RAHUL KR. VERMA
ADVOCATE

SOCIAL MEDIA CRIMES

Question No.1: What is the social media networking and its effects?

Answer. Now in these days, more and more people, regardless of their age and gender, are signing up for profiles on online social networks for connecting with each other in this virtual world. Some have hundreds or thousands of friends and followers spread across multiple profiles. But at the same time there is proliferation of fake profiles also. Fake profiles often spam legitimate users, posting inappropriate or illegal content. Fake profiles are also created while misrepresenting some known person to cause harassment to him/her.

The most common targeted websites/apps for creating 'Fake Profiles' are as Facebook, Facebook Massanger, Instagram, Twitter, LinkedIn, Whatsapp, Telegram, Snapchat, MySpace, Hike etc..

Question 2: what are the Web/Online Threats?

Answer: Web-based threats, or online threats, are a category of cybersecurity risks that may cause an undesirable event or action via the internet.

Web threats are made possible by end-user vulnerabilities, web service developers/operators, or web services themselves. Regardless of intent or cause, the consequences of a web threat may damage both individuals and organizations.

Internet-based threats expose people and computer systems to harm online. A broad scope of dangers fits into this category, including well-known threats like phishing and computer viruses. However, other threats, like offline data theft, can also be considered part of this group.

Web threats are not limited to online activity but ultimately involve the internet at some stage for inflicted harm. While not all web threats are created deliberately, many are intended — or have the potential — to cause **Access denial, Access acquisition or** Unauthorized or unwanted use of computer and/or network services.

As we continue to rely more on the web for daily living, it will keep exponentially rising as an attractive attack option for malicious parties. Convenience and a lack of caution around web use are among the top concerns that continue to pose new risks to privacy and security.

While targets are typically computer-based, human victims ultimately experience the lasting effects of a web threat.

Question No. 3. What are the Advantages of social networking sites?

Answer. Social networking sites are the major platform on the internet for communication and exchange of information since the early 21st century. In the early stage of the social networking era, people from all around the world started using to connect with friends and families to share and communicate through photos or text messages. Since the development and rapid growth of the internet speed, the usages increased more towards generating and sharing media such as photos, GIFs, and videos.

There are many different social media sites for different purposes, for example, Linkedin is a social network for professionals, while Snapchat is a social network targeted mostly at teenagers. There are also many drawbacks and benefits of social media platforms. Modern social networking sites are not just about connecting and sharing information, such platforms are being used for many different purposes. Most people are still using social media for "social purpose" while many are using for the business purpose. Government, security agencies, researchers, etc are also using social media for official purposes.

Though the usages and user behavior in different social media sites may differ, there are common pros and cons of all social networking sites or social media platforms. For example, there are more advantages for photographers or artists using Instagram while he/she may not get more benefits or attention on Twitter. Similarly, a journalist or author may have many pros of using Twitter.

It is many advantages such as:-

1. Networking without border:
One of the primary goals of any social networking site, networking is a primary feature any social media platform has to offers to consider the platform as a social networking site. One of the most important and noteworthy advantages of social networking sites is that it enables everyone to connect no matter which country they belong to.

2. Instant News and Information
Before the social media era, we used to communicate on email and instant messengers like Yahoo, AOL, and MSN. All those IMs and communication tools were mostly one to one communication. But on Social networking sites, communication can be one-to-many instantly. We do not have to look for the

news by visiting different news websites, the news will find us on modern social networking sites like Facebook, Twitter
And there are other advantages of social media is exisiting in the cyber world such as Great marketing channel for Business, Awareness and activism, Exchange of ideas and Collaboration, Stay in touch,

Question No. 4: What are the disadvantages of social networking sites?

Answer: As far as Disadvantages of Social Media Sites are concerned..

It is like any other tool available for humans, Social Media Websites also have many disadvantages if you do not use them consciously. Unware social media users may encounter many different types of problems while using social networking sites. Here we list a few but most important cons of social media that everyone should be aware of.

1. Addiction. The compulsive behavior developed due to social networking sites like Facebook, Instagram, Tiktok, YouTube, etc leads to negative effects. Social networking addict constantly checks Social Media Feed or checks out people's profiles for hours and hours. The compulsion to use social media can make one social media addict. Researchers at Chicago University concluded that social media addiction can be stronger than addiction to cigarettes and alcohol.

2. Mental Illness. Social networking sites are linked to an increased risk of mental health problems like depression, anxiety, and loneliness. Too much time spent scrolling through social media can result in symptoms of anxiety and/or depression. Teenager's mental health is often negatively affected by this culture of comparison as well.

3. Frauds, Scams. This is yet another challenge for social media companies. There are billions of fake accounts on various social networking sites including Facebook, Instagram, and Twitter. Facebook removes more than 3 billion fake accounts in six months and Five percent of Facebook's monthly active users are fake, the company said.

4. Misleading Information. This is probably the most challenging problem for social media companies. Fake news and misleading information can go viral in no time on social media platforms. On Facebook, more than 80% of people who react to the link do not read the complete article or content. Due to which many publishers and spammers are misusing the platforms by sharing fake and misleading information.

And Cyberbullying, hacking and privacy issues are other disadvantages of social media.

Question No. 5: What are the common crimes being committed on or as a result of Social Media in the present time?

Answer; There are many such as:-

1. The most commonly reported and seen crimes that occur on social media involve people making online threats, cyber bullying, harassing, and stalking others online. While much of this type of activity goes unpunished, or isn't taken seriously, victims of these types of crimes frequently don't know when to call the police. If you feel threatened by a statement made online about you, or believe that the threat is credible, it's probably a good idea to consider calling the police.

I would like to discuss one case with you on online stalking which was reported in the newspaper on 03.04.2021, wherein in Delhi A "Cyber Stalker" Who Harassed Girls, Uploaded Pics Online, was Arrested.

In this case, a 25-year-old man was arrested by Delhi Police for allegedly stalking a minor girl in Delhi-NCR and later uploading her morphed pictures on social media. The accused had uploaded abusive contents and nude pictures of the girl on Instagram after having a heated discussion with the girl's friend on Instagram. The accused who works in an event management company - was caught from his Faridabad home after cops received information on his internet activity and location from the social media sites. Two mobile phones used in crime have been seized from him.
"He has disclosed that earlier he had heated discussion with the complainant's friend on Instagram. Later he created a fake profile of the complainant girl to take revenge. Thereafter, he sent abusive contents, nude pictures and later threatened and abused the complainant. The accused is "habitual of using WhatsApp, Facebook and Instagram for making girl friends by creating fake profiles" as the police said, adding that a similar case had been filed against him at the Faridabad Cyber Police Station.

Question-6: what are the Facebook relate Crimes?
Answer: Facebook has been such an integral part of our lives that even recent crimes are cropping up that involves Facebook as an accessory. And it's not limited to cyberstalking, identity theft, distribution of child pornography materials, etc. These crimes are pervasive on the internet but they **only represent the tip of the iceberg**.
The type I'm referring to involves some creative, bizarre and unthinkable crimes that are linked to Facebook, for example that recent story about a mother

who tried to sell her two minor kids on Facebook for $4000), ironically to bail her boyfriend out of jail.

1. Jailed over Facebook Friend Request

In 2007, in one case one person was ordered by magistrates not to contact his wife after he was found to be harassing her with phone calls and text messages. When he **sent a 'friend request'** via Facebook to her despite the restraining order, His wife reported him to the police. He was consequently arrested and sentenced to ten days of imprisonment.

So while he is told to have no form of communication with his wife, online or offline, in this case, it was Facebook who had automatically conducted the friend request, landing him in jail.

2. Suicide By Social Bullying

The infamous suicide of a victim is a classic case of **cyberbullying**. The victim was subjected to taunts and bullying for months before taking her own life.

She had been receiving abusive text messages, harassment on her Facebook wall and on school grounds over girl-boy relationship disputes. But this had not been considered a cause to her suicide until **one of her bullies wrote 'accomplished'** on the poor girl's Facebook wall on the day she hanged herself. Further digging revealed that a group of schoolmates had been carrying out of bullying campaign against the victim which continued even after her death. The public pointed fingers at the school authority for not doing enough to prevent the tragedy from happening, but at least in this story, justice was served. In this case, Six teenagers were charged for a variety of criminal offences, including statutory rape , "civil rights violation", stalking, and even assault and battery.

3. Fatal Attraction: 'It's Complicated'

As I read the several murder cases that are linked to Facebook posts, it struck me that all of them were triggered by **relationship conflicts**.

I see it in one case wherein the accused who killed his wife, after she changed her Facebook profile **from 'married' to 'single'** back in 2009, as well as in the case other case who was murdered by her boyfriend in 2010 after **seeing her with another man on her Facebook page**.

In a separate incident, one accused had brutally hammered his ex-wife, before slitting her throat and leaving her bloodied body to be found by their five-year-old son – all because she had taunted him on Facebook.

Although murders that happened because of jealousy in a relationship are relatively common, using Facebook intensified the actions involved as it is a very public platform. When one posts evidence about a failing relationship, the other party may experience a **punctured ego** (especially men) particularly when he is implied to be the cause of the failure. Things will get ugly when you wash your dirty linen in public.

4. Facebook Impersonation.

Online identity thefts are rampant across the world. We see it in the thousands of fake profiles of celebrities on Facebook and Twitter, with some **successfully misleading others into thinking they're genuine profiles**. Nevertheless, identity theft can turn into a serious offence depending on what is done with the fake profile. Most people are not aware that there are **laws out there to protect against online identity thefts**.

5. Blackmailing on Facebook

Divorces turn people crazy, well at least that's what happened with 23-year-old Nigerian woman. She **posted a picture of his ex-husband on Facebook** and **tagged him as a member of the Boko Haram**, a violent jihadist terrorist group in Nigeria.

Her ex-husband, reported her to the police after getting calls from friends over the weekend, mistaking him as a genuine member. In addition to the post, a caption was found below the picture, which reads:

"This is one of the Boko Haram any time you have contact with him, bomb him."

Adeniyi was duly arrested and when asked of her reasons, she replied said it was because her husband threatened her and her child.

6. Sharing Animal Torture on Facebook.

In one case, A mouse was decapitated with a steak knife by a person in Australia. Worse still, the repugnant video was posted on Facebook. The horrendous act took the poor mouse 40 seconds to die. She was convicted after being **charged with animal cruelty.**

7. Snap. Post. (Think). Share.

It is your Facebook account but sometimes there are just some things that are too inappropriate to post.

The next time you want to post suggestive photos of yourself, do take a moment to think it through. There are number of syndicate across the world who made full use of such photos, particularly of Asian girls for their call girl service on Facebook.

They featured photos of beautiful girls that were lifted from their Facebook pages without their knowledge, and asked them to pay a sum of money to reserve their services.

Recently, one advocate was arrested in Madhay Pradesh in one case wherein he download a photograph of a lady judge and sent birthday wish to her along with her downloaded photograph from her facebook account, which was without her consent.

We're less likely to get carried by our emotions after we set the boundary between what should and shouldn't be shared on Facebook. As a note of precaution, **always exercise discretion in how much you are willing to share about yourself on Facebook**.

Question no. 7. What are the Fake online friendship/ Honeytrap cases?

Answer: Developing online friendship over social media (with no real-life familiarity and using the emotional connect to trick you in transferring funds on some pretext such as medical emergency, legal troubles, problems in a foreign country etc. are very common in these days. Creation of fake profile of a person and posting offensive content including morphed photographs on the fake profile is very common in these days.

Recently in one case a woman was arrested in a honeytrap case in Mangaluru. In this According to the police, Ms. X sent a "Hi" message on WhatsApp to one man in February this year. When the latter asked for the former's introduction, she replied that she had sent the message inadvertently. A few days later, she again sent a "Hi" message and man called her back. She introduced herself as a girl from Bengaluru and then, the two continued to talk and chat on WhatsApp for the next few days. On April 15, **the two had an intimate video chat** and then, she blocked his number. On April 20, he was called to an unidentified place where a group of five persons demanded a ransom of ₹30 lakh for not releasing the video footage of the intimate chat in the social media. He paid the amount in two instalments and then lodged a complaint with the police on June 30. The police traced Ms. X and arrested her and a case was registered for offences under Sections 120 (B) (criminal conspiracy), 384 (extortion), 420 (cheating) and 506 (criminal intimidation) of Indian Penal Code and under Section 66 (E) of the Information Technology Act against her. So be careful on

social media platform while chatting with some strangers or click on unwanted intimidated applications.

Question 8. Please tell us some cases on Blackmailing and sexual harassment.

Answer: I would like to discuss one case on online blackmailing case with you which was reported in the newspaper on 06.01.2021, wherein an Indian-Origin Hacker, hacked into the computer accounts of over 574 girls and young women to exploit them has been sentenced to 11 years in prison for blackmail, voyeurism and cybercrimes by a UK court. In this case accused gained unauthorised access to hundreds of social media accounts and went on to commit blackmailing crimes while sitting in London as per the UK's Crown Prosecution Service.
In this case, this accused who gained unauthorised access to hundreds of social media accounts, **in particular from Snapchat**, and went on to commit blackmailing crimes. He used to threaten his victims that if they didn't send him nude images of themselves, he would post intimate images of them to their friends and family. Some of the women complied and in at least six cases he went on to carry out his threats. He was an extremely manipulative man who inflicted emotional and psychological damage on young women and with one victim even attempting suicide, while also getting gratification from their images and videos. He had admitted a total of 65 offences - including hacking, blackmail, and voyeurism.

So, I request to all of you that social media users, please not to store intimate images of themselves and to secure and protect their data and please "Don't share your passwords even if you think it's a trusted friend that asks you for them, it might not be,".

There is another case from Delhi which was reported on 20.12.2020, in which a Man was Arrested For Blackmailing 100 Women Using Fake Nude Pictures.

In this case, a 26-year-old man, accused of blackmailing at least 100 women, has been arrested in Delhi for trying to extort money from a south Delhi resident by allegedly blackmailing her with threats of circulating her indecent photographs on the social media.

According to the police, accused has been arrested earlier in similar cases in Chhattisgarh and has confessed to the crime. He used to demand money and pictures of his victims' private parts and the mobile phone used to trap women has also been recovered.

On the basis of the complaint of the victim, a case of extortion, sexual harassment and criminal intimidation was filed. The accused “hacked into her account on Instagram (which is a very popular image sharing app)” and he would post her nude pictures if she did not meet his demand for money. He also demanded money from people in her contact list.

As per the Delhi Police's Cyber Cell to blackmail and extort money from women, he used to take their profile pictures from their social media accounts, morph them and create fake profiles. He would then allegedly send his targets a threatening message stating that their nude pictures were with him. When his targets sought proof, he would send their morphed picture to scare them.

Online Sexual Harassment.
There is one case of sexual harassing of a Delhi based woman on social media and threatening to defame her by making her pictures viral on WhatsApp by a Assam based 24 year old man, which was reported in the newspaper. He used to harass the Delhi-based woman via chat and video calls and later threatened her.

Delhi Police on the basis of the complaint of the victim, registered a criminal case under section 354 A (sexual harassment and punishment for sexual harassment), 509 (word, gesture or act intended to insult the modesty of a woman) and 506 (punishment for criminal intimidation) of the Indian Penal Code and IT Act and the probe was taken up.

During the course of the investigation, through surveillance and technical analysis, the police managed to locate the mobile number of the accused and he was zeroed down at somewhere in Assam. The accused disclosed that he had a habit of making friends on social media. After befriending them, he later intimidated them by threatening to make their chats and pictures viral on social media platforms to defame them. So be careful making new friends on social media.

There is another famous case of a Supermodel who filed a Complaint Against a Man For Cyber Harassment, which was reported in the January 2020.

In this case, a very famous Supermodel and Former Miss India (World) has filed an FIR against a man, who has been tagging her name into objectionable content.

According to Victim, the accused put up some adult content tagging her name on his portals Indiascoops.com and Indiaspeaks.live, and also sent the same to various other websites for publication.

The Victim said that "The matter started in November 2019. Somebody started creating fake news articles and started tagging her and putting objectionable pictures of girls in a bathroom with their faced blurred and putting the name of some girl called “X” who Former Miss India (World). This is a non-existent name, but this man was doing this for some reason. She was his new target."

The Victim said that "He started sharing these fake news articles under the garb of her name, who is a famous model, all these instantly got linked with her. He made some fake Twitter accounts and created some horrendous news articles and some bathroom pictures and circulated it on his portal. He has taken out pictures with no heads from porn sites and written her name on them. It's all appearing under her Google name”.

Recently one case of sexual harassment is reported in respect of Photos Of some of the Bengaluru College Students Uploaded On some Porn website, in which two persons have been arrested.

The action comes after a group of students, on learning about their social media photos being misused, met the police to complain about the incident. The accused have taken the photos of the girl students from their social media accounts. The photos on the porn website have now been deleted by the police action.

"I request the families of the victims to be the most supportive, especially during these testing times, when we're staying at home most of the time. The authorities should have been much more vocal in empathising with the students. Their response becomes crucial to how most parents respond as well,".

There are number of other kind of social media crimes in the cyber world as Social Engineering, Surface Net/fake Recruitment agencies, Online grooming, online human trafficking, Drug Abuse, Buying Illegal Things and vacation Robberies etc. etc.

Question 10: What is Online Child grooming?

Answer: A unique feature of child grooming which takes place on the internet is the relative ease with which groomers are able to operate and gain a child’s trust online.

Earlier this month, newspapers reported that a 13-year-old girl from Tirupur was lured and raped by a 21-year-old man in Chennai. What makes this incident even more shocking is that the rapist had befriended the victim first on Facebook and sexually assaulted her after having gained her trust online. This

incident brings to light a growing concern surrounding child safety issues on the internet, namely, ‘online grooming’.

Child grooming is generally understood as the practice of befriending and forming an emotional bond with a child by a person with the objective of sexual abuse. "These 'friendly molesters' become acquainted with their targeted victim, gaining their trust while secretly grooming the child as a sexual partner."

Child grooming incidents have increased with the advent of the internet, where such incidents are increasingly taking place online, through public chatrooms and social media. In India too, such instances have been reported in the past. Last year, two teenagers were arrested in Kolkata for kidnapping and rape of a 15-year-old girl whom they had befriended on Facebook. Another instance of online grooming was reported in December 2016 where a teenage girl was raped by a Facebook friend in Mumbai. More recently, in January 2017, a minor girl in Cuttack alleged rape by a boy whom she had met through a social networking site. With the proliferation of smartphone users in India, child grooming incidents can only be expected to rise in future.

A unique feature of child grooming which takes place on the internet is the relative ease with which groomers are able to operate and gain a child’s trust online. The anonymity provided by the internet and the social media addiction (which is prevalent today among children before they even enter teenage) are factors which have contributed to the rise of child grooming online.

Another reason could be that it is difficult for parents to monitor the activities of their children on the internet. This makes it easier for child groomers to approach children online with the intent of befriending unsuspecting victims. Further, social media interaction has grown by leaps and bounds in the recent past making it the perfect modus operandi for child groomers.

Question no. 11: what are the Preventive Measures/Precautions your will suggest to our viewers?

Answer; I must suggest to the views to follow some practises to safe themselves such as:-

1. Block profiles from public searches.
2. Restrict who can find you via online search.
3. Limit what people can learn about you through searching on net.
4. Log out after each session.
5. Don’t share social media credentials.
6. Don’t accept friend requests from unknowns.

7. Don’t click suspicious links.
8. Keep the privacy settings of your social media profile at the most restricted levels, esp. for public/others
9. Remember that information scattered over multiple posts, photographs, status, comments etc. may together reveal enough about you to enable a fraudster to steal your identity and defraud you. So, apply maximum caution while sharing anything online.
10. keep activate your two factors authentication security.

Question no. 12. What are the legal provisions against the social media crimes in India?

Answer: Yes, Information Technology Act, 2000 is specifically enacted by our parliament to deal with the social media crime apart from some provisions of Indian Penal Code. Chapter XI consisting Section 65 to 78 and Chapter XII consisting Section 80 to 85 of the IT Act, 2000 are dealing with such kind of social media crime as well as other cyber-crimes. But before bringing the criminals of cyber-crimes to the justice delivery system, we must create awareness among the general masses to report such cyber-crime to the police and other law enforcing agencies.

Thanks.