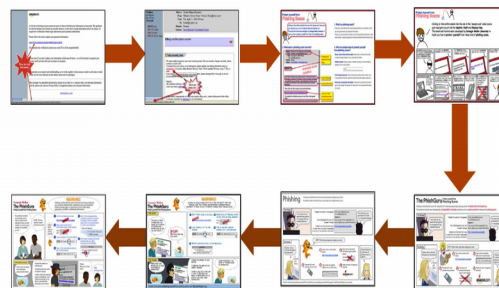


Introduction to Human Computer Interaction
Prof. Ponnurangam Kumaraguru (“PK”)
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture – 20
Continuity of Usable security

(Refer Slide Time: 00:16)

Iterations



Welcome back to the course. This is a course on Introduction to Human Computer Interaction. We are continuing on the topic on usable security. I hope you were able to actually understand the slides with respect to different types of solutions, unusable security and also thought about some aspects of usable security problems in the last one week. I am going to continue the lecture where I left last time. This is the slide, this is the last slide we had in the last week’s lecture which is different iterations that we did while building the phish guru solution. The one on the left top is the first iteration and then it continues till the right the top corner and then the iteration continues until the left bottom corner.

I will walk you to each one of the designs that we made and I will actually talk about what are the different design decisions that we made. So, I think one of the big things that you will end up making while building solutions is actually make these kind of design decisions. And these design decisions actually are the important decisions that you make while designing any systems.

(Refer Slide Time: 01:27)

First intervention

The screenshot shows an email from amazon.com. The email text includes a link to update personal information: <http://www.amazon.com/ccc/cc/obids/sign-in.html>. A red starburst annotation with the text "They are not the same" points to this link and the actual browser address bar URL at the bottom: <http://www.amazonaccount.net/ccc/cc/obids/flow/sign-in.htm?ID=2467720-522613>. The email content includes: "At the last reviewing at your amazon account we discovered that your information is inaccurate. We apologize for this but because most frauds are possible because we don't have enough information about our clients, we require this verification. Please login and reenter your personal information.", "Please follow this link to update your personal information:", "Please note: If you don't update your information within next 48 hours , we will be forced to suspend your account until you have the time to contact us by phone.", and "Thank you for your attention on this serious matter and we apologize."

Download this as a file

NPTEL

The first intervention that; you build. So this is just a very simple version where it just shows that, the link in the email. So, there is a annotation saying that the link in the email is not the same as the link that it is actually taking you to which is the link in the email says Amazon dot com whereas, if you look at the URL at the bottom of the browser, you will see that Amazon account dot net slash e, x, e, c, which is not where which is not the domain that it is showing you in the email. That's the first iteration.

(Refer Slide Time: 01:58)

Intervention: eBay

The screenshot shows an email from eBay. The email header includes: "Subject: Up-date Billing Information", "From: 'Member Service Team' <Service.Team@ebay.com>", "Date: Tue, April 11, 2006 4:09 pm", "To: bznath@cognax.com", "Priority: Normal", and "Options: View Full Header | View Printable Version". The email content includes: "Billing confirmation center", "eBay Security Center", "We were unable to process your most recent payment. Did you recently change your bank, phone number or credit card?", "To ensure that your service is not interrupted, please update your billing information today by clicking here.", "If you have the original link still open in a new window, please disregard this message as we are processing the change you have made.", "Regards, eBay Member Services Team", "Learn more about selling", and "This is not ebay.com". A red starburst annotation points to the "clicking here" link and the actual browser address bar URL at the bottom: <http://www.koz.com/ebay/mc26@ebay.com>. The email content also includes: "If this email is inappropriate or in any way violates eBay policy, please help protect other eBay community members by reporting it to us immediately."

NPTEL

Here is the second one which is very similar to the first one because the first one has the URL itself. In the second one, the URL in the email is not a domain name and everything it is just clicking here. Again the URL that it is taking you to is very different from what the email is supposed to be saying did the email is actually from eBay and the URL is actually KUSI dot org which is very different. Here is another design.

(Refer Slide Time: 02:25)

Protect yourself from Phishing Scams

Clicking on links within emails like the one in the "amazon.com" email you've just read puts you at risk for identity theft and financial loss. This email and tutorial were developed by Carnegie Mellon University to teach you how to protect yourself from these kind of phishing scams.

1. What's a phishing scam?

- Scammers send fake emails impersonating well-known companies to trick you into giving them your personal information.
- Giving up your personal information such as Social Security Number, credit card number, or account password will lead to identity theft and financial loss.

2. What does a phishing scam look like?

Subject: Revision to Your Amazon.com Information
From: "Amazon" <service@amazon.com>
Date: Tue, April 11, 2006 4:04 pm
To: bamsb@cogsis.com
Priority: Normal
Options: View Full Header | View Printable Version

amazon.com PHISHING SCAM EXAMPLE

At the last reviewing at your amazon account we discovered that your information is inaccurate. We apologize for this but because most friends are unable because we don't have enough information about our clients we require this verification. Please login and restore your personal information.

Please follow this link to update your personal information:
<http://www.amazon.com/cc0bMv0jgn-3n-hm>

(To complete the verification process you must fill in all the required fields)
<http://www.amazon.com/cc0bMv0jgn-3n-hm?720-3229111>

3. What are simple ways to protect yourself from phishing scams?

- Never click on links within emails:** Never click on links within emails or reply to emails asking for your personal information.
- Initiate contact:** Always access a website by typing in the real website address into the web browser.
- Call customer service:** Never trust phone numbers within emails. Look it up yourself and call the customer service when email seems suspicious.
- Never give out personal information:** Never give out personal information upon email request. Companies will rarely ask for your personal information via emails.

Annotations:

- Professional & legitimate looking design
- Urgent messages
- Account status threat
- Links don't match with status bar when mouse is moved over

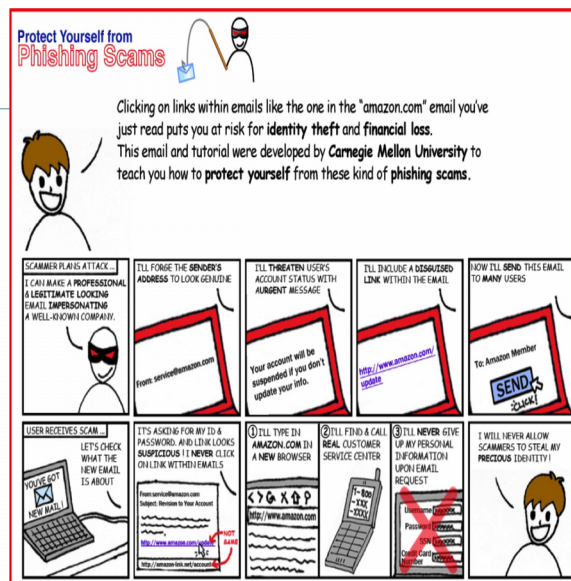
NPTEL

This design is probably the first design where we kind of thought about presenting the e-mail itself to the user showing that these are the annotations in the email which you should be looking for. Some parts of the e-mail that you have already known for example, left and top corner; you already know what is presented there which is some information about the system itself and there are these characters that we have put there which shows which presents these information. A relation to your Amazon dot com information and from Amazon, service at Amazon dot com is highlighted. It says professional and legitimate looking design and next it says urgent message in the text, account status thread; links do not match with status bar when mouse is moved over right.

So, that is the connection from the first 2 designs also which is linked is not matching. One of the main reasons why these phishing emails are so effective is that the only way by the only difference from the legitimate email for a phishing email is just the link that it is taking you to that that link. And some parts of information which is that I presents

with the urgent urgency you brought something, it present a presence about some status something is changing, account is changing, you have to actually verify your account on all of that and of course the link itself. This is on the left hand side. On the right hand side, if you see this presenting information about what is the phishing scam, what are the simple ways to protect yourself from phishing scams continuing with the designs, let us walk.

(Refer Slide Time: 04:03)

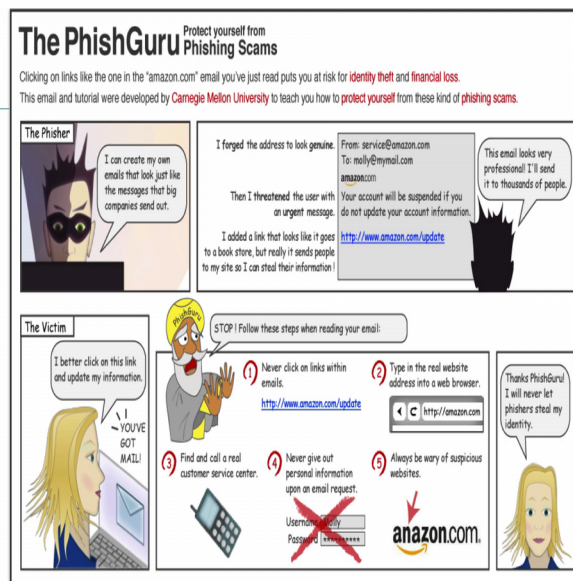


Let me walk you through other designs. Here is another one. So, in this case what we did was, we converted the information that is presented mostly like in the textual form, in this design that is flashed on the screen towards a design which is more cartoon as right; cartoons I mean I am sure many of you read cartoons. The information is presented in a very cartoon. For example, tintin type format right; all the information that is there in this slide, in this design is very similar to the one that is on the screen that I am the earlier design.

It is, but it just that is presented in a way that this cartoon is actually talking to you, scammers plan acts. I can make a professional and a legitimate looking website e-mail impersonating a well-known company. So, this is kind of the information that is there on the left hand top corner of the cartoon a strip and then it goes on to the right. I will force the senders address to look genuine and I will threaten, use this account status with the urgent with an with urgent message and everything right. So, these are kind of messages

that are, information that are presented even in the earlier design. And then at the bottom one you will see for example, user receives scam, let us check what a new email is all about it is asking for my ID and password and a link looks suspicious; I will never click on link with an e-mails. I will type in Amazon dot com in a new browser, I will find them call real customer service centre. I will never give out personal information upon e-mail request right. So, these are kind of the so to say instructions that we want the users to be.

(Refer Slide Time: 05:38)



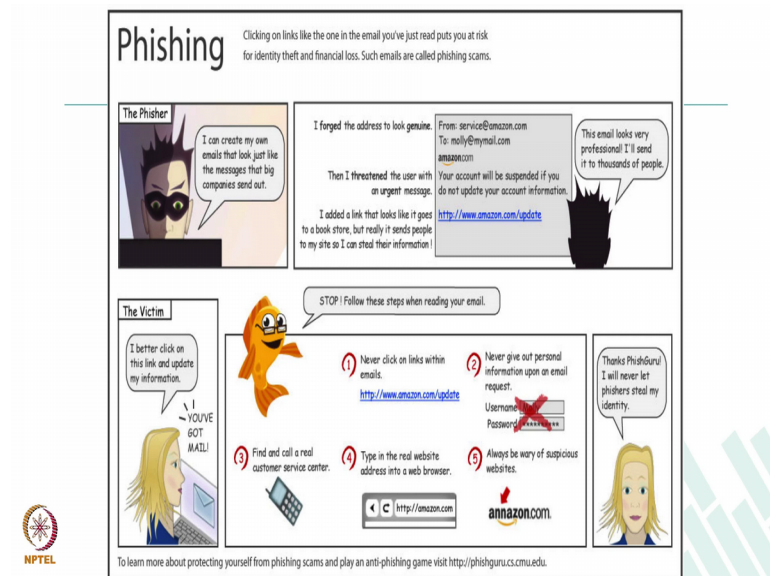
It is another design. This design became more the standard design that we started following after some point of evaluation which I will talk about as we move forward. So, there, there were multiple characters created; one is the phisher so to say which is on the left end top and then there is a victim and that there is also this PhishGuru character per say itself. So, the phisher character is represented on the top strap which is, I can create my own e-mails, I forge addresses, this e-mail looks very professional; I will send it to thousands of people and victim is getting the e-mail and PhishGuru saying stop.

Follow these steps when reading your e-mail, never click on links, find and call a real customer service all of that and at the end of the victim says thanks PhishGuru, I will never let phishers steal my identity. There is a lot of design principles that were used in creating these designs which I will walk through one by one as we move forward.

Ah look at this. So, one interesting experience about the character here is that, this character we created this character because probably to some extent buyers from our

side, buyers from my side in terms of creating a stereotypical character for let us take teacher, guru or a person who is actually well educated all of that. But unfortunately, I got a very from the user studies, I got a lot of inputs on not to have these kind of stereotypical characters. So, we end we up actually changing the character, changing the PhishGuru icon.

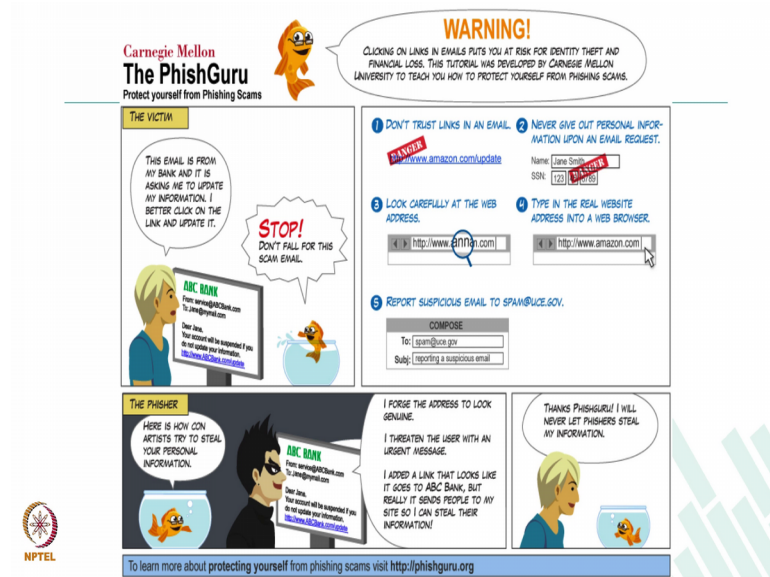
(Refer Slide Time: 07:13)



So, to say to something which is gender neutral, gender neutral helps because it is helping you to understand. There is no buyer's will people are actually reading these instructions materials from a gender neutral character; that is the reason why we went from a character which is biased towards the character which looks at least gender neutral.

So, the phisher, the victim, all information is just the same he just changed the character that. And even in this case, we were actually modifying the instructions to look very different.

(Refer Slide Time: 07:48)



For example, in this design, there is only phisher, victim and PhishGuru. Look at this design that is official character has changed a victim character change to some extent, information present it slightly differently where the instructions have come on the top right. From this design, what we did was, we also did some focus group discussions with different age groups to understand what they think about these designs. Interestingly we did focus group discussions with people of different age groups.

(Refer Slide Time: 08:13)

Focus group studies

- One with age group 18 – 55 and another with age group greater than 65
- All age groups will read the interventions
- Everybody liked the gold fish and the comic script format
- Participants did not like the phisher character



For example, one was between 18 and 55, the other one was actually more interesting which is 65 plus year old people were part of the Focus group discussion. All groups, all age groups will read the interventions. At least they said that they will do it everybody like the goldfish on the comic strip. Participants did not like the phisher character. So, these kind of characters, some participants were not very appreciative of the character per say itself.

(Refer Slide Time: 08:38)

Carnegie Mellon
The PhishGuru
Protect yourself from Phishing Scams

WARNING!
Clicking on links like the one in the email you've just read puts you at risk for identity theft. A phishing scam uses fraudulent email and web pages to steal bank account information, passwords, and other confidential information.

How you were tricked
This email is from my bank and it is asking me to update my information. I better click on the link and update it.
STOP!
Don't fall for this scam email.
From: service@Wombank.com
Dear Jane,
Your account will be suspended if you do not update your information.
<http://www.Wombank.com/update>

How to help protect yourself
1. Don't trust links in an email.
<http://www.wombank.com/update>
2. Never give out personal information upon email request.
Name: Jane Smith
SSN: (123) 456-789
3. Look carefully at the web address.
<http://www.wombank.com>
4. Type in the real website address into a web browser.
<http://www.amazon.com>
5. Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.
Credit Card Statement
For customer service call 1-800-xxx-xxxx
6. Don't open unexpected email attachments or instant message download links.
My Inbox
Here is the updated document.

How phishers trick you
Here is how con artists try to steal your personal information.
I forged the address to look genuine.
I threatened the user with an urgent message.
I added a link that looks like it goes to Wombank - but it really sends people to my site so I can steal their information and money!
Thanks PhishGuru! Where can I learn more?
Visit phishguru.org

NPTEL

So, keeping that feedback in mind, we updated the design and we what we had was we ended up having 2 different designs. So, one is the one that is on the slide now which is looking at the phisher, the victim, the PhishGuru characters. Instructions all of it has in the 4, only the phisher character slightly modified.

(Refer Slide Time: 08:57)

Carnegie Mellon
The PhishGuru
Protect yourself from Phishing Scams

WARNING!
Clicking on links like the one in the email you've just read puts you at risk for identity theft. A phishing scam uses fraudulent email and web pages to steal bank account information, passwords, and other confidential information.

Do you know any time an email asks you to take an urgent action and type in your account number or social security number, it is probably a scam?
Really? How do I protect myself from these scams?
Follow these steps to protect yourself

- 1 Don't trust links in an email.
<http://www.wombank.com/update>
- 2 Never give out personal information upon email request.
Name: Lane Smith
SSN: 123 456 789
- 3 Look carefully at the web address.
<http://www.phish.com>
- 4 Type in the real website address into a web browser.
<http://www.amazon.com>
- 5 Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.
Credit Card Statement
For customer service call 1-800-xxxx-xxxx
- 6 Don't open unexpected email attachments or instant message download links.
My inbox
Here is the updated document.
[Click Here](#)

How phishers trick you
Here is how con artists try to steal your personal information.
I forged the address to look genuine.
I threatened the user with an urgent message.
I added a link that looks like it goes to Wombank - but it really sends people to my site so I can steal their information and money!

Wombank
customer.service@wombank.com
Dear Jane,
Your account will be suspended if you do not update your information.
<http://www.Wombank.com/update>

Thanks. Where can I learn more?
Visit phishguru.org

NPTEL

Look at the other one. This one is a more a conversation type between 2 people um. So, left end top if you see, do you know any do you know any time an email asks you to take an urgent action and type in your account number or social security number, it is probably a scam. Really, how do I protect myself from these scams? So, it is like a conversation between 2 people and the same instructions are presented and a phisher was also, a gender was changed for the phisher and the conversation ends by saying the thanks where can I learn more. And the character saying that go to this URL.

So, those are the final 2 decisions that we ended up actually using in a large, large number of studies which I shall go through one by one.

(Refer Slide Time: 09:40)

First lab study results

- Security notices are an ineffective medium for training users
- Users educated with embedded training make better decisions than those sent security notices



Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., and Nunge, E. Protecting people from phishing: the design and evaluation of an embedded training email system. CHI '07, pp. 905-914.

So, as we have seen in the content before in the in the last few weeks that, one of the important aspect of this course is evaluation right. You have to design, you have to understand what to design, iterate it and then go ahead and evaluate it. I think scientifically evaluating what you created is actually one of the strengths of the HCI. So, to say topic and if you become if you become a user experience engineer, if you become a user experience product manager, your goal will be actually to evaluate scientifically and evaluate very comprehensively the product that you have built. So, let me walk you through thermal evaluations.

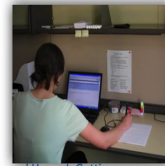
So, first the simplest ones which is a lab study that we did to show that the security notices that we get an e-mail or which is presented on a website saying protect yourself from fake e-mail. So, read this privacy policy to understand what changes have happened and Facebook, nobody reads any of them right.

So, that is the first conclusion that we wanted to actually draw. Security notices are an ineffective medium for training users. User educated with the embedded training make better decisions and those sent a security notices. That is a simple comparison that we did which is to compare users who got the security notices an email and who got these PhishGuru e-mails in that e-mail and then we found that people who got this straining through PhishGuru was able to make decisions on the fake phish, on the phishing emails better than the ones that got in security notices.

(Refer Slide Time: 11:14)

Second lab study results

- Users educated with PhishGuru retained knowledge after seven days
- Users trained with embedded did better than users trained with non-embedded



Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., and Hong, J. Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. e-Crime Researchers Summit, Anti-Phishing Working Group (2007).



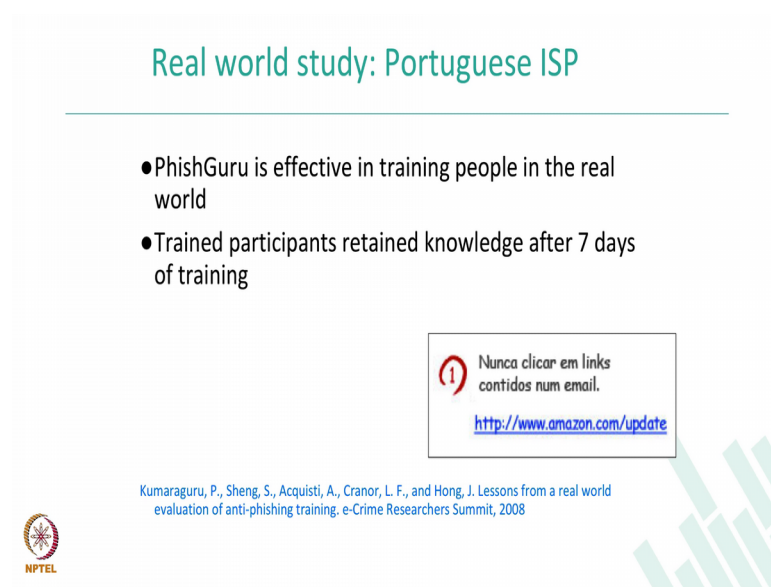
Here is another one another study that we get. So, this is a picture of a user who is actually sitting in the lab, doing the study where this person is act as a executive assistant for somebody and they are actually going through the e-mails of that they have received. And make doing actions as mentioned the e-mail for example, one e-mail was mentioning that please, get an appointment for me to meet with somebody and please send click on this link to get. We are arranging a conference, please click on this link to let us know how many people from your organizations are attending.

These kind of e-mails which look slightly legitimate also and we got participants to react to these emails and when as and when they react we would capture how they reacted and use it for our analysis of how they reacted with the phishing e-mail. So, anyway, many of the emails that we kept were just buffer e-mails to see how users react to general e-mails, but our focus was on only on studying the phishing e-mails that we sent. Users educated with PhishGuru retained knowledge after 7 years, 7 days retain knowledge is that knowledge retention is nothing but if I teach you ; for example, now I am teaching you HCI that I am I taught you about a way of evaluating a solution and you for example, focus group discussion; you will understand what a focus group discussion is in this context let us take after few days that is called knowledge retention.

And knowledge transfer which also be evaluated is that knowledge transfer is given that you learnt it in one context, can you apply into to a different context and use that


knowledge that you gained, that is called knowledge transfer. So, these 2 are interesting methods to evaluate in knowledge science or learning science domain. Useless train with embedded did better than users train with non-embedded which I think we proved even in the study one.

(Refer Slide Time: 13:11)




Real world study: Portuguese ISP

- PhishGuru is effective in training people in the real world
- Trained participants retained knowledge after 7 days of training



Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., and Hong, J. Lessons from a real world evaluation of anti-phishing training. e-Crime Researchers Summit, 2008



The next study that we did was interesting is because they it was a study that was done in the real world for the first time, where we partnered with the Portuguese ISP and the ISP actually was ready to do these kind of PhishGuru e-mails to their employees and we want to study how the employees behave with these kind of e-mails.

So, this was the introduction to taking the study which was done mostly in the lab to actually a real world experiment and nothing was controlled. Even that it is a real world, we can control really anything except for the all employees being from this company nothing was controlled. PhishGuru is effective in training people in real world training participants retain knowledge after 7 days of training. So, those are the 2 important conclusions all of these research are published as papers. I put the citations at the bottom of the slide. So, if you are interested, feel free to take it.



The instruction here which says in Portuguese about please be aware of links in e-mails. We translated all the designs that we developed into Portuguese and sent that designs to the company for them to host it and get the phishing e mails when they when clicked the users were redirected to this particular training material.

(Refer Slide Time: 14:34)

Real world study: CMU

- Evaluate effectiveness of PhishGuru training in the real world
- Investigate retention after 1 week, 2 weeks, and 4 weeks
- Compare effectiveness of 2 training messages with effectiveness of 1 training message

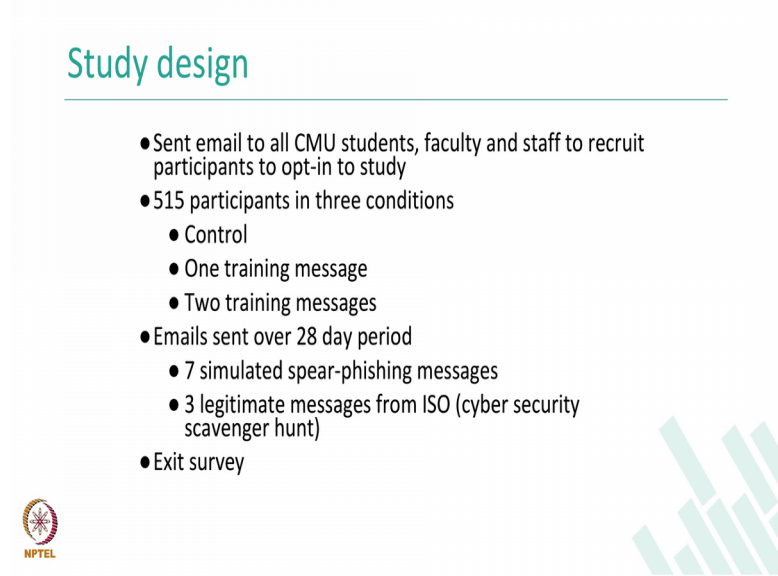
P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair, and T. Pham. School of Phish: A Real-World Evaluation of Anti-Phishing Training. 2009. *Under review.*



So, continuing on the topic, now I will walk you through another study that we did where we tried studying the PhishGuru and the embedded training system in the campus Carnegie Mellon University. So, here what the goal for this study was to find out how effective this training methodology is in real world and for a long period of time. In the study done in a Portuguese it was done for a week whereas in study done in CMU, it is actually going to be for 4 weeks to study how effective this training material is and the goals are evaluate effectiveness of PhishGuru training in the real world investigate retention after 1 week, 2 weeks compare effectiveness of 2 training messages with effectiveness of 1 training.



Basically, the goal is to find out, if I send, if I get you to see only one training message how effective you are in terms of identifying phishing e-mails versus if I get you to see 2 training messages that is the goal.

(Refer Slide Time: 15:30)



Study design

- Sent email to all CMU students, faculty and staff to recruit participants to opt-in to study
- 515 participants in three conditions
 - Control
 - One training message
 - Two training messages
- Emails sent over 28 day period
 - 7 simulated spear-phishing messages
 - 3 legitimate messages from ISO (cyber security scavenger hunt)
- Exit survey



So, let me walk you through what the study design is and given that it is an NCI course, let us spend more time on actually at studying the study design, decisions that were made and how the e-mails were sent out and what kind of data was collected.

So, emails was sent out to CMU students, faculty and staff whoever said that they would like to participate in the study e-mails were sent out. 3 conditions were kept going back to the discussion that we had before about ah; within study and between study design. Control condition, one training message and 2 training messages and e-mails were sent out for 28 a period of 28 days and at the end exit survey was filled by the participants on the day of 35 and definitely to study the false positive effect of false positive messages.

We wanted to actually send out legitimate e mails that is if I send out legitimate e-mail, before you are getting trained on phishing which says the do not click on links. If the legitimate email has a link, the way you would behave should not change after I have trained you about not to click on links. These are called false positive errors. So, false positive should not change when I do the intervention for training you on embedded training.

(Refer Slide Time: 16:43)

The slide features a light blue background. At the top, the title "What study design?" is written in a teal font. Below the title is a thin teal horizontal line. Underneath the line, a single bullet point reads "• For 2 different solutions – PhishGuru & PhishX". In the bottom left corner, there is a small circular logo with a star and the text "NPTEL" below it. In the bottom right corner, there is a decorative graphic of several teal bars of varying heights, resembling a bar chart, with the number "40" centered below it.

So, if you really look at what study designed to be done, again I am connecting to the point of between study design and within study design that we saw which is in one method where you have 2 sets of people looking at 2 designs a and b that you have built whereas, in the other study design you will have a large set of people looking at both the designs. And there are pros and cons that we saw we in all of these designs.

So, I let you to think about what design would you have if there was a design called PhishGuru and let us consider PhishX as another solution. If you were to evaluate these 2 designs, what kind of study design would you have and please post it on the mailing list, we can see what are the different methods that people think about evaluating these 2 designs.

(Refer Slide Time: 17:31)

Comparing Two Alternatives

- Between groups experiment
 - two groups of test users
 - each group uses only 1 of the systems
- Within groups experiment
 - one group of test users
 - each person uses both systems, randomized ordering
 - can't use the same tasks or order (learning)
- Between groups requires many more participants than within groups



Now, let us look at the all I am assuming that you would have thought about how study, what is the different ways to evaluate these 2 systems, but let us let me give you the answer for how you can actually evaluate them. The 2 alternatives that you can think of: one is between group design, the other one is within group design. Between group design is the design where you have 2 groups of test users. Each group uses only one of the systems like for example, let us say you want to test apple I phone versus the android phone.

You get 10 participants use apple I phone 10 participants use the android phone that is all whereas, in the within group, 20 participants actually get to use the I phone and android, they get to use both the systems, but some users would get to use the I phone first and some users would get to use the android phone first and clearly you can see that between subject design requires more participants then within because you have number of, because you have only one set of people using one of the systems at this build.

So, now I will let you to actually think about what are the pros and cons of these design methodology itself right because in the within group you are going to have the problem of, if I get to see apple first versus, if I get to see android first, the learning effect is also there. What I see first will actually influence what I see next and there are many other design constraints also actually having in both of them which is between and the within design.

(Refer Slide Time: 18:58)

Implementation

- Unique hash in the URL for each participant
- Demographic and department/status data linked to each hash
- Form does not POST login details
- Campus help desks and all spoofed departments were notified before messages were sent



So, in terms now let us go back to the study design. Unique hash in the URL for each participant has to be kept because the problem is, if I have a user who gets my phishing e-mail, I want to actually track the user until they have clicked on the link they have given the information so that I can keep track of who this participant is. Interestingly, we also got the demographics and department status data for each of the participants. So, we could actually keep this hash and track the user, which user is following which user is giving away the information, which user is not even clicking on the link.

We also did one thing which was very much necessary that we spoke to the help desk of the campus to tell them that if anybody forwards this e-mail to you, you should actually respond it in this scammed manner because what would happen is let us take, if somebody sends out forwards the phishing e-mail that we sent to the participants, forwards of the IT help desk, an IT help desk forwards to everybody in the camp saying here is a phishing e-mail, then I think that the whole study would the study design and the whole purpose of the control thing that we were trying to do in terms of the e-mails getting out to all the participants would be lost the purpose of the study would be lost.

So, we were trying to control that by letting the ITL desk also be part of the study itself and let them give them a canned message with they would send out to somebody e-mails them this is a phishing e-mail.

(Refer Slide Time: 20:23)

Study schedule

Day of the study	Control	One training message	Two training messages
Day 0	Test and real	Train and real	Train and real
Day 2	Test		
Day 7	Test and real		
Day 14	Test	Test	Train
Day 16	Test		
Day 21	Test		
Day 28	Test and real		
Day 35	Post-study survey		

Now, let me walk you through the study schedule. So, this slide is slightly dense. Let me slowly dissipate the content in this slide and hopefully you will be able to understand how complicated the study was. So, let us go over the first column. First column is the day of the study in 0, 2, 4, 7, 14, 16, 21 and 28. These are the days in which when the e-mails were sent out. 3 conditions in the study, control and now I am looking at the row. Control one training and two training message, control one training and two training message.

And now on day 0, there was a test e-mail and a real e-mail that was sent. The reason why you want to send out test and real and any of these kind of testing should happen on control condition is that you want to know what the baseline is of the of the participants without any interventions. If you look at the column for the control, there is no intervention which is more.

So, like a training message in this case it is all test, test and real test, test and real test, test, test and test and real ; that is for the control group. So, that would just show you what the baseline is. One training message train and real on day 0, test, test and real test, test, test and test and real, the reason why you want to have real on day 0 with all the 3 conditions is that with the real you will be able to understand how they react to a legitimate message that is sent before the training has happened, before any intervention has happened. So, in that case, you will be able to understand baseline for not just in the

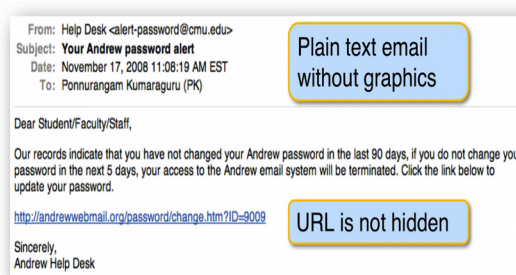
control group, baseline for one training message and 2 training message also. So, this would just tell you how participants in the one train message and the 2 train message reacted to the email which was a real e-mail before they were exposed to training. So, if the training works well, the responses that, we should have on the real in day 0 and the real in day 28 for one training should not be very different. That is the intention or that is the so to say expectations of the training influence. It should not influence the users just to become too scared about the training messages.

Do not click on links therefore, I will stop a click on any links that I get in the e-mail; we want to avoid that. A training methodology should avoid that 2 training message. Last column, train and real on day 0 and then test, test and real and then on day 14, there is a train again which is participants in this group will get an e-mail when they click on the link. They will be taking to the training material that I showed you then there is test, test, test and real and then post survey on day 25 for all the 3 conditions.

So, what is this help this train, this methodology. So, the way the reason why I am going through this study design slightly more in detail also is that, any study that you do you should be able to represent it in this way where you can walk through the study design in detail giving the details about how, what data you collected and how you collected the data. So, I hope that helps if any questions, please drop it on the mailing list.

(Refer Slide Time: 23:33)

Simulated spear phishing message

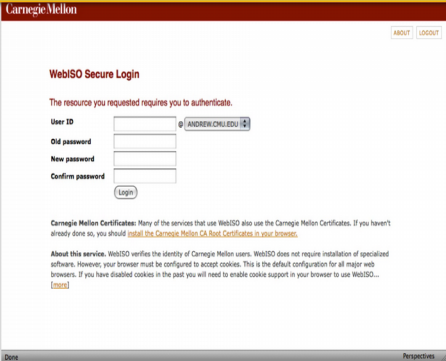



So, Simulated spear phishing messages, so here if you look at the message, it is clearly as plain text. There is no images nothing and there is also a URL which is not hidden in this case Andrew web mail dot org is not the real URL for going and checking the e-mails in the campus and they if you look at it there is also this ID equal to 0 zero 9009 which is the user for us to track.

(Refer Slide Time: 24:01)

Simulated phishing website

<http://andrewwebmail.org/password/change.htm?ID=9009>

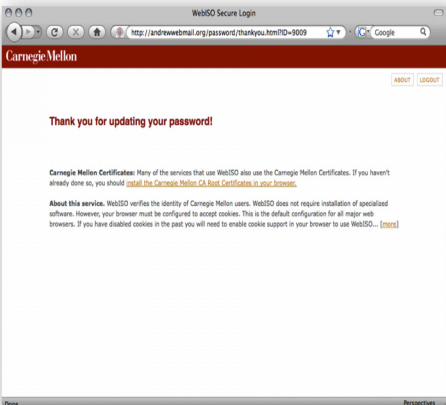





And when they click to the link, they will go to this page which looks very very similar to the web ISO secured login page of the campus and but the URL is very different.

(Refer Slide Time: 24:15)

Simulated phishing website

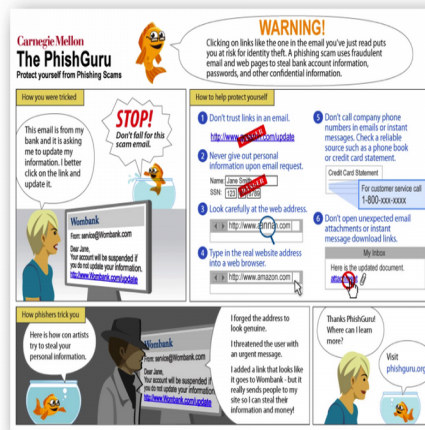




And when they give the username and password, they will get this message called thank you for updating your password and the URL will be different. And for the interventions, we sent out the intervention which is which is one of the things that I showed earlier.

(Refer Slide Time: 24:21)

PhishGuru intervention



So, now let us look at the outcomes, again some of these slides are slightly dense ah.

(Refer Slide Time: 24:30)

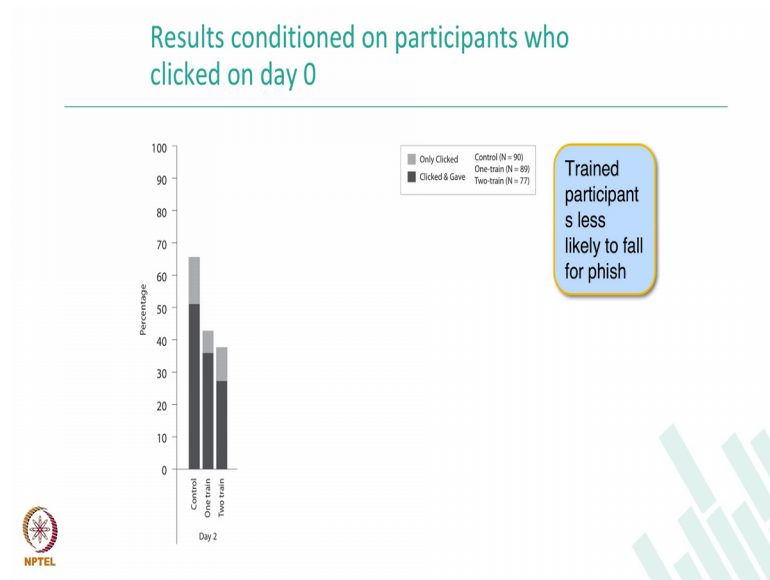
Effect of PhishGuru

Condition	N	% who clicked on Day 0	% who clicked on Day 28
Control	172	52.3	44.2
Trained	343	48.4	24.5

Because I think it is going to show you the results of the analysis that was done with the data that we have received. So, in this case, the first column is Condition, Control and Trained. Trained is the summation of the both one training and two training, N is the

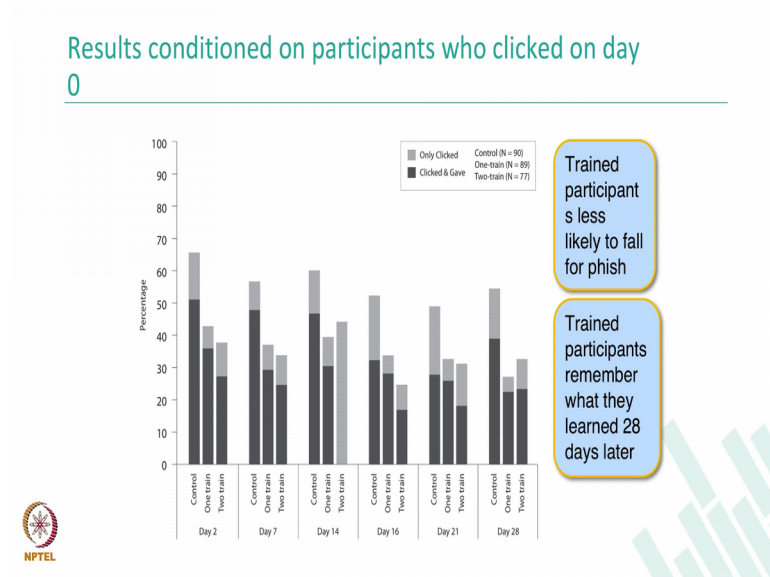
number of participants in that condition, percentage who clicked on day 0, just shows the percentage of people who clicked on the link that was sent on day 0, percentage who clicked on day 28. So, if you look at the percentage of control 52 and 44 and for the trained it is 48 and 24, so all the statistics and everything is already written in papers and published. We will not get into the gory details of the statistics between these numbers, but I will tell you the story because here if you see in control 52 and 44 there is no statistically significant difference whereas, in the trained 48 versus 24, there is statistical significant difference and therefore, you can argue that the training had some effect in people are not clicking on links on day 28.

(Refer Slide Time: 25:35)



So, now if you look at this slide, what it showing is results conditioned on participants who clicked on day 0 which means people who ever clicked on day 0 is what we are seeing which is these are the people who clicked on the link when they sent them on day 0 which is day 2, day 7, day 14, day 16, day 21 and day 28.

(Refer Slide Time: 25:54)

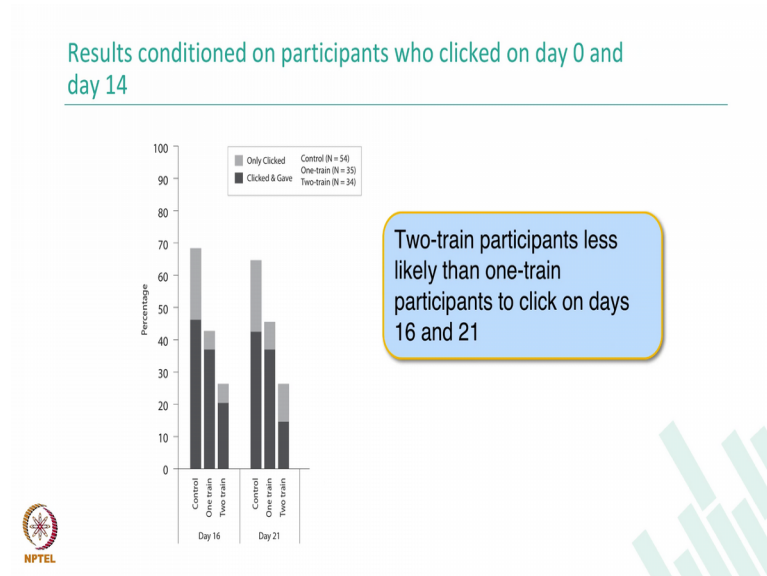


So, what does this show? This shows that trained participants are less likely to fall for phishing because if you look at the training conditions, which are one train or two train, all of them are lower than the control conditions. Look at this: on day 2, it is lower; on day 7, it is lower; on day 14, day 16, day 21, and day 28. All of them are lower compared to the control condition, whether you look at clicking and giving, or only clicking, or together the training condition participants and lesser.

Training participants remember what they learned 28 days later. So, how do you find this? This you can see that on day 28, you will see that the percentage of people who clicked and gave and clicked is actually lower than the training material. Training participants remembered what they learned 28 days later, which is the number is not falling down a lot or number which is basically clicking on is not increasing a lot.

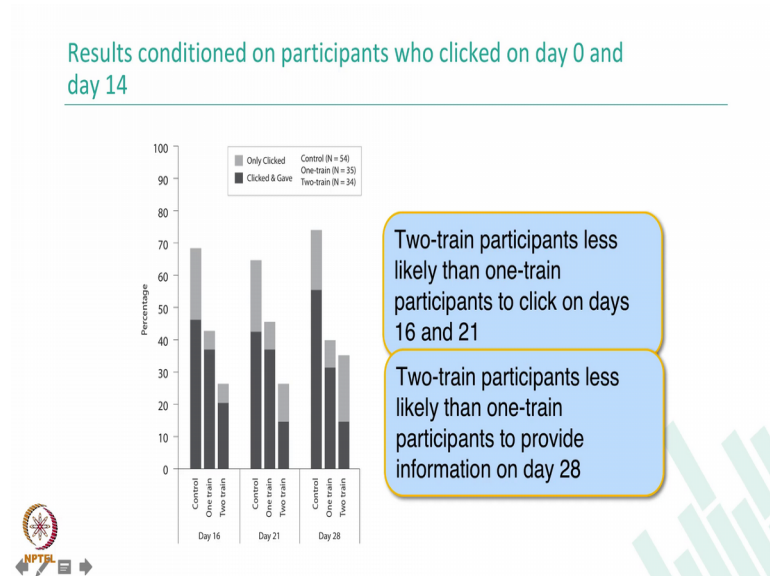
We trained them on day 2, one training material, one training and two training conditions. If you see the number there and if you basically look at the numbers that are highlighted, you will understand that the participants on day 28 clicked links which is statistically very similar to the people who are on day 2 who clicked on day 2. I hope that makes sense. So, continuing with the analysis that we saw, which is for conditioning on day 0, we find that trained participants are less likely to fall for phishing and trained participants remember what they learned 28 days afterwards.

(Refer Slide Time: 27:33).



Let us move on to some other analysis. Here is an analysis that will give you another set of insights into the data which shows that results conditioned on participants who clicked on day 0 and day 14, which is that they have seen the both the training materials. Now we are trying to see how these kind of participants behave by taking the data on day 16 and day 21, 2 train participants less likely than one train participants to click on day 16 and day 21. So, how you will infer this? You will infer this by looking at this 2 train bar which is less always less than the one trained bar in the day 16 and day 21 and you also see that 2 train participants less likely than one train participants to provide information on day 28.

(Refer Slide Time: 28:20)



Which is to click and gave is lower in day 28 compared to one time. I hope that makes sense right. So, what basically it is showing that, it is showing that the training that was done through embedded methodology like phish who do helps and people remembering the training and not being able to click on links, not being able to give on not give information even after some time when the training was done.

(Refer Slide Time: 28:49)

Legitimate emails

Condition	N	Day 0	Day 7	Day 28
		Clicked %	Clicked %	Clicked %
Control	90	50.0	41.1	38.9
One-train	89	39.3	42.7	32.3
Two-train	77	48.1	44.2	35.1

No difference between the three conditions on day 0, 7, and 28

No difference within the three conditions for the three emails

So, that is the key crux of the whole number of studies that was done. If you remember there is another important insight that we wanted to check, whether the training makes

users to be more scared and not click on legitimate emails. So, that is the table that is provided on the screen now which is these are the legitimate e-mails. If you remember it was sent on day one to real.

Everything that was real in the table is actually the legitimate e-mails. So, keeping that in mind, so let me go back and show you where the reals are. So, if you look at here, the reals are in day 0, day 0 and day 0 for all the 3 conditions and then there is a real on day 7 to all the 3 conditions correct. These are the e mails that we have analyzed on this table to show that the training the. So, if you look at this which is there is no difference in the control group right.

So, no difference between 3 conditions day 0 or day 7 and day 28 which is 50, 41 and 38 there is no difference, 39, 42 and 32, there is no difference. 48, 41 and 50s, 35 is no different. So, what does this mean. This means that whatever conditions you are, one train 2 train or control condition there is no difference between you clicking on the legitimate e-mail between the different conditions on different days.



So, that is looking at the columns, you can also look at the rows now. There is also another one that you can no difference within the 3 conditions for 3 conditions for the 3 e-mails right. So, what does this show. This shows that there is no difference between basically there is no difference between columns and rows right. So, that shows that the legitimate e-mails that were sent to people either before the training or after the training, the difference was very low. Therefore, that the training did not impact users on making wrong decisions on true legitimate emails. That just shows a false positive did not increase in short.

So, there are many other kinds of data that were collected for example, some qualitative responses were collected from participants saying.

(Refer Slide Time: 30:54)

Most participants liked training, wanted more

- 280 complete post study responses
- 80% recommended that CMU continue PhishGuru training
 - “I really liked the idea of sending CMU students fake phishing emails and then saying to them, essentially, HEY! You could've just gotten scammed! You should be more careful - here's how....”
 - “I think the idea of using something fun, like a cartoon, to teach people about a serious subject is awesome!”





How did they like the study, what did they get out of the study did they like, did they like them being stopped in between when they click on the link and everything. So, I am just showing you some qualitative results from the data that was collected on the post study. It just shows I really like the idea of sending CMU students fake phishing e-mails and then saying to them essentially, hey, you could you could have just got scammed; you should be more careful, here is all. I think the idea of using something fun like a cartoon to teach people about a serious subject is awesome. So, basically here is a summary of the 3 or 4 studies that they showed.

(Refer Slide Time: 31:34)

Summary from this study

- People trained with PhishGuru were less likely to click on phishing links than those not trained
- People retained their training for 28 days
- Two training messages are better than one
- PhishGuru training does not make people less likely to click on legitimate links



The summary is people trained, but PhishGuru were less likely to click on phishing e-mail links than those not trained. People retrained, retained their training for 28 days which is they remembered what they were training for 28 days. 2 training messages are better than one training message. If people saw 2 twice the training material they seem to be more aware make better decisions compared to one training message PhishGuru training does not make people less likely to click on legitimate emails, that is what I was saying right now, which is legitimate e-mails the reactions to legitimate e-mails did not change because of checking.

(Refer Slide Time: 32:08)

Summary of studies

Studies	Results
Lab study I	<ul style="list-style-type: none"> • Security notices are ineffective • Users educated with PhishGuru made better decisions
Lab study II	<ul style="list-style-type: none"> • Users in embedded condition retain and transfer knowledge more effectively than other conditions even after 7 days
Real-world study I	<ul style="list-style-type: none"> • PhishGuru is effective in training people in the real world • Trained participants retained knowledge after 7 days of training
Real-world study II	<ul style="list-style-type: none"> • People trained with PhishGuru were less likely to click on phishing links than those not trained • People retained their training for 28 days • Two training messages are better than one • PhishGuru training does not make people less likely to click on legitimate links



So, here is the summary of all the slides; that last slide just showed either so to say inferences. This is showing you what all study was done last study 1, last study 2 which is comparing security notices making the PhishGuru understand how PhishGuru is working and effectiveness of PhishGuru evaluation. And real world study 1 is the Portuguese study where the content was converted into Portuguese and evaluated. Real world study 2 showed that it is it is perfectly possible to train people when these kind of embedded training concepts are applied.

(Refer Slide Time: 32:42)

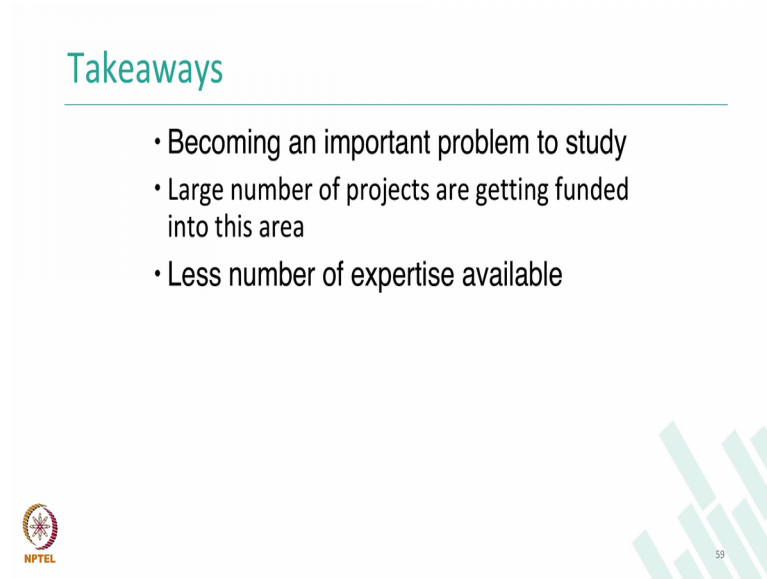


So, one last thing I wanted to say here before I have come, I wrap up this topic of usable security is that training games right. So, it is not only that these kinds of serious wave methods of training should be taken which is oh click on a link and then when they click on the link, it should be present training material should be presented on things like that. So, you could even make it a fun part which is. So, in this case, if in the screen if you see, e is for legitimate URLs, r is for reject phishing URLs, t is for ask father for help. So, basically we created a character called anti phishing film which is from that left top and there is a PhishGuru any ways on the right bottom.

So, same using learning science principle, teaching teachable moments teachable moments in terms of making the errors while playing the games and presenting it in front is essentially they have to look at this URL in the game and they have to press e, r or t and depending on how many how many they get they get actually score number of roms, life, lives totally that they have was 3 and totally 2 minutes were given to capture about 8 or 7 URLs. So, that is the way, that is another way of actually educating people about phishing and merging the usable security solutions.

And the interesting part about this game was when we built it became popular where people started playing it very regularly. So, you could actually go look up anti-phishing fill and there is a paper also that we have were we now analyzed the data that we got and we got and analyzed how people actually play at this game.

(Refer Slide Time: 34:18)



The slide features a title 'Takeaways' in teal text at the top left. Below it is a bulleted list with three items. In the bottom left corner is the NPTEL logo, and in the bottom right corner is a stylized bar chart graphic with the number '59' below it.

Takeaways

- Becoming an important problem to study
- Large number of projects are getting funded into this area
- Less number of expertise available

NPTEL

59

So, conclusion for this whole usable security area is becoming an important problem to study, I think day by day the more and more we start using our phones, the more and more we start using more technologies the whole decision making of usable security is going to be necessary because everywhere you are kind of setting, your privacy settings, doing default changing our default settings and everything. So, usable security is becoming more and more important and definitely a large projects are getting founded and if you are interested in continuing looking at this problem, I think there is potential ways of solving bigger problems in this area.

With that I will wrap up the continent on usable security and if there is any question, please feel free to drop a note on the mailing list and we will take it from there.