words, each state has their own way of dealing with different types of cybercrimes being committed on a daily basis. This paper discusses a few of the many Acts and legislations available in the United States that govern cybercrimes.

  Congress combats cybercrimes by enacting several laws such as The Computer Fraud and Abuse Act of 1984 (CFAA). At the time such it was difficult for federal law enforcers to use such legislation to indict anyone because of the difficulty of writing such an Act. The Act however requires major proof that personnel suspect has or have accessed computers without authorization which in turn can be a major limitation. In 1994, the Act was altered again to meet new complications that arose such as malicious codes which at the time were bugs, viruses, worms and other programs that were intended to harm or modify data on a computer. After applying it was now equipped to prosecute any individuals who broke the law in terms of using programs with the intent to reason harm to the computer or the use of structures without the information of the lawful owners of that computer.

In 2002, Cyber Security Enhancement Act was passed. The Act helped law agencies to increase punishments which were set out in the CFFA which in turn means hasher punishments for individuals who willingly committed computer crimes in the end result of even bodily injuries etc. Those punishments can range from 5 to 20 years, or even life imprisonment.

- Internationally

  All laws aren't the same in many countries especially when it comes to cybercrimes. For different countries have specific laws governing problems such as cybercrimes. For example, in some countries such as India accepted. The Information Technology Act which was passed and enforce in 2000 on Electronic Commerce by the United Nations Commission on Trade Law. However, the Act states that it will legalize e-commerce and supplementary modify the Indian Penal Code 1860, the Act 1872, the Banker's Book Evidence Act1891 and the Reserve Bank of India Act 1934.

IV. CAUSES OF CYBERCRIMES & METHODS OF COMMITTING

There are many ways or means where cybercrimes can occur. Here are a few causes and methods of how cybercrimes can be committed on a daily basis: Hacking, Theft of information contained in electronic form, Email bombing, Data diddling, Salami attacks, Denial of Service attack, Virus / worm attacks, Logic bombs, Trojan attacks, Internet time theft, and Web jacking. (http://www.naavi.org/pati/pati_cybercrimes_dec03.htm).

- Hacking: In other words can be referred to as the unauthorized access to any computer systems or network. This method can occur if computer hardware and software has any weaknesses which can be infiltrated if such hardware or software has a lack in patching, security control, configuration or poor password choice.
- Theft of information contained in electronic form: This type of method occur when information stored in computer systems are infiltrated and are altered or physically being seized via hard disks; removable storage media or other virtual medium.
- Email bombing:This is another form of internet misuse where individuals directs amass numbers of mail to the victim or an address in attempt to overflow the mailbox, which may be an individual or a company or even mail servers there by ultimately resulting into crashing. There are two methods of perpetrating an email bomb which include mass mailing and list linking.
- Data diddling: Is the changing of data before or during an intrusion into the computer system. This kind of an occurrence involves moving raw data just before a computer can processes it and then altering it back after the processing is completed.
- Salami attacks: This kind of crime is normally consisting of a number of smaller data security attacks together end resulting in one major attack. This method normally takes place 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. This form of cybercrime is very common in banks where employees can steal small amount and it's very difficult to detect or trace an example is the "Ziegler case" wherein a logic bomb penetrated the bank's system, which deducted only 10 cents from every account and deposited it in one particular account which is known as the "penny shaving".
- Denial of Service attack: Is basically where a computer system becomes unavailable to it's authorize end user. This form of attack generally relates to computer networks where the computer of the victim is submerged with more requests than it can handle which in turn causing the pc to crash. E.g. Amazon, Yahoo. Other incident occurs November, 2010 whistle blower site wikileaks.org got a DDoS attack.
- Virus / worm attacks: Viruses are programs that can embed themselves to any file. The program then copies itself and spreads to other computers on a network which they affect anything on them, either by changing or erasing it. However, worms are not like viruses, they do not need the host to attach themselves to but make useful copies of them and do this constantly till they consume up

all the available space on a computer's memory. E.g. love bug virus, which affected at least 5 % of the computers around the world.

- Logic bombs: They are basically a set of instructions where can be secretly be execute into a program where if a particular condition is true can be carried out the end result usually ends with harmful effects. This suggests that these programs are produced to do something only when a specific event (known as a trigger event) occurs. E.g. Chernobyl virus.
- Trojan attacks: The term suggests where a program or programs mask themselves as valuable tools but accomplish damaging tasks to the computer. These programs are unlawful which flaccidly gains control over another's system by assuming the role as an authorised program. The most common form of a Trojan is through e-mail. E.g. lady film director in the U.S.
- Internet time thefts: This form is kinds of embezzlements where the fraudulent uses the Internet surfing hours of the victim as their own which can be complete byobtaining access to the login ID and the password, an example is Colonel Bajwa's case- in this incident the Internet hours were used up by a unauthorized person.
- Web jacking: This is where the hacker obtains access and can control web site of another person, where he or she can destroy or alter the information on the site as they see fit to them. This type of method of cybercrime is done for satisfying political agendas or for purely monetary means. An example of such method was MIT (Ministry of Information Technology) was hacked by the Pakistani hackers whereas another was the 'gold fish' case, site was hacked and the information relating to gold fish was altered and the sum of $ 1 million was demanded. http://www.naavi.org/pati/pati_cybercrimes_dec03.htm.

V. THEFT CRIMES AND CYBER TERRORISM

Cyber terrorism may be defined to be where the deliberate use of disrupting activities, or the risk thereof, via virtual machine, with the purpose to further public, political, spiritual, radical or to threaten any person in continuance of such purposes. (Denning, D)Theft crimes can include: Credit/Debit Card Fraud, Identity theft, Non – delivery of Goods and Servives, Phony Escow Services, Ponzi/Pyramid method.
(http://www.horizonsfcu.com/content.php?c_id=26)

- Credit/Debit Card Fraud-is the unlawful use of a credit/debit card to falsely attain money or belongings. Credit/debit card numbers can be stolen from leaky web sites, or can be obtained in an identity theft scheme.
- Identity theft –this is when someone seizes another's individual information without his or her awareness to commit theft or fraudulency. Typically, the victim is led to believe they are revealing sensitive private data to a genuine business, occasionally as a response to an e-mail to modernize billing or membership information etc.
- Non-delivery of Goods and Services-goods or services that were acquired by individuals online those were never sent.

VI. REAL LIFE EXAMPLES

In terms of companies losing money due to cybercrimes here are some cases where cybercrimes had the upper hand. For example, in 2007 it was reported that TJX systems network was illegally accessed. Reportedly 45.6 million credit and debit card numbers were stolen over a period of more than 18 months by an unknown number of intruders who leave was relieved to be Albert Gonzalez. In the wake of that breach, several analysts have estimated TJX's costs could run as high as $1 billion, including legal settlements and lost sales. Another example was a former network engineer at Gucci was charged with hacking into the company's network, deleting data and shutting down servers and networks. Sam Yin, 34, of Jersey City, N.J., used an account he secretly created while employed by the luxury retailer to access the network after he was fired in May 2010. Yin created a VPN token in the name of a fictional employee and took it with him after being fired. On Nov. 12, Yin broke into Gucci's network and deleted several virtual servers, shut down a storage area network and erased from an email server a disk containing corporate mailboxes. Yin's actions cost Gucci more than $200,000 in diminished productivity, restoration and remediation expenses. Then another case was with David L. Smith in Aberdeen Township, New Jersey created the Melissa virus first appeared on the internet in March of 1999. It spread rapidly throughout computer systems in the United States and Europe. It's estimated that the virus caused 80 million dollars in damages to computers worldwide. Listed below is a graph of how

ISSN 2278-3083

International Journal of Science and Applied Information Technology, Vol.7. No.1, Pages : 23-29 (2017)
Special Issue of ICSIC 2017 - Held during 23-24 September 2017 in Amman Arab University, Amman-Jordan
http://www.warse.org/IJSAIT/static/pdf/Issue/icsic2017sp04.pdf

cybercrimes affected individuals around the U.S. in recent times:

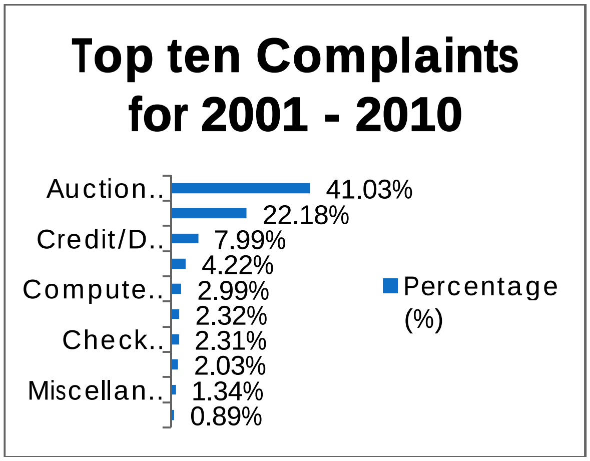


Fig. 1: Top 10 IFCC taken from IC3 reports.

According to the IC3 report the following chart above show the top ten (10) complaints or attack that is surfacing the internet today and throughout the years of 2001-2010 However, each year was different from each other mainly to deal with the latest in technology at the time and how easy some infrastructure could have been penetrated at the time. However, what is stable all through the years was the cyber-attack of Auction Fraud which is almost 41.03 %. This attack is very popular due to many individuals using the internet to purchase goods and services throughout the world on a daily basis for any needs and essentials.

The next popular attack and still is the Nigerian Letter Fraud, here goods or services that were acquired by individuals online those were never sent or the seller never receive payment for goods. The rest of the different attacks are range from .89 % to 7.99 % however, still play a big role in cybercrimes such as credit card fraud which was a next upcoming major attack in today society where it is the unlawful use of a credit/debit card to falsely attain money or property. Credit/debit card numbers can be stolen from leaky web sites, or can be obtained in an identity theft scheme.

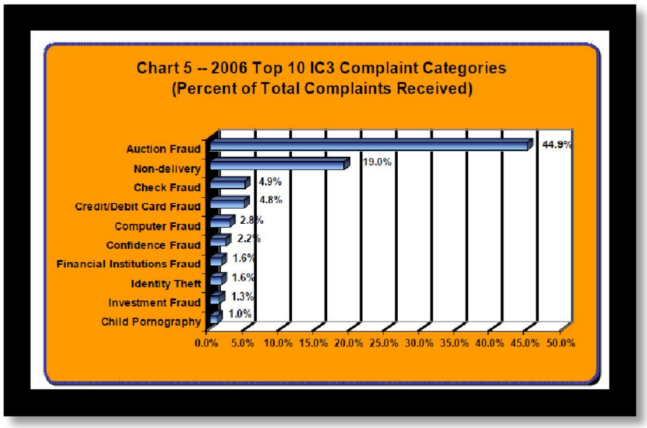


Fig. 2: 2006 Top 10 Complaints from IC3 reports.

The chart above showed the complaint category from 2006. From the chart it can be seen that most of all the complaints came from auction fraud which can be easily taken placed on any website such as eBay or Amazon for such base cybercrime attacks. The chart above is basically stating the percentage of each top ten complaints category that has been surfacing the internet throughout the year of 2006. At the time, cybercrime or attacks like child pornography, investment fraud, identity theft, financial institution fraud, confidence fraud, and computer fraud was at a minimum. However, Auction fraud and non delivery cybercrime attacks was on a rise during that year.

Figure 2: Yearly Comparison of Complaints Received Via the IC3 Website

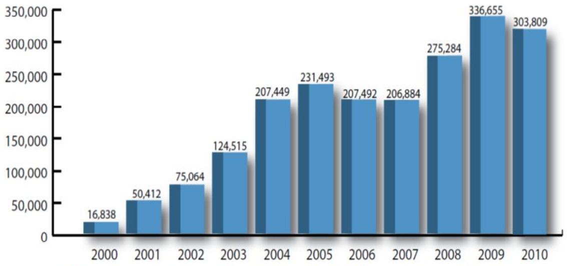
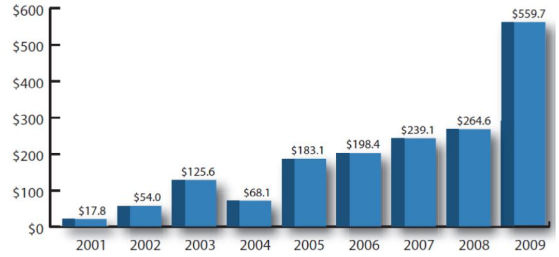


Figure 2: Yearly Dollar Loss (in millions) of Referred Complaints



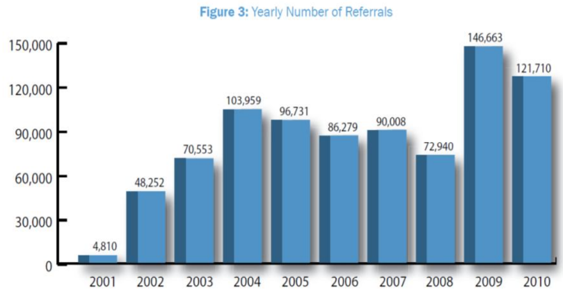


Fig. 3: Yearly loss, complaints, and referrals - IC3 reports.

VII. PREVENTION & PROCEDURE

In this modern age, it seems almost impossible to avoid being a victim of cybercrime, with all the advancements in technology which make it easy for someone to perform cybercrimes. In light of this, there are some ways however to avoid becoming a victim of cybercrime. Most internet browsers email service, and Internet providers provide a spam-blocking feature to prevent unwanted messages, such as fraudulent emails and phishing emails, from getting to your inbox. However, every user must ensure to turn them on and do not turn them off whatsoever. Also, users must install and keep up-to-date antivirus programs, firewalls and spyware checkers. Along with keeping them up to date, users must make sure that they run the scans regularly. There are many companies out there that provide free software, but there are other you can purchase, along with that of the many produced by the leading companies providers; in addition, those companies provide free version of their paid or subscription antivirus software. Encryption of information that you do not want anyone to have unauthorized access to is a good way to avoid some cybercrimes; information such as password and credit card information for example. Encryption software runs your data through encryption algorithms to make it unintelligible to anyone who tries to hack into your computer.

Another good precaution is to be weary of who you divulge your personal information to. Try to avoid unknown websites, in particular those that ask for your name, mailing address, bank account number or social security number. When doing online shopping make sure website is secure, look for urls that starts with "https" and/or have the Trustee or VeriSign seal. If you do not see these anywhere on the site, you run the risk of submitting credit card information and other personal information to a site that maybe a fraud.

Another way to avoid being a victim of cybercrimes is to avoid being susceptible to common frauds, such as inherences letter, letter asking for your help in placing large sums of money in overseas bank accounts, foreign lotteries, and phony sweepstakes. Those mentioned activities are all methods used by cyber criminals to get your personal information and money. If it sounds too good to be true, it probably is. Educate children about the proper use of the computer and internet and make sure to monitor their online activities at home and school alike. They should only have access to a computer located in a central area of your home and you should regularly check all browser and email activity. A wise thing to is to use parental control software that limits the type of sites the user can gain access to. In schools, there should be restricted websites and other user restrictions that will help protect the user and entity from cybercrime. Likewise, companies should educate and have written policies governing the workplace pc and its network use to diminish the risk of cybercrime against the company.
One definite way to ensure that you don't fall victim of cybercrimes is to disconnect your computer entirely from the internet. If there is no network, then you don't have to worry about any cyber-attacks. However, this option is not the most viable one in our interconnected society. The truth is, it is up to you to take the necessary precautions to avoid potential cybercrimes.

VIII. CONCLUSION

Cybercrimes will always be an ongoing challenge despite the advancements being made by numerous countries. Most countries have their own laws to combat cybercrimes, but some doesn't have any new laws but solely relies on standard terrestrial law to prosecute these crimes. Along with outdated laws to combat cybercrime, there are still feeble penalties set in place to punish criminals, thus doing no major prevention of cybercrimes' which affect the economy and people's social lives on a large scale by those criminals. Consequently, there is a desperate need for countries on a global scale to come together and decide on what constitute a cybercrime, and develop ways in which to persecute criminals across different countries.

It is recommend that until sufficient legal actions can be put in place where individual countries and global ways of persecution criminals, self-protection remains the first line of defense. The everyday individuals and businesses need to make sure they are educated on what to do in terms of prevent in becoming the next victim of cybercrimes. This basic awareness can help prevent potential cybercrimes against them.

It is almost impossible to reduce cybercrime from the cyber-space. Looking back on the many different acts passed, history can be witness that no legislation has thrived in total elimination of cybercrime from the world. The only possible step is to make people aware of their rights and duties and further making more punishable laws which is more stringent to check them. Undoubtedly, the different Acts were and still are historical steps in the virtual world as we know it. This further suggests that there is a need to convey modifications in the Information Technology Act so it can be more effective to fight cybercrimes. Caution should be employed for the pro-legislation educational institutions that the requirements of the cyber laws are not prepared so rigorous that it may delay the growth of the commerce and demonstrate to be counter-productive to many. Remember, cybercriminals are evolving as well in terms of computer knowledge per technological advancement made.

REFERENCES

[1] Center, Finjan Malicious Code Research. "Web Security Trends Report." Securing your web (1996-2008): 1-20.

[2] eSecurity Planet. 2011. 16 January 2011 <http://www.esecurityplanet.com/trends/article.php/3871456/Cyber-Crooks-Doubled-Their-Take-in-09-FBI.htm>.

[3] Al_Zyadat, W., Al-Zyoud, F., and Alhroob , A.,Smooth Handoff Process Cluster_Based In Vehicular Ad Hoc Networks, International Journal of Computing Academic Research (IJCAR), Vol. 6(3), 101-109, 2017.

[4] Justice, Bureau of Justice Assistance U.S. Department of. "Internet Crime Complaint Center." 2009 Internet Crime Report (2008): 1-26.

[5] Phil Williams, Cert Coordination Center. "Implications for Business." Organized Crime and Cyber-crime (2002): 1-7.

[6] SOPHOS. "SOPHOS." Security Threat Report 2009 (2008): 1-20.

[7] Vanlalnunsanga, M. (n.d.). Statistical Report on Cyber Crime. Retrieved 01 29, 2011, from Scribd: http://www.scribd.com/doc/19720457/Statistical-Report-of-Cyber-Crime

[8] KSHETRI, NIR. "Positive Externality, Increasing Returns, and the Rise in Cybercrimes." Communications of the ACM 52.12 (2009): 141-144. Academic Search Premier. EBSCO. Web. 22 Jan. 2011.

[9] Wall, David S. "Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace." Police Practice & Research 8.2 (2007): 183-205. Academic Search Premier. EBSCO. Web. 25 Jan. 2011.

[10] "TREND MICRO 2011 THREAT PREDICTIONS." Computer Security Update 12.1 (2011): 1-3. Academic Search Premier. EBSCO. Web. 14 Jan. 2011.

[11] Wall, David S. "Catching Cybercriminals: Policing the Internet." International Review of Law, Computers & Technology 12.2 (1998): 201-218. Academic Search Premier. EBSCO. Web. 19 Jan. 2011.

[12] Khalid A. Kaabneh, “High Fidelity Image Watermarking Using FWT by Exploiting the RGB and HSV Models”, International Journal of Computer Technology and Applications (IJCTA), V. 5(2), April 2014.

[13] ror.html)

[14] Ghosh, Sumit. "The Nature of Cyber-attacks in the Future:A Position Paper." Information Systems Security 13.1 (2004): 18-33. Academic Search Premier. EBSCO. Web. 19 Jan. 2011.

[15] Stephens, Gene. "CYBERCRIME IN THE YEAR 2005." Futurist July 2008: 32+. Academic Search Premier. EBSCO. Web. 15 Jan. 2011.

[16] Wall, David S. "Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime." International Review of Law, Computers & Technology 22.1/2 (2008): 45-63. Academic Search Premier. EBSCO. Web. 18 Jan. 2011.

[17] Kaabneh, K., Tarawneh, H., Alhadid, I., Encrypted data Inquiries Using Chained Perfect Hashing (CPH), In International Conference on Mathematical Methods & Computational Techniques in Science & Engineering, University of Cambridge, UK., 2017.

[18] Al-Hadid, I., Khwaldeh, S., Kaabneh, k., Tarawneh, H., Efficient Big Data Transfer Technique for Static Routing Networks, International Journal of Applied Engineering Research, Vol 12 (9), pp 2071-2078, 2017.

[19] Gomolski, Barb. "Mr. President, cybercrime is much more than just a pesky computer virus." InfoWorld 23.13 (2001): 98. Academic Search Premier. EBSCO. Web. 22 Jan. 2011.