International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 3 (September '2017)
Proceeding of - International Conference on Recent Trends in Computational Life Science and Information Technology,
Conference held at Tiruppur Kumaran College for Women,Tirupur,Tamilnadu, India.

CYBER CRIME AND SECURITY

D.Kaviya vikashini,
PG Student,
Tirupur Kumaran College for women,
Tirupur,Tamilnadu,India.

P.Sangeethaa,
Software Tester,
Cognizant Technology Solutions,
India.

K.Umaiyal,
PG Student,
G.R.Damodaran College of Science,
Coimbatore,Tamilnadu,India.

Abstract: The emergence of new types of crime as well as the commission of traditional crimes by means of new technologies is called as "Cyber-crime". Computer crime is defined as criminal activity involving an information technology infrastructures including illegal access like unauthorized access, illegal interception is done by technical means of computer data from or within a computer system, data interference like illegal damaging, deletion, deterioration, modification or suppression of computer data, systems interference like interfering with the functioning of a computer system by inputting, transmitting, damaging, misuse of devices, forgery is also called as ID theft . Cybercrime is a relatively new phenomenon. Services such as telecommunications, banking and finance, transportation, electrical energy, water supply, emergency services, and government operations rely completely on computers for control, management, and interaction among themselves. Cybercrime would be impossible without the Internet. . Other than computer viruses, specific crimes dealing with computers and networks (such as hacking) and the facilitation of traditional crime through the use of computers (child pornography, hate crimes, telemarketing/Internet fraud).

Keywords: Cyber crime, Cyber security,Hacking, Transactions

I. INTRODUCTION

The development of technology has made human beings dependent on Internet for all his needs. Social networking, online shopping, storing data, gaming, online studying, online jobs, every possible thing that man can think of can be done through the internet.With the development of internet, cyber crimes are also highly-developed. Cyber crimes are committed in different forms. A long time back, there was lack of awareness about the crimes that could be committed through internet. In the matter of cyber crimes,where the rate of incidence of cyber crimes India is also increasing day by day.
In a survey published by the National Crime Records Bureau report (NCRB 2011), the incidence of cyber crimes under the IT Act has enlarged by 85.4% in the year 2011 as compared to 2010 in India, whereas the growth in incidence of the crime under IPC is by 18.5% as compared to the year 2010. Visakhapatnam records the maximum number of incidence of cases. Maharashtra has rise up as the center of cyber crime with maximum number of incidence under cyber crimes. Hacking with computer systems and obscene publication were the main cases under IT Act for cyber crimes.[1]

II. EXAMPLES OF CYBER CRIME

Identity Theft

One ordinary form of cyber crime is identity theft. Hackers and scammers may use fake emails to trick victims into giving up passwords and account information, or they may use specialized programs called key loggers to track what a user types when logging into bank or credit accounts. Once they have this personal information, they may be able to access existing accounts or make purchases with the victim's credit cards. If a hacker can discover a user's social security number and other identifying information, he can parlay that data into credit accounts in the victim's name and cause considerable damage.

Transaction Fraud

Simple economic fraud is another common crime in the online sector. A scammer may offer an item for sale through an auction site with no intention of delivering once he receives payment. Alternatively, a criminal might purchase an item for sale using a stolen credit card, or claim a fraudulent chargeback after receiving the goods.

Hacking

Another cyber crime is the practice of hacking, illegally circumventing security to access someone else's computer system. Some hackers explore for sheer curiosity, finding their way into unfamiliar systems for love of the challenge, in some cases going so far as to alert system owners to security loopholes. Others hack for their own reason, either to steal information, gain control over systems for their own purposes, or simply to cause as much damage and disorder as possible.

Piracy

Piracy is the copying and distribution of programs, movies, music or other intellectual property without permission. Groups of dedicated pirates take the source material, remove

any protection the data might have and then pass the unprotected results on to file sharing networks and distribution sites. The movie and recording industries in particular have fought the misuse of their intellectual property by filing extensive lawsuits against file sharers, while software companies fight piracy through expanded and intrusive copy protection schemes.[7]

Other Crimes

Other crimes which exist in the real world may also take place online. Those who trade in child pornography, for instance, often take advantage of the anonymity provided by the Internet when interacting with their fellow criminals. The drug trade also has an online module, as dealers use alternative currency and nameless Web providers to peddle their goods. Even users looking for legal drugs may find a gray market on the Internet where they can purchase medicines without a prescription from other countries, although in some cases these sellers may provide expired, inaccurate, or even dangerous compounds to unwitting purchasers.[2]

III. CYBER SECURITY

Cyber security also known as computer security which protects the computers, networks and data from unauthorized access.[3]

Necessity of Cyber Security

Information is the most valuable asset with respect to an individual, cooperate sector, state and country. With respect to an individual the concerned areas are:

- Protecting unauthorized access, disclosure, modification of the resources of the system.
- Security during on-line transactions regarding shopping, banking, railway reservations and share markets.
- Security of accounts while using social-networking sites against hijacking.
- One key to improved cyber security is a better understanding of the threat and of the vectors used by the attacker to circumvent cyber defences.
- Need of separate unit handling security of the organization.
- Different organizations or missions attract different types of adversaries, with different goals, and thus need different levels of preparedness.
- In identifying the scenery of the cyber risk an organization faces, the interplay of an adversary's capabilities, intentions and targeting activities must be considered.[6]

IV. VPN

VPN stands for virtual private network. It is designed to protect personal information every time we go online. They are usually used as means to surf the web anonymously due to the fact that VPNs mask your real IP address which is used to track your online activity and trace your location.VPN protect you from vicious cyber crimes like identity theft and fraud in which millions of citizens regularly fall victim to.[4]

Through VPN, the data we send and receive over the network is highly *encrypted*. Even though if we connect to insecure public networks. For instance, if you are in a public place and connect to their public network using a VPN, a person with a malicious Web browser plug-in won't be able to track your online activities, or obtain your personal information. Sensitive information like username and password of your bank account, will be routed through the VPN tunnel and encrypted before reaching the specified destination onto the internet. Therefore, if a person tries to access that sensitive information, they will only find the inaccurate, encrypted data instead of your real personal information. Moreover, VPN service provider today alert their user when such malicious action takes place.

Many VPN services nowadays protect their users by anti-malware, anti-spyware software. In other cases, if you accidentally download a virus on your computer, your VPN will stop the download before the affected file is transferred to our computer. Stealing passwords and usernames through anti-virus software, anti-phishing software are also avoided by VPN services. VPN is one of the security measure which protects the data from cyber crime.[5]

V.CONCLUSION

As cyber crimes are growing in a large scale it affects individuals, businesses and national security. Cyber security measures were taken to find out the possible solution. And there is a need to create awareness among the people and educating them on being safe online and to know about the pros and cons of the internet usage. Different countries should work together to combat cybercrime to reduce the damage to critical infrastructures and to protect the internet from being abused.

VI.REFERENCES

[1] https://techterms.com/definition/cybercrime
[2] http://cybercellmumbai.gov.in/html/cyber-crimes/index.html
[3] https://www.fireeye.com/current-threats/what-is-cyber-security.html
[4] https://www.hotspotshield.com/resources/what-is-a-vpn/
[5] https://www.techhive.com/article/3158192/privacy/howand-whyyou-should-use-a-vpn-any-time-you-hop-on-the-internet.html
[6] https://securitycommunity.tcs.com/infosecsoapbox/articles/2016/02/22/necessity-cyber-security-and-risk-management-todays-digital-era
[7] http://www.thewindowsclub.com/types-cybercrime