Privacy and Security in Online Social Media Networks
Prof. Ponnurangam Kumaraguru ("PK")
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Week – 6.1
Lecture – 19
eCrime on Online Social Media

Welcome back to the course Privacy and Security in Online Social Media, this is week 6.

(Refer Slide Time: 00:17)

So, what we have seen until now is generally, overview of online social media. We have had a lot of hands on tutorials about Linux, Python, Twitter API, Mongo DB, MySQL and then I went into topics like Trust and Credibility, then we saw Privacy, last week we saw what is Policing how online social media is being used by police organizations specifically in India and what research problems, what questions that you can actually study from the data that you collect from these social media services.

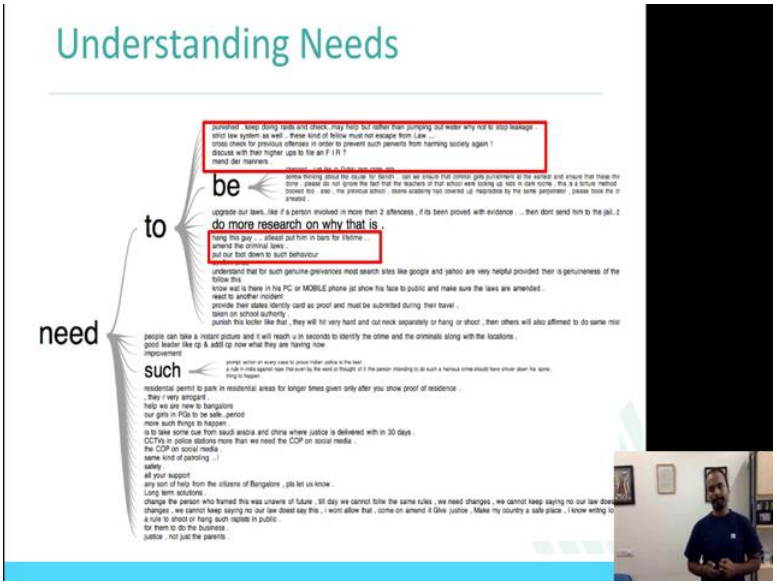
(Refer Slide Time: 00:56)

Let me just quickly tell you what we saw. Multiple police organizations have actually adopted using Facebook, Twitter, for sharing for interacting with the citizens and that is the topic that we saw in the context of policing. A specific question that we saw was how we can actually use this data from social media to collect actionable information.

(Refer Slide Time: 01:19)

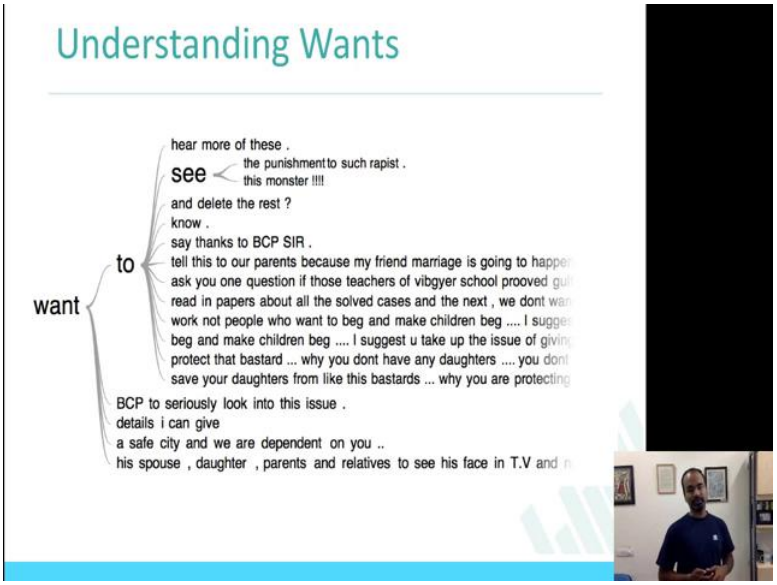
Is it possible we can collect some actionable information? Is it possible to use this information for making any interesting judgments?

(Refer Slide Time: 01:33)



In this context we also saw that how we can use the text content that is posted on these social media services to take some actionable information. For example, this tree shows how you can understand the needs of citizens who are posting on these networks. Like for example it says, need to be punished, need to hang this guy. So, these are the needs from the citizens who are posting this content on Facebook or Twitter or other social media services.

(Refer Slide Time: 02:10)

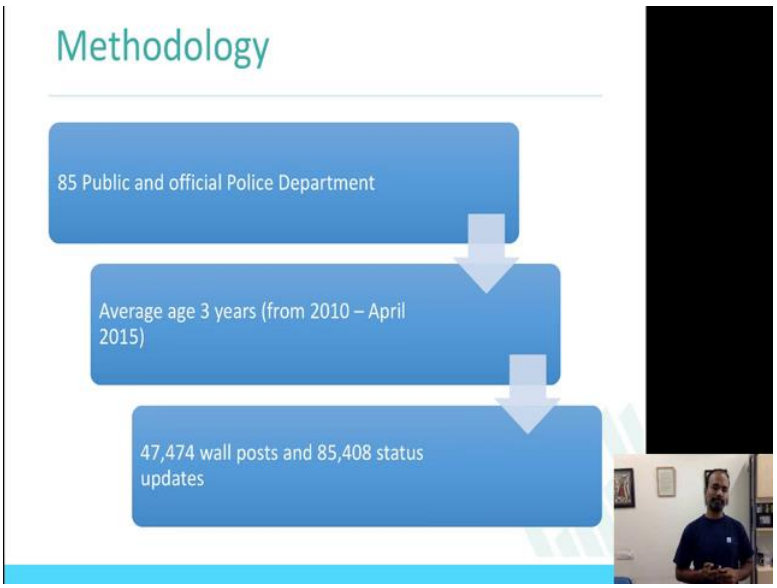


Then you can also look at understanding wants, which is what is that citizens are interested in wanting from police, this we like want to hear more of these, here want to see the punishment of such people, want to say thanks to BCP Sir. This is something we saw earlier and we are just going to quickly brush it only.

(Refer Slide Time: 02:30)

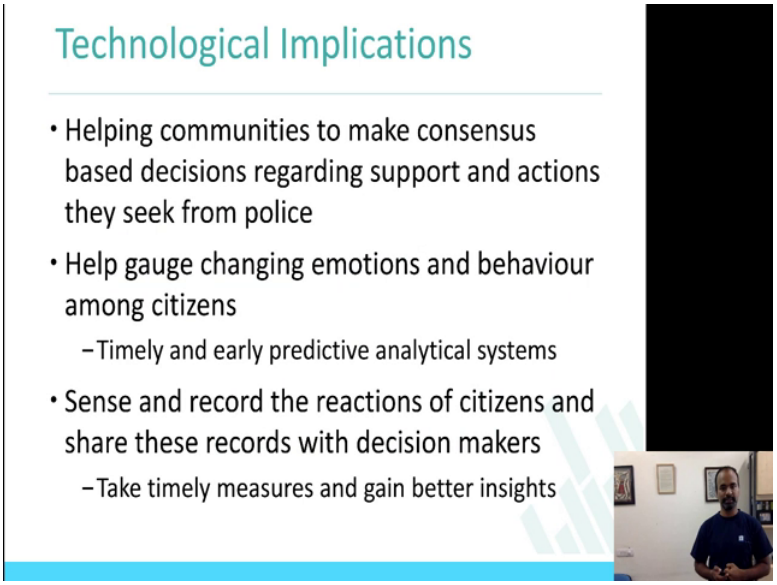
The four questions that we saw specifically where, topical characteristics, what topics are being discussed, how the engagement between police and citizens are happening, what emotional exchanges are happening between citizens and police, specifically we also looked at arousal, violence and topics around that. Finally, we looked at cognitive and social orientation, linguistic attributes, unigram, and bigram, and topics around that.

(Refer Slide Time: 03:04)



In this data specifically what we saw was collecting data from 85 publicly and official departments between this period of a 2010 and 2015, the analysis was done on 47,474 wall posts and 85,000 status updates.

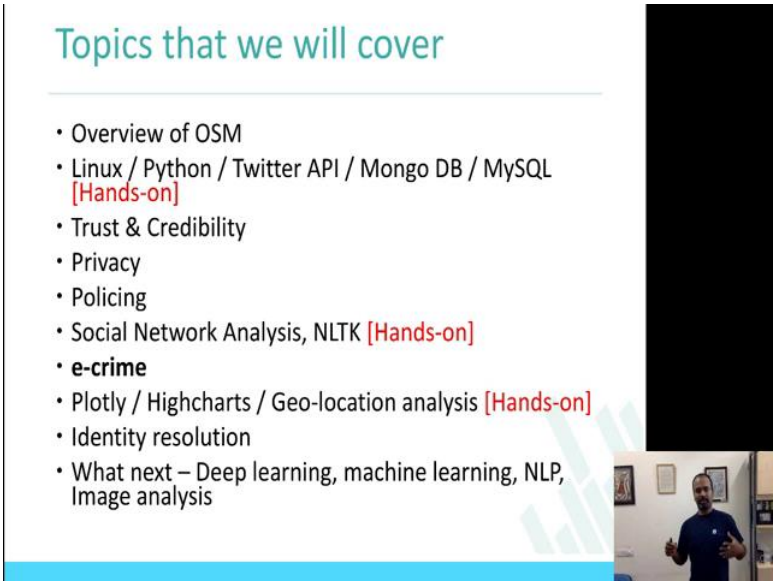
(Refer Slide Time: 03:22)



And of course, the technical implications of doing all this is helping communities to help the police organizations, build technologies which can be used by citizens to interact with police better, build technologies that police can use for interacting with citizens better and making the society a safer place to live.

So, that is the broader goal of studying these concepts on social media. As I said in the last week also I would really like to see people talk about their city police organizations and interactions if any, on the forum, I have not seen anything much until now, but I think for now many of you may just understanding the content that is just the content itself. But it is actually great to see some going to see some interesting questions, students are asking in the forum.

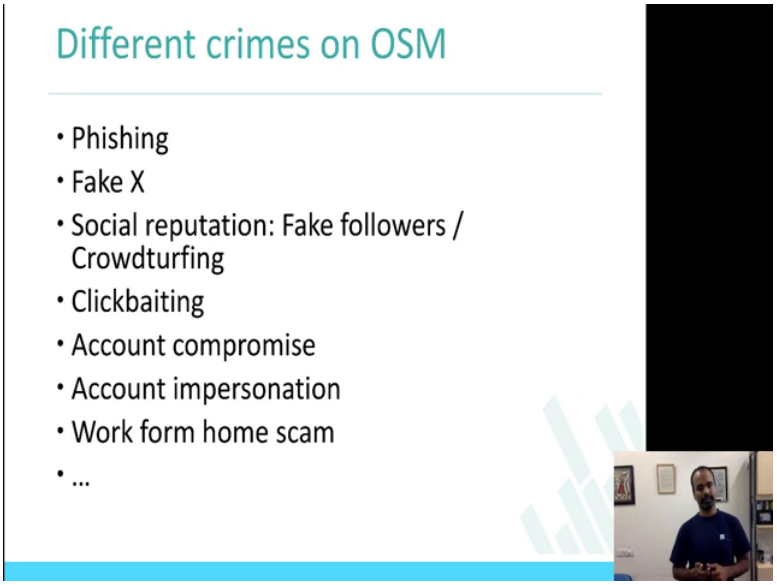
(Refer Slide Time: 04:19)



So, what we will do now is we will move on to another topic from here. The topic now I want to look at is e-crime; e-crime, cyber crime anything that is around electronic crime, but focus it only on the social media context. Crimes happen all around the places using the internet, using the web, but people will focus on these kind of crimes only that is happening on social media.

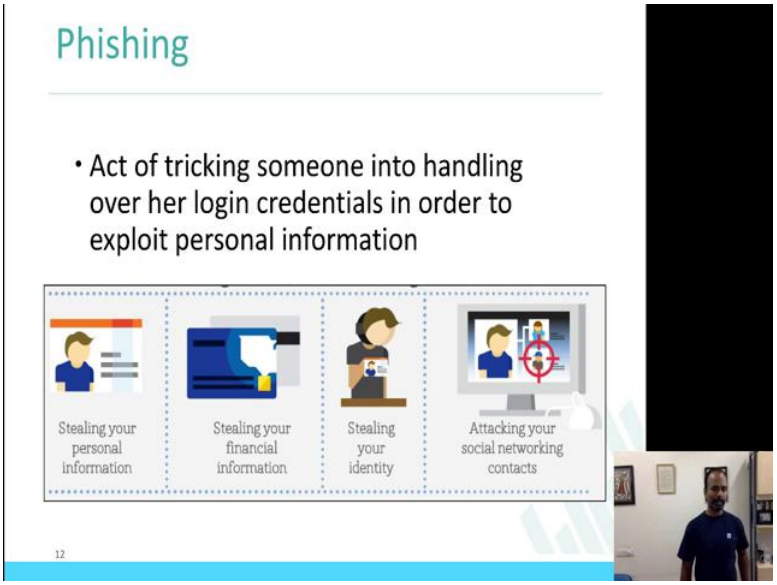
And as the pattern on the course, we will do some basics now in the first part of this week then I will get into some research questions or questions that one could answer using the data that is been collected on crimes from these social media services itself. We will do these hands on tutorials also, which is looking at social network analysis tools and then NLTK. And there are other hands on tutorials also that are we have planned over the course of next few weeks.

(Refer Slide Time: 05:21)



So here is a list of not a comprehensive list, here is a list of crimes that I thought I will cover before getting into details of any one particular topic. We are going to look at one or two topics in detail, but before that let me just walk you through some crimes that happen on online social media. I am sure some of this we are already aware but let me just brush it to get your sense of what the crimes that are going on in these social media services.

(Refer Slide Time: 05:51)



The first one which is phishing, and again these are not arranged in any particular order and they are not comprehensive at all. The phishing problem on social media services, the act of tricking someone to into handling or logging details which is basically there is a, in traditional ways in emails, in email domains you get emails which says please click on this link or please click on the links to update a password or your account is expired click on this link to activate your account.

When you click on this link you are taken to a fake web site which sometimes looks like a legitimate website, but sometimes it does not need to be looking like a legitimate website also. And when you go there it is asking for username, password and when you give the username, password, you are basically sharing the credentials to someone else.

And these kind of emails have been playing around for a long time and there are many sophisticated attacks that has happened using these emails; phishing itself, just phishing, sphere phishing. Sphere phishing is a way by which you target a set of people. For example, in this course I could just target only the people who are taking this course saying as though it is email coming from PK at IIIT, saying please click on this link to know further links that I have actually posted on the web about the course. And then, of course, some of you may be interested in what I am speaking about the course and you

will click on the link, but it is not actually a legitimate email or a legitimate link. So that is about sphere phishing, but then there are other types of phishing also, which is whaling where the specific CEO's of a company are targeted while sending out these phishing emails. There are many different types of phishing attacks that have been going on. So, that is traditional.

But now when you move on to the social network, these attacks have also calculated the social media services also. For example, a link on to the Twitter timeline will tell you that please click on this link to get some money and then when you click on this link or please click on this link to change the Facebook password that you have created, there was some problem in your access with Facebook; click on this link to update the password.

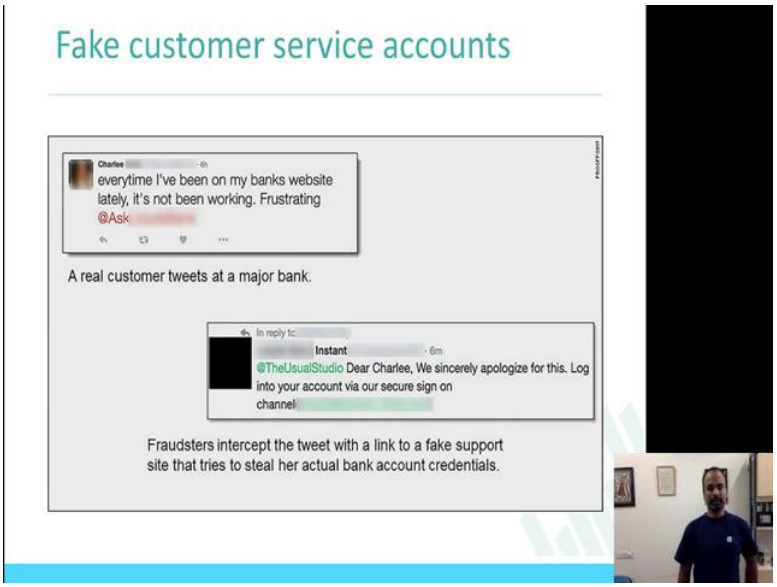
As in the traditional way if you click on this link you will end up actually going to a fake website and giving away the credentials, that is phishing and I mean you can think of it as a phishing as in the traditional ways in emails itself, but spreading on the social media services. There could be a link on Facebook, there could be a link on Twitter; there could be an email to say, please click on this image to get some more information about a topic and it could actually take you to a fake website. So that is phishing.

(Refer Slide Time: 08:44)

So, specifically the examples in phishing that are going on now or have been around for sometime is Facebook technical support sent you a notification saying that, there is some problem in your account please go verify. Facebook new login system that is emails going around which says that Facebook has invented a new login system and click on this link to create your account on this new login system or merge this account to the Facebook account and things like that, these emails have been going around.

And if you really look at it, Facebook credentials are becoming more and more important, because if I know your Facebook credentials I actually get to know your friends, I actually get to know your pattern of usage, interest and topics that you may be interested in spending time. These things can be used against you. So that is the reason why Facebook credentials are also becoming more and more popular, compared to the email address, compare to the financial account details that one was also chasing before. That is phishing.

(Refer Slide Time: 09:50)



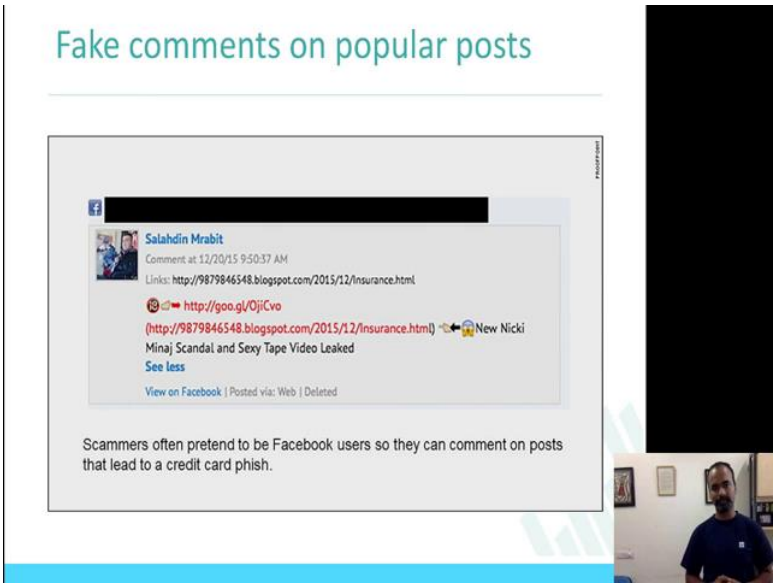
Let me walk you through some fake things that are going on online social media also. Here is one which is fake customer service accounts which is, I have a problem I actually post a tweet saying I have problem with this bank. For example in this case every time I have been on my bank's website lately, it has not been working, frustrating. They are

actually tagging the right bank; they are tagging the right organization. For example, we could actually think of the same thing tagging HDFC Bank, ICICI Bank. These kinds of organizations have legitimate accounts and people using Twitter can tag them.

So, what happens now? This is a real tweet and real customer asking for real problem. What the fraudsters do is they look at this tweet, they have mechanisms to figure out these kind of tweets are going on. They actually reply to these tweets as though it is the bank which is replying to this tweet. And they will create accounts which are very similar to the real account and reply to the post as though the real account, real organization is actually talking to you. In this example the Usual Studio Dear Charlee, We sincerely apologize for this - login to your account via secure sign on channel blah blah blah.

This is the customer service account; fake things that is going on, which is real customer tagging or connecting to a real bank organization or an organization. The fraudsters create accounts which are very close to the real account and actually start interacting with the customer. These is fake customer service account problem. This particular example is on Twitter, but one could think of such problems being on all social networks also. Because all of these legitimate organizations are actually using social media to interact with their customers.

(Refer Slide Time: 11:48)

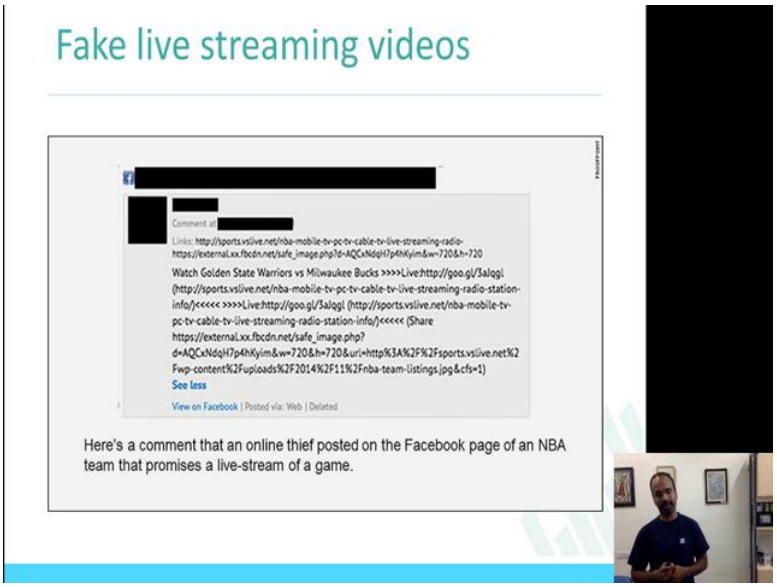


Here is the second one, fake comments on popular post. I think some of the posts that that become very popular. Let us take the prime minister was talking about it, if it was Obama who is talking about something these posts become very popular. And when these posts become very popular there are also lot of comments. For example, now I am sure if you look at the Olympics Facebook page or the twitter handle or the hashtag, people are actually talking a lot about things that are going on in the Olympics in the context of Facebook page and Twitter accounts also.

Therefore, what scammers do is that they actually pretend to be Facebook users so they can comment on this. For example, I could create an account, I could create Facebook account which looks very legitimate, I can start posting on these Olympics relevant post which are very popular and I will kick you from that to a fake website, and get your information. And if you too click on this link I will give you also down somemalware in your code and things like that.

So that is a second type of a fake thing that is going on, which is fake comments on popular posts because the reason why it is popular post is that it gets in more and more fashion, and more people actually get to see it, it is connected to the topic that people are more interested on.

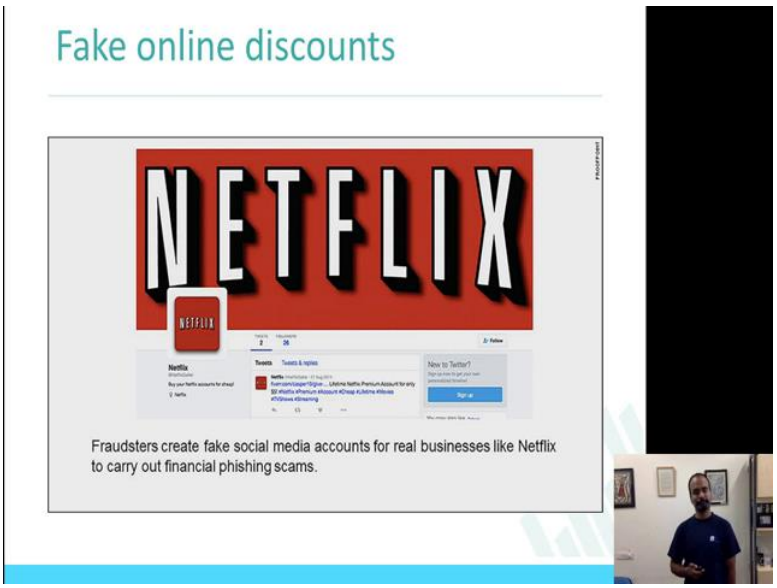
(Refer Slide Time: 13:12)



The third one is fake live streaming videos, which is particularly in the context of Olympics and cricket matches, world cups and things like that, there is tendency of actually looking for these matches in live. Here is an example where this post is actually saying live video for this match, right? If you are interested in watching it in your laptop, in your phone you tend to actually look at these pages, look at these links which talks about this game and tend to actually taking into a fake website.

Fake live streaming videos, which is there is no video, there is no real video which is connected, but the scammers actually tend to take the users to fake things. And they do this in the context of some games that are going on, some events that are going on, some shows that are going on. For example, currently in terms of Rio somebody says that currently India has won medal and here is the video of the match. So, that is the kind of scam that is going on in the context of live streaming videos.

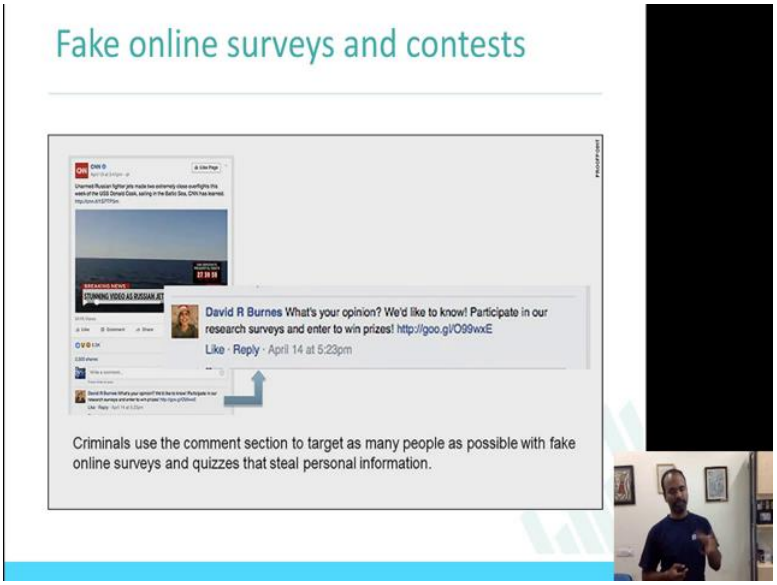
(Refer Slide Time: 14:27)



The next one is fake online discounts which is, scammers take the real account, real organization in this case - Netflix, it could be anything Facebook, it could be Flipkart, it could be any real organization. They create fake accounts that looks like real business and they are actually carry out business using these fake list, but giving you discounts. Like for example Netflix could say that, this page which is a fake page, it could say that there is

a 10 percent discount in Netflex account that you open now. 40 percent discount for the next 6 months, if you open the account right now. These kind of posts can actually lure people into using these fake accounts, fake pages, fake services. So, that is the next fake crime that I thought we will talk about.

(Refer Slide Time: 15:25)

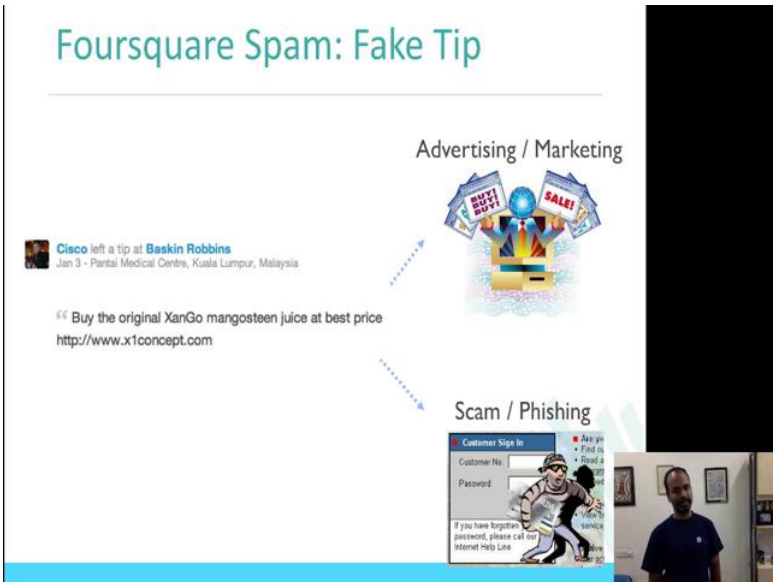


Next type is, Fake Online Surveys and Contests. These kind of scams have been around for a long, long time, where the criminals of these scammers get you to get survey, fill the survey to get some money, to get some information. For example, how do you know your personality? Personality test and find out other people who are bonding your date, who has the same personality and things like that, while these kind of things have been around for a long time. And there were also contests, win 1000 Rupees for filling on this survey. So these have being there in traditional ways now these have moved on to the social media services. Here is an example where, what is your opinion, we would like to know, participate in our research surveys and enter to win prizes, here is the link.

Again this is a fake claim, this could actually be malicious, and this could actually be collecting personal information. But the source of starting this is getting you to click on the link a survey or contest. So, that is the last cyber fake version that I thought I would actually mention it to you. Quickly a few fake crimes that you can think of - fake

customer service account, fake comments on popular post, fake live streaming videos, fake online discounts, and fake online surveys and contests. So, these are the different types of crimes that can be go scams that can be happen on social media services.

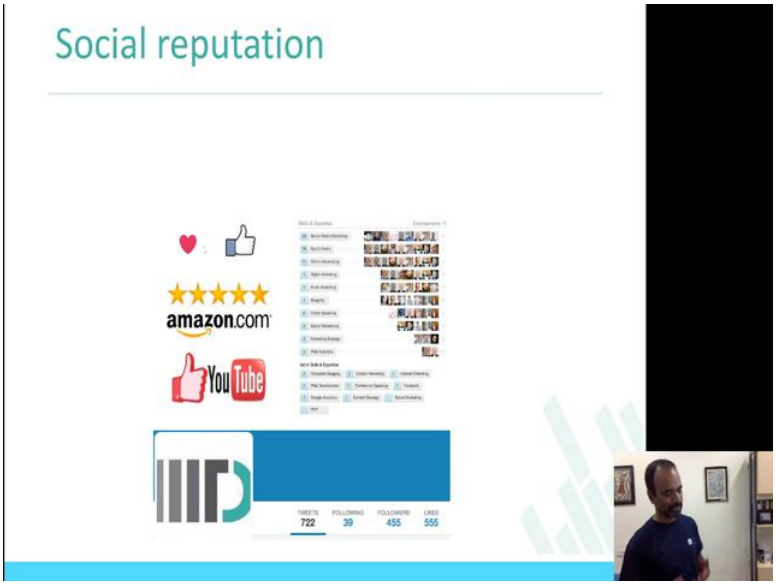
(Refer Slide Time: 17:01)



Here is few more, I mean I think if you look at my first slide where I showed you different types of fake crime things I was going to talk about, fake was that part. Now here is another one which is a Fake Tip: Foursquare is the most popular location based social network. In this foursquare for example I could actually walk into IIIT and then say that I have checked into IIIT Delhi. So that is the check in, and you can also leave a tip, I go to Saravana Bhavan. I eat food at Saravana Bhavan and I say that the food is pretty good. So, in that tip, people actually, the scammers and the criminals actually post information that can take you to a fake website.

For example, here by the original XanGo and mangosteen juice at best price, this link. This is the tip posted on particular location, so it is taking you to link which could be actually phishing so, it is also studying, giving you information, advertising about such certain productd. So that is the fake tip, the information that are posted in a tip that is not relevant to that particular venue, and taking you to a fake content is the problem here. So, that is the fake account foursquare.

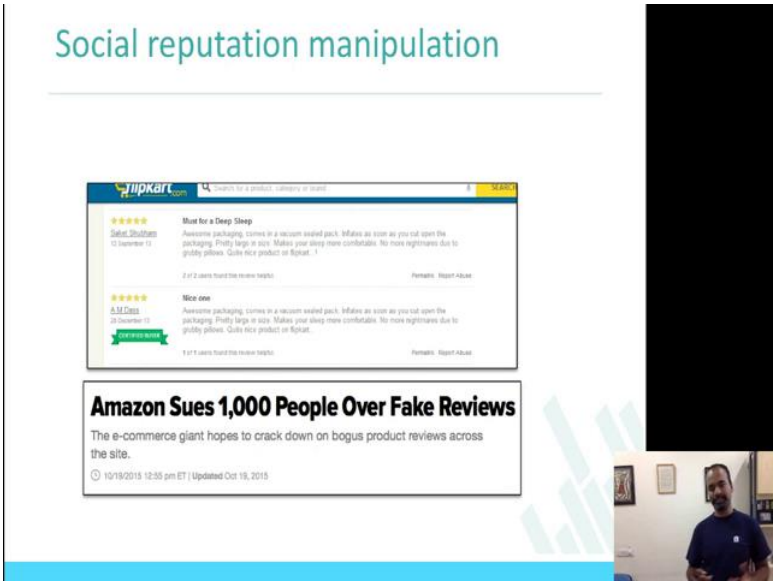
(Refer Slide Time: 18:23)



Social reputation has become such a big deal now, everybody talks about I have 2.5 million users and then 2.5 million followers, then the number of likes that you have on your page is becoming the way that people measure your influence in the society. Even among friends, it does not have to be the celebrities, politicians, even among friends you are more, more curious about how many friends other have. The social status is now being measured by the presence in social media; by the number of likes that you get on posts, number of friends that you have, it is becoming more and more popular.

For example, Facebook likes and Amazon reviews, YouTube likes, the endorsement that happens on LinkedIn where you are endorsed for a particular topic, how many people have endorsed you, what topics have you been endorsed. These are becoming a measure of influence in the society, number of tweets, number of followers, number of followings, all of them become a measure by which people think of your social reputation. But the problem is all of them also have problems, because of these ways by which creating social reputation has happened, you can actually manipulate these social reputation also.

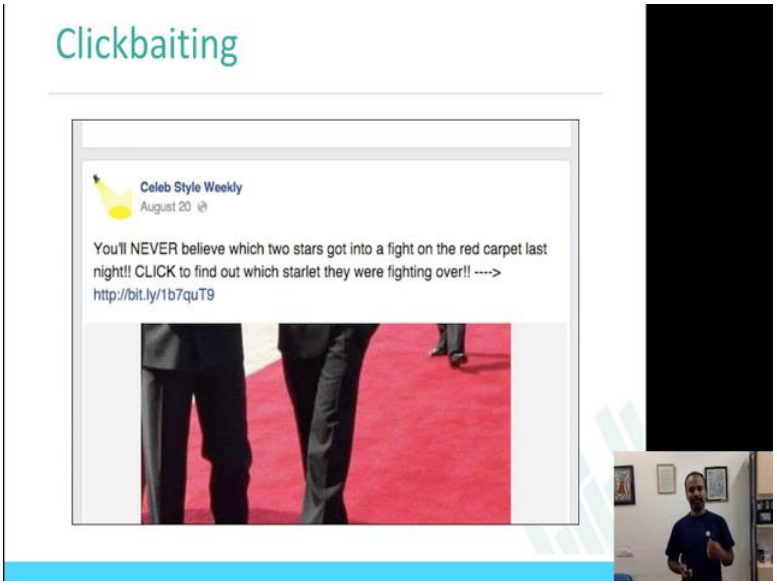
(Refer Slide Time: 19:48)



In this case, some examples that I had put in here is Flipkart, social reputation can be manipulated by actually writing good reviews about product. So, reviews become a big way by which you can actually manipulate the social reputation of the product, of the company, of the seller, all of them can actually be manipulated. It is actually a very big problem in terms of studying Amazon's reviews or Flipkart's reviews also for products.

Here is a case; Amazon sues 1000 people over fake reviews. People have been studying with reviews problem for a long, long time. It is not only reviews, it is also about studying the fake followers, studying the fake endorsements, all of them are actually relevant problems. If anybody is interested in taking up some of these, these are actually very interesting problems, very challenging problems also and very real world problems which is, you can actually look at the solutions that you build, becoming / influencing people's thinking.

(Refer Slide Time: 20:52)



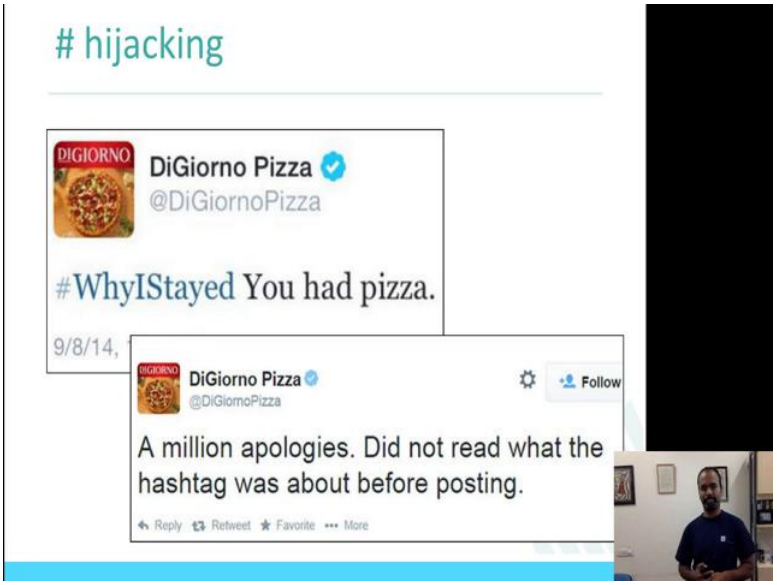
Here is another problem in terms of crimes on social media. Clickbaiting, where you are actual director your keeping the website, so you go read a particular page of news or something, there they present you with information which is sometimes relevant sometime not relevant and they take you to a fake website. So, here in this case also, the link here, this information was actually presented in one of the social media services where it was taking it to a fake website. Clickbaiting - getting you to click on links which are not legitimate.

(Refer Slide Time: 21:31)

Hashtag hijacking; hashtag hijacking is also becoming a big issue these days, I assume all of you know what a hashtag is. Hashtag is the way by which a particular set of tweets, if you want to talk about now Olympics you use hashtag Rio 2016. So that is the way of using hashtag Rio 2016, you are saying that the content that I am posting is connected to this topic, so Twitter can actually bring in all these posts which has hashtag Rio 2016 and show it to people who are interested in it. So, that is the logic behind using a hashtag.

In this example where CocoCola has actually posted tweet which says, 'Time for a Royal Celebration hashtag Royalbaby'. Here what coke is doing is, coke is actually using a hashtag which is very popular otherwise for actually selling their product. That is hijacking right, royal baby is nothing relevant to coke. They are kind of using it to promote their products. So that is one way of hijacking the hashtag.

(Refer Slide Time: 22:40)



Here is another example also. Why I stayed was a hashtag that was trending, was getting popular so this pizza, DiGiorno Pizza thought of using this popular hash tag actually to sell to mention about pizza. They used this hashtag why I stayed because you had the pizza, but unfortunately this also back fire, here is the post that they had to actually apologize for doing this post. A million apologies, did not read what the hashtag was about. The hashtag was actually used in some of the context where people were actually using this hashtag talk about a particular situation. Therefore, taking the hashtag which is not relevant to this topic, using it for selling a product is actually hijacking.

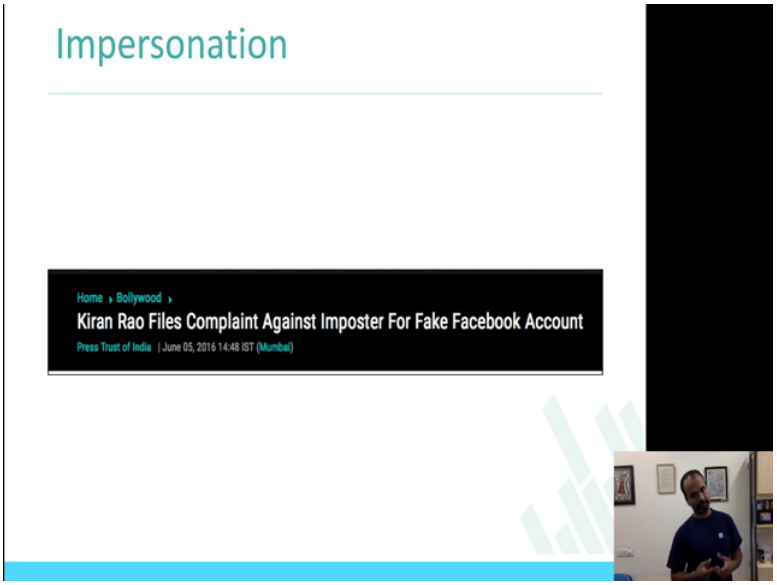
Now just further talking about for example, you would say something about what you are doing now with the hashtag Rio 2016 which will actually show up on people who are looking at timeline for the posts which has Rio 2016. So that is the problem in with hashtag hijacking.

(Refer Slide Time: 23:49)

Compromised account, I have actually shown this particular tweet even in my trust and credibility section, but I brought this back just to tell you different problem, I think I explained the problem then but I will explain it in the context of e-crimes also. Compromised account, where The Associated Press is a verified account and this account was compromised for sometime which is, somebody else had access to this account and the tweet was, Breaking: Two Explosions in the White House and Barack Obama is injured' I am sure you can all agree that the effect this tweet must have had.

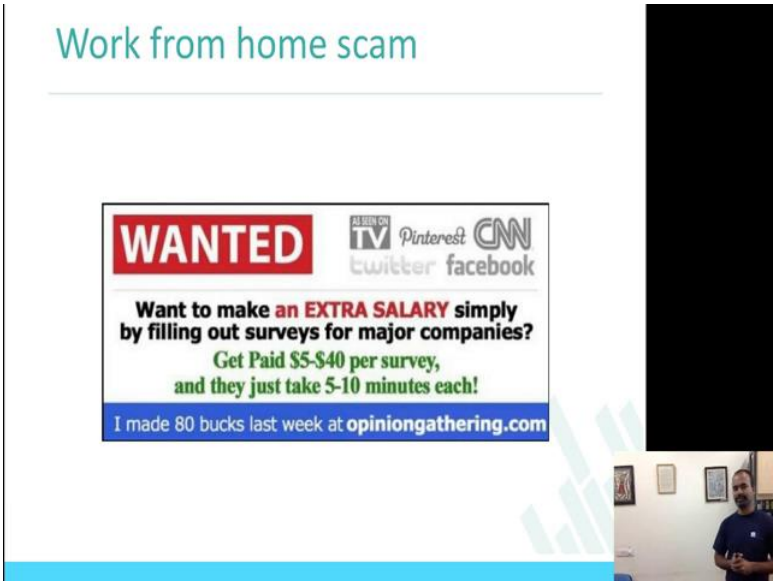
This is account compromised, somebody else getting access to your account because of leak of username password and getting that to misuse, getting the account to be misused also. That is compromised account.

(Refer Slide Time: 24:40)



Impersonation: Impersonation is also another problem which is I can take an account like for example, any of you in the class I can take some details of you that I know pictures, and your city, and the information that I could collate from online sources, use that to actually create an account which as though looks like it is you. Here is a complaint that Kiran Rao has actually filed saying that fake account has been created, and there are many, many fake accounts like this. If you know remember the policing section I also showed you about the fake account of police organizations also. And it is not just about individuals, even organization's accounts are actually created fake.

(Refer Slide Time: 25:28)



Here is another interesting problem which is, Work from home scam. Again these things have been in traditional ways for example, if you are driving down somewhere in the signal, you will see a post which says, 'want to won 1000 Rupees a day sitting at home please call this number' these kind of scams are being there. Here is an example of a scam that went popular in Pinterest where this image was actually floating around, 'want to make an extra salary simply by filling out survey for major companies, here is a website to go to. You get paid 5 to 40 dollars per survey. This is work from home scam. Again there is a lot of scams which are similar to these work from home scams, different versions that are very popular on social networks. So, this is an important scam also.

With that I will actually wrap up my first part of the week 6, where I thought I will just introduce you to different scams, different crimes, because we will talk about crimes in this week, looking at different crimes some data was collected, what kind of analysis could be done, what kind of solutions that we could build in reducing these problems of crimes on social networks.