INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

THE STUDY OF PROGRESSION OF TECHNOLOGY AND THEIR AMPLIFICATION OF DIFFERENT TYPES OF CYBERCRIMES

RUTUJA S. DESHPANDE.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: Due to the increasing use of Internet a huge number of cybercrimes are occurred and it is very difficult to know their behavior as well as understand them hence it is difficult to restrict the victimization in the early phases of the cyber-attacks. Cybercrimes are responsible for the interruption of normal computer of normal computer functions and has been known to cause the success of many companies and personal entities. The perception of risk has been established an important part of the study of human aspects of security research. This research paper will show the usage and progression of technology has amplified different types of crimes such as theft crimes and terrorism. This paper will display the data about the cybercrime has increase over the period of 10years or more as well.

Keywords: Cybercrimes, Technology

PAPER-QR CODE

Corresponding Author: MS. RUTUJA S. DESHPANDE.

Access Online On:

www.ijpret.com

How to Cite This Article:

Rutuja S. Deshpande, IJPRET, 2016; Volume 4 (9): 487-493

INTRODUCTION

The Internet system includes and connects local, regional, national and international networks. The benefits of Internet or Network technology are numerous, starting with its unique suitability for sharing information and ideas. In our modern technology-driven age, keeping our personal information private and secure is becoming more difficult. The truth is highly classified details are becoming more available to public database, because we are more interconnected than ever. Our data is available for almost anyone due to interconnectivity. Technology promise to ease our daily lives continuously; however there are dangers of using technology.

Cybercrime are any crime that cause harm to another individuals using a computer and network. Cybercrimes can occur by issues surrounding penetration of privacy. When privacy is lost by unlawfully individuals, it gives way to high profile crimes such as hacking, cyber terrorism, spamming, and warfare.

Now a day, E-mails have displaced traditional letters, online web representation is more important for businesses than printed publicity materials. The availability of ICTs and new network based services offer a number of advantages for society. In general, especially for developing countries.

Harassment via E-mails, sending letters, attachment of files and folders it’s a common type of harassment. At present, harassment is common as usage of social sites i.e. facebook, Twitter etc increasing day by day.

According to Norton,” Over the last 18 months, an unpleasant change has swept across the internet. The threat landscape once dominated by the worms and viruses starts by irresponsible hackers is now ruled by a new breed of cyber criminals. Cybercrime is motivated by fraud, typified by the bogus E-mails sent by” Phishers” that aims to steal personal information.”

“The challenge is not to enable the individual’s mastery of an application so much as to convince the individuals to avoid digital risks by adopting appropriate security tools and application settings, despite the financial and time costs of doing so.”

Materials & Methods

The term Cybercrime is most important for today’s technological world. There are so many ways where cybercrimes can occur. Generally the theft & nuisance over the web is major concept of cybercrime but recent technology move towards the sentimental nuisance. The major types of cybercrime & their methods are discussed below:

1. **Hacking**:

It is referred to as the unauthorized access to any computer system. This method can occur if computer hardware or software has poor password choice, security control configuration.

Example of hacking include breaking the password of password-protected websites.But acts relataed to the term”Hacking” also include acts such as the use of faculty hardware or software implementation to illegally obtain a password to enter a computer system,setting up “Spoofing”website.

Three main factors have supported the increase number of hacking attacks:

1. Inadequate and incomplete protection of computer system

2. Development of software tools that automate the attacks and

3. The growing role of private computers as a target of hacking attacks.

2. **Phishing**:

Another form of fraud activity is the use of Phishing. Phishing is occurs when an identify criminal goes online and poses as a corporation. For example, amazon, eBay or Paypal. An individuals in need and requests personal information. Phishing include financial transfers, credit card frauds etc.

3. **Web Jacking**:

Web jacking occurs where the hacker obtains access and control website of another person where he or she can destroy or alter the information. Attackers that are using this method are creating a fake website and when the victim opens the link a page appears with the message that the website has moved and they need to click another click. If the victim clicks the link that looks real. Then he or she will redirect to the fake page.

Such method was MIT (Ministry of Information Technology) was hacked by the Pakistani hackers.

4. Logic Bombs:

It is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are meeting. e.g. A programmer may hide a piece of code that starts deleting files such as salary database trigger.

These are basically contains a set of instructions where he or she can be secretely execute into a program. If a particular condition is true can be carried out the end results usually ends with harmful effect.

Symentec reported that the malware also contained a component that was capable of wiping Linux machines.

5. Internet times Thefts:

This type occurs at the time of access to the login ID and the password. For example: In Colonel Bajwa's case-incident the internet hours were used up by a unauthorized person. Logging in to a social network site was chosen because it is very common activity and is often paid little attention to or even preveived as annoying.It suffers from the common problem of IT security mechanism, science it is a barrier keeping users from achieving their primary goal, which in this case is to take in a social networking site.

RESULTS & DISCUSSION

1. Effects on technical fields (**Technology):**

The growth of information society is accomplished by new and serious threats. Cars, traffic control, air conditioning and telephones also depend on the smooth functioning of ICTs 23(Information and Communication Technology). Online fraud, online banking, online shopping, hacking attacks are some examples of computer related crimes that are committed on a large scale every day. The financial damage caused by cybercrime is reported to be large.

2. **Effects on Market**:

The internet allows for illicit (not allowed) markets to be created and maintained. The internet provides its users with an opportunity to hide their identities. For instances, Cyber criminals can use different website to trade goods illegally through various sources.

3. Effects on Youth or Young Generation:

The Indian youth have immediately taken to social networking sites. Some of them have gone to the great extent of getting addicted to the social networking sites like Facebook, twitter, Orkut, MySpace etc. In so many crimes, girls and young woman's or younger's are to be target of attack for cyber criminals too. So many younger's who were more affected by cyber criminals undergoes severe mental pain or disorders, depression. They are not even in a position to share their cyber problems with others.

Hence, the need of the proper way of awareness to all youth who interact or communicate through social networking sites. And this could be achieved only through a perfect co-ordination between parents, teachers.

Laws of Cybercrime:

The evolution of information Technology (IT) gave birth to the cyberspace.

Though the word crime carries its general meaning as "a legal wrong that can be followed by criminal proceedings which may results into punishment." Whereas cybercrime may be "unlawful acts wherein the computer is either a tool or target or both."

The world 1st computer specific law was enacted in year 1970 by German state of Hessen in the form of "Data Protection Act",1970'. With the advancement of cyber technology. It is under the circumstances of Indian parliament passed it's "Information Technology act,2000' on 17th October to have its exhaustive law to deal with the technology in the field of e-commerce, e-governance, e-banking as well as punishments in the field of cybercrimes.

In 1998, The Digital Millennium Copyright Act was passed. This Act basically altered Title 17 of the United States code to WIPO (World Intellectual Property Organization) which was to combat with new technology. This Act excludes the modification of information of inventor, the terms and environments for use of such set work or the purpose of its intent. The act provides a way in which civil preparations can be applied as well as criminal punishments for violation.

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.

Cyber Security:

An anti cybercrime strategy should be an integral element of cyber security strategy. The ITU global cyber security agenda, as a global framework for dialog and International Corporation to coordinate the international response to the growing challenges to cyber security and to enhance confidence in the information society.

Hence to maintain security use platform based Authentification and Authorization, Avoid storing sensitive data in hidden fields, use managed code, avoid use of weak cryptography, run with least privilege account etc.

Awareness of Own Negligence and Mistakes:

It is the most common thing that arising due to own mistakes or negligence. Users may "Leaving an account logged in" or "choosing a weak password" stated as a risk. Particularly weak passwords are a risk which security professionals and researchers have tried to get the general population to take seriously for a very long time. Users are not aware that they are actually doing these and other security-relevant activities wrong.

CONCLUSION:

The cybercrime as a whole refers crime that are committed against individuals with a criminal motive which is harm the reputation of the victim or cause physical or mental harm, harms the modern technologies telecommunication networks such as Internet(emails) and mobile phones(SMS).Such crimes may threaten a nations security and financial health.

A computer can be a secure of evidence. The everyday individuals and business need to make sure they are educated on what to do in terms prevent in becoming the next victim of cybercrimes.

The basic awareness can help to prevent potential cybercrime against them. To enforce effective cyber security, there is a critical need to develop integrated and inter-locked policies. These policies need to be developed through a consultative and collaborative process across public sector, private sector and civil society, bringing together expiries from health sector, education sector, technology and related institution, and the important is, the young digital citizens who are the greatest users of ICTs need to be directly involved in developing cyber security solutions.

Hence, there is need to convey modifications in the information Technology act, so it can be more effective to fight cybercrimes. Safety practices like, at the time of game sites viruses can be downloaded, password sharing, forwarding chain of emails should be prohibited.

REFERENCES:

1. Shilpa Yadav,Tanu Shree, yashiks Arora-nternational Journal of Scientific and engineering research , Volume 4,Issue 8,August 2013,ISSN 2229-5515.

2. Elne Paryag and Ashre Griffin-IT Capstone research paper

3. Nadia haque-Asian Science Volume 8,E-ISSN 1911,November 2012.

4. J.Blythe,J.Camp snd V.Garg,"Targeted Risk communication for Computer security ,"in Proc.IUI,2011.

5. Marian Harbach, Sascha Hahl, Mattew Smith 27th computer security foundation Symposium IEEE 2014.

6. Vineet Kandpal and R. K. Singh; "Latest Face of Cybercrime and Its Prevention In India"; in International Journal of Basic and Applied Sciences Vol. 2. No. 4. 2013. Pp. 150-156

7. Goldenberg, J, Libai, B, Muller, E: Talk of the network: a complex systems look at the underlying process of word-of-mouth. Marketing Letters. 12(3), 211–223.

8. Salma Abbasi and Myra Manawar e Worldwide Group.