Indian Netizens Are Yet Not Aware About Cybercrimes
Prachi Bharadwaj
C.S.E Student
Department of Computer Science and Engineering
Dr. A.P.J. Abdul Kalam Technical University, Lucknow (Formerly Uttar Pradesh Technical University), India

Abstract:
As per the reports and various organisation studies, it has been recorded that people in INDIA are still not aware of the cybercrimes and frauds taking place on various online and social media platforms. As per The New Indian Time Express: - “FBI stated INDIA is on the 3rd position among the top 20 crime crimes in the world”. The Hindu states over half of INDIA’S Netizens a victim of cybercrime \(^1\). India has witnessed a 457% rise in cybercrime from the year 2011 to 2016, a recent study said \(^2\). With the daily increasing numbers, it is crystal clear that INDIANS are still unaware of the cybercrimes and frauds taking placing and the practices to prevent the crimes against them. The lack of knowledge is giving more such privilege to the hackers to do such crimes. As per resources LIVE MINT “every 4 out of 10 INDIANS have experienced cybercrime”. INDIANS are still not using the internet with utmost responsibility and care. Thus the victim of cybercrime.

I. INTRODUCTION
Indians still unaware about WHAT CYBERCRIMES exactly are?
As per the data, the number of cybercrimes is getting doubled every upcoming year, this is most probably due to the lack of awareness in the country specially among the masses. Since the attackers search for the victim who is usually unaware about the security measures against cyber world hence it is easy to convince them and tackle them to get all the possible data required to do the necessary possible task. The chances are that the masses who are attacked, the most of them are like to be the senior citizens, small businesses owners, uneducated masses and children. As per The Times of India- “Cybercrimes against senior citizens makes up-to 10% of the total cybercrimes reported in India”. This is due of lack of awareness about the cyber frauds among them. Another study says that “in India every 10 minutes a new cybercrime takes place”. \(^4\) The above data clearly defines Indians are still not able to cope with the security measures in order to safe themselves from the cyber frauds, this is due to the fact that people still don’t know about what exactly cybercrimes are, how dangerous they are, how crimes takes place and how to be safe from them?
Only the Indians who are well-educated, technically sound, have taken part in the cyber security meeting or seminars, part of the schools where the cyber security campions took place once. Only those portions of people are aware about what exactly cybercrimes are and how to deal with them. But this population makes very less percent when compared was the whole country data.
Total number of cybercrimes reported across India from 2012 to 2018[5]
The graph 1 shows how linearly the crimes are increasing this too due to the increase in technology use but lack of awareness on how to use and be cautious.

What government is doing to prevent Cybercrimes?
We can see government is trying the level best to prevent cybercrimes from the following statements: -
Launch of online cybercrime reporting website/ portal www.cybercrime.gov.in. Launching of the Inter-Ministerial Committee on Phone Frauds for the various departments in India. Launching of www.mha.gov.in website. National Cybercrime Reporting Portal, www. cybercrime. gov.in launched by the central government to enable complainants against all types of cybercrimes, including net and online frauds the reports could be filled anonyms too. Setting up the new Cybercrimes cells in States and Union Territories for reporting and investigation of Cyber Crime cases. Government has set up cyber forensic training, investigation labs and forensic labs in various places in India. Imparting training to Police Officers and Judicial officers in the Training Labs established by the Government. Launching of the new Women Helpline to provide 24-hour emergency and non-emergency response to all women affected by violence. The official representatives are conducting seminars in schools to educate and train the young minds about the cybercrimes. Due to lack of awareness among the masses, the Indian Netizens are not able to take the advantage and boast them up with the facilities provided by the Indian government.

The only possible way to bring down the crime rate against children is that it should be made mandatory by the government to study crime security in primary schools to save the generation from crimes and from the impact or aftermaths of such crimes. Cybercrimes have a great negative impact of child’s mental growth and health. Although many teachers may be techie and experts with modern technology. This doesn’t mean that they’re prepared to provide guidance on cyber security and cybercrimes. First of all, the teachers should be trained in such a manner that they don’t force the students just mug up the subject in order to gain marks. The subject should be taught with more practical sessions and less theory sessions. The subject should be taught to the students with more hands-on experience rather than mugging up the definitions so that they are able to replicate the same teachings at their home.

Should Cyber Security be the part of the formal education in India?
According to Wikipedia- from 2013 stated that there were 229 million students enrolled in different accredited urban and rural schools of India. From Class I to XII. Besides parents, school plays a major role in child’s overall development the government should start introducing cyber security as a subject in the primary schools to train the children from the early age since this future generation should be made aware of the technology that they are using day and night and how this technology misuse could be a boon or curse. Thus, training the school going children would be beneficial to the government in future, because training the new generation about the cyber security will bring more aware future leaders to the society. Training the future leader at an early age will be fruitful to the government itself. Teaching such new security techniques will make the learning chain more powerful since these kids will teach the same at their homes and thus spreading awareness indirectly within the society. As per the BBC report the attackers are more likely to attack children for such crimes due to their innocence and lack to awareness towards cybercrimes.

Graph 2. Source- survey conducted with a sample size approx. 100 people

Over 55% of Netizens in 16-36 age group victim of cybercrime[9]
Source: - The Business Standard
According to the 'Norton Cyber Security Insights’ report 39% netizens have either experienced ransomware themselves or know someone who has. Netizens unknowingly admitting to sharing passwords of various accounts. When it comes to Wi-Fi usage, 30 per cent people agreed to have used their neighbour's Wi-Fi network without their permissions without actually know what is it used for, compared to 22 per cent of the overall respondents. While overall, one in four consumers regularly use public Wi-Fi connections available at airports, coffee and shops, this rises to 33 per cent among the crimes. Netizens also put cyber security at risk, by installing a third-party app and giving access to files while online and turning off their security software to gain access to free public Wi-Fi.
The above discussed issues and the number of victims can only and only be fixed by right knowledge and right understanding which could only be done by quality cyber awareness programmes among the masses.

Common forms of cybercrime in India

This include:
- Phishing: sending fake email messages in order to get personal information from internet users;
- Misusing personal information (identity theft);
- Hacking: shutting down, taking unauthorised access and misusing websites or computer networks;
- Spreading hate and inciting terrorism;
- Distributing child pornography;
- Grooming: making sexual advances to minors.
- Misuse of social media websites and threatening attacks
- Social engineering attack
- E-commerce and e-trading fraud
- E-banking fraud
- Online human trafficking
- Online drugs trafficking

The government rightly takes cybercrime very seriously, and we are working hard to fight it.

Spam calls and text messages

Scam calls which includes fraud attempts, money swindling and unknown links, accounted for 6% of all spam calls made in India in 2019 as per truecaller report. On an average, an Indian received 25.6 fake calls a month in 2019, a 15% increase from previous month. India stands on the 5th position in terms of most spam called country in the world, in 2018 as per truecaller. Another issue is that every 1 out of 3 women in India received sexually harassing calls and SMSs “on a regular basis”. Indians receive an average of 61 spam messages per month, the study revealed, and is the 8th worst country in the world in this regard, source by Truecaller. VOIP Calls are creating a way for hackers to choose and generate any country random number to call victims and try to get the maximum details as much as possible. Crimes caused using e-banking, e-commerce or any third-party app/portal while making online payments due to lack of policy and security awareness Indian Netizens not aware of the common types of cyber frauds as per the survey conducted among the sample size of approx. 100 people. It has been observed that masses don’t know about the laws, terms and conditions of the third-party websites while using e-banking or e-commerce and hence paving the way for the hackers to attack them.

It is always recommended never save your card details, bank details or personal details on any website be it like famous websites like amazon, flipkart, snapdeal and many more. The hackers can attack their database and get all your essential details. This practice can only be brought with proper awareness among the masses. Even another type of attack coming up nowadays is Phishing attack in this attacker sending the fake mails of fake websites to the victims and due to lack of knowledge about the crimes, the victims tends to click on the infected mail and opens the link. The link can ask for the details or from the link attacker can get the control over the victim’s device. Hence lack of awareness can lead up-to losing their device controls. The same could be done by social engineering by getting the victims details over a fake-call. One must know distinguish between the fake and real mails.
Since on public profile there is nothing private so anyone can use the photo or any other detail of the kid to misuse and to harass the kid. Giving apps permission to access their personal information is dangerous especially the mobile location. The hackers can track the kid’s every single movement and this could be dangerous. Since kids like to catch the attention of and gain approval from their peers, some like to post content to be popular or to gain a likes and followers from others in their online community, brag about the previous weekend’s adventures. This information is enough for an attacker to follow them, see the kid’s details and know their lifestyle. The best solution to above problems are only right education and awareness. Kids must try to keep all their accounts private and make friends on social media whom they know in person and not to accept of friend request of random people even if the request seems to be coming from the girl’s account because hackers tend to make the fake profile of girl since it is easy to win a friendship if the girl is sending a request.

**SEX Trafficking and child pornography on internet**

Usually the attackers first know the child by seeing his/her profile and tries to connect to the victim who are usually children who are depressed, vulnerable, isolated from the family and friends after connecting to the victim the attackers try to win the trust of the victim any-how that could be pampering, sending e Gifts, sending e-vouchers and many more just in other to make them feel special. After winning the trust the attacker ask to share their photos and videos with them. These attackers post such pics on the dark web or on internet and earn money via sex trafficking.

**Unawareness on Social Websites**

Children are posting a tremendous amount of information on their online public profiles, so it is vitally important from them to use strict privacy settings Normally kids tend to start speaking to strangers online, playing over-18’s games and being exposed to violent and sexual content that is not appropriate for their age. Teens overwhelmingly choose Snapchat, Instagram and Facebook. Of course, kids also flock to Twitter, WhatsApp, and used for microblogging, live video streaming, video/photo-sharing, texting, and chatting/dating. Teens especially under 13 years are spending enormous amounts of time on a daily basis communicating with unknowns, putting them at greater risk. Teens are not aware of the crimes that they could face and they are using social media recklessly.

**The consequences of such unawareness are:**

Foremost risk is kids talking to any stranger on social media without knowing the aftermath of the conversation. They don’t know the true identity of that person. All too often, we hear the cases of adult male who makes a fake social media profile, and over time grooms a child, wins the child’s trust, and ultimately asks for nude/obscene photos (possibly threatening/blackmailing the child if he or she denies). This is dangerous. Sharing their details without the knowledge of the stranger’s background. Children with open profile are more likely to be messaged by the strangers and harassed by attackers.

Since on public profile there is nothing private so anyone can use the photo or any other detail of the kid to misuse and to harass the kid. Giving apps permission to access their personal information is dangerous especially the mobile location. The hackers can track the kid’s every single movement and this could be dangerous. Since kids like to catch the attention of and gain approval from their peers, some like to post content to be popular or to gain a likes and followers from others in their online community, brag about the previous weekend’s adventures. This information is enough for an attacker to follow them, see the kid’s details and know their lifestyle. The best solution to above problems are only right education and awareness. Kids must try to keep all their accounts private and make friends on social media whom they know in person and not to accept of friend request of random people even if the request seems to be coming from the girl’s account because hackers tend to make the fake profile of girl since it is easy to win a friendship if the girl is sending a request.

**SEX Trafficking and child pornography on internet**

Usually the attackers first know the child by seeing his/her profile and tries to connect to the victim who are usually children who are depressed, vulnerable, isolated from the family and friends after connecting to the victim the attackers try to win the trust of the victim any-how that could be pampering, sending e Gifts, sending e-vouchers and many more just in other to make them feel special. After winning the trust the attacker ask to share their photos and videos with them. These attackers post such pics on the dark web or on internet and earn money via sex trafficking.

---

**The Cycle of Abuse**

The figure 4 clearly explains the entire process of sex trafficking. Online grooming takes place in a short time or over long time. During the initial stag attacker can appear innocent, but often involve some level of deception. Attacker (usually an adult) attempts to establish a relationship to gain a child’s trust, he can lie about his age or may never reveal his real identity to the child, even after establishing online relationship. Often, the groomer will talk about the topics child like’s and will try to relate to the child. These tactics lead children to believe that the groomer is the only person who understands him/her. After
the child’s trust develops, the groomer use sexually explicit conversations to test child’s natural curiosity about sex. Predators often use pornography and child pornography to lower a child’s inhibitions and use their adult status to influence and control a child’s behaviour. The graph 6 below shows the main reason of such activities is again lack is awareness among the parents as well as the children. People are not aware of online human trafficking as well of online sex trafficking.

The only and only ways to protect children against such frauds is to impart right education to the children at the right age in their schools so that they are not the victim of such crimes and teach them the correct use of internet. Proper use of social media accounts with utmost privacy and sincerity.

Online human trafficking
This is also increasing many reasons are like due to rise of unemployment in the country the people get fooled online by the traffickers and goes to the place where the traffickers call them to meet up and they get misused. The other reason could be the dating apps and fraud people talking on such apps who convince the girls to meet them up at a specific place and then they girl is the victim of human trafficking. This is all due to lack of awareness on the online platform. Basically, the attackers target those victims who are finically weak, depressed, isolated, don’t find themselves fit for the society, being a victim of body shaming and many more reasons. These attackers praise them, make them feel special and one fine day they make them the victim of human trafficking. This is lack of awareness among people that the person behind the screen is unknown and can’t be trusted blindly.

Online Drugs Trafficking
This is another kind of the crime with the serve punishment if found guilty in the court. Online drugs trafficking is not only confined to India, it is increasing rapidly in various parts of the world. Basically, the attackers look for a victim who is financially unstable and they try to contact them up via any web platform, they build the trust and victim think them as the well-wishers. The attackers offer the victim usually with a deal that if they take the drug or a simple bag (without disclosing the items bag will carry) to so and so place then they will be given a huge amount. The victim who is usually financially unstable didn’t think the carrying drugs is a crime and found guilty would end their entire life into jail. The victims also don’t cross check the details of the attackers neither they meet them in person nor they call them up to know their identity the entire planning-plotting and conversation is usually done chat via an online platform. Hence when the victim is caught red-handed and arrested in charge of drugs trafficking by police.

The victim tries to uses the online platform to contact to the traffickers to seek for help but they are found no-where on web. Thus, even if you are suffering from financial or any kind of instability people should be aware of such type of well-wishers on internet. Right awareness should be among people that carrying and supplying drugs is not the solution. The government should make people aware about the laws for carrying drugs so that people don’t commit such type of crimes be it online or offline.

Graph.6. Source- survey conducted with sample size of approx. 100 people

Graph.7. Source- Survey conducted with the sample size approx. 100 people

Young Girls/Women being victim of obscenity or sexual harassment
This is the most heated topic and matter of concern and dignity for the country. The such types of crimes take place due to lack of awareness and irresponsibility among the girls and women while using internet and social networking sites. One could say that the attackers doing such type obscene crimes could be mentally sick or have been in an inferiority complex once in their lifetime that’s why they are doing such obscene things. Women especially girls should NEVER attend any UNKNOWN VIDEO calls on what’s app or any other app under any circumstances. The attackers video call females and when the receiver answers they wait for the victim to show the sudden and suddenly they start flashing their private parts and takes the screenshot of the video call that’s done for the friction of seconds. The victim declines that call as soon as possible but he attacker who took the screen shot in friction of seconds uses the photos on various adult websites with the victim phone number. This is all due to lack of awareness among the girls. They should not answer any unknown video call such incidents are common to happen. The only solution is that the females should be made aware not to answer the unknow video calls, even if the girl answers the call unknowingly then she must make the camera face the rooftop or ceiling of the room, or cover the camera entirely black by putting the thumb and not to show her face until she knows the person is genuine or known to talk.

Graph.8. Source- Survey conducted with the sample size approx. 100 people
Online Romance giving rise to Cybercrimes

Women, middle-aged people, and individuals with higher tendencies to anxiety, romantic idealization of affective relations, impulsiveness and susceptibility to relational addiction are at higher risk of being victims of the scam. Online romance scams are, in other words, relationships constructed through websites for the purpose of deceiving unsuspecting victims in order to extort money from them. The scammer always acts empathetically and attempts to create the impression in the victim that the two are perfectly synced in their shared view of life. After this hook-up phase, the scammer starts talking about the possibility of actually meeting up, which will be postponed several times due to apparently urgent problems or desperate situations such as accidents, deaths, surgeries or sudden hospitalizations for which the unwitting victim will be manipulated into sending money to cover the momentary emergency. Using the strategy of “testing-the-water”, the scammer asks the victim for small gifts, usually to ensure the continuance of the relationship, such as a webcam, which, if successful, leads to increasingly expensive gifts up to large sums of money. When the money arrives from the victim, the scammer proposes a new encounter. The request for money can also be made to cover the travel costs involved in the illusory meeting. In this phase, the victim may start having second thoughts or showing doubt about the intentions of the partner and gradually decide to break off the relationship. In some cases, the scammer may ask the victim to send private photos that can be used to blackmail to further bind the victim to the scammer.

Once the scam is discovered, the emotional reaction of the victim may go through various phases:

feelings of shock, anger or shame, the perception of having been emotionally violated (a kind of emotional rape), loss of trust in people, a sensation of disgust towards oneself or the perpetrator of the crime and a feeling of mourning. The user of such websites should be alert, emotionally balanced and controlled. One can’t start expelling the emotions on the virtual platform until you really know that the person is genuine or you have a reference from a common friend. Being alert and sound is the only precaution to such crimes and having the proper awareness with such types of crimes will help you to figure out the person talking you on the social platform is genuine or not.

Measures to spread Awareness among the masses

Following steps could be considered and should be taken by the government to put a brake to such crimes: -

1. First of all the people should learn about the online crime reporting official website of the Indian government i.e. www.cybercrime.gov.in and have the general idea who it is working. The school students should be made aware of this website since children learn fast and they could spread the news fast. The citizens should learn the website URL as they know the URL of famous websites like those of Facebook, Instagram, twitter and many more.
2. Sending SMS’s to masses mobile phones to make them aware of the government crime reporting website.
3. Putting up banner and hoarding in public places to make them aware of the website and some popular cybercrimes like kyc fraud, oix fraud and may more.
4. Let’s make the social media work in an innovative way, the government can send notifications to citizens social media accounts daily or on regular basics. Put up awareness story on social media accounts as ads and regulate these on regularly.
5. Kids are most active on social media on Instagram and snapchat. So do the government can try to use these accounts to do spread awareness. The government official cyber crime account could be set up and should be promoted and at least the story should be circulated in form of ads to spread awareness about the crimes and other measures that the officials think necessary for the public to know.
6. From the figure we can see the major states and cities with maximum cybercrimes. The government should try to reduced the crimes by introducing awareness campaigns to such places and more send kind of sms to the people to make them alert about such crimes. The officials should make people aware of such stats making people realise that an irresponsible attitude can led up-to millions money to the hacker.
about the latest crime happening in the country and the safety precautions to overcome such crimes especially with girls.

5. As we know, now honourable Supreme Court of India have started sending summons via what’s app so if the Supreme Court can send official notices via what’s app in the similar way the cybercrime department can also send the awareness and other cyber crime related precautions to masses via what’s app in the form of audio message, video message or pdf document.

6. The caller-tune of the mobile can be changed with time to time with the message of cyber security as India did in the case of COVID-19 pandemic, by making people aware of the symptoms of the COVID-19 Pandemic.

7. Newspaper ads and pamphlets are the other few ways to aware the common masses in the easiest way possible.

8. The young generation are more active on YouTube the cyber security team can start posting videos about the various cybercrimes and how to prevent them in the simplest way possible with the verified YouTube so that people can verify content posted is real and genuine.

9. Even the cyber crime officers can collaborate with the famous YouTubers in India and spread the message of cyber aware in the easiest way possible. These famous YouTubers already have good amount of crowd following them so it will be easy for them to spread the message among the masses in one go.

10. The government can start collaborating with the Famous Dignities of the Bollywood and ask them to spread cybercrimes awareness via their blogs, social media accounts and via commercial tv ads. Since people follow the stars or famous dignities they like and are likely to remember what they say. Hence asking such dignities to help in cyber awareness would be a great help to the cyber department of India.

11. The police should train the masses on how to report the obscene content on internet then they came across it. This training could be done on online free session, via YouTube or SMS. Many people came across obscene content online but they don’t know how to report it, teaching them how to report will decline the rate of spreading of such type of nude and obscene content every evening to tell the locals about most reported cyber-crime that is being reported in their local police station and send the SMS in which the details are mentioned like

- Top 3 cybercrimes reported in the police station with number of cases
- Method used by the attacker
- Precaution for the public

SMS with all the above details should be send to the masses mobile numbers daily as per the police station they fall under. The SMS should be send by each Police station to every citizen of India but according to the police station they fall under so that people come to know which type of the cyber crime is happening in their area. For instance - The police station in SADAR BAZAR, Agra should send the message to all the people/ local residents who come under SADAR BAZAR police station. The SMS sent will be able to make local people of SADAR BAZAR area aware about Cybercrimes and they will be more alert next time while using the internet.

SADAR BAZAR Police-Station, Agra
Top 3 Cyber Crimes reported on 02/07/2020
1. Photo blackmail - 12 cases
2. KYC fraud - 07 cases
3. E-banking - 03 cases

Photo blackmail - In such a crime the victim sends her photo or involve in a video call with unknown person and thinks that he is genuine But later the same person blackmails the girl, ask for ransom and threatens her that pictures would be leaked on adult websites if she refuses or denies to pay the amount.

Precaution - Do not share your photos with any unknown person, whether girl or boy. Never answer a video call from an unknown number and from an unknown person.

12. Removal of fear of police especially among kids about reporting the crimes to the police. The school should teach the kids about reporting the crime and not to be afraid from the police and investigation if any mishapening happens with them.

TECHNICAL SOLUTION- POLICING APPLICATION proposed

The police can start with a MESSAGING SYSTEM which can start sending SMS to the people about the everyday in the
The figure 7 is the example of the kind of the message the police station can send to its locals in HINDI language. The SMS should be sent in simple language without any technical terms in ENGLISH as well as in LOCAL LANGUAGE of that area so that everyone can understand the motive of the SMS.

II. CONCLUSION

It’s good that Indians are learning quickly how to use and be more active on internet. We know that a coin has two sides – bad side and good side. We should use the internet for the learning and other purpose but on the other hand not to make using internet curse for others by looting them or misusing their privacy that’s what usually a attacker do. The people should know the pros and cons of everything or every single app that they are using in their smart phones. They should be enthusiastic in learning all the possible pros and cons of the apps. This enthusiast will only come when people will be made aware about cyber-crime and the flaws in each and every app that they are using in their day to day lives. The government have come forward with the cyber experts in the country to make people aware and not to bring down the people trust while using such apps. Like government is promoting cashless payments but thousands of cases are reported in the country regarding cashless payment apps like paytm, e-banking crimes. So, the people or netizens loose hope and trust in using the internet or advance technology. The government if promoting cashless or e-payments then other hand the government should make people aware on how to use e-payments platforms wisely and what types of cyber frauds can happen and how to prevent oneself from being the victim of while doing cashless payments. Then only the rate of cyber crime will come down. Only introducing the new technology should not be the goal teaching them how to use wisely with all the precautions should be the goal. The teaching could only be imparted with right knowledge and right understanding. The people on the other hand should be curious and try to make themselves be aware about the latest cybercrimes happening in the country. If the netizens are not interested with all the cybercrimes, then at least they should have the urge to have the knowledge of the cybercrimes that could take place on the apps or the social websites that they are using in order to keep themselves only safe.

III. REFERENCES