International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 1464-1466 www.ijaem.net ISSN: 2395-5252

Cyber Security for Women during COVID-19 Pandemic

Mrs. Rambha Kumari

Ph.D. Scholar, Deptt.of Family Resource Management, College of Community Science, G.B.Pant University of Agriculture and Technology, Pantnagar, Uttrakhand

Submitted: 25-06-2021 Revised: 06-07-2021 Accepted: 09-07-2021

ABSTRACT—Indian citizens are suffering from second wave of COVID-19 pandemic and in this time protection is needful with all aspect for all human beings. There has been a spurt in cyber crime among women during lockdown situation. It has made the stalkers much bolder. Cyber crime is one of the big threat of our country. According to data of the national commission for women (NCW), 54 cyber crime complaint were received online in april 2020 in comparison to 37 complaint received online in april 2019. There were 412 genuine complaints of cyber abuse from march 25 till april 25, 2020. Out of these, 396 complaints were serious in nature. In India 71 crore people are using the internet. Out of which 25 crore are women. In 2018 revealed that 6030 cyber crimes were registered by women (NCRB Data). Therefore it has made the stalkers much bolder. However in this virtual world awareness is most important key to protect cyber crime for women. Women should knowing about IT rule, principles and using social site.

Index Terms— Awareness, Crime, COVID, Virtual

I. INTRODUCTION

India is second most populous country in the world. The percentage of the female population is 48.04 compared to 51.96 percent male population and in this time people are suffering from second wave of COVID- 19. It is affecting on society in the way of direct or indirect so security is needful with all aspect for all human beings. Security means we can say that in the sense of personal health, economic, education etc. This wave is too strong which cause social distancing is important so that we can break the virus chain. Lockdown is only one of the factor that can control the pandemic.

Human borns in real world and they are for real world but now a days according to situation they are surviving in virtual world. In the situation of lockdown most of the women spend more time in virtual activities like whatsapp chatting, video calling, online shopping etc. In the virtual life they do not alert own personal security that results cheated by cyber fraud. Cyber crime is not new but now a day it is happening with large number of women.

According to data of the national commission for women (NCW), 54 cyber crime complaint were received online in april 2020 in comparison to 37 complaint received online in april 2019. There were 412 genuine complaints of cyber abuse from march 25 till april 25, 2020. Out of these, 396 complaints were serious in nature. In India 71 crore people are using the internet. Out of which 25 crore are women. In 2018 revealed that 6030 cyber crimes were registered by women (NCRB Data).

Women are soft in nature so easily cheated by cyber criminal.

Cyber crime is one of the big threat of our country. It has increased along with the world. In this area lots of criminal present which we can not see with open eye so one of the important key of cyber security that is awareness. Awareness is most important thing for all women for cyber security. Awareness will come through learning, listening and understanding. If cyber attacks on any person they should taking immediate respond so that criminal can not go away out of range. Immediate response is compulsory because time is no more and cyber criminals are very cunning. We can not prevent cyber crime without awareness. Do not spread personal information to others and always do responsible for social networking. We should knowing about IT rule, principles and their use. Women will change their mind then cyber attack will be decrease. The status of women in India will be many change in all regions of recorded Indian history.

II. TYPES OF CYBERCRIME

Here are some specific examples of the different types of cybercrime:

- Email and internet fraud.
- Identity fraud (where personal information is stolen and used).
- Theft of financial or card payment data.
- Theft and sale of corporate data.
- Cyberextortion (demanding money to prevent a threatened attack).
- Ransomware attacks (a type of cyberextortion).
- Cryptojacking (where hackers mine cryptocurrency using resources they do not own).
- Cyberespionage (where hackers access government or company data).

III. CATEGORIES

Cyber crimes can be basically divided into 3 major categories being on

1. Against Person :-

Cyber crimes committed against persons include various crimes like transmission of Child pornography harassment of any one with the use of a computer such as e-mail and cyber-stalking.

2. Against Property :-

There crimes includes unauthorized computer tress passing through cyber space, computer vandalism, transmission of harmful programmer and unauthorized use or possession of computerised information.

3. Against Government :-

Cyber terrorism is one distinct kind of crime in this category the growth of Internet has shown that the medium of cyberspace is being used by individuals and groups to threaten the international governments as also to terrorize the citizens of a country. This crime manifests itself in to terrorism when an individual cracks into a government or military maintained website. administration" features.

There are many different ways to categorize cybercrimes. However, here is one way to separate cybercrimes into five categories.

1. **Financial**. This is cybercrime that steals financial information or that disrupts firms' ability to do business. So, for example, when Target's credit card data were stolen, that was a financial cybercrime.

2. **Hacking**. This consists of unauthorized access to a computer system. This can be used to commit other crimes (such as when Target's computers were hacked) or it can be done to steal data or plant malware.

3. Cyber-terrorism. This consists of hacking that is serious enough to cause fear in target populations. For example, if a foreign country were to hack into American banks' records, it could cause enough fear that our economic system might be damaged.

4. Online illegal pornography. The most important type of this is child pornography. The internet gives unprecedented opportunities to disseminate illegal pornography. There are many examples of child pornography being widely distributed.

5.Cybercrime in schools. This consists mainly of people gaining personal information from young children who do not know better. The information can be used to harm the children or for purposes of identity theft.

IV. CYBER CRIME PREVENTION AGAINST WOMEN

Ministry of Home Affairs had constituted an Expert Group comprising of the official/academicians from NSCS, Ministry of Home Affairs, CDAC Cert-In, Indian Institute of Technology, Indian Institute of Science and IT experts to study the gaps and challenges, prepare a roadmap for effectively taking of Cyber Crime in the country and give suitable recommendations to take effective measures to prevent crime against women and children and create awareness in the society about these issues. Accordingly, a scheme for Cyber Crime Prevention against Women and Children (CCWC) has been formulated by the Ministry of Home Affairs. The proposed scheme was examined by NCW.

- **Online Women specific Crime Reporting Unit -**Interlink with NCW should be made in such a manner that if a woman wants to make a complaint about cybercrime to NCW, it should be sent to MHA Crime Reporting Unit with acknowledgement to NCW and a copy to the complainant. It will encourage quick disposal of the complaints that too with the assistance of the IT professionals
- **Monitoring Unit for Cyber Crimes-** Monitoring unit should provide monthly reports on the complaints received through NCW
- **National Forensic Laboratory-** Investigations of crime against women are delayed due to pending reports from forensic laboratories so NCW agreed to it.
- **Capacity Building-** It should include capacity building of protection officers appointed under Domestic Violence Act, 2005.

These days, it is common to hear about hacks and data breaches that happened simply because the key cyber security concepts weren't followed or because IT teams didn't get the buy-in and financial support they needed from senior management. Women need to understand the key terms and principles of cyber security to empower their communities instead of simply deploying technology and hiring people to manage it.

V. PRINCIPLES OF CYBER SECURITY

1. Security beyond Firewall

The introduction of new technology enabled the evolution of new, intelligent bots that show "humanistic" behaviour. Additionally, good bots like Google crawlers, are approaching websites to increase your company's value in the internet. Instead of looking for suspicious data new systems have learned to look for suspicious patterns of traffic to identify and protect against fraud.

2. Advanced Access Management

If you still use a username and password to access your systems you should seriously consider moving to an advanced access management solution. In today's world, a combination of username and password is no longer secure enough. Instead, so-called multi-factor–authentication (MFA) is the way forward. The principle is to use at least two independent authentication methods, e.g. username and password, plus a second authentication method such as a PIN, TAN, SMS, or simply an app on your smartphone.

3. Enhanced Application Security

Security measures on the network, most systems are secured with an antivirus solution. In days of cyber-attacks this is also no longer enough. Enhanced application security consists of two additional measures:

1) Security driven release management, where applications, related patches, and service packs are updated for security reasons and not for new functionality

2) Pattern recognition in the application that allows for automatic detection of suspicious behavior. Most of these systems come with a machine learning code.

4. Trusted Attack Simulation

One of the most important cyber security principles is to identify security holes before hackers do. Trusted Attack Simulation, simulates attacks from outside and inside your IT, and gives you a report that identifies potential security holes in your IT. Internal attack simulation is as important as external attack simulation. Only if you assume a hacker can sit inside your management network you will introduce the correct measures.

5.Data Encryption

Today you have to assume that your data can be stolen, both when it is in transit, or directly from your servers and storage, where the data is at rest. The data encryption principle addresses are two

1) Encryption in Transit (EIT).

2) Encryption At Rest (EAR).

Only after data is encrypted at both stages, EIT and EAR, data is secure and it is much harder to derive information from it if stolen any.

VI. CONCLUSION

On the basis of the above study we have concluded that cyber security is most important in the virtual life for every woman. Awareness is the primary key for cyber security however, there are so many legal provisions to protect for women from the cyber crime. These days government provided toll free number that will resolve the problems belongings to cyber attack. It has made by government of India and implementing effectively by people. Cyber crime is not protected at this stage in future, no doubt in future it will be really a weapon.

Legal provisions should provide assurance to users, empowerment to law enforcement agencies. In this way we can say that women will change their mind then cyber attack will be decrease and in future status of women in India will change in security sector with all aspect of recorded Indian history.

REFERENCES

[1]. The six principles of cyber securityby NEOS, IT available at blog.neosit.com

[2]. Cyber crime prevention against women and children available at http:/ncw.nic.in

[3]. The Hindu, cyber crime touches new high by Abhinav Deshpandey available at the hindu.com/opinion/editorial

[4]. Types of cyber crime by panda available at http://www.pandasecurity.com

[5]. World health organization available at who.int/india/emergencies