

**Online Privacy**  
**Professor Ponnurangam Kumaraguru**  
**Indian Institute of Technology Hyderabad**  
**Week 5**  
**Ethical about Studying Online Privacy**

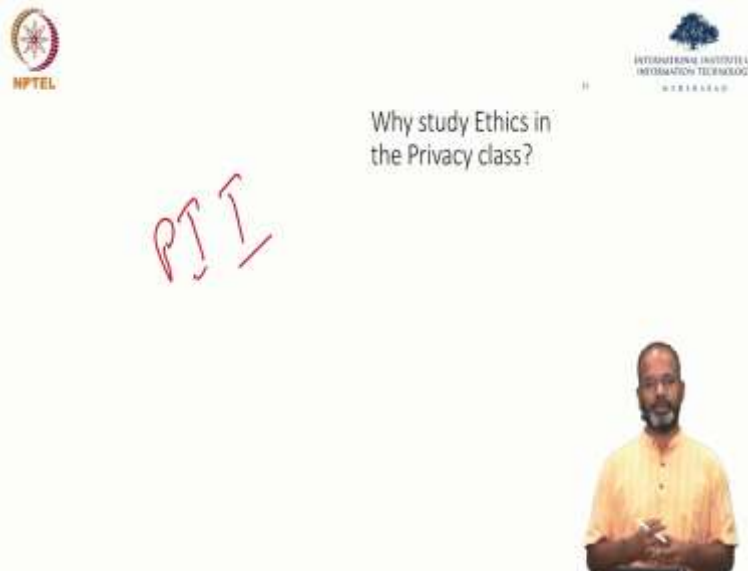
(Refer Slide Time: 00:16)



Now, let us look at the second part of this week's content, which is studying ethics in the context of privacy that is the course. What is ethics? If you just consider the broader definition of what ethics is, it is just being sort of say, reasonably appropriate in terms of doing somethings. Ethically, you would have heard this word, be ethical, when you are doing some things.

So, that is what we are going to study ethics in the context of course, is going to be how to design studies to collect data, how to analyse data, what data to collect in terms of privacy studies, what are the methods to get your study approved and information connected to that. That is what we are going to be studying in this section of the course.

(Refer Slide Time: 01:13)



Why study ethics? I think it is critical because as we always know, many of the studies, many of the data that we collect for analysis of privacy is actually going to have personally identifiable information. If you think about doing a user study on how people use browser extensions or how what all websites do people access while making a purchase, you want to get some level of personal details in that.

You are going to get what products they are buying, what time they are actually going to the website, all these kinds of information, which could potentially be used against them or which is potentially identifiable to that user also. Given that the studies are all about, in the context of privacy's personally identifiable information, sensitive information, all that it is very, very necessary for administrators, researchers, whoever is conducting the study to know the ethical part of conducting these studies.

(Refer Slide Time: 02:19)

NPTEL

INTERNATIONAL INSTITUTE OF  
INFORMATION TECHNOLOGY

Institutional Review  
Board (IRB)

What is it?  
Why do we need it?  
Why study ethics?

Academic  
Setting

One of the key component of ethics would be this institutional review board, particularly in the academic setting, I think this is all of that we will be talking about is in the academic setting. Because companies can collect data companies are collecting data, and they are using it, there is very meaning they have fair information practices and other controls over it.

But our focus on this course would be at the academic level, because most of you would be students, most of you would be conducting these studies in academic settings. That is what we will focus on. Institutional review board or it is also called as ethics committee in some context, some universities.

Institutional review board is a requirement now, more and more now organisations, academic settings, academic publications, are making it mandatory for studies to get the IRB approval, ethics committee clearance, so that the studies could be done ethically. Why do we need it? These are basically checks and balances. Because otherwise, I will show you some examples where studies have been done before the IRB creation and all where there is a lot of miss behaviour is happened, the data has been misused all of that.

(Refer Slide Time: 04:59)

NPTEL

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY

### Stanford Prison Experiment

Randomly assigned participants as guards or prisoners

1971

Arrested prisoners at home

24 UGs in the basement of a building

Authoritarian and draconian behaviour

Sadistic behaviour by guards

- Physical abuse
- Sexual humiliation
- Sleep on concrete

Images from the Stanford experiment  
(with thanks to Philip Zimbardo)

This is one of the classical example in terms of whenever ethics and studies are discussed. This was conducted in 1971 at Stanford University. The study was simple. The study was that they took 24 undergrads and they said that okay, half of you behave like a prisoner half of you behave like make guards and they said that they put the setting saying that okay, let us understand the behaviour of this prisoners and guards at in a particular context.

So, randomly assign participants as guards as prisoners arrested prisoners at home just to set the study in that mode 24 UGs in the basement of a building What came out after this study was set up was what created a big uproar. You can see the images, you can see images of physical abuse, sexual humiliation, getting people to not to go to sleep and torturing them or authoritarian, authoritarian or draconian behaviour of the guards happen.

Interestingly half the time meaning that this study also was designed and said that in a way that after some period, the roles switched, the guards became the prisoners and the prisoners became the guards, the behaviour continued. So, again, you can think of here there is no personal information, as I say motivated that IRB is necessary or ethical clearance is necessary, but this is abused to people.

One of the ways by which one of the studies that actually motivated thinking about control or experiments that are done very popularly called as the Stanford prison experiment.

(Refer Slide Time: 06:21)

The slide is titled "Stanford Prison Experiment". It features the NPTEL logo in the top left and the International Institute of Information Technology logo in the top right. In the center, there is a photograph of a wooden placard that reads: "Site of the STANFORD PRISON EXPERIMENT 1971 Conducted by Dr. Philip G. Zimbardo". To the right of the placard, a man in a yellow shirt is speaking.

Meaning it looks like there is a placard in the Stanford university which says there is a site of the Stanford prison experiment in 1971. It is that popular so if you just look up Stanford experiment, you will see lots and lots of references to this study and how influential the study was in thinking about the institutional review board.

(Refer Slide Time: 06:49)

The slide is titled "Milgram Experiment". It features the NPTEL logo in the top left and the International Institute of Information Technology logo in the top right. On the left, there is a diagram of the experimental setup with handwritten red annotations: "E" for Experimenter, "T" for Teacher, and "L" for Learner. The diagram shows a person in a blue shirt (E) operating a control panel, a person in a green shirt (T) holding a lever, and a person in a green shirt (L) in a separate room. To the right of the diagram, the text reads: "1961 Yale university", "Participants to obey Experimenter", "Shock", and "65% went to give 450V". A man in a yellow shirt is speaking on the right side of the slide.

Here is another experiment, which is also extremely popular in terms of showing the power of users. So, this study was conducted in 1961, in Yale University. So, this is an experimenter this

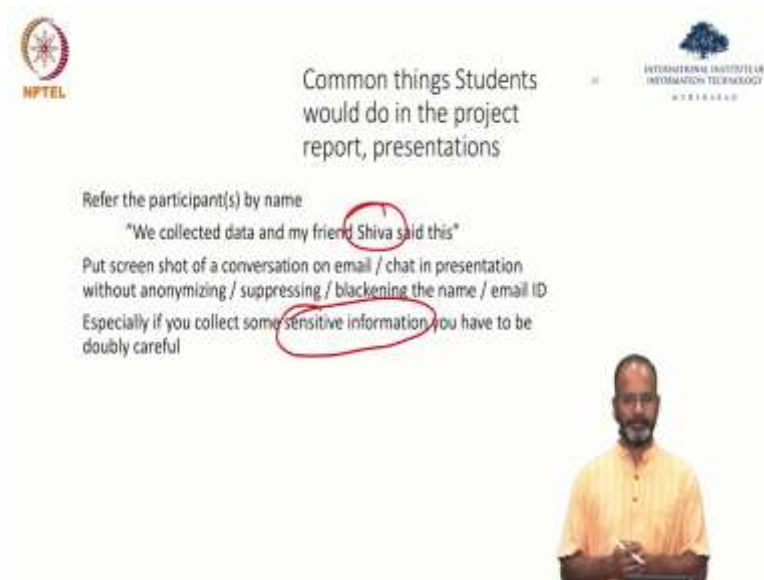
is a teacher, this is a learner experimenter teacher learner. So, they experiment, the way it was set up was, teacher would ask a question, and if the learner did not perform answer correctly, the teacher had the control of giving the voltage to the learner that is how it is set up.

So, if you see here, it is set up so that the learner could actually get shocked. As the learner made mistakes, the teacher can increase the voltage decrease the voltage, all of that was going on. Again, this is to show that how much power the teacher had and or the learner was what the study was interested, the researchers were interested in studying.

At some point, though, 65 percent of the participants 65 percent went to 65 percent of the teachers went to actually give about four 450 volts, to the learners, which is very high. And in reality, the learners did not get the shock. It was the learner was making noise, as though he or she was getting the shock, but never got the shock. Again, very popularly called as Milgram experiment, feel free to look it up. And if you have any questions about the study about the context, everything we I am meaning I am happy to explain something more in detail also.

But for now, this experiment is a way by which participants got shock which they did not I meaning learner thought that he or she was giving shock to the teacher thought that he or she was giving shock to the learner, but the learner did not get the shock. But it showed that how much of authority that the teacher thought that he or she had over learn, again an experiment to show how users without knowledge also the other part of the study is also the disruption part.

(Refer Slide Time: 09:26)



The slide features the NPTEL logo on the left and the IIT Bombay logo on the right. The main title is "Common things Students would do in the project report, presentations". Below the title, there are three bullet points: "Refer the participant(s) by name", "Put screen shot of a conversation on email / chat in presentation without anonymizing / suppressing / blackening the name / email ID", and "Especially if you collect some sensitive information you have to be doubly careful". The words "Shiva" and "sensitive information" are circled in red. A small photo of a man in a yellow shirt is in the bottom right corner.

Common things Students would do in the project report, presentations

- Refer the participant(s) by name
- "We collected data and my friend Shiva said this"
- Put screen shot of a conversation on email / chat in presentation without anonymizing / suppressing / blackening the name / email ID
- Especially if you collect some sensitive information you have to be doubly careful

I have seen very commonly part, students doing studies give these kinds of details out, which is we collected data and my friend Shiva said this when we are looking at project reviews, even in the reports that they will write, Shiva said this would be there that is the revealing the participant, put the screenshot of a conversation on email, chat and presentation without anonymizing or suppressing, blackening the name or email address.

For example, you would have had some conversation, you would see some, let us take a tweet, or a Facebook update from one of your friend, which you wanted to use it as motivational for point that you want to get across, you will take a screenshot and put it without actually anonymizing it. And then particularly if the if there is sensitive information, you really want to make sure that you do not reveal that information. As much as possible try and avoid using this information itself, using the screenshot itself. If it is necessary, please anonymize it.

(Refer Slide Time: 10:40)

The slide features the NPTEL logo on the left and the International Institute of Information Technology logo on the right. The main title is 'Institutional Review Board (IRB)'. Below the title is a list of items: 'IRB Application', 'Consent form', 'Proposal', 'Flyer', and 'IRB is only a floor not a ceiling!'. A small video inset shows a man in a yellow shirt speaking.

So, now let us look at what is the institutional review board. What is the application? What is the concern form? How do you build the consent form? What should be in the consent form? What is the proposal that you should write? What is the flyer that you can actually you should submit with the IRB application for getting it approved.

So, I have done many, many studies with IRB currently also have studies which in which IRB approval is needed. This takes some time and all institutions, whichever Institute you are part of, please go check if your institute as an IRB approval, even that itself would be an interesting data for me to also look at, which is please go look, I ask your institute, whether they have institutional review board or ethics clearance committee, and posted on mailing lists saying that institution name yes or no for the IRB.

You will also understand how the institute's look at these problems. An IRB is only a floor, which is that IRB only looks at the minimum requirement of doing the studies. You should be able to do more protection to the data that you are collecting, you should be able to, you should be more careful in terms of data that you are collecting and protect the data that you are collecting.



(Refer Slide Time: 12:10)

**70 Minutes interview, get paid \$20**

*Minimal ASK..*

Research group at **Carnegie Mellon University** is conducting a 70 minute user study

Qualification for participation:

- Must have an email account
- Ability to travel to Carnegie Mellon's campus
- Be at least 18 years old

**\$20 payment upon completion**

Let us, look at IRB applications. So, this is all of the content from now till the end of the IRB documents is all documents that I have used in my own studies. So, I am meaning I am happy I prepared it myself. So, I am happy to actually explain it in detail. Also, if there is anything particular that you want to know. So, this is a flyer, this is a flyer to show the how we did the study and how so these are information that was given for participants to understand what the study is, and sign up for the study.

(Refer Slide Time: 12:45)

**Proposal abstract**

This study investigates why people fall for phishing scams, as well as how effective various interventions are at educating people about these scams. Examples of existing phishing scams include sending fake emails from banks asking people to log into their web site, resulting in identity theft or financial loss for people that fall for these scams.

We want to test how effective standard email security notices are, where companies send notifications to people warning them of phishing scams. We also want to compare these security notices with an intervention we have designed, in which we mimic the structure of existing phishing scams and then train people who "fall" for our emails on how to avoid them in the future.

We plan to conduct the study with people who are non-technical and novices in the area of security and privacy. We plan to recruit our participants from in and around CMU and UPIT. During the study we will give our participants a fictional persona and ask people them role play as that person. We will show our participants different emails and ask them to handle those emails. We will take video screen captures and audio recordings of participants, and will also ask post study questions to understand how much they have learned.

These findings will help us understand how people make online decisions. The ultimate goal of this research is to develop tools, such as new email applications, that will enable consumers to make better decisions about which emails to trust with the real and real of



of security and privacy. We plan to create the phishing email to our research team and UPfit. During the study we will give our participants a fictional persona and ask people them role play as that person. We will show our participants different emails and ask them to handle those emails. We will take video screen captures and audio recordings of participants, and will also ask post study questions to understand how much they have learned.

These findings will help us understand how people make online decisions. The ultimate goal of this research is to develop tools, such as new email applications, that will enable computer users to make better decisions about which emails to trust, with the end goal of reducing vulnerability to computer security problems.

We plan to show about 20 emails for the subjects to make decision; we plan to do a between-subjects study with two groups, with approximately 10 people in each group. One group will be shown the emails which have security announcements and another group will be shown emails that have training emails with interventions we have designed.

No personally identifiable information will be collected or studied and no identifiers will be used (see Section on Confidentiality). Participants will receive a small monetary cash compensation for their effort and time spent in completing the interview.



So, the application goes with the proposal, the application goes to the consent form, the application goes with some more details about the study. So, the proposal is generally giving the details of what the study is. And there are some sections of the proposal that I will go through this study was about how people were using emails, and in terms of how they were actually reacting to phishing emails for the study.

So, just the details about the proposal itself technical details about the proposal, if you want to look at it. This study investigates why people fall for phishing scams, as well as how effective various interventions are at educating people about these scams. Just general details about the study, and then walking through the details in the email itself.

(Refer Slide Time: 13:35)



The slide features two logos at the top: NPTEL on the left and International Institute of Information Technology on the right. Below the logos, the text reads: **How subjects will be utilized**  
Around 20 people in and around CMU and UPitt will be interviewed for this user study.  
Subjects will be shown about 20 emails and they should take no longer than 70 minutes to complete the associated tasks.

A video inset in the bottom right corner shows a man in a yellow shirt speaking.

The details is not relevant to this class that is why I am not getting into details of the proposal itself. But the sections are very important for this class. Around 20 people in and around CMU, and UPitt will be interviewed for this study. As this again, details of how the subjects will be recruited in your case, probably you could again, so this is connecting to probably the projects that I said you should try as part of this course.

Please consider actually doing some data collection of human subjects. In the process, you will actually understand how to set up this IRB approval everything. So, this is about if you are doing an online study, you will say that look, I would use this survey monkey or I would use portals where I would get users to sign up and I would send out emails I would post on tweet, Twitter, I will post on Facebook to recruit participants.

(Refer Slide Time: 14:35)

**Confidentiality**

During the interview no personally identifiable information like name, address, etc. will be collected. One group of subjects will receive one set of emails and another group will receive another set of emails as said earlier in the proposal. All subjects will be asked the same set of pre and post experiment questions from the same protocol. The subjects will be chosen upon agreement of the subject.

The interviews, transcripts, audio files and study results will be treated as follows to maintain confidentiality and anonymity. Each interviewee will be assigned a random number. Only authorized members of the research group will have access to the audio files and transcripts. Audio files will be kept in password-protected computer by researchers affiliated with XXXXX. The consent form will be used for the purpose of record keeping.

be collected. One group of subjects will receive one set of emails and another group will receive another set of emails as said earlier in the proposal. All subjects will be asked the same set of pre and post experiment questions from the same protocol. The subjects will be chosen upon agreement of the subject.

The interviews, transcripts, audio files and study results will be treated as follows to maintain confidentiality and anonymity. Each interviewee will be assigned a random number. Only authorized members of the research group will have access to the audio files and transcripts. Audio files will be kept in password-protected computer by researchers affiliated with XXXXX. The consent form will be used for the purpose of record keeping.

This is one of the critical thing that the IRB, so what is IRB reviewer side also? It is going to be for example, in IIIT it is going to be faculty who are who understand these kinds of ethical ideas, ethical concepts. They are going to be part of the committee who is going to approve the study. It can have the external faculty or researchers are also part of the committee.

But it is an announced committee, which is a set of faculty who will look at the application and approve it. And of course, there is discussion also, which goes on, if they need any clarification, I have done some IRB applications where it goes back and forth with the committee and the

research group to answer questions and then IRB actually reviews it because they need more details if needed.

Confidentiality is something very critical that the IRB is going to look at, which is to say that, okay, once the data is collected, how are you going to protect it? Who is going to get access to it? How long will you actually keep this data all of that information is presented here. So, just to get some details, during the interview, no personally identifiable information like this would be collected, only anonymized members, authorised members of the research group allow access to the audio files and transcripts.

Because this was an interview study, audio files who would access to this what was mentioned here. So, it is very detailed, because it should actually give the IRB committee to have all the details for approval. So, essentially, this is to say that the pre study and the post is every study most of the times will have a pre component, which is collecting let us take demographics of the user collecting some information about the user and the study itself will happen in my in this case, how people react to phishing emails was there.

Pre would be getting the demographics of the study of the users, post would be looking at how telling the users that what happened and what we were trying to study all that. It is extremely also important to do this post study, not just debriefing, debriefing is most about what happened in the study.

Also, post component can also collect data from the users. Now, that you have done the study tell us what do you think about phishing emails? Would you do you still continue clicking on phishing emails as you did in the study? These kinds of questions could be asked in the post study, to get to know what the participants are thinking about that is what a post component of study is.

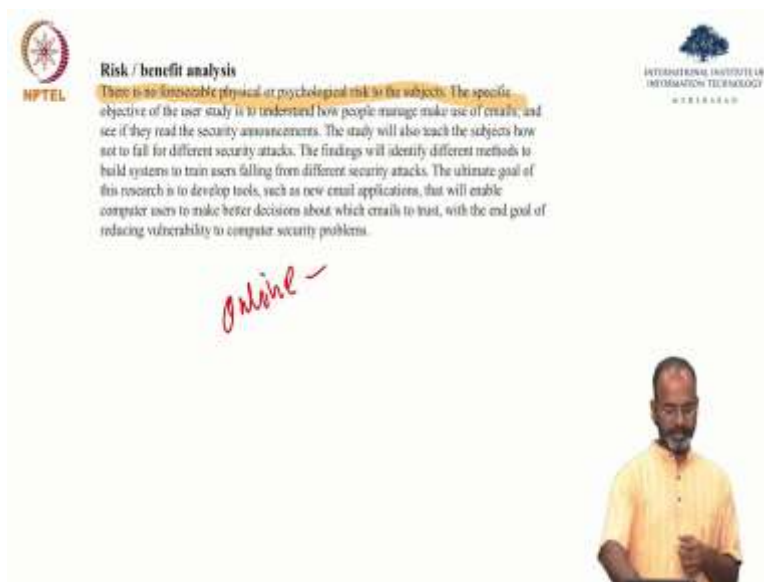
(Refer Slide Time: 17:35)



The slide features the NPTEL logo on the left and the International Institute of Information Technology logo on the right. The main text reads: "Officials authorizing access to subjects" followed by "Subjects will be recruited from the general population of Pittsburgh living in and around CMU and UPitt who are non-technical and also some group of students from CMU and UPitt will be recruited." A speaker in a yellow shirt is visible in the bottom right corner.

Officials, authorising access to the subject subjects will be recruited from general population of Pittsburgh, living in and around CMU and UPitt who are non-technical and also some group of students from CMU and UPitt will be recruited. So, this is basically telling the details about participants again.

(Refer Slide Time: 17:54)



The slide features the NPTEL logo on the left and the International Institute of Information Technology logo on the right. The main text reads: "Risk / benefit analysis" followed by "There is no foreseeable physical or psychological risk to the subjects. The specific objective of the user study is to understand how people manage make use of emails, and see if they read the security announcements. The study will also teach the subjects how not to fall for different security attacks. The findings will identify different methods to build systems to train users falling from different security attacks. The ultimate goal of this research is to develop tools, such as new email applications, that will enable computer users to make better decisions about which emails to trust, with the end goal of reducing vulnerability to computer security problems." A handwritten note "Online -" is written in red below the text. A speaker in a yellow shirt is visible in the bottom right corner.

The risk is another one that so confidentiality, as I said, and the risk is another one that the committee is going to look at. What level of risk is this? Why is this important? Because just for

our online studies, you could say that look, risk is very minimal and this, they are going to come look at some emails, do some research, reply to the emails, click on the links if necessary, and then move on.

But just think about it if it was a medical study. If you are actually a drug discovery study, if you have to actually give the participant a medicine and then come back and look at or stay with them for a few hours, look at the after effects of the study, or come back and look at the effect of the medicine after a month or so.

So, those kinds of studies will have higher risk. So, that is why risk is a key component in which minimal risk is what they would look for minimal medium, high risk is what IRB will look at, what level of risk is it accordingly, they would actually look at the application. So, in this case, in the context that we have put this, there is no foreseeable, physical or psychological risk of the subjects.

The specific objective of the user study is to understand how people make use of emails and see if they read the security announcements, the study will also teach the subjects how not to fall for different security attacks. The findings will identify different methods. So, just to say that, look, there is not much risk in this study that participants are signing up for.

(Refer Slide Time: 19:40)



The slide features the NPTEL logo on the left and the IIT Bombay logo on the right. The central text reads: **Subject recruitment**  
Subjects will be recruited by posting flyers around CMU and UPitt for recruiting people who are not technology savvy. By no means will we force anybody to participate in the interviews. We plan to use the sample questions at <http://www.surveymonkey.com/s.asp?c=220462099351> for screening the subjects for the study.

In the bottom right corner, there is a photograph of a man with a beard and glasses, wearing a yellow polo shirt, looking down at a device.

More details about subject recruitment, how subjects would be recruited.

(Refer Slide Time: 19:46)

**Sample Pre and post experiment questions**


**Pre-experiment questions**

- On average, how many total emails do you receive per day?
- On a scale of 1 - 7 where 1 is not at all likely and 7 is most likely, how likely do you reply to emails?
- Can you please describe some of the emails that you receive?
- Can you please describe the way in which you have organized your email inbox?

**Post-experiment questions**

- Ask if they have any comments or suggestions.
- If they didn't understand the cues or information provided, ask why.
- How confident were they while making decisions on clicking links and replying to emails.
- What do you think about the system or methodology of training?
- Did the method create awareness about phishing attacks?
- Do you think this method will help you learn techniques to identify false web site and emails?

*X is this the only way this data can be collected? Level.*



**Sample Pre and post experiment questions**


**Pre-experiment questions**

- On average, how many total emails do you receive per day?
- On a scale of 1 - 7 where 1 is not at all likely and 7 is most likely, how likely do you reply to emails?
- Can you please describe some of the emails that you receive?
- Can you please describe the way in which you have organized your email inbox?

**Post-experiment questions**

- Ask if they have any comments or suggestions.
- If they didn't understand the cues or information provided, ask why.
- How confident were they while making decisions on clicking links and replying to emails.
- What do you think about the system or methodology of training?
- Did the method create awareness about phishing attacks?
- Do you think this method will help you learn techniques to identify false web site and emails?

*X is this the only way this data can be collected? X RISK Level.*



So, another (( ))(19:48), one is the confidentiality risk another key component that IRB is going to look for, what are the kinds of questions that you are going to ask the participants So, as I said, pre experiment questions, which is, on average, how many total emails do you receive per day on a scale of 2 to 7? Not likely 7 is most likely, how likely to you to apply and all these are all questions that you would ask before they do the study.

And after the study, if they did not understand the cues or information provider ask for, taken the study, you showed them something and you realise that they could have got it, they did not get it,



you could make a note of it and then talk to them after the study saying why there are not understand that.

Two important components that IRB is going to look at, in addition to confidentiality that I said is, this the only way by which data can be collected? This question would IRB repeat for every single study, is this the way that is this the only way that the data could be collected? Can you do the study without actually interacting with human subjects? If so, please do that approach is what IRB requested way.

And the reason risk level, as I said, minimal, high risk is what they would look for.

(Refer Slide Time: 21:19)



Consent Form, I will actually walk you through the consent form in a second.


(Refer Slide Time: 21:23)



Human subject's clearance request, again, I will show you in the deck of slides. So, this is basically online tutorial content that you will have to go through to get certified that you are you are aware of how to do the studies with human subjects. And I actually summarised this deck of summarise the content in few points, we could actually look at that.

But I would highly recommend you to go look at the content and get this certified also, if you do it, please post it on, again, our mailing list. It is just about a 90 minutes video that you will have to look for, and answer some questions depending on I mean I think there is also not right, wrong answers. The test is about have you understood the content that is all.

(Refer Slide Time: 22:13)

 **Supporting Trust Decisions**

**NPTEL** Sponsor: National Science Foundation  
Principal Investigator: XXXXXXXX  
Affiliated Interviewers: Mr. Ponnurangam Kumaraguru  
Neither the funding agencies, nor these researchers will receive any financial benefit based on the study results.

This study has been approved by Carnegie Mellon University's Institutional Review Board (IRB).

Purpose of the study. The researchers want to understand how people manage online tasks effectively.


Interview procedure. You will role play as a person and access that person's emails. You will be asked to think aloud while in the study. In particular we will show you about 20 emails and ask you to react to the emails as you will do in real-world situation.


Compensation. The interview is expected to take maximum of 70 minutes, and we will pay you \$20 for your time and effort.


Risks / discomforts / costs. The experience is expected to be inherently interesting and a generally positive experience. There will be no (other) cost to participating other than your time.

Research benefits. The specific objective of the study is to characterize how people think and do while doing online tasks. The findings will identify things that people look for while making decisions. The ultimate goal of this research is to develop tools, such as new email notifications, that will enable computer users to make better decisions.

Right. By no means should you feel forced to participate in this interview. You can withdraw





 **Supporting Trust Decisions**

**NPTEL** Sponsor: National Science Foundation  
Principal Investigator: XXXXXXXX  
Affiliated Interviewers: Mr. Ponnurangam Kumaraguru  
Neither the funding agencies, nor these researchers will receive any financial benefit based on the study results.

This study has been approved by Carnegie Mellon University's Institutional Review Board (IRB).

Purpose of the study. The researchers want to understand how people manage online tasks effectively.

Interview procedure. You will role play as a person and access that person's emails. You will be asked to think aloud while in the study. In particular we will show you about 20 emails and ask you to react to the emails as you will do in real-world situation.


Compensation. The interview is expected to take maximum of 70 minutes, and we will pay you \$20 for your time and effort.


Risks / discomforts / costs. The experience is expected to be inherently interesting and a generally positive experience. There will be no (other) cost to participating other than your time.

Research benefits. The specific objective of the study is to characterize how people think and do while doing online tasks. The findings will identify things that people look for while making decisions. The ultimate goal of this research is to develop tools, such as new email notifications, that will enable computer users to make better decisions.

Right. By no means should you feel forced to participate in this interview. You can withdraw your consent and stop your participation in the interview now, or at any time, without affecting your relationship with Carnegie Mellon University and without loss of any benefits to which you may otherwise be entitled. If you are under 18, you cannot be interviewed.

Confidentiality. I understand that the interviews, transcripts, audio files and study results will be treated as follows to maintain confidentiality: Each interviewee will be assigned a random number. Only authorized members of the research group will have access to the audio files and







you to react to the emails as you wish in a non-work situation.

**Duration:** The interview is expected to take maximum of 70 minutes, and we will pay you \$20 for your time and effort.

**Risks / discomfort / costs:** The experience is expected to be inherently interesting and a generally positive experience. There will be no (other) cost to participating other than your time.

**Research benefits:** The specific objective of the study is to characterize how people think and do while doing online tasks. The findings will identify things that people look for while making decisions. The ultimate goal of this research is to develop tools, such as new email applications, that will enable computer users to make better decisions.

**Right:** By no means should you feel forced to participate in this interview. You can withdraw your consent and stop your participation in the interview now, or at any time, without affecting your relationship with Carnegie Mellon University and without loss of any benefits to which you may otherwise be entitled. If you are under 18, you cannot be interviewed.

**Confidentiality:** I understand that the interviews, transcripts, audio files and study results will be treated as follows to maintain confidentiality: Each interviewee will be assigned a random number. Only authorized members of the research group will have access to the audio files and transcripts. Audio files will be kept in password-protected computer by researchers affiliated with Dr. Lorie Cronor.

I understand that by giving my consent, I give Dr. Lorie Cronor and her associates permission to present this work in written and/or other forms for teaching or presentations to advance the knowledge of science and/or academia, without further permission from me.

**Contact information:** If you have any questions about this study, you should feel free to ask them before the interview, or anytime throughout the interview or by contacting:



I understand that the interviews, transcripts, audio files and study results will be treated as follows to maintain confidentiality: Each interviewee will be assigned a random number. Only authorized members of the research group will have access to the audio files and transcripts. Audio files will be kept in password-protected computer by researchers affiliated with Dr. Lorie Cronor.

I understand that by giving my consent, I give Dr. Lorie Cronor and her associates permission to present this work in written and/or other forms for teaching or presentations to advance the knowledge of science and/or academia, without further permission from me.

**Contact information:** If you have any questions about this study, you should feel free to ask them before the interview, or anytime throughout the interview or by contacting:  
XXXXX Carnegie Mellon University, Pittsburgh, PA 15213

For any questions pertaining to your rights as a research participant, our objections to the study, you may contact: IRB Chair, Regulatory Compliance Administration, Carnegie Mellon University, Warner Hall, Room 414, Email: [irb-revision@andrew.cmu.edu](mailto:irb-revision@andrew.cmu.edu)

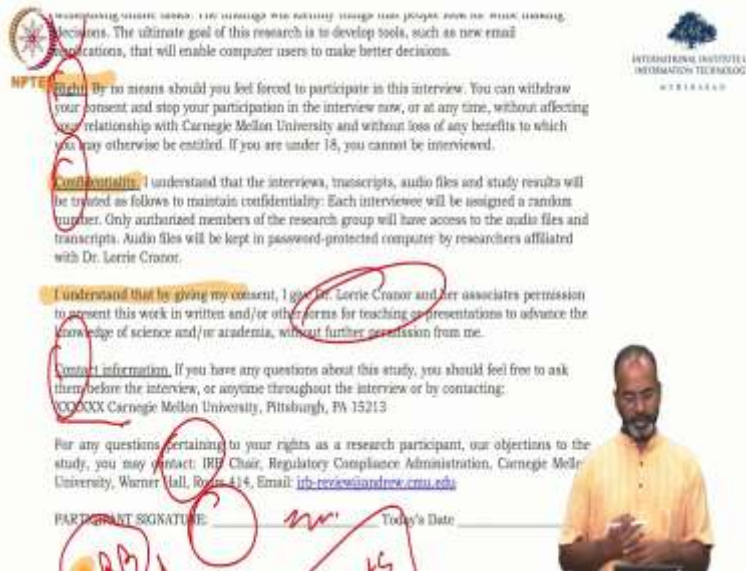
PARTICIPANT SIGNATURE: \_\_\_\_\_ Today's Date \_\_\_\_\_

*IRB Seal*  
*Alina Subjects*

Carnegie Mellon University



Version: 1/2007  
Revised: 1/2007  
Copyright: 2007  
NPTEL  
www.nptel.edu



So, here is an example of the consent form. The consent form is I mean, I am sure you would have been part of studies, I am hoping that some of you would have participated in studies where you signed up for such consent form. I mean I think even if you go to a restaurant now, where they have this huge burgers for the entire family (( ))(22:36), they get a consent form sign that saying, but look, we are not taking any responsible if anything happens to our health after this. That is the consent form that I am talking about.

So, this consent form is walking you through the same study in terms of email phishing study, it talks about purpose of the study, purpose of the study interview procedure, which is you will come into the lab, we will ask you questions, all that compensation, you will what you will get paid risk and discomfort and cost research benefits risk, as I said, minimal risk, high risk, what is the risk for being participating in the study, research benefits.

What are the benefits of the study if you participate? And if as researchers were able to understand what happens, it will help the society that is the argument we will make. Right is by no means should you feel forced to participate in this interview, meaning nobody is getting forced into being participant in a study.

And you can withdraw your consent and stop participating and interview now, or any time in the middle of the study also, confidentiality that I have already said. In the application, you say what all you going to do, generally consent forms like about a page or a page and half where you are

just summarising everything for the user. And the user actually signs here. Participant actually signs here and this is here would be IRB seal today, it could all be in digital.

But the IRB approval seal would be there and you actually present this to the users and users sign it and if you see here I can understand I can I understand that by giving my consent I give so and so that is my PhD thesis advisor under associates permission to present this work or return or, and or other forms for teaching presentation so that I can use it in this kind of training material that I am using this content in the training material for this course.

Contact information if you have any questions about the study, feel free to ask, feel free to call all that. So, that is about the consent form. This is just about one page consent form. In online form, you can just embed this into the study and people click I agree, you use that as your approval for the subjects and get them be part of the study. So, that is about consent form.

(Refer Slide Time: 25:20)

**Carnegie Mellon University**

**APPLICATION FOR IRB REVIEW OF RESEARCH INVOLVING HUMAN SUBJECTS**

Research Project Title: SUPPORTING TRUST DECISIONS - TRAINING MODULE

Anticipated Start Date: 10 May 2006 Anticipated End Date: 31 December 2006

Source of Funding (Optional): Internal  External: YYYYYY

Principal Investigator (PI): XXXXXXXX PI Title (Degree): PhD

PI's Department: School of Computer Science PI's Phone: \_\_\_\_\_

PI's E-mail: XXXXXXXXXX PI's Building & Room No: CIC 2107

If student, please complete:  
Faculty Advisor: \_\_\_\_\_ Department: \_\_\_\_\_  
Phone: \_\_\_\_\_ Building/Room #: \_\_\_\_\_ E-mail: \_\_\_\_\_

CMU's Co-Investigator:  
(1) \_\_\_\_\_ (2) \_\_\_\_\_  
(3) \_\_\_\_\_ (4) Aravindhan Kumaraguru (ISR, SCS)

**Concise Statement of Proposed Research with Details of Human Use Aspect**

Describe within the space below, in layman's terms, what is to be done so that a realistic estimate of the risks to the subject and the benefits of the project can be assessed.

APPLICATION FOR IRB REVIEW OF RESEARCH INVOLVING HUMAN SUBJECTS

Research Project Title: SUPPORTING TRUST DECISIONS - TRAINING MODULE

Anticipated Start Date: 10 May 2006 Anticipated End Date: 31 December 2006  
 Source of Funding: Opportunity-Internal External: YYYYY  
 Principal Investigator (PI): XXXXXXX PI Title/Degree: PhD  
 PI's Department: School of Computer Science PI's Phone: \_\_\_\_\_  
 PI's Address: 8-7534 PI's Building & Room No.: CIC 2207  
 PI's E-mail: XXXXXXX@cmu.edu

If student, please complete:  
 Faculty Advisor: \_\_\_\_\_ Department: \_\_\_\_\_  
 Phone: \_\_\_\_\_ Building/Room #: \_\_\_\_\_ E-mail: \_\_\_\_\_

CMU's Co-Investigator: (1) \_\_\_\_\_ (2) Prof. Anurag Kumar (ISJ, SCS)  
 (3) \_\_\_\_\_ (4) \_\_\_\_\_  
 (5) \_\_\_\_\_

**Concise Statement of Proposed Research with Details of Human Use Aspect**

Describe within the space below, in layman's terms, what is to be done so that a realistic estimate of the risks to the subject and the benefits of the project can be assessed.

The inclusion of females and members of minority groups and their sub-populations must be addressed in the development of the research design appropriate to the scientific objectives of the study. The research plan should describe the composition of the intended study population in terms of gender and racial/ethnic group. Provide a rationale for selection of study subjects.



APPLICATION FOR IRB REVIEW OF RESEARCH INVOLVING HUMAN SUBJECTS

Research Project Title: SUPPORTING TRUST DECISIONS - TRAINING MODULE

Anticipated Start Date: 10 May 2006 Anticipated End Date: 31 December 2006  
 Source of Funding: Opportunity-Internal External: YYYYY  
 Principal Investigator (PI): XXXXXXX PI Title/Degree: PhD  
 PI's Department: School of Computer Science PI's Phone: \_\_\_\_\_  
 PI's Address: 8-7534 PI's Building & Room No.: CIC 2207  
 PI's E-mail: XXXXXXX@cmu.edu

If student, please complete:  
 Faculty Advisor: \_\_\_\_\_ Department: \_\_\_\_\_  
 Phone: \_\_\_\_\_ Building/Room #: \_\_\_\_\_ E-mail: \_\_\_\_\_

CMU's Co-Investigator: (1) \_\_\_\_\_ (2) Prof. Anurag Kumar (ISJ, SCS)  
 (3) \_\_\_\_\_ (4) \_\_\_\_\_  
 (5) \_\_\_\_\_

**Concise Statement of Proposed Research with Details of Human Use Aspect**

Describe within the space below, in layman's terms, what is to be done so that a realistic estimate of the risks to the subject and the benefits of the project can be assessed.

The inclusion of females and members of minority groups and their sub-populations must be addressed in the development of the research design appropriate to the scientific objectives of the study. The research plan should describe the composition of the proposed study population in terms of gender and racial/ethnic group. Provide a rationale for selection of study subjects. Your proposal should contain a description of the proposed outreach program for recruiting females and minorities as participants.

This study investigates why people fall for phishing scams, as well as how effective various interventions are at educating people about these scams. Examples of existing phishing scams include sending fake emails from banks asking people to log into their web site, resulting in identity theft or financial loss for people that fall for these scams.

We want to test how effective standard email security notices are, where companies send notifications to people warning them of phishing scams. We also want to compare these security notices with an intervention we have designed, in which we mimic the structure





CMU IRB REVIEW APPLICATION



- Regarding the human subjects involved in the proposed study:
  - What is the age range of the subjects? **18 - 67 general users - no minors**
  - How many subjects are needed for this study? **Around 20**
  - Of the subjects studied, what will be the ratio females to females? **Approximately 50% males to 50% females**
  - Of the subjects studied, what percentage will be from minority groups? **Dependent on availability of people**
  - Are the subjects capable of understanding the nature of the study and the consenting process? YES [X] NO [ ]
  - What is the population source of the subjects to be studied? **Any general computer user in and around CMU and UPN.**
  - Indicate how subject recruitment will be performed: (Check appropriate boxes)
 

<input type="checkbox"/> CMU directory listing	<input checked="" type="checkbox"/> External advertising (radio, TV, publications, postings)
<input checked="" type="checkbox"/> Existing in investigator's files	<input type="checkbox"/> List of subjects from previous student recruitment efforts
<input checked="" type="checkbox"/> Email or web-based solicitations	<input type="checkbox"/> Other:

(Please elaborate)



2. Will any of the following classes of vulnerable subjects be involved in the proposed study?

	YES	NO	Comments
<b>Stolenator Minors</b>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	CMU students, but not
Minors	<input type="checkbox"/>	<input type="checkbox"/>	
Subjects with Compromised Mental Status	<input type="checkbox"/>	<input checked="" type="checkbox"/>	



	YES	NO	Comments
<b>Stolenator Minors</b>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	CMU students, but not
Minors	<input type="checkbox"/>	<input type="checkbox"/>	
Subjects with Compromised Mental Status	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Hospitalized or Institutionalized Subjects	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Pregnant Women	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Elderly	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Prisoners	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Subjects requiring certificate of confidentiality	<input type="checkbox"/>	<input checked="" type="checkbox"/>	



- If a clinical study, will a placebo or placebo procedure be used in this study?**  YES  NO
- Will the subjects receive intangible benefit from the study?  YES  NO
  - Are the subjects paid (monetarily) for entering the study?  YES  NO  
If yes, what is the amount and source of the funds? \$ **-420/person, NSF funding**
  - Are other inducements planned to recruit subjects? If yes, describe other inducements planned:  YES  NO



Here is the actual application form itself for the IRB application. First was proposal. First was flyer, then must proposal then must concerned form. Now, we have the application, applications just going into very details of the application, not necessarily in the paragraph format, but in the format that they have set up. Every institute has their own format, which they have used.

This is the format that CMU used for the study that I had done. So, asking you for details of the study period, who is involved, who is the PI, small description of the study itself and then details of what is the age of the group, participants, how many participants generally looking for equal balance between male and female.



What kind of participants would you get? Where the participants would come from? All of these kinds of details, I am going to share those documents also, as part of this course for you, it will be on the website, feel free to take a look at it. But the form generally looks for this details of the study risk. How will you? How will you recruit the participants?

How will you use the data that you are collecting? All that and then as I said before, even this right in a clinical study will placebo the placebo procedure be used in the study this form is generic. This form is not generally, this form is not only for the computer science department or the IT kind of study. This form is generally for anybody in an institute and therefore it also talks about the medical questions.

(Refer Slide Time: 27:14)

The image shows a screenshot of an Institutional Review Board (IRB) application form. The form includes the NPTEL logo on the left and the logo of the International Institute of Information Technology on the right. The form contains several questions and checkboxes:

- 5. Is subject's confidentiality/ anonymity in the project protected?
- 6. Are consent forms to be used?
- 7. Are provisions for subject's medical care available in the event of a personal (physical or mental) injury resulting solely from subject's participation in the research?     Not applicable
- 8. Indicate degree of research's physical risk to subject:  Minimal  Greater than Minimal  High
- 9. Indicate degree of research's psychological risk to subject:  Minimal  Greater than Minimal  High

Below these questions, there are three risk levels defined:

- Minimal Risk:** A risk is minimal where the probability and magnitude of harm or discomfort anticipated in the proposed research are not greater, in and of themselves, than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests.
- Greater than Minimal Risk:** A risk is greater than minimal where the probability and magnitude of harm or discomfort anticipated in the proposed research are greater than those ordinarily encountered in daily life or during the performance of routine physical or psychological examinations or tests.
- High Risk:** A risk is high where a moderate-to-high probability of serious adverse effects might occur as a result of participation in a research study.

Question 10: Do you or any individual who is associated with or responsible for the design, the conduct, or the reporting of this research have an economic or financial interest or act as an officer or a director for any outside entity whose interests could reasonably appear to be affected by this research project? YES ( ) NO (X)

(\*If yes, please provide detailed information to permit the IRB to determine if such involvement should be disclosed potential research subjects.)

The Investigator must also report any adverse event to the IRB as its Officers after its occurrence within ten working days.

I, the investigator, will agree to comply with the CMI's policies on the responsible conduct of research.

A presenter in a yellow shirt is overlaid on the bottom right of the form.

So, this is the one that I said before, which is minimal, greater than minimal risk and high risk. Depending on that the details of the review will happen. Minimal risk, not much of data is getting collected, not much of concern to the participants. It is okay to do the study. And please keep in mind these days, the conferences, journals are making it mandatory many of them ask this review explicitly while the paper is getting accepted, where the investigators in the study.

So, that is about the whole IRB applications. As I said, I will make this document also public, for all of you to access, and it will help you to go through what is needed for setting up this IRB approval.

(Refer Slide Time: 28:04)

NPTEL

INTERNATIONAL INSTITUTE FOR INFORMATION TECHNOLOGY

What is IRB committee looking for?

One being setup in IITB now

Is this the only way to collect the information that Researcher is interested in?

What protection is giving to the information that is collected?

Is there any implications of the data beyond the study?

NPTEL

INTERNATIONAL INSTITUTE FOR INFORMATION TECHNOLOGY

Is there any implications of the data beyond the study?

AVL Netflix

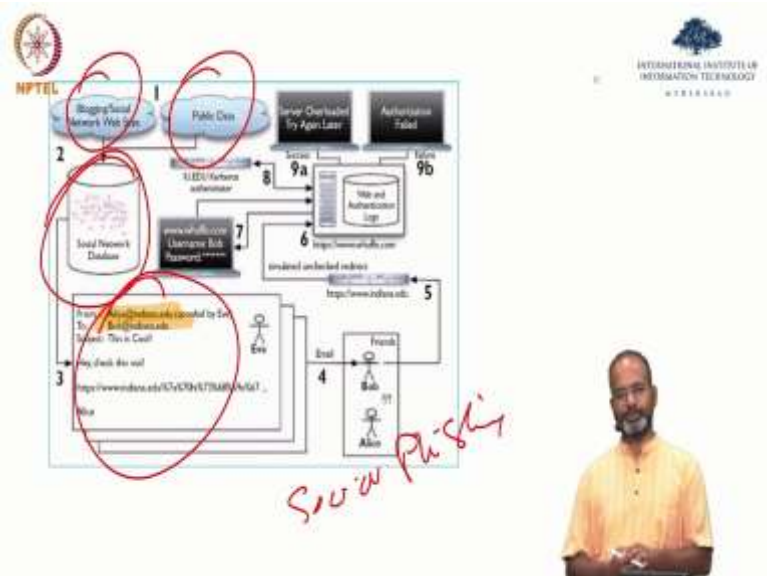
NPTEL

INTERNATIONAL INSTITUTE FOR INFORMATION TECHNOLOGY

What is IRB approval? Looking for there is there many as I said before they are only they are looking for is this the only way to collect information, what protection is giving is to the information that is collected, is there any implications of data beyond the study, because I think one component keeping the keeping our understanding of the AVL, Netflix.

All these data that has been made public and identifiability of the data that has happened after that, you also want to make sure that when you collect this data, when you have going to put the data also public make sure that the data does not get de identified all of that.

(Refer Slide Time: 28:56)



Here another study that which is more like the fishing study itself, which had some kind of after effect because of some connections that they made in terms of the study. So, this was a study done at Indiana University, Indiana University. So, what they did was, in short, again, please go look at the study if you are interested.

But in short, they collected some publicly available information, publicly available information connected it to put the data together and connected it to the Indiana university data of students, staff and faculty and then they figured out who is connected to whom. And then they sent out as part of the study as part of the phishing study. When they sent out the email, instead of the email coming from somebody from Indiana, they made this email coming from a person that they would actually know they are connected with.

The paper is called social phishing, feel free look at the paper if you are interested in it. So, this one, think about it, if you are going to get a phishing email, so it is coming from somebody from your institute is okay. But somebody whom you are connected with somebody whom you think that you have more stronger edges because they found that it was part of your social interactions is what the study did.

(Refer Slide Time: 30:23)

**Reactions for the study**

- Anger**
  - Unethical, inappropriate, illegal, fraudulent
  - Researchers fired
  - Psychological cost
- Denial**
  - Nobody accepted that they fell for it
  - Admitting our vulnerability is hard
- Misunderstanding over spoofing emails**
- Underestimation of publicly available information**

The slide features the NPTEL logo on the left and the International Institute of Information Technology logo on the right. A video of a man in a yellow shirt speaking is positioned on the right side of the slide.

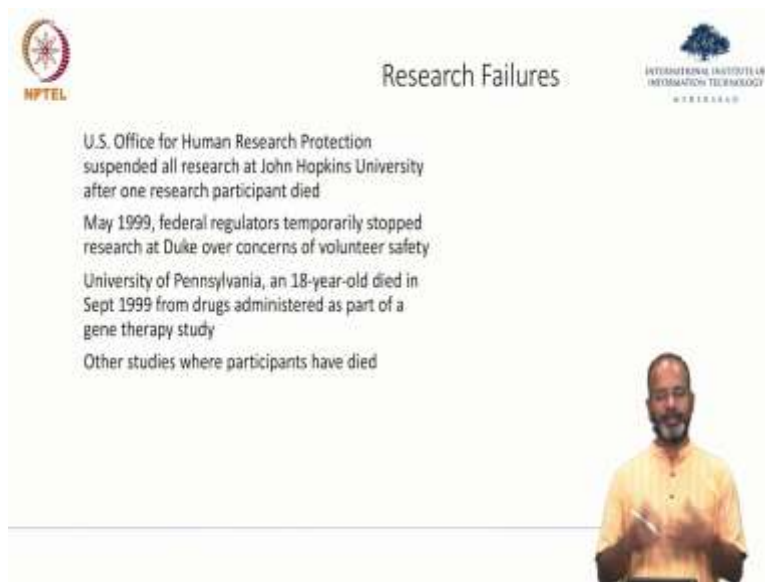
The slide displays a diagram of a social phishing attack. It shows a sequence of events: 1. A user receives an email from 'Frank' with a link to a website. 2. The user clicks the link, leading to a website. 3. The user is prompted to log in. 4. The user enters their credentials. 5. The user is redirected to a website. Handwritten red annotations include a circle around the email content and a larger circle around the diagram with the text 'Social Phishing' written inside.

**Reactions for the study**

The slide features the NPTEL logo on the left and the International Institute of Information Technology logo on the right. A video of a man in a yellow shirt speaking is positioned on the right side of the slide.

Those are lot of after effect for the study, unethical people thought that the study was unethical, illegal, fraudulent. Some effects on the researchers also, people denied that they fell for this kind of phishing attacks because the email was more targeted. The goal for the researchers was social phishing is more effective than normal phishing. Spear phishing is a word which is targeted, but social phishing is even more targeted, which is to pick up the relationship with people and then use it for sending phishing emails.

(Refer Slide Time: 31:09)



Research Failures

U.S. Office for Human Research Protection suspended all research at Johns Hopkins University after one research participant died

May 1999, federal regulators temporarily stopped research at Duke over concerns of volunteer safety

University of Pennsylvania, an 18-year-old died in Sept 1999 from drugs administered as part of a gene therapy study

Other studies where participants have died

So, 1960s 1970s, say short about Stanford, and Milgram, and then Indian universities, probably around 2003, 4, 5 this one, few more examples at the university level, because one question you could ask, which I think I get asked multiple times is that when you think about all the stuff what happens to the researcher who gets the problem. These kinds of experiments goes into a mess. What kind of effects can it have? Right paper getting rejected is their paper not going through a conference is definitely at a research level. But here are some examples of the institute level.

US office for human resources protection suspended all research at Johns Hopkins University after one research participant died, all of this is public you can take a look at them. In 1999, federal regulators temporarily stopped research at Duke University, of a volunteer safety. There were some safety issues with the participants who took the study and therefore Duke University's research was completely shut.

University of Pennsylvania 18 year old died in September 1999 from drugs administrators as part of the gene therapy study, the gene therapy study was stopped after this. And the university also had trouble taking up these kinds of research in future. So, I think the effect can happen a researcher, faculty paper getting not accepted. It could happen at the institute level where Institute's funding are getting stopped.

(Refer Slide Time: 32:48)

The slide contains the following text:

**Principles of Research with Human Subjects**

**Respect for Persons**  
individuals have autonomy and choice  
people cannot be used as a means to an end  
provide protection to the vulnerable  
provide informed consent and privacy

Logos for NPTEL and the Indian Institute of Technology Kharagpur are present in the top left and right corners, respectively.

So, next few slides is I hope, everything is clear until now, if you want to take a pause, in the video, pause the video and take simulate the content that you have gotten until now for this ethics part. So, what I did was this is part of the principles of human research with human subjects. This, is basic content when you do the 90 minute the video that I have later in the slide, you will understand the importance of how to take care of human subjects.

A few high level principles are respect for persons. I think these are very philosophy in some sense. That is why I said that having that clearance for the IRB would really help you to respect human subjects. I am sure all of you respect people and take care of subjects otherwise also, this is only a requirement in the IRB that this certificate is needs to be presented. Individuals have autonomy. People cannot be used as a means to an end philosophical, provide protection to the vulnerable provide informed consent and privacy.

(Refer Slide Time: 34:07)

The slide features the NPTEL logo on the left and the International Institute of Information Technology logo on the right. The title 'Principles of Research with Human Subjects' is centered at the top. Below the title, the word 'Beneficence' is written in bold, followed by a list of four points: 'kindness beyond duty', 'obligation to do no harm', 'obligation to prevent harm', and 'obligation to do good'. At the bottom of the slide, a man in a yellow shirt is shown from the chest up, looking towards the camera.

NPTEL

Principles of  
Research with  
Human Subjects

INTERNATIONAL INSTITUTE OF  
INFORMATION TECHNOLOGY

**Beneficence**  
kindness beyond duty  
obligation to do no harm  
obligation to prevent harm  
obligation to do good  
minimize risks, maximize benefits

Beneficent kindness beyond duty, basically, it is arguing that be kind to the participants. Please meaning there have been incidences where participants would show up in a study and they would actually feel bad cry, think that something went wrong and you really have to respect them and allow them to probably sign off the study if needed, and take care of the compensation if needed, and then let them go.

(Refer Slide Time: 34:40)

The slide features the NPTEL logo on the left and the International Institute of Information Technology logo on the right. The title 'Principles of Research with Human Subjects' is centered at the top. Below the title, the word 'Justice' is written in bold, followed by two points: 'treat all fairly' and 'share equitably burdens and benefits'. At the bottom of the slide, a man in a yellow shirt is shown from the chest up, looking towards the camera.

NPTEL

Principles of  
Research with  
Human Subjects

INTERNATIONAL INSTITUTE OF  
INFORMATION TECHNOLOGY

**Justice**  
treat all fairly  
share equitably burdens and benefits

And then be fair also, I think that is also an important thing be fair in terms of selection of the participants, which is male, female, if you are doing studies where other types of fairness is needed, please consider that and then also shared equitably, the burdens and the benefits. This is again keeping the participants in mind, feel obliged to take care of the participants in general.

(Refer Slide Time: 35:16)

NPTEL

Federal regulations, implementation

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY

Respect for Persons → Informed Consent  
Beneficence → Assessment of risk and benefits, minimize risk  
Justice → Fair selection of participants

That is philosophical. How does this translate the three aspects that we served, respect, for persons beneficent and justice, if you translate that into actionable items for us to do, it is basically informed consent, assessment of the risk, which is minimal and maximal a fair selection of participants. That is a translation, if you really look at how you can use it, those are three things that you should keep in mind.



(Refer Slide Time: 35:44)

The slide features the NPTEL logo on the top left and the International Institute of Information Technology logo on the top right. The main content is a white box with a blue header that reads 'PHRP' and 'About PHRP'. Below the header, the title 'ABOUT PHRP ONLINE TRAINING, INC.' is displayed. The text inside the box states: 'The Protecting Human Research Participants website and online training course are a product of PHRP Online Training, Inc.' It then describes the mission of PHRP Online Training: 'The mission of PHRP Online Training is to provide current and accessible training to ensure ethical and safe practices whenever research is being conducted with human participants. PHRP Online Training provides realistic practice scenarios for core concepts following IRB requirements, as well as exam questions to ensure course integrity. Learners can select from two courses to align with their research areas. PHRP reflects a mix of research types with a particular emphasis on biomedical research and PHRP 500 was created for those engaged in social, behavioral, and educational research.' At the bottom of the box, the URL 'https://phrptraining.com/about-phrp-course' is provided. A presenter in a yellow shirt is visible in the bottom right corner of the slide.

That is the link to the online tutorial that I said it will be super nice if some of you can go take a look at the content and have the certificate also.

(Refer Slide Time: 35:55)

The slide features the NPTEL logo on the top left and the International Institute of Information Technology logo on the top right. The main content is the text 'Work we have seen where IRB would have been necessary?' centered on the slide. A presenter in a yellow shirt is visible in the bottom right corner of the slide.

I also had a question to all of you, which is work we have seen where IRB would have been necessary some of the research that we have already seen, papers that we have seen. I would it would be nice if you can think about what studies IRB necessary and what where all IRB was necessary as part of the content that we have already seen.

(Refer Slide Time: 36:25)

The slide features the NPTEL logo on the left and the International Institute for Information Technology logo on the right. The main title is "Ethical Security Studies". Below the title is a box containing the abstract of a paper titled "Conducting Ethical yet Realistic Usable Security Studies" by Amir Herzberg and Ronen Mappeli. The abstract discusses the challenges of evaluating security mechanisms in a way that is both ethical and realistic, focusing on the role of users in detecting attacks. A presenter in a yellow shirt is visible in the bottom right corner of the slide.

And please post it in the class, please post it in the class mailing list of which studies do you think IRB was required IRB needs to be done. Here is the last part of this ethics for our course, which is conducting ethical at realistic usable security studies. There is also paper written how to do this, I will go through this paper very quickly.

(Refer Slide Time: 36:55)

This slide shows the full abstract and the beginning of the introduction of the paper. The abstract is highlighted in yellow. The introduction starts with "In the usable security field, the focus is on the behavior of the user. The aim of studies in the field, is to find where users". A presenter in a yellow shirt is visible in the bottom right corner of the slide.

So, this is the paper talking about what are the important aspects of how to conduct the studies. This paper is emphasising the points that I have said already, I have taken it from IRB

applications and everything. Feel free to read the paper in full. But here are some important aspects of the paper that is relevant, requires users to act naturally.

One of the important thing of doing the study ethical is to getting the environment natural to the study to the realistic environment that you want to keep. You want to study people accessing emails, when they are actually on a train when they are moving, it would be very nice to set up a study where you collect data in a similar scenario as in the real world. As close as possible I am sure you cannot do all the data collections as always, as you need. But try and do as close as possible where wherever appropriate.

(Refer Slide Time: 38:05)

On our system, the users had a real account to a real system, but one of low-sensitivity (an exercise-submission system). As discussed on section II, we took a different approach of supplying a positive reward for detecting attacks, which acts as a substitute for users' fear of giving away their highly-sensitive-site credentials to an attacker.

*Study's environment:* Users might act more cautiously in an unfamiliar environment. On the other hand, if the study takes place in a University's computers lab, they might be less cautious since they trust the University conducting the experiment, especially if there is an experimenter next to them, see results reported in [9].

INTERNATIONAL INSTITUTE FOR INFORMATION TECHNOLOGY

ON TECHNOLOGY. Downloaded on October 19, 2021 at 11:18:03 UTC from IEEE Xplore. Restrict

A studies environment users might act more cautiously in an unfamiliar environment. On the other hand if the study takes place in the university's computers lab, they might be less cautious since it trust the university conducting the experiment especially if there is an experimenter next to them. So, arguing that set it up in a way where the participants feel more comfortable.

(Refer Slide Time: 38:34)



the attacks. Also, since we emphasized that the bonus points depend on the detection rates, users felt some sense of risk (afraid to lose bonus points).



### III. DIVISION TO GROUPS - FAIRNESS AND BIAS ISSUES

On our study, the users were provided different defense mechanisms, and some mechanisms turned out to be much better than others (there was also a control group which did not have any defense mechanism). We promised to reward the users (with bonus points) based on their detection rates. Is this fair? Is it ethical?

In order to test several defense mechanisms and their combinations, the division of users into groups of different defense mechanisms is a must. The 'unfairness' of the reward being dependent on performance is not really harming the subjects, since their 'costs' of participation are any



were users who participated both years and did not cooperate in the first year. We believe the reasons for the improved cooperation are:



- 1) Most users are willing to help researchers in a scientific study and afraid to disappoint them.
- 2) Users that continued the experiment from the first year knew that the bonus points were indeed granted; this gave them a larger incentive to cooperate and detect the attacks. Also, since we emphasized that the bonus points depend on the detection rates, users felt some sense of risk (afraid to lose bonus points).

FAIR

### III. DIVISION TO GROUPS - FAIRNESS AND BIAS ISSUES

On our study, the users were provided different defense mechanisms, and some mechanisms turned out to be much better than others (there was also a control group which did not have any defense mechanism). We promised to reward the users (with bonus points) based on their detection rates. Is this fair? Is it ethical?



Users were more cooperative in the second year than in the first - only 10% did not cooperate, and 52% of them were users who participated both years and did not cooperate in the first year. We believe the reasons for the improved cooperation are:

- 1) Most users are willing to help researchers in a scientific study and afraid to disappoint them.
- 2) Users that continued the experiment from the first year knew that the bonus points were indeed granted, this gave them a larger incentive to cooperate and detect the attacks. Also, since we emphasized that the bonus points depend on the detection rates, users felt some sense of risk (afraid to lose bonus points).

### III. DIVISION TO GROUPS - FAIRNESS AND BIAS ISSUES

On our study, the users were provided different defense mechanisms, and some mechanisms turned out to be much better than others (there was also a control group which did not have any defense mechanisms). We promised to reward the users (with bonus points) based on their detection rates. Is this fair? Is it ethical?

In order to test several defense mechanisms and their combinations, the division of users into groups of different defense mechanisms is a must. The 'unfairness' of the reward being dependent on performance is not really harming the subjects, since their 'assignment' of participation are anyway negligible. This can also be compared to a medical study in which some of the participants receive a weaker medicine as a placebo, and do not gain the full benefits of participating in the study. When there are unequal groups in a study, which are not based on participants' characteristics, the most equitable division to groups is a random one. We believe this coincides with the justice guidelines in [7].

Another issue we had to deal with was the use of rep-

and feasibility in real-life, the difficulties to implement it on a user study, and of course ethical issues. Luckily for us, it was rather easy and not unethical to implement a classic phishing attack (sending a spoofed email with a link to a spoofed login page), and also to spoof the system's homepage.

Other scenarios are more problematic without user consent, and some are even illegal. On our experiment we had two such scenarios, and despite the problems they arose, we still wanted to simulate them. The first was to coax the combination of our defense mechanisms along with standard browsers' invalid certificate error pages. In a real-life attack scenario, users will encounter an invalid certificate error page mostly on a phishing attack, where the browser tries to establish an SSL connection with what it believes to be the correct website, but is actually a spoofed website. This usually happens due to a spoofed DNS response that came from a poisoned DNS server. Since the spoofed website does not present a valid SSL certificate to the correct site's URL, modern browsers display an error page and prevent users from accessing the (potentially spoofed) site unless they approve or add an exception. Conducting an actual phishing attack involves spoofing a DNS entry in some DNS servers. On a controlled and limited environment (for example, our University's DNS servers) such an attack might not be considered illegal, but even then, this kind of spoofing affects many users and exceeds the scope of the study.

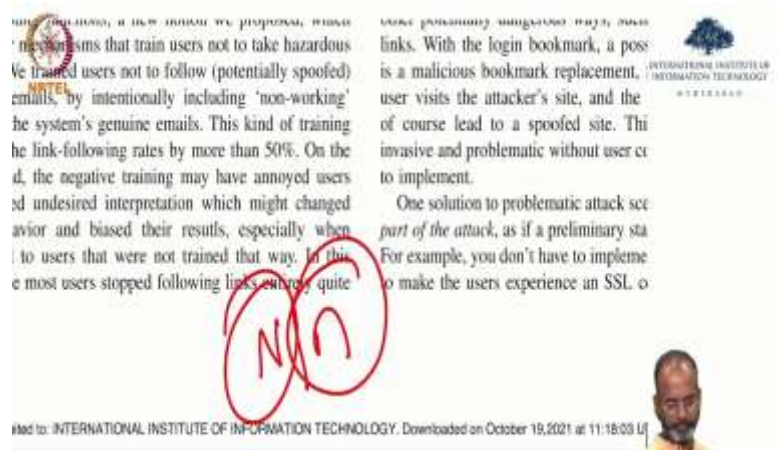
The second problematic scenario relates to one of the defense mechanisms we used - a login bookmark. Users that were assigned the login bookmark, could only reach the site's login page via their personal bookmark. This assures that the users will reach the correct URL, on every normal login, and could also train them to always login via their bookmark and avoid reaching the login page in



Fairness, I think fairness is becoming more and more important. I think there is also fair principles that people are writing about in research papers, go take a look at it or later at some point in time we can talk about it. Fair principles, how the data should be made public? What is the necessity of making the data public? All of that.

But this fairness is about fairness and bias in terms of selection of the participants, which are already mentioned about gender distribution, the probably educational distribution that you want to keep all that you have to keep in mind while selecting the participants for the study. Because otherwise the results are also going to be biased. You want to study how people and you also want to keep in mind that the distribution that you are selecting having in the study also is very closer to the distribution that is otherwise in the population.

(Refer Slide Time: 39:42)



The slide contains text on the left and right sides. On the left, there is a paragraph about training users not to follow hazardous links, mentioning a 'Report Phishing Page' button. On the right, there is a paragraph about malicious bookmark replacements. A large red 'N' is drawn over the text. At the bottom right, there is a small image of a man in a yellow shirt. The slide footer includes the text 'ntel to: INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY. Downloaded on October 19, 2021 at 11:18:03 L'.

If you have taken statistics class it could be said as N and n population and sample have the sample as close to the distribution of the population.

(Refer Slide Time: 39:55)



The slide contains text on the left and right sides. On the left, there is a paragraph about a challenge in conducting usability security studies. On the right, there is a list of references. A large red 'N' is drawn over the text. At the bottom right, there is a small image of a man in a yellow shirt. The slide footer includes the text 'ntel to: INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY. Downloaded on October 19, 2021 at 11:18:03 L'.

Sometimes it is hard. But try as much as possible that you can get it.

(Refer Slide Time: 40:01)



As, as responsibility researchers have a responsibility to know how to conduct research ethically. That is what I was trying to get across, in these deck of slides. To show you that, what is the importance of data collection, how you can actually keep in mind all this ethics part while collecting data that we will stop the week 5 content.

Again, to summarise week 5, we had first part we studied cookies, and what is the effect of cookies? Why cookies are important? What are the negative effects of cookies that are happening today? How can you actually analyse these cookies? And then the second part was about ethic ethics in terms of conducting studies. Why do we need institutional review board?

What are the nuts and bolts of doing the study and some examples of studies which is which is gone wrong and I am going to expect you to post about the studies that we have seen in the class where IRB may have been required. Thanks again for listening to the week 5 class.