National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

Human Security in Information and Cyber Era

Madhumita[1], Kavya V[2], Nair Rathish[2]

[1]Assistant Professor Department of Computer Application Soundarya Institute of Management and Science, Soundarya Nagar, Bangalore, Karnataka, India

[2]Department of Computer Application Soundarya Institute of Management and Science, Soundarya Nagar, Bangalore, Karnataka, India

ABSTRACT

This case studies brief note on aspect of human security in today's world. The role of social media, cybersecurity and cyberterrorism are playing high role in society and influencing forth destruction of human security. We are witnessing a technological revolution wherein in the tip fingerbone can know from present Government status to the thought so fin decidual people over networking. Social media is a great facilitator, which has not only brought people together but has bought much more worries too. It was revealed that Social networking sites permit for information to spread very quickly amongst the public. The biggest threat in technological era is no one can predict the time and source of brutal activities. Though Government is taking initiative to spend more and protect their data from cyberhackers or terrorists it has been highly difficult to disclose it. Social media, wiki leaks etc. are making Government efforts ruin. These are imposing threat to human security, and there is a need for greater Government security and awareness amongst citizens to safeguard their information.

Keywords : Cybercrime, Identity theft, Human Security, Privacy issues, Cyber Security

I. INTRODUCTION

Cyberwriters imaginary space, which is created when the electronic devices communicate, like network of computers. Cybercrime refers to anything done in the cyberspace with a criminal intent. Computer fraud can be an untrustworthy misrepresentation of the fact proposed to prompt another to abstain from doing something that causes loss. Computer crime can be summarized as a criminal activity which involves information technology infrastructure, in addition to unauthorized access, illegal interception, any data interference, computer or systems interference, abusage of devices, forgery, blackmail, embezzlement, and some electronic fraud s. Cybercrime can cause harm to any organisation.

To fight the fast-spreading cybercrime, governments and businesses must have collaboration globallybasicallyto develop any impressive model that somehow controls the threat. The internet is basically used for the betterment of life, to make people aware of world- wide activities, enhances the speed of life as well and makes users technically strong and up-to-the- mark. Asther use technology's increasing day-by-day, the crime is also increasing gradually. It covers all the formsofcrimesand thefts related to computer networks. Some of the criminals are technically expert and educated having deeper and remarkable knowledge regarding the technology

The purpose orthopaedist Understanding Cybercrime its Phenomena, Challenges and Legal Response is to assist everyone in understanding the legal aspects of cybersecurity and to help harmonize legal frameworks.

As such, it aims to help better understand the national and international implications of growing cyberthreats, to assess the requirementsofexisting national, Regional and international instruments, and to assist in establishing a sound legal foundation. It provides comprehensive overview of the most relevant topics linked to the legal aspects of Cybercrime and focuses on the demandsofdeveloping countries. Due to the transnational dimension of Cybercrime, the legal instruments are the same for developing and developed countries.

Cybercrime

Cybercrime is an activity done using computers and internet. We can say that it is an unlawful act wherein the computeractsaseithera tool or target or both. Computer crime, cybercrime, electronic crime orchid-tech crime basically criminal activity where a network or computerise target, source, or place of the crime. Network crime encloses wide range of illegally potential active activities. Whenever a person tries to steal information, or cause damage to computer network, this is assumed to be entirely virtual in which the particular information exists in digital form but the damage caused is real, which ceases the machine and has no physical consequence. A computer may act as a source of evidence, even though not directly or completely used for the criminal purposes, it acts as an excellent device for keeping the record and has given the in charge to encrypt data. If the evidences are obtained and decrypted, it will be assumed to have a greater value to the criminal investigators.

Cybercrime can be basically categorized in two ways: -

Computershare

Busing a computer to attack other computers, through network.

E.g. Hacking, Virus/worms, Do attack, etc.

Computerasweapon

Using a computer to commit real world crime.

E.g. Cyberterrorism, Credit card fraud etc

Varioustypesofcybercrimes There are several types of cybercrimes that are occurring in the
networking world some of these are as written below

1. Financial fraud
2. Sabotage of data and other networks
3. Theft ofproprietaryinformation
4. System penetration from outside
5. Denial of service
6. Unauthorised accessbyinsiders
7. Employee use of internet service privileges
8. Viruses

Here the picture depicts the top countries having threat foyer crime

Threats to be aware of: -

Hacking

Hacking is a term used to describe actions taken by someone to gain unauthorized access to a computer. The availability of information online on the tools, techniques, and malware makes it easier for even non-technical people to undertake malicious activities. The process by which cybercriminals gain access to your computer. In hacking, the criminal uses variety of software to enter person's computer and the person may not be aware that his computer is being accessed from a remote location. This is a type of crime wherein a person's counterstroke into so that his personal or sensitive information can be accessed. Find weaknesses in your securitysettingsand exploit them in order to access your information. Install a Trojan horse, providing a back door for hackers to enter and search foryourinformation.

Phishing

Phishing is a crime mostly used by the criminals because it is one of the easiest ways to execute and it can produce the outcome sorresultsthey're looking for with less effort.

Websites, text messages, and fake emails are created to look as if they are from some authentic companies. Basically, these are sent by some criminals to steal and acquire some personal and the financial information from you. This may also know as “Spoofing”.

Phishing is used by the strangers to "fish" or steal for information about you basically those that you would not disclose to a stranger, like your bank details, PIN, and some other personal details. What it does: Trick you into giving them information by asking you to update, validate or confirm your account. It is often presented in a manner than seems official and intimidating, to encourage you to take action. Provides cyber criminals with your username and passwords so that they can access your accounts and steal your credit card numbers.

Malware

Malware is the most common way to infiltrate or harm your computer. The term malware is nothing more than “malicious software”. Different malwares are Trojan, key loggers, spyware.

1) Alterfilesordelete them.

2) Intimidate you with scare ware.

3) Reformat hard drive causing you to lose all the useful information.

4) Steal some sensitive information.

5) Send emails using your identity.

6) Take charge ofyoursystem.

Computer Vandalism

Damaging or destroying data rather than stealing or misusing them is called cybervandals. These are program that attach themselves to a file and then circulate.

Cyber Terrorism

Terrorist attacks on the Internet are by distributed denial of service attacks, hate websites and hate E-mails, attacks on service network etc.

Software Piracy

Theft of software through the illegal copying of genuine progressors counterfeiting and distribution of products intended to passport original.

CYBER SECURITY

A branch of technology basically known as cybersecurity or information security applied to networks and computers, the objective carries protection of data or information and the property from the thefts, natural disaster, or corruption, and allowing the property and information to remain productive and accessible to its users. The Cybersecurityimpliesto the processes and the technologies which are designed to protect networks, computers and the data from the unauthorized access, attacks, and vulnerabilities delivered via the Internet bycyber criminals.

In countersecurity threat is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm.

Example: malware, virus, spam’s, spywares

Who is Cyber Security Hacker?

A securityhackerisa person who seeks and exploits weaknesses in a computer system or computer network. Hackers maybe motivated bay multitude of reasons, e.g.: profit, protest, challenge, enjoyment, grudges or revenges.

Hotdishes hacker communicate with target?

Using targeted email

Fake emails

Fake website

Malicious web-link address in your email or social media

e.g.: Facebook, WhatsApp

Challengesovercybercrime occurrence:

Capacity to store data in comparatively small space as there is need to be right memory space to store. Also, if insist access like passwords such as individual name, mobile number, date of birth etc which is predictable. Complex and negligence of data may lead to leakage ofdata or piracy. Loss of evidence leads to cybercrime and human security issues.

Example: Receiving a text from an unknown number saying you have won and that you need to claim money/prize.

Prevention tipsforcybercrime:

1. Update firewalls (infrastructure defence systems) up to date.
2. Make sure that system is configured safely and securely.
3. Always choose strong passwords and securitychecksfor social networking sites, email boxes, and for systems.
4. Do not respond to unfamiliar mails.
5. Protect system with some best security software.
6. Shield or protect personal information from unknown people or strangers.
7. Safe browsing, and do maintain some good system hygiene.
8. Keep updating passwords, and login id's at least once or twice in one or two months and make them strong.
9. Do protect data and personal information and avoid being scammed.
10. Never send personal information and data via mail or anetodermas.
11. Make system clean time to time and review social media sites as well.
12. Do not respond to any spam email and be cautious
13. Do not visit / link to unknown and dangerous website.
14. All external drives must be scanned.
15. Be aware of surroundings– never reuse a password.
16. Do not connect to public free WI-FI network using company laptop.

Conclusion

In this modern era of technology, the role and usage of internet is increasing worldwide rapidly, therefore it becomes easy for cybercrime in also access any data and information with the help of their knowledge and their expertise. The cybercrime as a whole refers to Offences that are committed against individuals or groupsofindividualswith a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directlyorindirectly, using modern telecommunication networks such as Internet and mobile phone. Such crimes may threaten a nation'ssecurityand financial health too. Issues surrounding this type of crime have become high-profile, particularly those surrounding cracking and child grooming. A computer can be a source of evidence. Even when a computer is not directly used for criminal purposes, may contain records of value to criminal investigators. So, the network must be secure as no one can access the information of the computer by providing the necessary security.

Cybercrime is an awful act that needs to be tackled firmly and effectivelyeitherbywell known people or Government. There is a need to create more awareness among the people and basically usersofinternet about cyber space, cybercrime and some more aspects. So, it is seriously advised to take some previous precautions while operating the internet before attaining loss. Security nowadaysisbecoming a prominent and major concern hence it's always best to take care of the networks which is being used and must be provided with assured security. Itsalwaysbetterto take certain precaution while operating the net.

Future Scope

Human securitise main aim ofurace study and hence it is more concerned over it. Basically, this paper demon tradeshow ignorant we are in the security purpose and ways to keep secure and cope up with the threats that may occur. The new implementations that can be done overtire Biometric system, in future Retina detection i.e., Iris detection can be a revolutionary system. As fingerprint also being done forgery's threat to rely on it. A lot of research is still going on in this area to build a more secure system despite offal disadvantages.

Example: According to our opinion using smart card with fingerprint detection makes system more secure. Thus, combination of

II. REFERENCES

[1]. Biometric with technologies makeshighlyeffective in security.

[2]. To conclude, the usage of biometric systemsmainlyiris detection will increase a lot more securityto humansin upcoming dayswith the support ofstable technologiesand more cost effectiveness.

Cite this article as:

Madhumita, Kavya V, Nair Rathish, "Human Security in Information and Cyber Era", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 177-181, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT194733