"Education through self help is our motto" - KARMAVEER

National Level Seminar

on

"Cyber Crime And Cyber Security" (CCACS-2017)

15th & 16th December 2017

Sponsored By

B.C.U.D.,Savitribai Phule Pune University, Pune

Organized by

DEPARTMENT OF COMPUTER SCIENCE

Rayat Shikshan Sanstha's

R. B. Narayanrao Borawake College, Shrirampur

Dist- Ahmednagar - 413 709 (MS) India

Phone: (02422) 222347

Email ID: rbnbcollege@gmail.com **Website:** www.rbnbcollege.com

ISBN: 978-81-932117-9-3

Proceeding

INDEX

CYBER SECURITY AND CYBER CRIME

Mr.Chandratre Y.V
HOD, Computer Dept.
C. D. Jain College of Commerce
E-mail :cyogiraj@gmail.com
Cell : 9404245561

Mr. Lande R.D.
Assistant Professor
C. D. Jain College of Commerce
E-mail : landerohidas@gmail.com
Cell : 9657633124

▸ *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. 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.This paper alsoaims to discuss on : the definition, laws governing them, Causes of Cybercrimes &methods of committing cybercrimes, who they affect, and cybercrime prevention procedures. The paper will show the usage and progression of thetechnology has amplified different types of crimes such as theft crimes and terrorism.

Keywords:- Security, Network Security, Computer, Privacy, Cyber Crimes.

▸ *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 shift 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.

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.

▸ Definition of Cybercrime

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 operationswith malevolent programs¨.

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. Cybercrimes are any crimes that cause harm to another individual using a computer and a network. Common internet users may be unaware of cybercrimes, let alone what to do if they fall victim of this cyberattacks. Cybercrime is motivated by fraud, typified by the bogus emails sent by "phishers" that aim to steal personal information" (Cybercrime 2011).

Causes of Cybercrimes &Methods of Committing

Hacking, Theft of information contained in electronic form, Email bombing, Data diddling, Trojan attacks, Denial of Service attack, Virus / worm attacks.

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.

Denial of Service attack:

Is basically where a computer system becomes unavailable to its 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 occursNovember, 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 thencopiesitself and spreads to other computers on a network which they affectanything on them, either by changing or erasing it. However, worms are not like viruses, they do not need the host to attach.

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.

Theft crimes:-

Theft crimes can include: Credit/Debit Card Fraud, Identity theft, Non – delivery of Goods and Services.

Credit/Debit Card Fraud-

Credit/Debit Card Fraudis 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.

▶ *Prevention and 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.

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. 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 URL 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.

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.

▶ *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.

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.

Business should employ practices where their employees follow proper safety practices to ensure that integrity and confidentially of stored information is kept at all times to combat cybercrimes. Safety practices like ensuring that staying off game sites on company time where viruses can be downloaded, forwarding chain emails, leaving workstation unattended or password sharing over virtual mediums should be prohibited.

References :

1. PawanDuggal, "Textbook on Cyber Law", Second edition, Universal Law Publishing.
2. https://en.wikipedia.org/wiki/Cybercrime
3. https://www.slideshare.net/aki55/cyber-crime-and-security
4. http://paperpresentationtopicsandpapers.blogspot.in/2010/01/cyber-crime-and-security.html