International Journal of Engineering, Science and Mathematics
Vol. 12 Issue 5, May 2023,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Cybercrime and Cybersecurity: Issues and Challenges

PARISHA, Assistant Professor
Department of Computer Science
MNS Govt College Bhiwani

Abstract

Today our society has grown so fast and with the advancement of technology, everyone can make use of the internet for different facilities like fund transfers, online education, online shopping, etc. Unfortunately, it has a dark side also i.e. an evolution in crime i.e. Cybercrime.

This article focuses on cybercrime and cybersecurity. It also reflects on different types of cybercrimes, and measures to handle them. Cybercrime is any harmful act bethroted by or against a computer or network. It is the use of the computer as an instrument to furtherillegal ends, such as committing fraud and stealing identities. There are many types of cybercrimes like identity theft, internet fraud, hacking, etc. Cybersecurity is the protection ofdata , best practices and technologies that can be used to protectthe cyber environment and organization. So, this is an era of online processing, maximum ofthe information is online and prone to cyberattacks. Their behaviour is difficult to understand hencedifficult to restrict in the early phases of the cyberattacks. Hence need for cyber security forany user and prevention and remediation procedures could prevent a lot of potential problems.

Introduction

"Cybercrime refers to any lawbreaker pursuit skilledby using anynetwork, devices, and the internet. The mainobjective behind committing cybercrimes includesfew gains, personal gains and creating mess within an organization or an individual's life"[2]"Cyber security is aart to shield computers, networks, programs, personal data, etc., from uncertifiedapproach and caution"[3]. It is an activity by which information and other communication systems are secured and safeguard against the attempt to use other's information or passwordand making changes or misuse of the device. Cyber security is made to secure a system against different threats. It includes the method of securing threats against computers, networksand data from unauthorized access or strike that mayharm them or escapade them in someway[3]. Cyber security is a technical outlook to affix systems from any attacks which can be made.

There are different kind of attacks available:

Cyber theft

Cyber theft is a kind of theft which is made by anyone in stealing information of an individual, that data may be related to a burglary in context to money or property, important data i.e.financial data to gain benefits.

Email Frauds

These are the frauds which are made through email, few emails are intentionally sent so that one can click on these links and whatever data is stored on their device is copied to the person who is sending these spam emails and all passwords, and bank details can be stolen by these methods.

Social media Frauds

These kinds of frauds are created on different social media sites. They create a few fake profiles, which can harm a simple person.

Cyberbullying

With the advancement in technology, new trends among students are browbeaten on social media. Any annoyer may use a few words to persecute or torment someone openly on some platform, but that is not a good practice. This has a bad effect on an individual.

Quizzes

These are hidden threats which collect your information related to personality. They have included some terms and conditions, which allow whatever data you have entered that data will be provided to a third party. These app developers collect information related to your personal data, profiles, IP addresses, friends etc, Never attempt such quizzes.

Phishing

Suppose you get an email from Facebook. In that emails, some updating links will appear and they will ask to click on that links. These kinds of fake links will collect your personal information so that they can misuse your personal data for financial gain.Never click on these email links.

Hidden URLs

On Twitter, there are few URLs available, these can divert someone to the site which can download malware and personal data can be hacked. Never click on such advertisements or posts.

Cyber extortion

It involves inthreatening an organisation and in return demands some money to recoup important projects.

Spyware

It is miscellaneous software in which a person wants to access the details of someone else to steal data and capture his data to threaten him financially. By downloading software this spyware enters your system and they can steal your passwords and personal details.

Adware

Whenever any application is downloaded on your system, Adware is accidentally installed onto your system. They get benefits from each view or click on an advertisement window.

Botnets

Botnets harm your server. How to make secure your organization's data? Bot+Nets means robot in networks. They may send spam emails and execute focused infringement into a company's financial data, analysis about the market and other profit information. Cybercriminals use malware to take control of our programs and other tasks.

Hacking

It is the activity that look for Intransigence of electronic devices such as laptops,computers,tablets or our network.It is unlawful activity practised for some financial gains or it may be act of fun for some hackers.

Some Cyber safety Measures are discussed below

1. Try to use strong passwords

Take care in using strong passwords which include numbers, alphabets, special characters, and uppercase and lowercase letters. Never use your common names, or phone numbers because these can be easily cracked. Use different passwords for different accounts, sites, online shopping apps, and gaming apps.

2. Avoid using unknown URLs.

Never click on suspicious URLs, check URLs on google for security reasons and check whether they are justified by executing the address through a search engine. Forgery URLs are often analogous to real website addresses, so try to focus on this fraud. Prepare your device for secure online agreements or transactions by enabling this facility on your device before carrying out any financial transfers.

3. Never click on links provided by spam emails.

A few unknown people send spam emails to thousands of users and a link is attached for collection of information. If a user clicks on that links then their personal information will be lost. Ensure the senders' address is known before clicking on any links or files.4. Never click on attachments in untrusted websites.

4. Never connect to unknown hardware to your computer

Through USB flashes and hard drives, anyone can throw malware on your system. Making connections on such devices may be harmful to break your system security. If connected,then use Antivirus software to make your system secure.6. Never share your personal information unless you are sure it is necessary and secure to do so.

5.Untrusted websites should be avoided

Never move to websites that are unknown because they may steal your data as they have malware and it may endanger your security system.

6.Never share your personal details

Nowadays information is collected through some phone calls, try to avoid it and protect yourself from fraud and thefts.

7.Update your operating system and software apps time to time.

Whenever there is damage in the security system, it needs to be cured instantly so immediately update your software to avoid any theft. They also protect your data and information. Also, update your operating system to enhance your security system.

8. Never use open Wifi services on airports and hotels

Never use available wifi services on airports to make any sort of online transactions or if in case used immediately change your passwords and other secure data.

We can use VPNs .In this all encrypted data is sent on network system.

Few Cyber security solutions

The importance of cyber security solutions begins with providing the best protection from cyberattacks. Proper awareness is required to keep your software and devices safe from threats. Few systems have been discussed to protect your system from cyber threats.

1. Antivirus

Installation of proper Antivirus software is the first way to protect your system from unwanted users. It detects unsafe software and gives us a message not to use this app, it may harm your system. It also detects the virus and removes it immediately.

2. Secure Internet

Internet security programs initiatecourse of action against strike to assure the security of devices and networks. These programs secure the system against different strike at networks, operating systems, and other applications.

They usesdifferentways to protect the transfer of data, including encryption.Firewalls are used for system security.We will discuss in detail.

3. Firewalls

These are filters which secure the system, thus protecting the devices connected to it. Firewalls prevent virus journeys from being implanted into systems. Checkpoints are created by firewalls so that secure and safe thing can enter through that network. They hide your private network from the public one.

Conclusion

Cybersecurity can be considered as a set of measures and suggestionsessential to forbidCybercrime. Electronic source data whether it is personal, govt or any other require major security. A slightcarelessness be a high cost to an individual. So proper awareness and attentiveness is required to keep a check on your data and information and make it secure from illegal users or hackers.

References

1. Carline,J(2017,August6)Geneva Convention in Cyberwarfare

2. Cybercrime Prevention Tips(Norton)Retrieved April 28,2015.

3.Rekha A & Radhakrishna R(2014). Piracy in the digital Age:Is ethical awareness turning into action?(pp1-4). Chicago,IL:IEEE.

4.Cybersecurity Ventures,(2018).https://cybersecurityventures.com/hackerpocalypsecybercrime-report-2016/

5.Cybercrime In India:A comparative Study-M.Dasgupta

6.Cybercrime:A reference Handbook-Bernadette H.Schell,Clemens Martin.

7.Prof R.K.Chaubey,(second e.d2012),An Introduction to Cyber Crime and Cyber Law,Prof Tayal Vimlendu(2011)

8.Holt,T.J and A.M Bossler 2016.Cybercrime in Progress.Crime Sciences Series.NewYork:Routledge.

9.Internet Society(2015) "Global Internet Report2015:Mobile Evolution and Development of the Internet"Geneva Switzerland.