Volume 9, Issue II, March 2020, ISSN: 2277-1255
BHARTIYAM INTERNATIONAL JOURNAL OF EDUCATION & RESEARCH
A quarterly peer reviewed International Journal of Research & Education

AWARING PARENTS ABOUT CYBER CRIME

***Ms. Sunita**

Abstract

Cyber crime is a new breed of worldwide crime plaguing the world. Basically, cybercrimes are crimes conducted via the Internet with the use of computers or related devices. Cyber crime may threaten a person or a nation,s security and financial health. Now a day's cyber crime is becoming a last growing area of crime. Anyone in the world can become the victim of it. May criminals are taking the advantage of it and they do criminal activities. It contains many activities like Trogen attack, Virus, haking, information theft, stealing money while transactions etc. So it becomes necessary for us to be aware of cyber crime and cyber law made deal with cyber crime. In this paper, I have discussed the types of cyber crime, which can help people to identify the crime that they have been victim of and have discussed the cyber law, its awareness program and Information Act 2000.

Key Word: Cybercrime

Introduction:

Cybercrime is an upcoming crime. Basically, cybercrimes are crimes conducted via the Internet with the use of computers or related devices. Its beginning can be traced to the growing dependence on computers in modern life.

We all are at risk. The threat is serious and it is growing. Cybercrimes are becoming more dangerous and sophisticated. Parents, as well as kids, are at risk. However young people are more prone to cybercrimes, because relatively they are more active on the Internet and in most cases naïve on Internet safety.

There are various kinds of cybercrimes out there, each bringing consequences with it. Other scams steal identity or credit card information. Cybercriminals are modifying their ways to target fast-growing mobile platforms and social networks where consumers are less aware of security risks.

However one of the best ways to avoid being a victim of cybercrimes and protecting sensitive information is by making use of impenetrable security that uses a unified system of network which is sent to other users.

***Assistant Professor VASMM, Bahadurgarh Email: sunitasharma93550@gmail.com**

Cyber World: A world full of charms and attractions

The present time of Computers, Laptops, Androids, and Internet etc. creates a world full of charms and attractions especially for the young generations they are devoting their entire time to this Cyber World. Computing power, development in communication technology and Internet Created a parallel world; a society within the large human society. We call that "Cyberspace". Cyberspace is a virtual community consisting of people connected to the internet. Present day youth or we can say students are the major part of this Cyber World. This world is full of fantasies and in other language; we can say is full of artificialities and hypocrisy. To live in the online world, a person needs a new online personality but it doesn't need to be an exact copy of his/her real life. Anonymity is guaranteed in Cyber World. Most people have entirely different personalities ranging from using aliases for names to changing their behavior and even gender. For example a shy and fearful mama's child can become an internet hero. A person who can't even look at girls in the real life can acts as a playboy in the internet or a virgin in real life can even have cyber- sex. As the students belong to a generation which lacks maturity, so they are attracted to this imaginary and hypocritical world full of charms and attractions, more easily than adults.

Impacts Of Cyberspace

In the busy schedules of every individual in today's scenario people hardly get time for a lot of basic things. In such situations internet is like a life savior for them. Not only internet provides them informational resources making their work easy but also gives them various resources for entertainment making them not hit boredom. Social networking is a wide entertainment network itself. The internet is a virtual library of information. There are search engines like Google and Yahoo at service 24 hours a day and 7 days a week. You can get information like who was the first person to fly a plane or the dollar's current value. Just a click is all what is takes, from clothes to grocery all is at your doorstep. Social networking also plays a major role in cyberspace. One cannot imagine his/her life without facebook and twitter. Social networking has become so popular among youth that it might one day replace physical networking. People are more into meeting new people and making new friends through social media that they are losing their own identity. People are forgetting giving time to family relations rather they are more comfortable spending time virtually. They use various apps to get over any sort of depression or problem. Technically, the disadvantages outweigh the advantages more because of the security and dangers that is entitles within. You never know who is accessing your personal information but

apart from security issues there are much bigger consequences of getting too involved in cyber world. From mental to social well being, from schedule to body clock, from family relations to morals everything is damaged to a greater extent.

Types Of Cyber Crime:

Cyber crimes can be of the following types

A. Hacking- In this type of crime person's computer is accessed by criminals without the knowledge of person from remote locations. Hacking is done to access the personal, confidential or sensitive information from person's computer. Hacking can also be done to change the passwords of login accounts either of social networking sites or any other business transaction site and use the information against them.

B. Theft- When a person violates or breaks the copyrights of a particular website and download songs, games, movies and software is known as theft. There are many websites which allow downloading the data that is copied from other websites. It is known as pirated data as the quality of data is not up to the mark.

C. Identity theft- In this type of crime, criminals steal data about person's bank account number, credit card number, debit card and other confidential data to transfer money to his account or buy things online by acting as the original person i.e. the criminal stalks the identity of person and thus it is known as identity theft. This theft can result in huge economical loss to the victim.

D. Defamation- In this attack, the criminal hacks the email account of a person and send mails using abusive languages to known persons' mail accounts so as to lower the dignity or fame of the person.

E. Malicious software- These are the programs or software that are used to access the system to steal confidential data of the organization or this software can be used to damage the hardware and software of the system.

F. Cyber Stalking- This is the type of attack where online messages and e-mails are bombarded on victim's system. In cyber staking, internet is used to harass an individual, group or organization by using defamation, identity theft, solicitation for sex, false accusations etc.

G. E-mail harassment- In this type of attack, the victim is harassed by receiving letters, attachments in files and folders Email.

How Parents Can Protect Their Children Against Cybercrimes:

Here are some quick tips that parents can follow to protect their children from being a victim of cyber crime –

1) Questionable websites should be avoided.

2) Use safety programs. Teach your kids online safety rules.

3) Keep back-up volumes so that one may not suffer data loss in case of virus contamination.

4) Moreover avoid getting into huge arguments online It has been rightly said that "Prevention is better than cure" so. We should follow certain rules while operating the internet. So one should keep in mind the following:

A. Be cautious on meeting online introduced person.

B. Big organizations should implement access control system using firewalls, which allow only authorized communications between the internal and external network.

C. The use of password is most common for security of network system. Password should be changed after regular interval of time and should be alpha numeric and should be difficult to judge.

5) Basically, cybercrimes are crimes conducted via the Internet with the use of computers or related devices.

Good Habits:

Cyber criminals rely on our laziness and depend on our bad habits to make us vulnerable. Replacing bad habits with good habits isn't difficult; it's just a matter of re-training yourself.

- **Avoid unsecured wireless**. Stay on the cellular network whenever possible. If you must use Wi-Fi, make sure it requires a password and check on the security.

- **Bring your own tools**. Use your own laptop and Internet hot spot. Be in control of your own security.

- **Practice Selfie Awareness**. Photos which are shared online reveal a lot of information such as any landmark in the background can pinpoint a location, even if you have restrained yourself from tagging in the photo. A vehicle license plate, a security badge, a keypad a company logo – these are all key pieces of information that are often ignored when framing a photo.

Steps to take to stay safe online

Following the below safely measures for posting information does not guarantee safety but it can eliminate the risk of exposure just as locking the door to our homes limits the ability for a burglar to easily enter the house.

- Pay attention to the information that can be identified in photos. Ensure that your photo background does not show your actual location.
- understand the privacy settings associated with the site.
- Set appropriate privacy and security setting and choose a complex password that has nothing to do with the information that has been posted online.
- Be careful when installing third party applications.
- only accept friend request from people that you know. (it is strongly advised that you do not accept friends- of- friends).
- Read the privacy policy and terms of service.
- consider all information public.
- Of course none of this is to suggest that you should step using social media entirely. The dangers internet in social networking stem precisely because of its power and use fullness. But as in all things, with great power comes great responsibility Here are a few tips to keep you safe as you enjoy facebook, Twitter instagram and all other social networks:-‘
- make sure your account information and posts are onlyavailable to the people you want to share with. Even then aviod felling out lost of personal information in your profiles. Details like your hometown, birthday and siblings names can easily be used to get around password reset security so that information should not appear on your facebook profile.

- If you are posting something you wouldn't want your parents to see or your boy friend if so, that's probably not something you should post at all on social media.
- Especially when it comes to your children or other menors, do not post anything that might be remotely considered compromising or embarrassing and don't share plans that can let other find them.
- you never want to post information that tells people when you will be away from home for an extended period. There have been many many instances of stalkers using this information to confront victims, or buglers using it to break into homes. save your vacation post when you get back home.

Conclusion:

With the increase in the users of internet, the increase in cyber crimes can also be seen. Hacking is the method in which the criminals get access to the victim's system without their knowledge. Cyber crime can be done mainly by using the technique of hacking. All the persons who use internet and especially those make money transactions through internet must be beware of the cyber criminals. It is the need of today's world to have knowledge about the crimes that are associated with the internet. It is the duty of each one of us to be aware of the basic internet security like changing the passwords regularly, keeping long passwords, avoids disclosing personal information to strangers on the internet or entering credit card details on unsecured websites to avoid any fraud, etc. Government is also making efforts to have a control on these cyber crimes. Government has made cyber laws to help people learn about the cyber crimes and cyber security. IT Act 2000 is made to deal with the cyber crimes. People who have been the victim of cyber crime should come forward and file a complaint against the crime in special anti cyber crime cells. Government should also employee officers with very high intelligent quotient and the knowledge about all the cyber crimes. This will help to catch the criminals very easily and all the criminals must be given hard punishments which can a lesson for millions of other cyber criminals. Awareness of the persons using internet will definitely help to curb the cyber crimes and once, all the people are aware of the cyber crime, no criminal would ever think to commit the cyber crime.

REFERENCES:

1. Information regarding cyber laws, IT Act 2000 from http://www.cyberlawsindia.net/cyber-india.html

2. Grooming attacks of children available from http://www.peacepalacelibrary.nl/2013/10/protecting-children-from-cybercrime-online-child-grooming/

3. An introduction to cyber crime from http://www.crossdomainsolutions.com/cyber-crime/

4. Phil Williams, Organized Crime and Cybercrime: Synergies, Trends, and Responses, Retrieved December 5, 2006 from Available: http:// www.pitt.edu/~rcss/toc.html

5. Parthasarathi Pati - Cyber Crime

6. V. Shiva Kumar - Cyber Crime - Prevention and Detection

7. Dr. B.Muthukumaran – Cyber Crime Scenario In India

8. Nagpar R. - What is Cyber Crime?

9. Duggal Pawan - Cybercrime