

MILLENNIALS ON SOCIAL MEDIA AND CYBER SECURITY

Dharna Sehgal, Arti Vaish

E-Mail Id: dhaarnasehgal.ballb19@sushantuniversity.edu.in, vaisharti@gmail.com

Sushant University, Gurugram, Haryana, India

Abstract- In the modern day social media has become the most essential aspect in the modern society. These web based programmes help millennials to interact in the society with their friends, family and even with strangers, which is why understanding internet is extremely important. As much as a good time they have on the internet they do get in trouble sometimes, where cyber security plays an important role. This paper aims on how the generation Y has to have a better understanding of the internet where they know what is good and bad for them, what is right or wrong for them. Having a good and protected environment on the web will help the youngsters to have a safe place to be in. Since internet's instantaneous information, the broad reach of media influence makes it a glam space for generation Y, This research paper helps in explaining how social media is helping the young minds in their mind programming and how they have an impact over them, It also focuses on elaborating how to be safe on the web, keeping in mind all the instances which have had happened with youngsters on the internet.

Keywords: Cyber security, social media, millennials.

1. INTRODUCTION

Cyber security is an extremely vast terminology which covers all the applications of the latest technologies, processes functions and controls to safeguard the network, systems, devices, programmes and data from cyber-attack. It protects the computer systems from the unknown and unauthorized access. It focuses to reduce the rising risk of cyber-attacks and protection against illegal and unauthorized exploitations of the systems, data network. The entire cyber security's main emphasis is to help protect the integrity, confidentiality and set up of computer system against the illegal access. It safeguards all organizational assets from both internal and external threats as well as the damages caused by the natural disasters. Talking about cyber security also includes talking of internet as its most important aspect. Internet is one of the best innovations in the world of technologies. It is a vast network that connects people and computers all over the world. The invention of internet has helped the people to get connected even from far off places where they can communicate from anywhere and everywhere. The internet is one of those inventions which is now widely used by the people living worldwide. Using the internet is like a child's play, which is why it is widely used by the youngsters living worldwide. Even the surveys mark that 40-60% of the generation Y, the millennials make the most out of the internet. Youngsters right from 18 years to 34 years use internet for various different purposes. Website visitors within the age bracket of 18- 34 years mark and constitute as the largest group of online users in the entire world. Since it is predominantly used by most of the youngsters it is extremely important for them to understand what is good and bad for them. This automatically makes cyber security for the millennials an indispensable part of their life.

Social media is computer based application of technology, it provides a base on the internet where people interact with each other, share content with each other and make adequate use out of the social platforms, these socially available platforms include Facebook, Instagram, YouTube, LinkedIn and various other sites. The website shows that the maximum use on the web in of the youngsters within the age bracket of 20-40 years. The online content consumption of the generation Y includes sending emails, keeping up with friends, streaming music, watching movies, chatting and also video calling. It also includes research for work and keeping up with the news and other important information around the world. Surveys also present that they also indulge in online product shopping, looking for movie reviews, restaurant reviews, booking online tickets is another thing done by the youngsters. In a survey conducted in order to find out about the privacy concerns of the millennials, it was recorded that many of them did not bother over their privacy concerns and settings, while some of them did think about the personal data protection as important. Since every person uses a smart phone these days they also use social media, as it helps them surf on the websites and it helps them share some content on the networking sites. Social media helps the youngsters to get in touch and interact well with their friends and family and even with people who are strangers to them. Since social media is one of the best leading platforms to transfer knowledge in the world, it is predominantly used by youngsters than any other demographic. But as it is said everything has its own pros and cons. Social media also has its own.

1.1 Better Interactivity

The platform offers fantastic opportunities for student learning and it helps them with their education. In the present scenario of the covid world it is the only platform which is helping them interact and stay in touch with the teachers.

1.2 Good Connectivity

It is also helpful for common connection, one of the biggest advantages of social media is its extreme power to connect with people.

1.3 Knowledge

Giving and receiving knowledge and information becomes so fast, sharing ideas, opinions, thoughts and reviews becomes so easy, everything is just out there and so easily operational.

1.4 Engagement

Since engaging with each other is really an essential in the real life it is also important an internet existence in the in terms of engagement, the youngsters have a good command over it be it with their peers, friends, mentors or teachers.

1.5 Time to time information sharing

It makes conveying of messages so easy with just a click of a button, it eases student teacher information exchange easy. It also helps with the interaction with parents really simple.

1.6 Absenteeism of physical interaction

As almost everything is almost possible on the internet it could reduce the confidence for the face to face interaction with people. Because as it is important to know the web, it is extremely important to communicate with others in the real world.

1.7 Distraction to users

It definitely distracts the focus and diverts the attention of people, it also leads to a lower attention span and lack of concentration level for the future.

1.8 Bully on the web

Cyber bullying – social media platforms have become a base hub for online trolls and bullying on the web. Young people would write means messages about other people. This could highly impact the mental health of the millennials.

1.9 Time killing

It has become an easy past time method for the people at home or at work even while driving and at eating, this could really harm the productivity in the long run.

2. IMPORTANCE OF CYBER SECURITY

All the extremely sensitive information is of a great value to cyber criminals and the data thieves and the wrong doers, which is why it is so important to protect the data and information and have adequate knowledge of cyber security. The youngsters are often blamed for killing the traditional ways of behavior. As technology plays an important part in their day to day lives, the millennials can easily adapt to the new technologies and new ways of being. They are always on the go on their smart phones, laptops and tablets. It can-not be ignored that the millennials have an increasing influence on the world around them. The new addition of devices to the corporate networks is increasing rapidly and hence the attack of unforeseen vulnerabilities is also increasing. While 45% of millennials say they do not trust companies to keep their personal data safe and do not share it, they tend to be careless about device and application security Millennials eager to reap the benefits of new technologies must be mindful of keeping valuable data within their devices secure. Understanding why protecting devices and accounts is essential to growing an organization and critical to driving cyber security efforts. It is extremely important to keep the children safe from the potential threats. It keeps your personal information and passwords safe from cyber-attack. Almost everyone uses social media these days and everyone have had experienced some of the things like photo morphing, cyber stalking, bullying, fake accounts or sharing of passwords.

A recent survey of 3,359 people between the ages 18 and 26 in nine countries found:

- 63% click on potentially dangerous links
- 42% share passwords with non-family members
- 74% in the U.S. use unsecured public Wi-Fi despite well-documented security risks

The internet awareness is as much important as the internet knowledge is. As the millennials are much more tech-savvy than the other generations, they become easy targets to the cyber criminals and cyber data thieves. They are one of the most common victims of the crimes since it is so easy to make them a target. As they are so familiar with the internet their lax attitude makes them stuck in vulnerable situations. As we know that the millennials are in a habit of operating in a fast pace life, and they are also considered as the digital natives with an “all things digitally” approach to many aspects of their lives. Cyber-attacks are a constant threat to almost every individual as well as

every organization. The only reason cyber-attacks depend on the sheer decision making ability and human interactions of the people.

3. HOW TO IMBIBE CYBER-ATTACK PROTECTION?

A solid and effective security awareness training program significantly can reduce the risk of cyber-attacks. The youngsters should always check if they have been involved in data breach or not, the strengths of the passwords are really important and easy to hack so keep them strong. The shady emails should not be opened, always check the email id before you open the mail. Avoid the opening of random emails without thorough check. Always keep your device strongly protected with the help of anti-viruses. Millennials have immense amount of trust in technology so the functionality becomes easy with less consideration of risk. So the awareness programs should be aimed to spread caution while downloading data and storing data and work only on those site where you have grate trust in them. As they always prefer using their own devices this leads to a loss of control of data. The usage of personal devices mixes the personal information with the organizational data and hence varying the levels of security it also creates more backdoor sources for data and information. Also the awareness programmes can-not distinguish between work and home usage of computer systems. Special awareness programmes focused on how to protect personal devices and how to treat private and personal information safely. They use social media really heavily as it allows them to stay connected but also creates increased attacks medium. Sensitive information could be accidentally disclosed. Millennials should have awareness over the social media vulnerabilities. This could inculcate safe social media usage habits. If millennials are trained well they are likely to create a safe social space with less cyber-attacks. Researches show that young people have a shorter attention span since a lot of information is processed in their minds. The awareness efforts should be aimed to that only. Awareness sessions which are shorter and more affective, the awareness training should be aimed towards videos which are brief and that hit the aim. Good informative screensavers can be a method in spreading awareness, even the posters, laptop sleeves and coffee cup sleeves could be used as a medium of cyber safety protection. Even though they have a shorter span of attention they are more likely to have intellectual curiosity. They have a nature to explore certain things and come up with interesting conversations and readily available information is something which will feed their curiosity. The information and awareness material should be made available easily or that can even be posted online. Even videos also play an important role in spreading awareness because people can watch them anytime at their own will. They are really socially conscious and they want to create a positive impact in the world to make it a better place. The programmes should be aimed also towards the well-being of every one as a whole. The generation Y will always prefer things which are quicker and convenient and hence efficient programs can also be incorporated for the responsibility so that the awareness staff should also work.

4. SECURITY AND ITS LEGAL FRAMEWORK

The main governing legislation of the cyber space is the Information and technology act, 2000 which is the IT act. It defines cyber security as the protection of the information, equipment, devices, computer, computer resources and communication device and information stored therein from illegal or unauthorized access, disclosure, use, disruption, modification or destruction. In addition to the provision of legal recognition and protection for transaction carried through the electronic medium data and various other means of electronic communication. It also focus on information security, defines reasonable practices of safety and security which should be strictly followed. The Information Technology act not only extends to the whole of India but it is very much applicable to all and any offence or contravention which is committed outside India by any person. The act also extends to imprisonment, penalties and a framework of compensation and damages which should be paid to the claimants. One of the relevant information in these times can be made with the present scenario of the dependence of millennials over zoom. This led to number of unknown people crashing over into the zoom meetings. It definitely was causing some disruption with the flow of particular session. Also because of the data leak a lot of Chinese digital platforms on the web were also been banned by the Indian government. The principal of this act is to offer reliable legal security to e commerce, with real time records with the involvement of the government. As the attacks were getting frequent with the human tendency to misuse the technology a list of amendments followed in the act. It had special mentions with grave punishments and penalties safeguarding the e- governance, e-shopping, e-banking and other e-commerce sectors.

Section 43- is applicable to people who harm and damage the computer system without the owner's permission, the owner under this section has the full right to claim compensation for the entire damage in such a case.

Section 66- incase a person id found to be dishonest or commits any act in section 43 fraudulently with imprisonment up to three years or a fine up to five lakhs.

Section 66B- it incorporates the punishments for fraudulently receiving stolen communication devices or computers, which confirms a probable three years of imprisonment. The term can also be topped with rupees 1 lakh of fine, depending upon the severity.

Section 66C- This section scrutinizes the identity thefts related to imposter digital signatures, hacking of passwords or other distinctive identification features. If proven guilty the imprisonment of three years might also be backed with a fine of 1 lakh rupees.

Section 66D- This section was inserted on the demand, which focused on the punishing cheater who were impersonating computer resources.

The ever increasing cyber-attacks are currently ruling major newspaper headlines globally, causing unanticipated damages across industries and its individuals. The major types of cyber thefts are data breach identity theft, financial theft and internet time thefts among others. Though cyber security is advancing every day, hackers are also constantly upping their game and are finding ways to break into new systems. This reinforces the need of better cyber security systems but cyber laws as well. Further to mitigate the cyber-crimes efforts of the fraudsters need to be controlled and the law makers need to find the potential loopholes in the cyber-security landscape and fix them in real-time. The persistent efforts with constant vigilance are the crucial controlling factors which could control the escalating risks nationwide. There are so many cyber-attacks around us which are targeted directly towards the millennials. All these attacks become a part of cyber-crimes and need our serious attention.

5. CYBERCRIME

It is defined as a crime in which a computer is the object of the crime or is used as a tool to commit an offence. The crime could be attempted with the use of a device to access users system with its personal information, confidential business data, information related to government or disable the device which they use. It is also considered a crime when these information are sold in the market. It can also be defined as a criminal activity which targets and uses a computer or a network to cause harm. Mostly not all the crimes on the web created by criminals they could also be carried by individuals or even some organizations. Unfortunately Internet is not all about academia, friends and family connections. It is a huge space and it can be risky place for kids as well. There are number of dangers in the cyber space but mostly what happens is the cyber bullying and exposure to explosive content.

Types of Crime targeted to the millennials:

5.1 Identity theft

The most common thing happening on the internet is the fake profiles. Stealing other person's identity or their online account to post or send humiliating information. Misuse of other profile pictures. **LEARNING-** Keep your profiles locked and limited only to your known.

5.2 Cyber bullying

Youngsters when using the internet often become victims of cyber bullying. It could be done by any one, any stranger or anyone in your close circle. **Learning –** Always connect with people who you know and not people with unknown names or fake profiles

5.3 Photo morphing

It is the altering digital images so that the other person is in an embarrassing situation. It is done out of fun or rage and can also be harmful for lowering the confidence and dignity of people. **LEARNING-** Always make your profiles private, always lock your profiles and do not accept unknowns on your social media accounts.

5.4 Cyber stalking

This is a widely prevalent cyber-crime that is a risk to children online. Any-one can conceal their identity or use fake accounts or fake names to start a conversation online. **LEARNING-** Just like in childhood we were taught not to talk to strangers similarly not to talk to strangers online now.

5.5 Password attacks

Sometimes due to easy passwords the accounts get hacked. Teenagers are often observed sharing their passwords with their friend, which also lead to attacks. **LEARNINGS-** Keep a strong password and keep it to yourself. Do not share it with friends or even strangers.

6. CASE STUDY

6.1 Bullying

The Gurgaon police issued notice to a school with connection to an objectionable video on social media platform. Some boys were beating up other students in the washroom and the video was uploaded. The boys were severely punished over such an act. **LEARNING-** always convey to your teachers in school whenever something happens with you. Do not feel alone.

6.2 Kidnapping

A 16 year old was kidnapped by his friends and demanded money from parents. On knowing the involvement of police they killed him. LEARNINGS- Always inform your parents about where you are going. Share you location with your parents

6.3 Manav Singh Case

A seventeen year old boy names Manav Singh jumped from the 11th floor pf his building and he ultimately lost his life. During the controversy of the bois locker room, a teenage girl took to her Instagram and narrated a story of how she was raped over 2 years ago by Manav. She explicitly said that she had no proof about the same. The story told by the girl was immediately believed and the boy was declared a rapist as soon as the threats started coming in, within an hour Manav plunged his death. A 17 year old boy gave up his life over some serious allegations put up by a girl on Instagram. LEARNING- Always speak your truth and if you are being blackmailed let your parents know about that.

6.4 Bois locker room case

A group of boys on Instagram had a proper group where they shared morphed images of girls which were humiliating. The even shared their pictures and spoke about them in an objectionable manner. Later on a proper investigation was set up. LEARNINGS- Always choose your friend circle wisely, stay with people who you feel safe with. Always take a step back where you feel something objectionable is happening.

CONCLUSION

We all are well aware of the amount of time we spend on the internet, the way we get influenced easily on the internet. As we are so vulnerable it is important for us to understand what is good for us and what is bad for use, since every things has its own pros and cons. Cyber space battle is the infringement that we fight on everyday basis, India really needs strict and stringent laws and policy in better place to combat these major specific issues. The legal framework does not have sufficient levels and concerns to the sectors. Hence it is really important to address these major loopholes. As we choose to stay connected and we are moving towards assimilation of larger data sets, interacting with one another, this opens an entire eco system to a larger threats from society. It is completely on the individuals as well as the body corporates to preserve the safety and privacy of the data. As we welcome the impending legislation, companies in the healthcare and the banking & financial services sector are ensuring that they rely on their own technical and organizational security measures to ensure that the data available with them is not corrupted or is subject to any unwarranted and unauthorized access. Since social media is universally accepted, it has a huge impact over the lives of people. This research paper attempts to explain well about the advantages and disadvantages of social media over millennials. As it has both a positive as well as a negative impact over the youngsters. The proactive vigilance observed by the body corporates and private individuals, is also being supported by the insurance industry, where cyber-security insurances have garnered immense popularity, and are augmenting the lack of an effective legal regime. It is often said that the future is a click away, it is important that the click does not lead to any pernicious portal. All organizations need to understand their threat environment and the risks they face, address their cyber-security problems, and hire the most appropriate people to do that work. As much as social media is important for us so is our protection on the internet, and as we are the ones who consume most of the cyber space we need to be safe on the web. Hence cyber security is really important for the young minds as they are initially in a developing stage they should have the basic acumen of knowing what is right and what is wrong for them. Every step on the internet is really crucial for own protection. The young generation should be able to overcome the cons and disadvantages as well as the pros, so that it makes it a safer and much better place to be in. They should consume the internet well and not let the internet consume them. Hence having a strong, legalized and strict legal framework of cyber security is extremely important for the gen next. The government should be taking up awareness campaigns in each and every school and should talk to children so that they do not fear any-thing happening to them without their consent. In this way the millennials would have a safe space to be in, they could live a healthy and happy life which will automatically create better and productive generation ahead for the entire world.

REFERENCES

- [1] https://www.banalytics.tech/?gclid=CjwKCAiA78aNBhAIEiwA7B76p_nSfW8fkjcxz6PDWPz1xYt1RltOSIUqCs_MxozIQU8GntdUFXCexoCpAQA_vD_BwE
- [2] <https://economictimes.indiatimes.com/tech/internet/dear-millennials-here-is-why-you-are-a-soft-target-for-cyber-criminals/articleshow/61020568.cms>
- [3] <https://www.vu.edu.au/about-vu/news-events/study-space/5-easy-ways-to-protect-yourself-from-cyber-attacks>
- [4] <https://cybeready.com/cybersecurity-awareness-training-for-millennial-employees>
- [5] <https://www.appknox.com/blog/cybersecurity-laws-in-india>
- [6] <https://www.britannica.com/topic/cybercrime>
- [7] <https://www.ibm.com/topics/cybersecurity>

