Cyber Crime and Security: A review

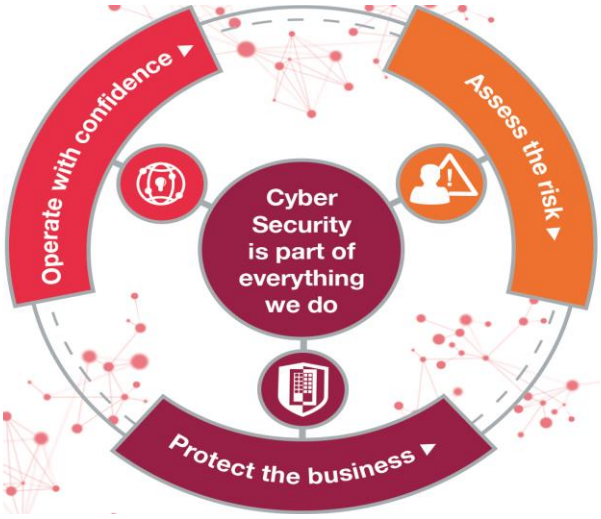
[1]Kunal Mayur Raj, [2]Sarika Kumari

Department of IT, C.V. Raman College of Engineering, Bhubaneswar[1]
rajkunalmayur@gmail.com[1], kumarisarika246@gmail.com[2]

Abstract— ***This is a well known fact that Cyber Crime nowadays has became one of the most easy thing to be done by a computer expert. In this paper I have mentioned about some of the serious Cyber Crime activities done by people for destroying organization network, stealing someone's valuable data, documents, bank accounts and transferring money to their own, etc. This paper will provide detailed information about cyber crime, modes of cyber crime and security measures including the better way of preventing our data, information, bank accounts etc from cyber crime in a better way. Finally I will go for a research on the crime made by the misuse of cyber crime in some of the field and areas like in the Financial crimes, Cyber Pornography, Intellectual Property Crimes, Email Spoofing, Email Bombing, Web Jacking, Data Diddling, Virus/Worms Attack, Salami Attacks, Cyber Deformation etc and also try to find which type of cyber crime is most practiced by those criminals over computers and finally I will get the main objective of my term paper and will successfully find out a better prevention way from these crimes.***

Index Terms— **Intellectual Property Crimes, Web Jacking, Data Diddling, Cyber Security- A barrier towards crime.**

I. INTRODUCTION

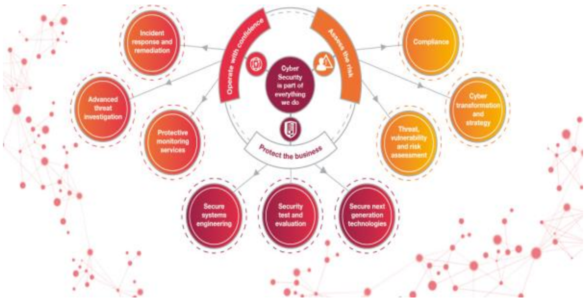


Cyber Security is a part of everything we do. It protect our files and gives us security from being theft via online. It assesses all the risks, protect our business from being looted by preventing our necessary files and documents from being stolen and also helps us to operate with confidence.

Cyber Security is a better approach to prevent Cyber Crimes which are nowadays considered as a bigger criminal offences committed by the use of Internet or else by the use of social media for sexually, mentally or psychologically harassing someone with the help of uneven or unwanted pictures clicked or unknown videos made and shared with the help of links in the social media. It provides a better and a safer way to protect our necessary data and documents which on losing has the power to destroy us. It is well known that the thiefs who do their work with the help of hacking are day by day trying to improve and upgrade their techniques and making them more reliable and strong that without being caught they can easily commit crimes and steal necessary documents or money or bank balance. It not only individually but also helps in protecting the cyber environment of an organization.

Cyber Security came into existence by the time when the computer hackers who are specially expert in hacking any servers started breaking computer networks and stealing all the data which are either confidential or have the powers to destroy someone's empire. These crimes have become nowadays easier in all means as user have no time to go for the checking of privacy policy before installing any applications over their system or before allowing any system application to access files and medias of your device, sometimes users get trapped by **email spoofing, spamming, or bombing** and they by mistake or by paying less attention open the links, or get register to some fake or hacked websites or give necessary and essential details to some sites which later on use those information to steal money, shares, or important documents which have the power to build up or destroy someone's empire. Few hackers who have gained much more knowledge about it generally break into someone's account or security system for getting some thrill in their life as they are so fond of taking these types of risks in their life but others do it generally for getting all the important data for which he/she could get enough money.

II. TECHNIQUES


Incident response and remediation
Advanced threat investigation
Protective monitoring services
Operate with confidence
Cyber Security is part of everything we do
Assess the risk
Protect the business
Compliance
Cyber transformation and strategy
Threat, vulnerability and risk assessment
Secure systems engineering
Security test and evaluation
Secure next generation technologies

A. Cyber Security

Cyber Security acts as a barrier which eventually protects our sensitive personal and information related business world with advance techniques of detection, prevention and quicker response to different attacks which are usually done online nowadays. It actually prevents our data from involving in these attacks or prevents the attacks to be done. It helps us to protect our necessary data from anyone who tries to steal it as they having the intentions of destroying someone's business or just for thrilling purpose as stealing necessary documents is just a joke or fun moment for them.

B. Privacy Policy

As the required fields ask for the email address on a website we should always go for the checking of its privacy policy because some websites are often hacked which more often shares all your data and necessary information to the person who have hacked those websites and he/she may use your personal data for committing some serious cyber crimes with your name without your knowledge.

Whenever we install an application in our device especially in our mobile phones then while opening it for the very first time a pop up window itself opens which asks us to grant them the permission to access our files, photos, medias or contacts where we give permission without reading the privacy policy of the application. If it is a certified application than it's okay but if the application is fake or hacked than hacker will have easy access to our details and can provide us as much harm to us as important our details and documents are.

C. Software should be always be updated

If the company sends the updates for the operating system of the software of your device then immediately install them as soon as possible. Installing them sooner will prevent your system from attackers who can take better advantage from the older version of your operating system.

It is a well known fact that the updates which are available for our system always have something new and better with it and has a lots of bug fixing along with it which helps in a better and smooth performance of our system.

D. Choosing Password

Always use the password which is strong enough for anyone to guess which consists of both capital and small alphabets, numbers and special symbols so that it become very difficult for the criminals to guess and they may not be able to get into your account and which is a very easy technique to prevent such crimes. A good password always comprises of special characters, capital as well as small alphabets and some special symbols and numbers so that someone who is trying to get into your system cannot be able to enter into by just guessing your password as mainly for easy remembering we use our name or date of birth as our passwords.

III. APPLICATIONS

A. Protection of Business info

With the help of cyber security measures will provide comprehensive digital protection to your business. We will safeguard the documents which are either confidential or very necessary for the company or the data the rivals are always looking for. Cyber Security is especially came into existence to protect the business from downfall due to security issues as manual security is not at all enough to protect a company from being looted. A good company always prefer better Cyber Security measures for protection of their shares.

B. Protect Personal Information from being used illegally by someone else

If a virus is able to get into your account and get all your personal information of yours then they are quite capable of selling that information on, or even using it to steal your money. Whenever someone else get into our system without our permission they always try to steal important documents which are either important or confidential. We need to protect our data from these criminals are prevent these crimes from existence by accepting all the cyber security measures.

C. Different Computer Centre

Cyber Security is used in different computer organisations such as schools, colleges, universities, and different IT Sectors as each person whether a student, teacher, official or an employee has his/her login id and password to use the Internet facility provided. They must login with their respective login id to the cyber roam to get the access to the important data from the system which might be important or confidential.

D. Social Media

Different prevention methods are adopted by us to use our social media accounts safely by accepting all the safety measures instructed by them. From keeping good passwords to safeguarding our account we all keep our accounts safe from those crimes happening using these accounts. Nowadays social media has became one of the best way to commit cyber crime as these links which have the power to get into anyone's system are shares in a bulk by the help of **Facebook, Instagram and messengers like Whatsapp, Hike etc**.

IV. LIMITATIONS

- Makes the system slower than before.
- More costly for average user.
- Need to keep updating the new software on time as the older version will not provide effective productivity.
- Need to opt for a new version after a fixed time period.
- Need to be properly operated.
- Firewalls can be difficult to be configured correctly and efficiently.
- Incorrectly $^{\text{configured}}$ firewalls may block the user from performing certain actions or works on the internet, unless and until the firewall is configured correctly.
- Once used cannot be reused.
- Compatibility issues with many systems generally occurs.
- Need to be used properly.

V. PREVENTIONS

- Use of antivirus for the system
- Insertion of firewalls
- Un installation of software which is of no further use
- Maintaining backup of important files
- Checking privacy methods
- Checking of security setting
- Stay anonymous
- Set good passwords
- Never put your passwords in your documents.
- Never keep the passwords in the name or date of birth of yours.
- Never give your full name or address to strangers
- Learn more about Internet Privacy

VI. CYBER LAWS

Cyber crimes may involve all the criminal activities those are traditional in nature, such as forgery, theft, fraud, mischief and defamation, all of which are subject to the Indian Penal Code under IPC Section 469. The wrong use of computers and technology has also given birth to a gamut of new age crimes which are dangerous as well as illegal and are addressed by the Information Technology Act, 2000.

VI. CYBER CRIMES

A. *Email spoofing*

Email spoofing means that the email asking some necessary details of the receiver appears to have been generated from one sender but is actually sent by another sender who has manipulated the sender details. This manipulates the reader by providing the wrong details. In these we actually does not know the true origination of the mail as it does not have the true sender's email address which manipulates our mind as the sender may have used the email of someone we know or someone who is closer to us and we positively react to his/her mail and easily get trapped by this way.

B. *Spamming of Emails*

Email spamming generally means sending a trap mail to thousands of users randomly just like a chain letter. It helps in trapping some of the users who pays less attention to their emails while enrolling in any forms. In these it is quite possible that the mail is sent to someone who is not knowledgeable or who has no or lesser idea about mails and social media can be easily trapped by getting into the link by just opening their mail address.

C. Sending of codes through email which are malicious

E-mails are nowadays also used to send viruses or Trojans or something more dangerous through emails by sending a link of website or by an attachment which on visiting directly without your permission downloads the malicious code. It is also used in giving threat. Malicious codes are sent randomly to different users in search of some fools who can easily get trapped by sharing his/her data through the spam mail.

D. *Bombing of Emails*

Bombing of mails is eventually characterized by an attacker who is repeatedly sending a same email message to a particular address so that the user should mistakingly opens the link provided to him/her and get attacked. In this we often make mistake by sharing our data as we get repeated mails from these peoples and we don't find the mail fake and make the mistake of logging into these accounts and giving our personal details.

E. Sending emails of threat

Sending threatening mails sometimes results in heavy damage as the user allows to accept the demands of the criminals for safety of their documents or some else. This mails often threaten us as some are weak hearted people who gets scared of these types of mails and became ready to fulfil their demands as they want to protect themshelves and their families from threat.

F. Defamatory emails

Defamatory means damaging the good reputation of someone; slanderous or libellous. It sometimes works as the user doesn't want to lose his name and fame in the corporate and social world. This mail is sent with the the intension of destroying someone's name and fame in the society, company or in the corporate world.

G. Email frauds

Frauding with the help of email is an intentional crime done for the personal gain of data and information or to damage a particular person through email. Nowadays email has become a major platform of exchange of important files and documents as it is widely being used. This is generally based on greed of someone whose major intension is to get access to the codes to get your money from your account. They doesn't care about the destruction of name and fame of yours as they may or may not be your family, business or institute rival.

H. IRC related

IRC (Internet Relay Chart) comes under Application Layer Protocol that generally facilitates the communication in form of text. The process of the chat works on a networking model of client/server. IRC clients are the programs of the computer that can be installed by the user on their system or applications that are based on web technology running either locally in the browser or on server of 3rd party.

VII. CONCLUSION

Cyber Crime is now getting all the recognition it totally deserves. However, it is well known that cyber crimes are not going to be restricted that easily in the faster rate. It is observed that the Cyber Criminals and hackers are continuously developing and upgrading their technology to higher level to stay ahead of the laws so that they could easily commit crime without getting caught by today's Cyber Security measures and processes.

So, to make ourselves safer from the Internet criminals we need to use cyber security on a larger scale to keep us prevented and protected.

VIII. REFRENCES

[1] D. Muthusankar, B. Kalaavathi and M. Deepa, "Cybercrime Risk and Cyber Security on online service avoidance," IEEE Middle East Journal of Scientific Research 24, July 2016.

[2] Hossein Hooshmandi, "Cyber Security of Smart Grid and Scada systems," IEEE Trans Helshinki, 14-15 Paper 0245, June 2016.

[3] Bhawna Kumari, Yawar Jalees and Manju Gupta, "Cyber Security as a backbone of E-Commerce," IEEE Trans. International Journal of Advanced Scientific research and management, Vol 1 Issue 4, April 2016.

[4] www.wikipedia/cyber_security.com

[5] Subrata Paul, Anirban Mitra and Brojo Kishore Mishra,"Cyber Security and Human Rights", CSI CommunICatIonS, 2012

◈◈◈