PRIVACY, SECURITY & CYBER LAWS

Dr. Neeraj Tyagi[1] Mr. Sumit Kumar Baberwal[2], Ms. Nidhi Passi[3]

[1]Associate Professor, Deen Dayal Upadhyaya College, D.U. (India)

[2,3] Assistant Professor , Keshav Mahavidyalaya , D .U. (India)

ABSTRACT

With constant development and literacy over the years regarding the digital world many pros and cons are coming into picture. The trend of going 'on web' for career, jobs, recreational activities, friends, information, globalization etc. has increased the scope of development both for the learners as well as for the attackers. Our paper tends to understand the Privacy and Security concerns on net and the Cyber Laws regarding individual's endangering privacy. The Internet today because of its popularity is under various attacks. A knowledge regarding the dos and don'ts on the net is equally important to safeguard critical information.

Keywords: Privacy, Security, Cyber Laws

I. INTRODUCTION

People today are using the Internet 24x7 making it the biggest electronic market place. Everybody wants to be connected & share information. The most important is the online transactions related with shopping, marketing etc. People are using their creditentials to sign up with different sites, sharing their account details without actually being bothered about the privacy & security. The advancement in technology increases the opportunity of learning for non-adaptors and hence the online use. With the elevation in number of online users, security & privacy concerns have also increased. Password theft, account details capturing, gaining access of somebody's system, e-mail spamming etc are the major security concerns with online privacy.

II. PRIVACY & SECURITY

Privacy relates to an individual's personal information. Lack of Privacy means someone else could take control over that person by using particularly important leaked data. E-mail, social networking & online shopping are the basic services that everybody is availing now-a-days. While signing up with these sites, people provide their personal information. Marketers use latest technologies to find out what people are surfing over the net to analyze their needs & make the business strategies accordingly. But the level of information accessed by outsiders is not defined, so one needs to understand the concept of privacy. Privacy and security is related with the level of protection availed from a person's computer software, anti-virus software and the level of public access on the internet server they use [1]. Security defines the level of personal information being shared with others, knowingly or unknowingly. Most of the users assume that their information is secured as they are using secured protocols, well updated anti-virus but anybody who have adequate knowledge about the working of system, network & server can easily hack the system or even the network. Ex: Google mail service is supposed to be a secured application still around 5 million Gmail accounts got hacked anonymously last year. This is not only because of the poor security system of Google servers but the main reason behind this is the privacy & security settings selected by the users. Social engineering is what the intruders are using. Some privacy risks include:

- Phishing: Email messages coming from a genuine lookalike website or link i.e. from the bank, colleges etc which are designed to get the user's private information. Ex: Mail coming from XYZ saying that you won a jackpot, click to proceed & when the user clicks on the link, it gets redirected to a spoofed website asking to enter your confidential details like account number, credit card details etc.
- Pharming: cyber attack in which malicious code is installed on a personal computer or server; users are then misdirected to Fake Web sites without knowledge or consent. [2]
- Spyware/ Malware: malicious software running on the target's machine without his consent. The purpose is to collect the user's activity, private information & send it back to the spyware source when the system connects to the internet. These are viruses, Trojans which are sent to damage the remote system to access the gain.
- E-mail Spamming: same email is sent on bulk. The mail may redirect the user to phishing sites which contains malware.
- Session capture/ cookies stealing: users working online share their information in terms of cookies with the server. Cookies are the piece of information about the users authenticity, log information etc. Some cookies are temporary i.e. are deleted from the memory as soon as the user logout/ disconnects from the website but some are permanent. Cookie stealing is another way the hackers are gaining access to somebody's system.

The above mentioned cyber attacks are the most popular & common privacy risks associated with the online use. Users can take security measures to increase online privacy:

- Frequent change of passwords with strong selection, never keep the password as Date of birth, name etc
- Use of updated anti-virus & firewall is highly encouraged
- Don't allow any application to change your system settings without reading the terms & conditions
- Never use unreliable websites or websites with lower security level
- Clear the browser's history & cache consistently
- While banking or online transactions always work on HTTPS & take care of digital certificates of websites to avoid phishing attacks
- Don't provide your personal information to any spam

Even with the security measures taken by the users, still cyber attack is the biggest concern all over the world. E-commerce has increased the use of electronic exchange of information & money. Its high usage increases its risk of vulnerability. Some legal limitations should be implemented to control its flow. All over the world, cyber security laws have been formed to measure the level of disruptions in information exchange. As discussed earlier, the marketers analyze the online surfing data of users, to promote their business; cyber laws define the legal aspects of captured information. For a developing country like India where literacy rate is low, Cyber Security is very important. According to a study, number of cyber crimes in India will reach to around 3 lakh by the end of 2015.

Figure 1 below depicts the same.

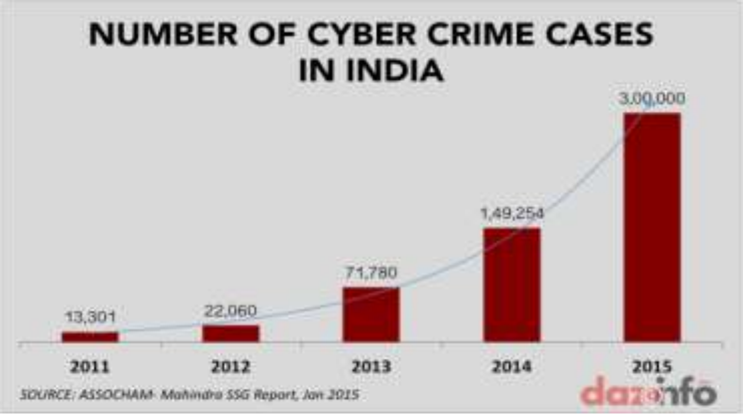

Figure 1(Source: [3])

III. CYBER LAWS

Cyber laws cover the legal aspects of information exchange. Every country has designed their own rules & regulations to fight against cyber crimes. Many people don't know what should they do when they face cyber crime. And many don't even know while committing that it's against law. Any type of security breaching against the defined protocols is known as cyber crime. In India, Information technology Act 2000 addressed the cyber crimes.

In 2008 some amendments have been done to the existing act.

Some aspects of IT Act are

- Email would be considered as a legal means of communication and could be produced at the time of legal actions for validity. [4]
- Use of digital signature by any subscriber to authenticate electronic records [4]
- Controller of certifying authorities for the issue of Digital signature Certificates [4]

Few sections under IT ACT, which are important:

- **Section 43(Penalty and Compensation for damage to computer, computer system, etc.)** – any person accessing, damaging, manipulating resources, storing information from any other person's computer is liable to pay the damages to the affected person. [5]
- **Section 65(Tampering with Computer Source Documents)** – any type of tampering including destroying/ altering the computer's source code which is maintained by law, shall be liable for punishment which may include imprisonment or a fine or both. [5]
- **Section 66-A (Punishment for sending offensive messages through communication service, etc.)** – any type of email message which is sent from a computer system to offence, provide false information, create annoyance/danger, insult, injury etc. could make a Person liable for punishment including imprisonment and fine. [5]
- **66-B (Punishment for dishonestly receiving stolen computer resource or communication device)** – anybody who tries to dishonestly retain someone's computer resource/device as if stealing is liable for the imprisonment or fine or both. [5]

- **66-C (Punishment for identity theft)** – anybody fraudulently using the e-signature, passwords or any other unique credentials is liable for the punishment. [5]
- **66-D (Punishment for cheating by personation by using computer resource)** – any type of impersonation done using computer resources is a punishable offence which includes the imprisonment or fine. [5]
- **66-E (Punishment for violation of privacy)** –anybody intentionally sharing/capturing/transferring someone's personal information electronically without his consent is liable to imprisonment or fine or both. [5]
- **66-F (Punishment for cyber terrorism)** – anybody trying to harm India's integrity, threaten the unity, breaching the security or sovereignty to spread terror amongst the people by

1. any computer resource denial to access to the authorized person
2. using the resources and information without authorization or exceeding the access role
3. Causing any type of destruction to computer/ computer resources knowing it's likely to cause any adverse effect on the lives of people or community is punishable with life time imprisonment. [5]

- **67 (Punishment for publishing or transmitting obscene material in electronic form)** – publishing or spreading any type of lewd or offensive material regarding any person in electronic form is a punishable offence. [5]
- **67-A (Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form)** –anyone publishing or spreading pornography content or nudity in electronic form is liable for punishment. [5]
- **67-B (Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form)** –

1. Publishing or transmitting sexual exploitation of children
2. Downloading or promoting sexual abuse of children in different electronic manners
3. Persuading children to online relationship for sexual exploitation to offend a reasonable adult on the computer resource
4. Abusing and provoking children online; or
5. Video graphing children's sexual abuse [5]

Anyone involving in this is liable to imprisonment and fine.

- **72 (Penalty for breach of confidentiality and privacy) -**anyone endangering someone's privacy by using confidential data without permission is liable to imprisonment or fine or both. [5]

IV. CONCLUSION

Internet has become a vital part in many applications and breaching of privacy and security could harm an individual in many ways. Although, it's not easy to finish online crime but still strict laws and regulations could help decrease them. More important than this is literacy and awareness amongst people regarding how they can secure critical information and how Cyber laws functions in this direction. Technology can be used for both good and bad purpose. Surveillance is needed to keep a check of attackers and simultaneously making the applications more and more secure. Spreading awareness about laws may bring fear to them ensuring the use of technology for ethical manners and not for crimes. The Law makers, Network service provider or other intermediaries and users have to together act vigil for information security.

REFERENCES

[1] "Concept of Internet privacy," [Online]. Available: http://nobullying.com/internet-privacy/.

[2] "Concept of Pharming," [Online]. Available: http://searchsecurity.techtarget.com/definition/pharming.

[3] "Growth Of Cyber Crime Cases In India 2011 – 2015," [Online]. Available: http://dazeinfo.com/2015/01/06/cyber-crimes-in-india-growth-2011-2015-study/.

[4] "IT ACT 2000," [Online]. Available: http://www.cyberlawsindia.net/Information-technology-act-of-india.html.

[5] "The Information Technology Act, 2000," [Online]. Available: http://www.cyberlawconsulting.com/ITACT2008.doc.

[6] U. Gori, MODELLING CYBER SECURITY:Approaches, Methodology, Strategies, IOS Press, 2009.

[7] S. M. I. S. L. W. L. C. L. P. C. F. I. Jing Liu and Yang Xiao, "Cyber Security and Privacy Issues in Smart Grids," IEEE COMMUNICATIONS SURVEYS & TUTORIALS, vol. 14, FOURTH QUARTER 2012.

[8] V. Hiranandani, "Privacy and security in the digital age: contemporary challenges and future directions," The International Journal of Human Rights.

[9] I. S. o. IIBF, Cyber Laws in India, M/s TaxMann Publishers.

[10] A. K. Maitra, "Offensive cyber-weapons: technical, legal, and strategic aspects," Springer Science+Business Media New York 2014.

[11] A. A. a. J. Earp, "A Requirements Taxanomy for Reducing Web Site Privacy Vulnerabilities," Requirements Eng., vol. 9, pp. 169-185, 2004.

[12] R. H. Weber, "Internet of Things- New Security and privacy challenges," Computer Law & Security Review, pp. 23-30, 2010.