CYBER CRIME AND SECURITY

[1]K.Indra

Assistant Professor,
Department of computer science,
Bishop Caldwell College, Tuticorin, India.

Abstract: Cyber-attacks ask those attacks begun on unsuspecting online users either employing a computer because the thing of the crime (hacking, phishing, spamming etc.), or as a tool to advance other criminal activities (cyber stalking, fraud, child pornography etc.). Cyber-attacks are increasing exponentially hence making cyber security to be a challenge during this digital age. Cyber security is to supply determent opposed the cybercrime, while cybercrime is that group of movements made by the people by creating explosion in network, stealing others important and private ,documents ,data, hack bank details and accounts and transferring money to their own.

I. INTRODUCTION

The word cyber security is used to point out to the security offered through on-line services to secure your online data. It additionally refers to the new technologies and tactics designed to secure computer systems, computer information and networks from unauthorized access, susceptibilities and attacks delivered though the internet. Cyber security is the collection of policies, tools, security safeguards, security concepts, guidelines, risk management approaches, best practices, training, actions, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets Computer can be considered as a tool in cyber crime when the individual is the main target of cyber-crime . In addition, cyber crime also includes traditional crimes that been conducted with the access of Internet. For example, telemarketing Internet fraud, credit card, identity theft, and account thefts. In simple words, cybercrime can be defined as any attach that been conducted by using computer or other devices with the access of internet. This action can give bad effects to other

II. WHY CYBER SECURITY?

Computer security is more important because it can provide the opportunity for the users to secure their important information present on the system and also in the network. It also helps in defending the computer system against different types of harmful technologies and secure the PC from damage (viruses, worms, bacteria and bugs). It also helps in check the network and secure it also from different threats. So, we should use computer security solution on some level to secure our information from different type of sniffing stolen problem. In general, Computer Security is basic for protecting the integrity, confidentiality, and availability of computer systems, data, and resources. Without confidentiality, trade secrets or personally identifying data can be lost. Without integrity, we cannot be sure that the information we have is the same information that was initially sent. Without availability, we could be denied access to computing resources

III. TYPES OF ATTACKS

DDoS Attacks: These are used to make an internet carrier unavailable and take the network down by way of overwhelming the website with site visitors from a diffusion of resources. Large networks of inflamed devices called Botnets are created via depositing malware on users' computer systems. The hacker then hacks into the machine as soon as the network is down.

Botnets: Botnets are networks from compromised computer systems which are managed externally by way of far flung hackers. The far flung hackers then ship spam or assault other computer systems via those botnets. It is also can be used to act as malware and carry out malicious obligations.

Social Engineering: Social engineering includes criminals making direct contact with you normally by smartphone or email. They want to gain your confidence and usually pose as a customer support agent so that you'll supply the vital facts wanted. This is normally a password, the company you work for, or bank records. Cybercriminals will discover what they can approximately you on the net and then attempt to add you as a friend on social debts. After they benefit get right of entry to to an account, they are able to sell your statistics or comfortable debts to your call.

Cyberstalking: This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically cyberstalkers use websites, social media and search engines to intimidate a user and instill fear. Usually, the cyberstalker knows their victim and makes the person feel afraid or concerned for their safety.

Prohibited/Illegal Content: This cybercrime entails criminals sharing and distributing inappropriate content material that can be considered extraordinarily distressing and offensive. Offensive content material can include, but isn't restrained to, sexual activity between adults, films with intense violent and films of crook pastime. Unlawful content consists of materials advocating terrorism-related acts and infant exploitation fabric. This kind of content exists each on the ordinary internet and at the dark web, and nameless network.

PUPs: pups or probably unwanted packages are much less threatening than other cybercrimes, however are a type of malware. They uninstall necessary software program for your system which include engines like Google and pre-downloaded apps. They could include spyware or adware, so it's a terrific idea to install antivirus software to keep away from the malicious down load.

Phishing: This type of attack includes hackers sending malicious email attachments or URLs to customers to benefit access to their accounts or laptop. Cybercriminals have become greater mounted and a lot of those emails aren't flagged as unsolicited mail. Customers are tricked into emails claiming they want to alternate their password or replace their billing facts, giving criminals get right of entry to.

Exploit Kits: Exploit kits need a vulnerability (Trojan horse in the code of a software) to be able to advantage control of a user's pc. They're readymade equipment criminals can buy on-line and use towards everyone with a pc. The exploit kits are upgraded regularly similar to regular software program and are to be had on dark web hacking forums.

Online Scams: These are generally in the shape of ads or spam emails that encompass guarantees of rewards or offers of unrealistic amounts of money. On-line scams include enticing offers which are "too properly to be authentic" and when clicked on can reason malware to intervene and compromise facts.

IV. Safety Tips

- **Use anti-virus/malware software :**Secure yourself from viruses by installing antivirus software and updating it properly. we can download anti-virus software from the Web sites of software companies, otherwise buy it in retail stores;
- **Secure your computer**
  - **Activate your firewall:** Firewalls are the primary line of cyber defense; they block connections to unknown or bogus sites and will keep out some sorts of viruses and hackers.
  - **Be Social-Media Savvy:** Make sure your social media profiles like Face book, YouTube, twitter are set to private. Keep your personal and private information locked down. Don't give out your telephone number, address, hangout spots or links to other pages or websites where this information is available
- **Use Strong Passwords** : Use different user ID / password containing at least 8characters. They should not be dictionary words. They should combine upper and lower case characters, digits and symbols, and change them on a regular basis.
- **Block spyware attacks :** Prevent spyware from penetrate your computer by installing and updating antispyware software.
- **Secure your Mobile Devices:** Be aware that your cell tool is prone to viruses and hackers. Download applications from trusted sources.
- **Install the latest operating system updates:** Keep your applications and operating system like Windows, Mac, Linux current with the latest system updates. Turn on automatic updates to save potential attacks on older software.
- **Protect your e-identity:** Be cautious when giving out personal details such as your name, phone number, address or financial information on the Internet. Make sure that websites are secure like online purchases or that you've enabled privacy settings (e.g. when accessing/using social networking sites).
- **Secure your Data :** Use encryption for your personal files such as financial records or tax returns, make regular back-ups of all your important files, and store it in different location.

V. Conclusion

Cybercrime, additionally known as laptop crime, is the use of a pc as an instrument to carry out unlawful obligations, such as committing fraud, trafficking in infant pornography and intellectual property has grown in significance as the pc has come to be important to trade, enjoyment, and authorities. There are common-feel steps which could prevent or lessen having one's economic facts stolen online; in addition to keep away from other scams and threats, however cybercrime in those regions persists in large part due to a lack of customer education. On this paper the idea of cybercrime and it its numerous types had been studied. In addition we mentioned a few equipment to be used for cybercrime everywhere in the global. Subsequently, it concluded with various strategies to be used to detect and recover from cyberattacks.

References

1. Amit Wadhwaand Smitha Nayak, "A Review on Cyber Crime: Major Threats and Solutions", ISSN No. 0976-5697 International Journal of Advanced Research in Computer Science, Volume 8, No. 5, May – June 2017
2. NEELESH JAIN1 , VIBHASH SHRIVASTAVA, ""CYBER CRIME CHANGING EVERYTHING – AN EMPIRICAL STUDY", ISSN: 2250-1797 International Journal of Computer Application Issue 4, Volume 1 (February 2014)
3. Rachna Buch*, Dhatri Ganda, Pooja Kalola, Nirali Borad ," World of Cyber Security and Cybercrime" , STM Journals , ISSN: 2455-1821 (Online), Volume 4, Issue 2
4. https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/