Major Social Media Threats, Case Studies and How to be Safe

Social Media Crimes and Threats


Username
Password
PHISHING


HARRASMENT
ABUSE
HUMILIATE
DISCREDIT
THREAT
VIOLENCE
CYBER BULLYING
ANXIETY
INTIMIDATE
DISRESPECT
ATTACKING


Fake Account

Fake Profiles

- 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 under:
- 1. Facebook
- 2. Instagram
- 3. Twitter
- 4. LinkedIn

Online Threats, Stalking, Cyber bullying

- The most commonly reported and seen crimes that occur on social media involve people making threats, 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.

Hacking and Fraud

- Although logging into a friend's social media account to post an embarrassing status message may be acceptable between friends, but technically, can be a serious crime. Additionally, creating fake accounts, or impersonation accounts, to trick people (as opposed to just remaining anonymous), can also be punished as fraud depending on the actions the fake/impersonation account holder takes.

Buying Illegal Things

- Connecting over social media to make business connections, or to buy legal goods or services may be perfectly legitimate. However, connecting over social media to buy drugs, or other regulated, controlled or banned products is probably illegal.

Sharing illegal content

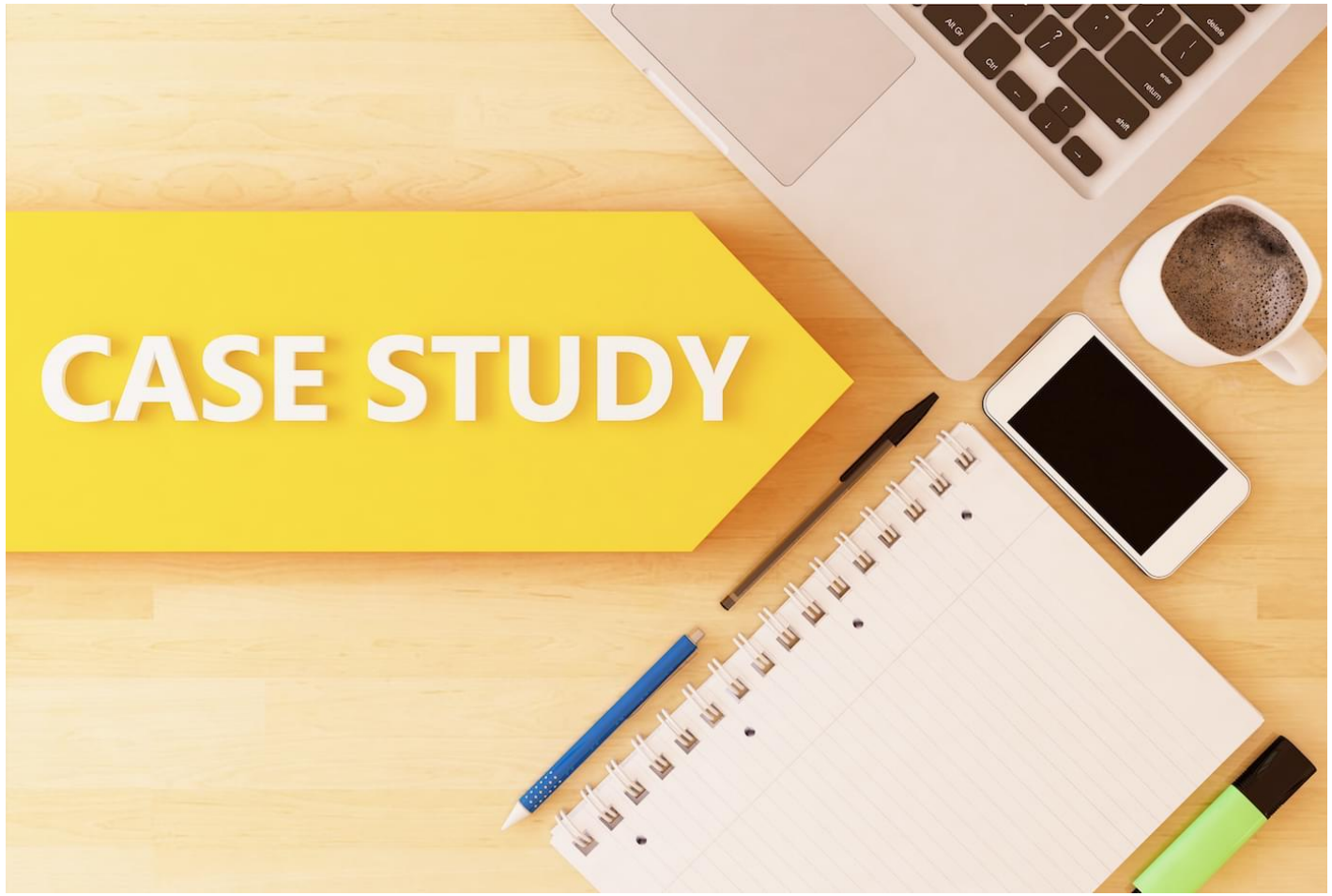
- Sharing illegal content like sexual content or any fake news is a Cybercrime in law.

Vacation Robberies

- Sadly, one common practice among burglars is to use social media to discover when a potential victim is on vacation. If your vacation status updates are publicly viewable, rather than restricted to friend groups, then potential burglars can easily see when you are going to be away for an extended period of time.

Fake online friendship

- 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.



Now Let's discuss some Case Studies...

Delhi Student Stalks Air Hostess Trainee On Instagram, Hides Identity Using VPN, Caught

- A Class 12 student was apprehended for allegedly stalking, threatening and harassing a 20-year-old woman on social media to have a sexual relationship with her.
- The matter came to notice on Wednesday when the woman, who is pursuing an air hostess course, approached police with her complaint alleging that she was being stalked by a person on Instagram, who sent her obscene content on the social media portal's messenger and insisted on having a sexual relationship with him, police said. After examining the complaint, police found that the accused also sent her an email using spoofed email. The girl stated that she was being "extremely harassed" for three to four days by the alleged profile user.
- Based on the complaint, a case was registered under Indian Penal Code Sections 354(D) (stalking), 506 (punishment for criminal intimidation) and 509 (word, gesture or act intended to insult the modesty of a woman) at Jagat Puri police station.

Man held for creating fake social media accounts

- A youngster who created fake social media accounts of a woman with morphed images as profile pictures was arrested by the Rachakonda Cyber Crimes police.
- He created fake Instagram and Facebook accounts of the complainant and sent friend requests and abusive messages to her friends and family members, stating that she is having an affair with him
- This is a case of defaming.

Bazee.com case

- CEO of Bazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi.
- The Mumbai Police and the Delhi Police got into action. The CEO was later released on bail. This opened up the question as to what kind of distinction we draw between Internet Service Provider and Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle cybercrime cases.

Preventive Measures/Precautions

- Block profiles from public searches.
- Restrict who can find you via online search.
- Limit what people can learn about you through searching on net.
- Log out after each session.
- Don’t share social media credentials.
- Don’t accept friend requests from unknowns.
- Don’t click suspicious links.
- Keep the privacy settings of your social media profile at the most restricted levels, esp. for public/others.Enable 2 level authentication on your social media accounts and email account.
- 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

References

- www.google.co.in
- https://www.thehindu.com/opinion/open-page/social-media-and-cybercrimes/article31819540.ece
- https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/9-social-media-threats-you-need-to-be-aware-of
- http://www.cybercelldelhi.in/socialmediacrimes.html
- https://www.ndtv.com/topic/cyber-crime

Efforts by:

Sahibjot Singh Aneja

(Intern at Gurugram police Summer Internship,2021)

#gpcssi