International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 10, ISSN No. 2455-2143, Pages 155-158
Published Online February 2023 in IJEAST (http://www.ijeast.com)

ROLE OF CYBER SECURITY IN WOMEN AND CHILD PROTECTION

Prof Shilpa S Jadimath
Head of The Department
Department of Computer Application
Chetan College of Commerce, BCA and BBA,
Hubli, Karnataka - 580031

Abstract— **Cyber Security in Women and Child Protection is on the forefront of the Government of India's mandate to make India a digital nation. In this light, the Government of India in partnership with the International Telecommunication Union launched the "World Plan for Women and Child Internet" (WPCI) in 2011. The aim was to align global Internet policies with the Sustainable Development Goals. Moreover, the Ministry of Women and Child Development (WCD) has issued an advisory – Cyber safety and Use of Internet for Women and Children. Based on this advisory, the National Internet Crime Report-2017 states that between April-May 2017, the number of reported cybercrimes of women and children across India increased by 15.5% compared to previous year. In 2016, 74,633 reported cases of cybercrimes were registered with the National Crime Records Bureau (NCRB).**

Keywords— **Cyber, Security, Women, Children, Protection**

I. INTRODUCTION TO CYBER SECURITY SYSTEM OF INDIA**:**

Any business, company, or individual that deals with data storage, backup, and protection needs to be aware of the vulnerabilities. The complexity of cyber security is not determined by technology but by organizational and strategic framework. You can set up your own internal cyber security practices and mitigate the risks or you can outsource it to specialists like us who will provide complete cyber security solutions to you.

Being in the business of providing cyber security solutions, we focus on the evolving security needs of our customers. We strive to give the latest and most advanced cyber security tools to our customers so that they can address all their cyber security challenges and remain protected against the ever-growing threats.

Technology is changing fast, and therefore, cyber security needs to change as well. You need to have a consolidated framework for protection that is unique for your organization. Our technology coupled with strategic framework ensures you full security protection against the latest threats.

II. ROLE OF CYBER SECURITY IN WOMEN AND CHILD PROTECTION:

Cyber Security in Women and Child Protection is on the forefront of the Government of India's mandate to make India a digital nation. In this light, the Government of India in partnership with the International Telecommunication Union launched the "World Plan for Women and Child Internet" (WPCI) in 2011. The aim was to align global Internet policies with the Sustainable Development Goals.

Moreover, the Ministry of Women and Child Development (WCD) has issued an advisory – Cyber safety and Use of Internet for Women and Children. Based on this advisory, the National Internet Crime Report-2017 states that between April-May 2017, the number of reported cybercrimes of women and children across India increased by 15.5% compared to previous year. In 2016, 74,633 reported cases of cybercrimes were registered with the National Crime Records Bureau (NCRB).

"Internet is a powerful tool which helps to create awareness, solve problems and strengthen cyber systems and networks. This policy will not only create awareness but also will help women and children in the digital space by providing them with the needed support to access the Internet. The policy will ensure safety and security of women and children using Internet," stated a senior official from the WCD Ministry.

To protect women and children from cyber crimes, WCD released a policy on Cyber Security and Women and Child Protection, India in March 2016. The Ministry, along with Telecom Regulatory Authority of India (TRAI) launched a national "Cyber Security Awareness Programme" in April 2017.

III. THE CYBER SECURITY POLICY PRESCRIBES THE FOLLOWING MEASURES:

The policy has recommended that Data Protection Authority be constituted in accordance with the provisions of the Personal Data Protection Act of Europe and the Information Technology Act, 2000 (previously, the Information Technology Act, 2000) as applicable in India;

1. The policy has highlighted the need to follow online behavioral codes, especially in an anonymous or online environment;

2. The policy has proposed an effective 'cyber security code of conduct'; and
3. The policy has emphasized upon the need for the formation of an inter-ministerial task force, inter-ministerial committee and a national cyber security crisis management plan. Digital India is an integral part of the Indian government's vision to transform India into a digitally empowered society and a prosperous economy. In the long run, this will help India join global economies as a leader in technology. The key drivers of this digital agenda are an expanded use of the Internet. According to a survey by Pew Research Centre, 87 percent of the Indian population own or have access to a mobile phone. In the next five years, mobile phones are likely to emerge as the primary interface to access the Internet. For instance, in June 2016, an amendment to the definition of "digital network" under the Information Technology Act, 2000, allowed Internet service providers to classify the number of devices on their networks as "calls", "pictures", "emails" or "social networking". Thus, this helps mobile phone manufacturers and companies determine the retail price of their products.
4. This policy also has guidelines that pertain to the legal framework in India that pertains to Internet usage for women and children. It requires public authorities to have a departmental policy to make all government websites accessible in Indian languages. For the web for children, it encourages Indian websites to cater to the interest of the child and provide diverse and inclusive content.
5. Furthermore, the policy states that "adequate and preventive measures should be put in place to ensure protection of privacy and personal data of women and children; and for this purpose a Data Protection Authority shall be constituted under the provisions of the Personal Data Protection Act, 2000". Even if we use data protection principles from other countries that are closer to us, we will still be an advanced country, which is unusual. — Sunny Tejwani, Advocate & Advocate of Peace
6. The policy also focuses on creating awareness about cyber security. It recommends training programmes for women on digital literacy, gender sensitivity and violence prevention. It also has provisions for training children.

Commenting on the policy, Sunny Tejwani, Advocate and Advocate of Peace, said, "This policy is essentially for women, children, poor people and minorities. It reflects the fact that it has adopted a universal approach, which is an attempt to develop an environment that works in practice, and not just in theory. The policy is a blueprint for how to approach a problem and to design a solution. In today's environment, there is a lack of accessibility to many government departments. Hence, the policy emphasizes the need to connect the central government departments with the states to integrate efforts to make the country a digital nation.

The central government in India has started the Digital India programme to provide access to information through high-speed internet. When the government in the Centre already has a website, how are states expected to go about providing universal access to the internet?— Subhasis Choudhury, Professor of Management Studies, IIM Bangalore However, the announcement made by the minister in the press conference was that in the next three years, a total of 1.8 million gram panchayats (GPs) and 6,000 talukas (tahsils) will be connected to the network. This is a significant shift from the original goal of a target of a 50-60-70 percent internet penetration rate in India by 2017. The shift is in line with the Prime Minister's vision of digital India.

IV. IMPORTANCE OF AI AND ML IN CYBER SECURITY:

Gartner also noted that the number of cyber security vendors has doubled in the past five years. This is due to the increased number of smaller organizations and the emergence of micro-cap firms that find it more challenging to source adequate security capabilities, the report stated. “In this environment, many organizations find themselves stretched to match their existing or anticipated security needs in a short period of time, which has opened the door for companies such as IBM, Microsoft and others to step in and sell AI and ML-based technologies to fill their gap. The rapid increase in the number of vendors competing in the cyber security market, coupled with the declining cost of these technologies, will make it harder for vendors to differentiate,” the report stated.

Gartner’s report comes at a time when enterprises are facing a lot of pressure to strengthen their security. With companies becoming more aware of the latest security threats, the threat landscape is witnessing an increased threat. According to the report, the volume of cyber threats will grow by 30 percent in 2018, up from 25 percent in 2017. “Organizations can expect to see continued growth of artificial intelligence in the cyber security market, as well as continued expansion of cyber threat ecosystems and consolidation. We will see a greater focus on utilizing AI to more quickly detect threats and more quickly remediate cyber attacks,” the report stated.

Enterprises are now spending more time investigating each breach instead of trying to defend against them, the report stated. This will cause increased “mis configurations and the need for large-scale security operations centres,” it added.

The report also suggested that companies will shift their focus to implementing automated response systems (ARS) to perform human-free investigations and remediation. Additionally, cyber security tools will continue to be augmented by new hardware such as intrusion prevention systems and endpoint security hardware.

To sum it up, we can say that Artificial Intelligence and Machine Learning will play a huge role in solving the security issues faced by organizations today. The report mentioned that companies will deploy AI and ML to support the analysis,

analysis and transformation of security threats, as well as remediate breaches.

As per the report, “Artificial Intelligence is projected to allow security professionals to ‘triage’ the vast numbers of alerts that they’re receiving, on an ongoing basis. As such, security experts may have the time to detect and respond to threats in a fraction of the time, compared with traditional approaches.” The automation will allow security analysts to focus on specific types of threats, Gartner said. “Organizations will also have the ability to rapidly remediate breaches as the systems will detect an attack and provide a set of actions that employees can then take in order to contain the threat and, if necessary, apply a patch or fix the affected systems,” it stated.

V. CYBER SECURITY TIPS FOR WOMEN AND CHILDREN:

The Internet is an easy and inexpensive way to access the information and services that we take for granted every day. As with many things, there are risks involved, and protecting yourself online can be challenging. Cyber Security Awareness is not complicated. Understanding how computers and the Internet work and staying current on security measures and new cyber threats can make you more secure and safer on the web. For a quick but effective overview of basic cyber security. Here are some cyber security tips for women and children:

1. Always keep devices such as computers and phones updated with the latest software.
2. Don't download software or applications from sketchy sources such as "app stores" where the applications have not been reviewed by a third party.
3. Don't click on links in emails or text messages. Instead, open the document or email in a separate window or tab.
4. Do not give out personal information over the Internet or reply to messages that you don't recognize.
5. Never give financial information such as credit card or bank account numbers or passwords to people or businesses that you don't know.
6. Keep your software up-to-date to keep malware out of your computer and check your software regularly for suspicious behaviors.

VI. CONCLUSION:

It is already a fact that the incidence of cyber crimes has increased manifold in the country. With more and more people using mobile phones, internet and social media, cyber crimes have increased substantially. As the increased use of online facilities brings with it many new types of threats and vulnerabilities, the Cybercrime Investigation Cell (CCIC) of NCR Police has taken up the task of strengthening the existing capacity of the district level units to fight and prevent cyber crimes against women and children.

A strategy has been evolved for making the best use of the existing resources and integrating into the police act the Cyber Crime Cell as a specialised unit for effective action against cyber-related offences in the district.

VII. REFERENCE

[1]. Cyber-security. (2014). Network Security, 2014(1), 4. https://doi.org/10.1016/s1353-4858(14)70003-0 (pp 23-26).

[2]. Fattah, S., Sung, N.-M., Ahn, I.-Y., Ryu, M., & Yun, J. (2017). Building IoT Services for Aging in Place Using Standard-Based IoT Platforms and Heterogeneous IoT Products. Sensors, https://doi.org/10.3390/s1710231117 (pp 24-26).

[3]. Okunishi, T. (2017). IoT (IoT Supporting our Life and Industry）. Nippon Shokuhin Kagaku Kogaku Kaishi, https://doi.org/10.3136/nskkk.64.283 (pp 283–283).

[4]. Chirume Cobb, M. J. (2018). Plugging the skills gap: the vital role that women should play in cyber-security. Computer Fraud & Security, 2018(1), https://doi.org/10.1016/s1361-3723(18)30004-6 (pp. 5–8).

[5]. Chaoyong, Z., & Aiqiang, D. (2018). The coordination mechanism of supply chain finance based on block chain. IOP Conference Series: Earth and Environmental Science, https://doi.org/10.1088/1755-1315/189/6/062019 (pp 189).

[6]. Cyber Security through Blockchain Technology. (2019). International Journal of Engineering and Advanced Technology, 9(1), https://doi.org/10.35940/ijeat.a9836.109119 (pp 3821–3824)

[7]. Manjunath, P., & Shah, P. G. (2019). Exploratory Analysis of Block Chain Security Vulnerabilities. Australian Journal of Wireless Technologies, Mobility and Security, https://doi.org/10.21276/ausjournal/2019.1.1.2 (pp 5–10).

[8]. Kilani, Y. (2020). Cyber-security effect on organizational internal process: mediating role of technological infrastructure. Problems and Perspectives in Management, 18(1), https://doi.org/10.21511/ppm.18(1).2020.39 (pp 449–460).

[9]. Dubovyk, V. B. (2020). ROLE OF OSCE IN ENSURING CYBER SECURITY. Law Bulletin, 12, https://doi.org/10.32850/lb2414-4207.2020.12.12 (pp 87–91).

[10]. Nair, S., & Ravi, O. S. (2022). CYBER AUTONOMY AND IT’S ROLE IN INDIA’S CYBER SECURITY. GLOBAL JOURNAL for RESEARCH ANALYSIS, https://doi.org/10.36106/gjra/1704945 (pp 1–3).

[11]. Chauhan, A. (2022). Role of AI in Cyber Crime and Hampering National Security. SSRN Electronic

Journal. https://doi.org/10.2139/ssrn.4272952 (pp 28-48).

[12]. Mison, A., Davies, G., & Eden, P. (2022). Role of Big Tech in Future Cyber Defence. International Conference on Cyber Warfare and Security, 17(1), https://doi.org/10.34190/iccws.17.1.73 (pp 583–590).