12 – Security Warnings

Lorrie Cranor

February 27, 2017

05-436 / 05-836 / 08-534 / 08-734 / 19-534 / 19-734
Usable Privacy and Security

Carnegie Mellon University
CyLab

institute for SOFTWARE RESEARCH

Engineering & Public Policy

Today's class

- Project feedback
- Evaluating security warnings
- NEAT and SPRUCE
- Design your own warning

Project feedback

- All teams should have received feedback
- From here on out, you should plan to check in with Lorrie, Javed, or Abby about once per week (via email or arrange a meeting) to go over study protocols, surveys, IRB submissions, etc.
- IRB protocols need to be submitted by March 6
- We suggest you start working on IRB protocol ASAP and go over it with us by Friday

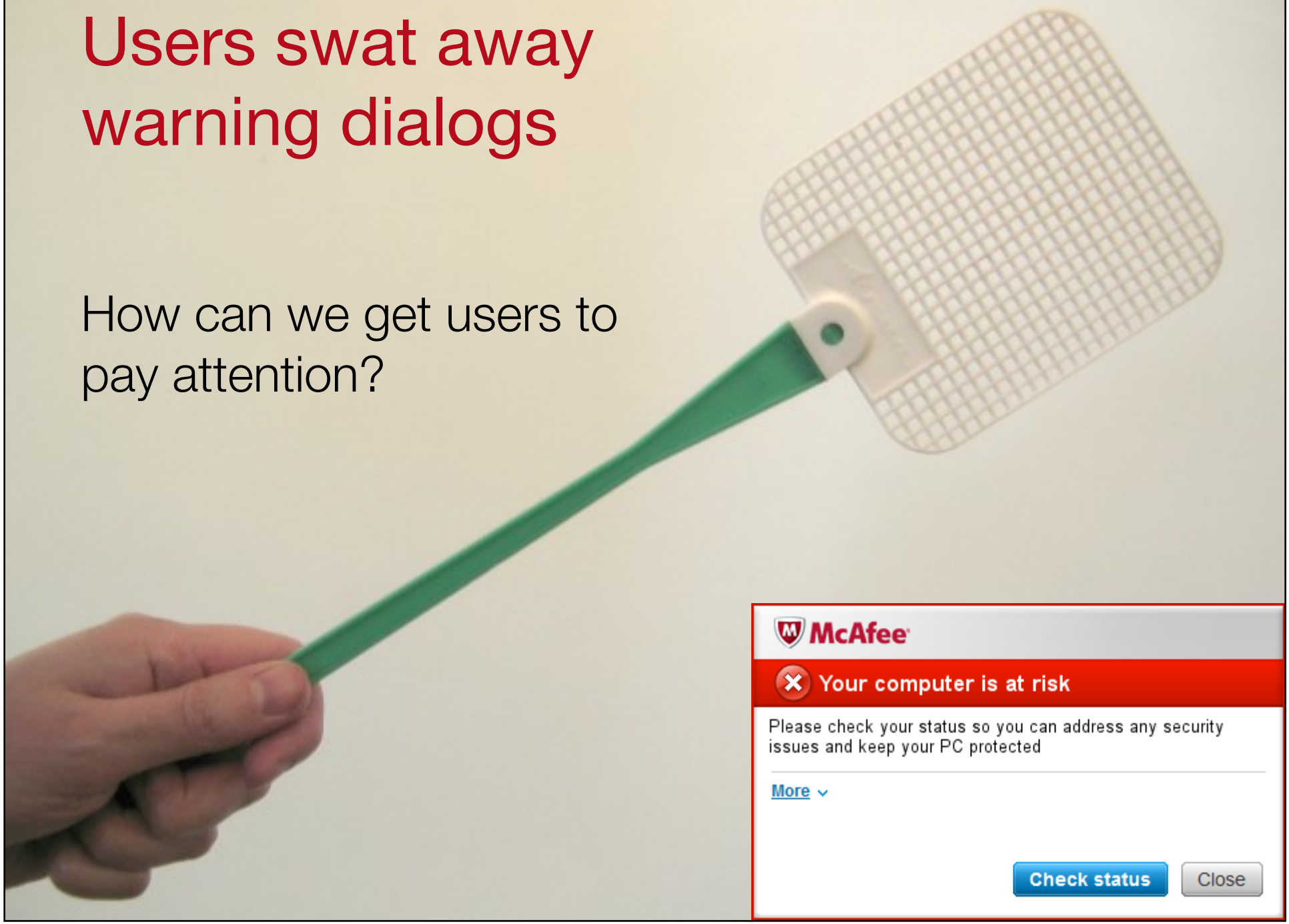
Evaluating security warnings


Security Error: Domain Name Mismatch
You have attempted to establish a connection with "www.whitehouse.gov". However, the security certificate presented belongs to "a248.e.akamai.net". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.
If you suspect the certificate shown does not belong to "www.whitehouse.gov", please cancel the connection and notify the site administrator.
View Certificate
Cancel
OK

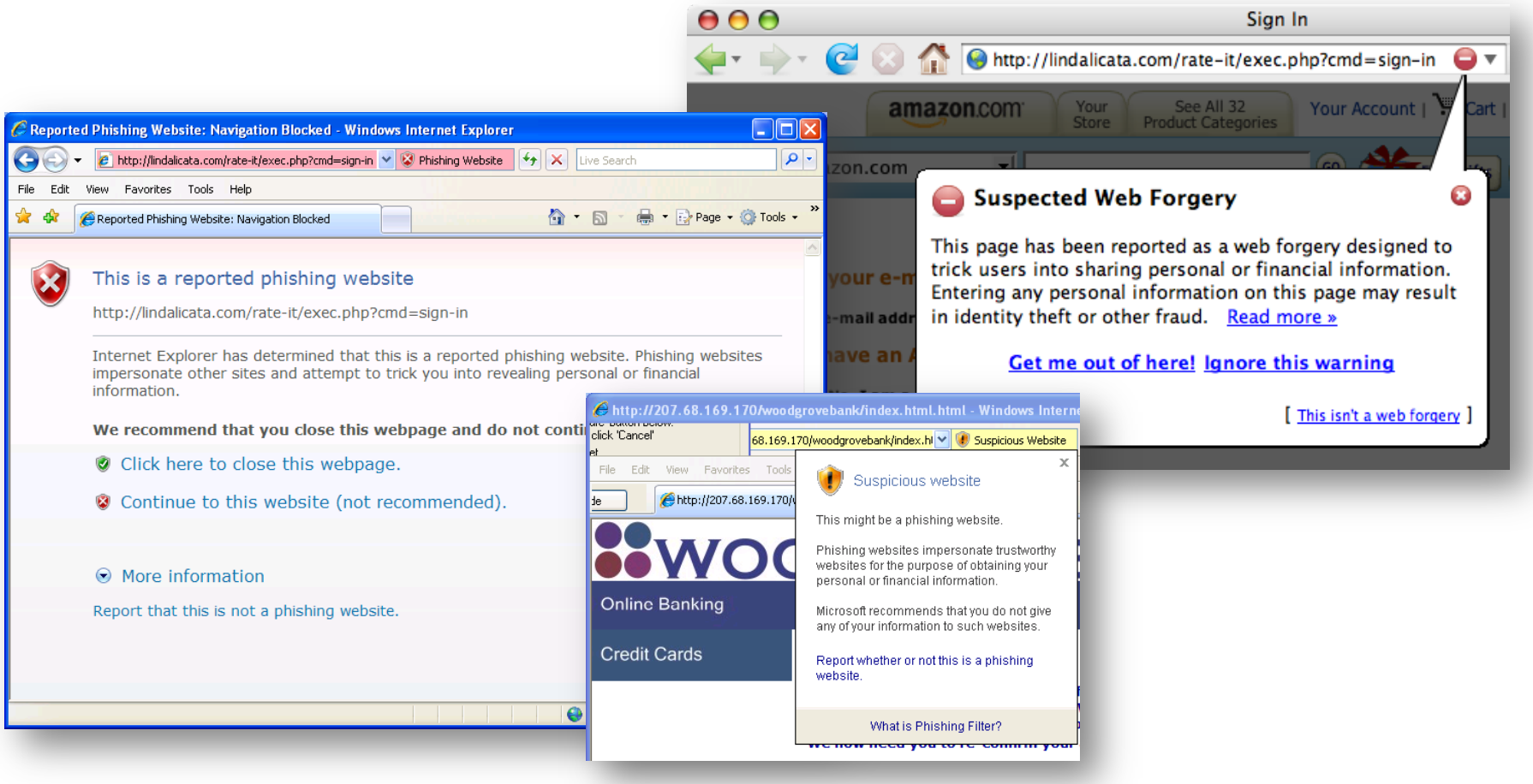
Image courtesy of Johnathan Nightingale

Users swat away warning dialogs

How can we get users to pay attention?



2007 Phishing warnings study



S. Egelman, L. Cranor, and J. Hong. **You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings**. CHI 2008.

Study design challenges

- Observe users interacting with warnings without them knowing we're interested in warnings
- Make users feel like they are under attack without actually putting them at risk

Required a little deception

- Lab study on online shopping
- Purchase paper clips from Amazon
- Answer questions about shopping (for another study)
- **That's when we phished them**
- Check email to get your receipt
- **That's when they fell for it**

Your Amazon.com order (#102-6801884-2225735): your approval required Inbox

"Amazon.com" <order-update@amazonaccounts.net> to me show details Jun 13 Reply

Hello from Amazon.com.

We wanted to let you know that there is a delay with item(s)

Please approve this delay so that we can continue processing your order. (Note that if we haven't received your approval by the end of business tomorrow, the item will be cancelled.

page in Your Account:

http://www.amazonaccounts.net/gp/signin/104-3310393-0927909.htm

http://www.amazonaccounts.net/gp/signin/104-3310393-0927909.htm

you can make changes to unshipped orders, cancel unshipped items, track shipped packages, modify your account settings, and do much more.

Please note: This e-mail was sent from a notification-only address that cannot accept incoming e-mail. Please do not reply to this message.

Thanks for shopping at Amazon.com, and we hope to see you again.

Sincerely,

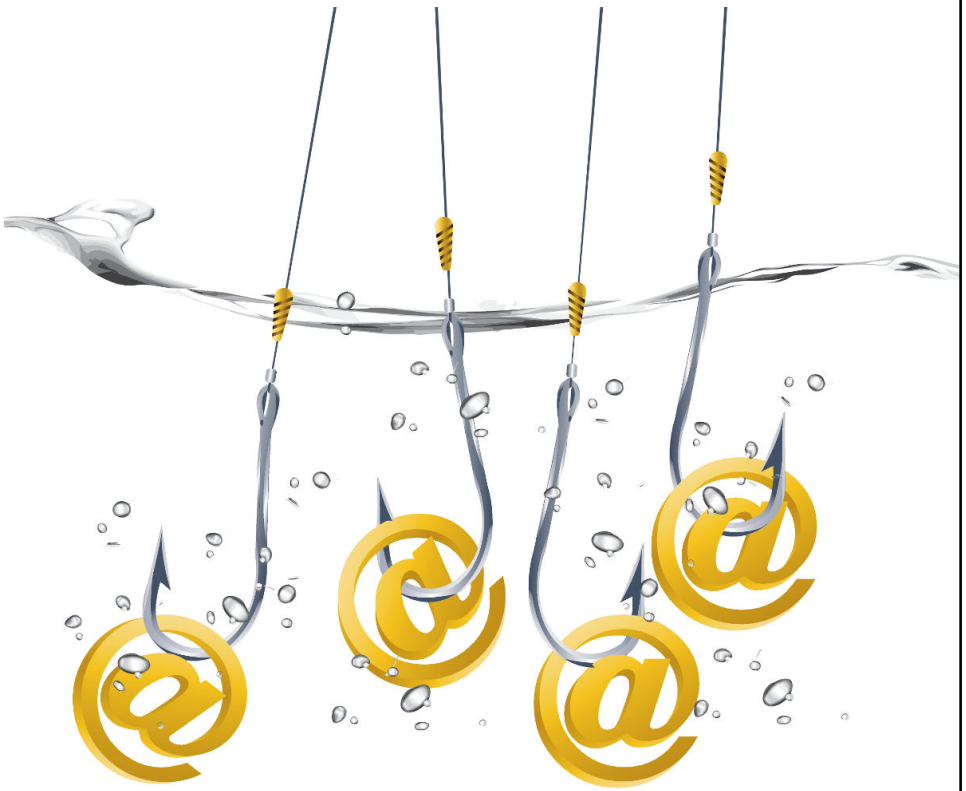
Customer Service Department
http://www.amazon.com
==========
Check your order and more: Order Update

More issues to address

- Anti-phishing systems snagged our emails
- Amazon lawyers called CMU lawyers

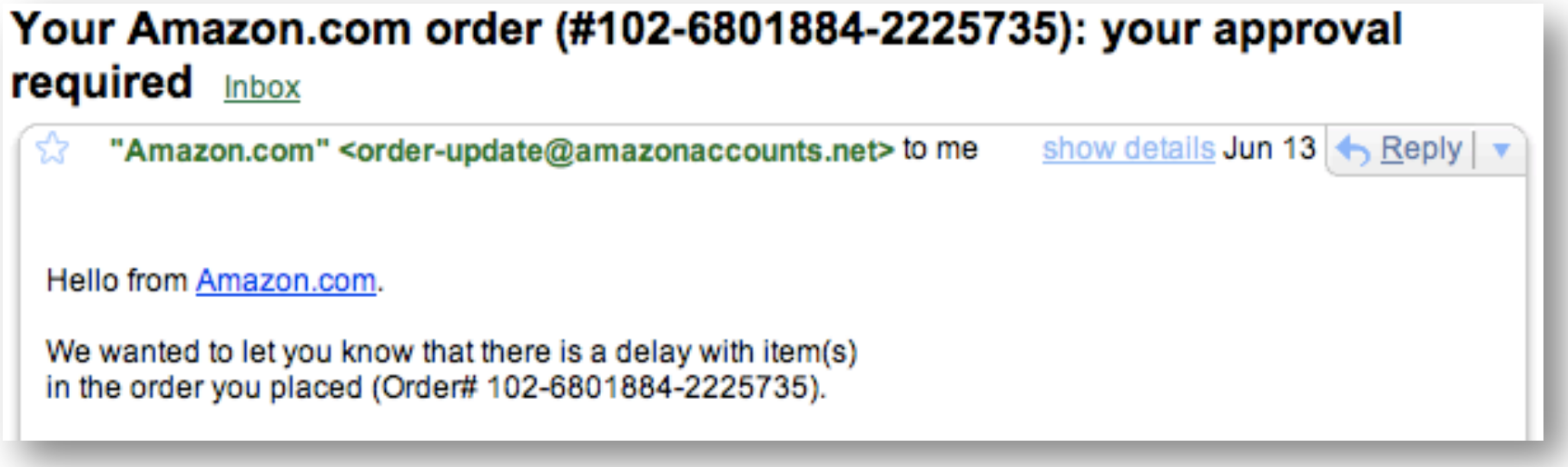
Success!

- Most participants got phished
- Significant differences between conditions
- Observed interesting user behavior that helped us understand root cause of failures



Confused by domain names

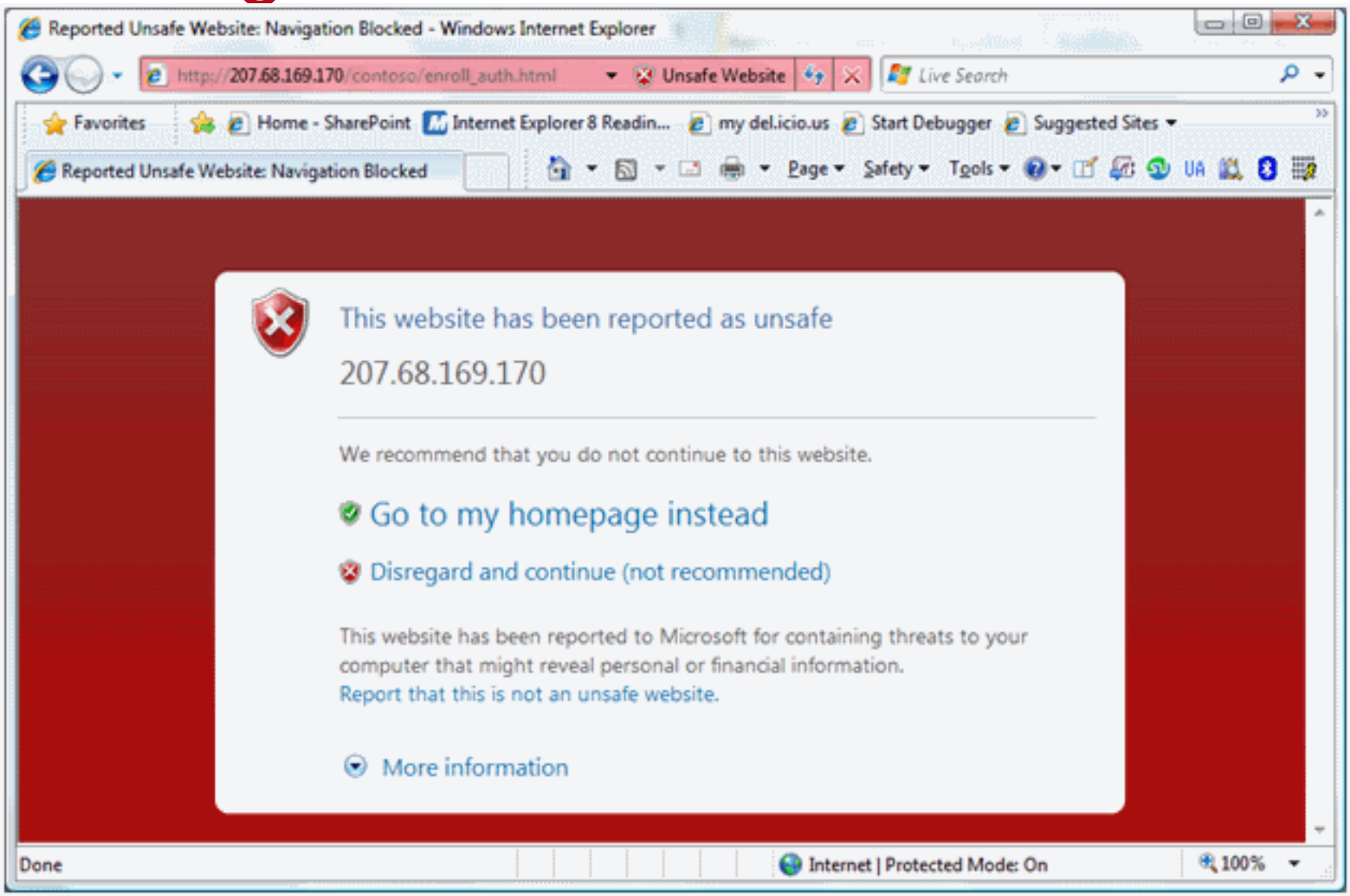
“The address in the browser was of amazonaccounts.net which is a genuine address”



Confused mental models

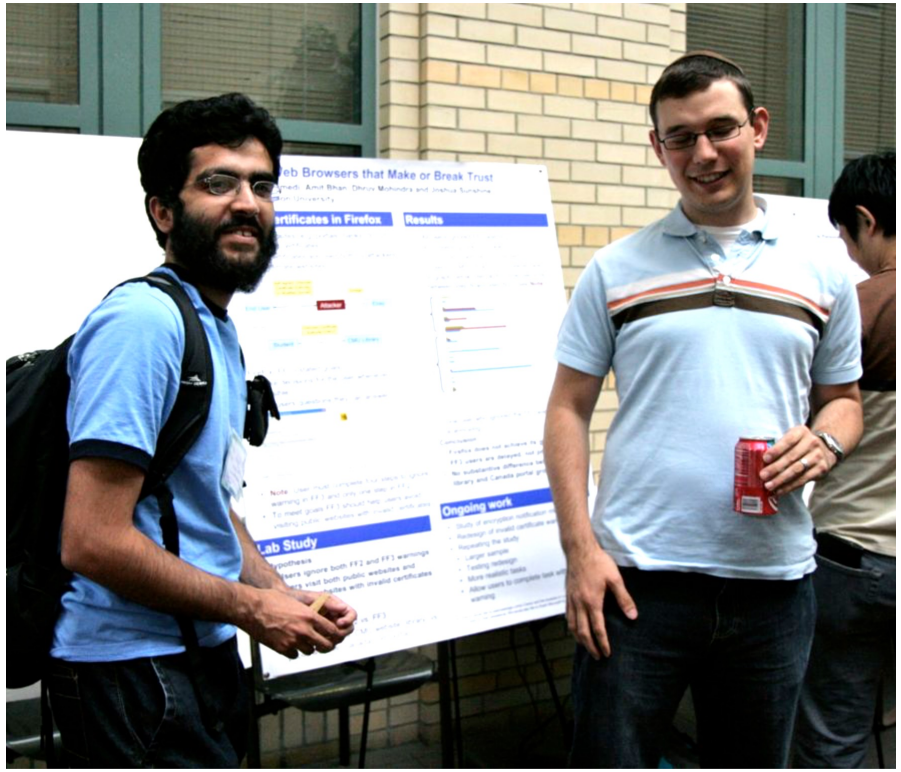
Some users repeatedly closed their browser, returned to the phishing email, and clicked on the link again

Research led to better phishing warnings



2008 SSL certificate warning study

- Test SSL certificate warnings
- Design a better warning



J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, L. Cranor. **Crying Wolf: An Empirical Study of SSL Warning Effectiveness.** USENIX Security 2009.

How do you know when you are actually at risk?

Some hazards are ALWAYS dangerous

Some hazards are context dependent

Computer security dialogs context dependent

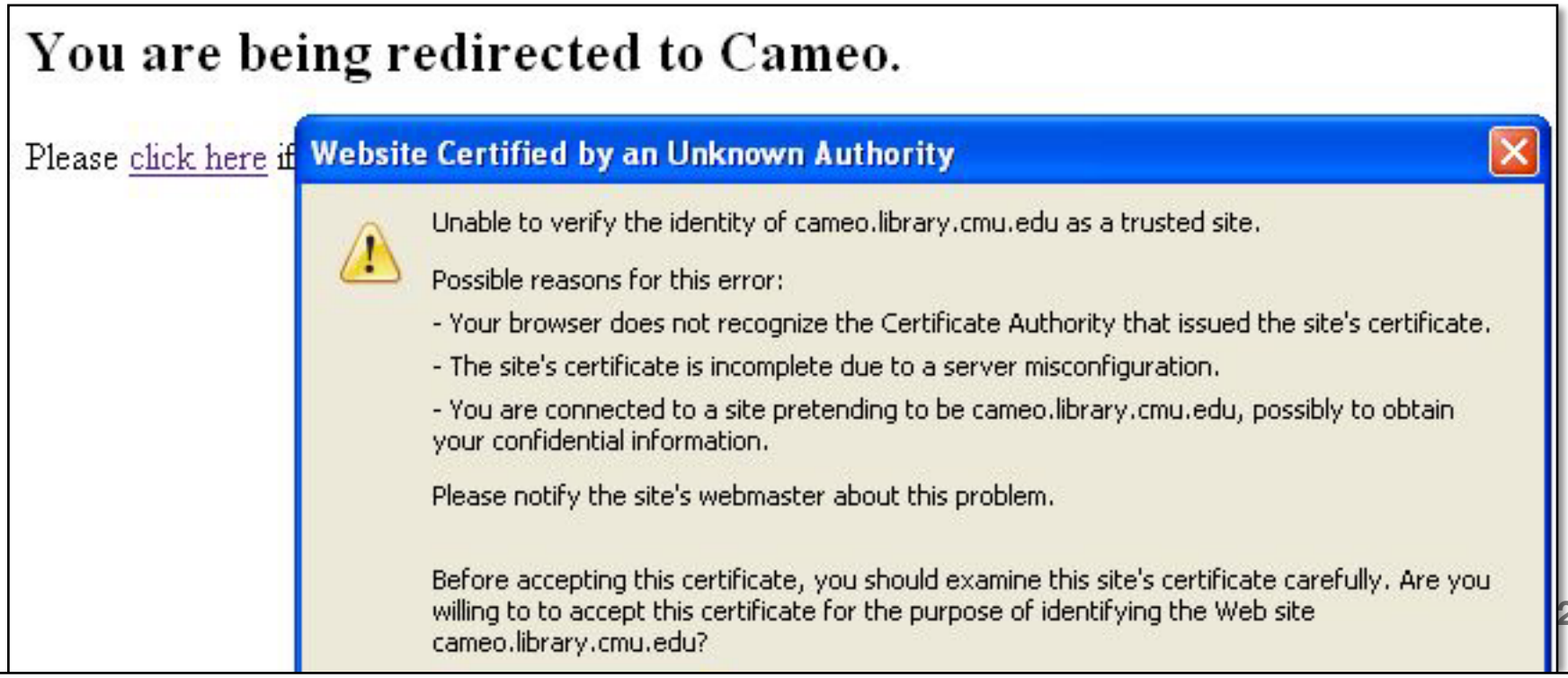
- Security warning dialogs more like warnings on wine than warnings on poison
- Software developers place burden of assessing risk on users

A good warning helps users determine whether they are at risk

- Stops users from doing something dangerous in risky context
- Doesn’t interfere with non-risky contexts
- Need to test warnings in both contexts

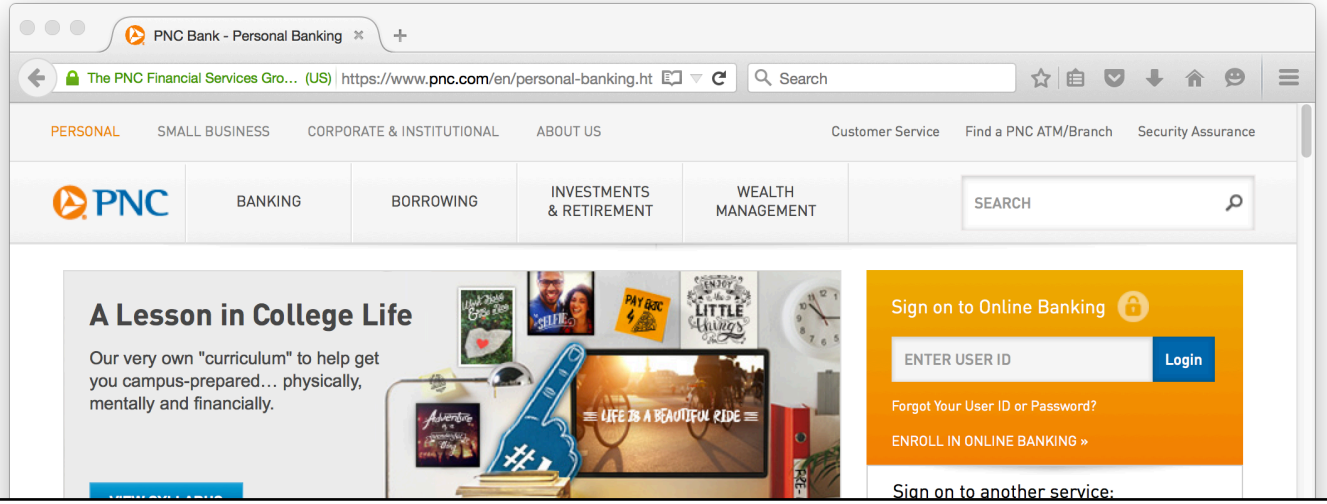
Non-risky context

- Visit CMU “Cameo” library web site
- Encounter self-signed certificate (familiar experience)



Risky context

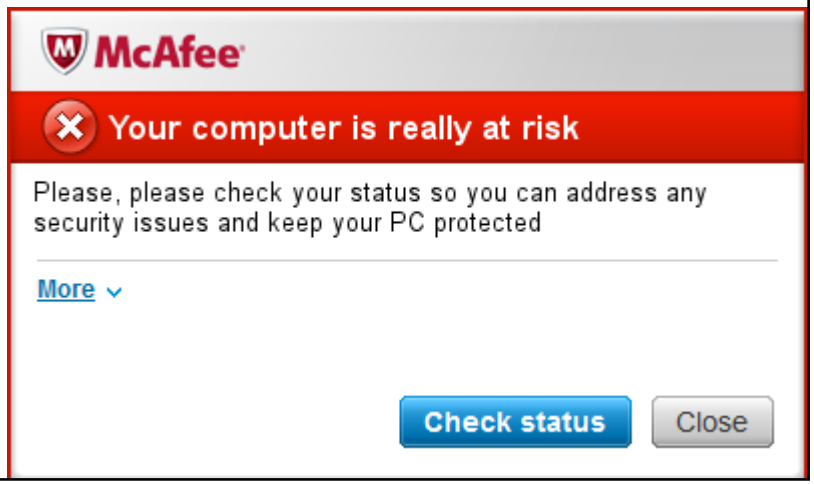
- Put users in situation where they have something they care about at risk
  - Come to our lab and check bank account balance online
- Make users think they are actually at risk
  - Use web proxy to do man-in-the-middle attack



This may or may not be legal in the state of Pennsylvania

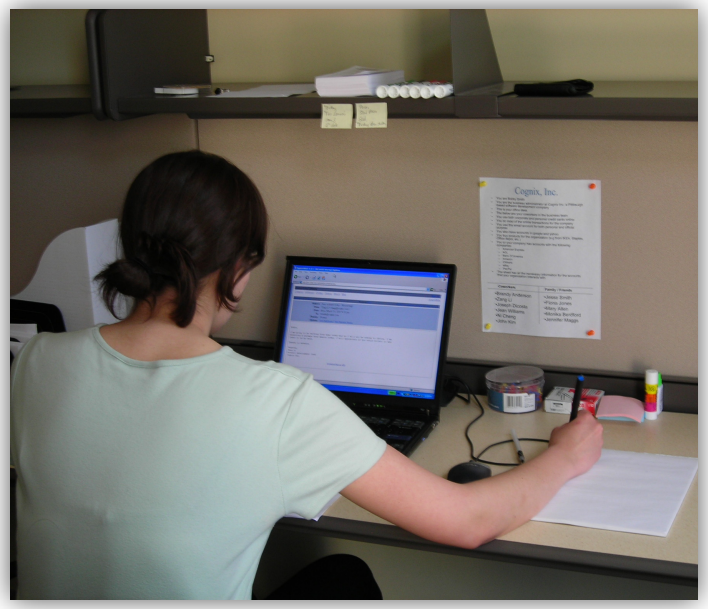
New plan

- Remove root certificate from browser
- Web site certificates can’t be verified
- Visits to secure sites will trigger warnings



Lab study challenges

- Participants may feel safe
- They may think they have to do everything we tell them
- Their priority may be to finish study fast and get paid



Provide easy alternative tasks

- Framed as information-seeking study
- 4 tasks including CMU library and bank account tasks
- Instructions for completing tasks online or by phone
  - E.g. login to http://www.pnc.com or dial 1-888-762-2265 for telephone banking
- Provided lab phone and computer

So what happened?

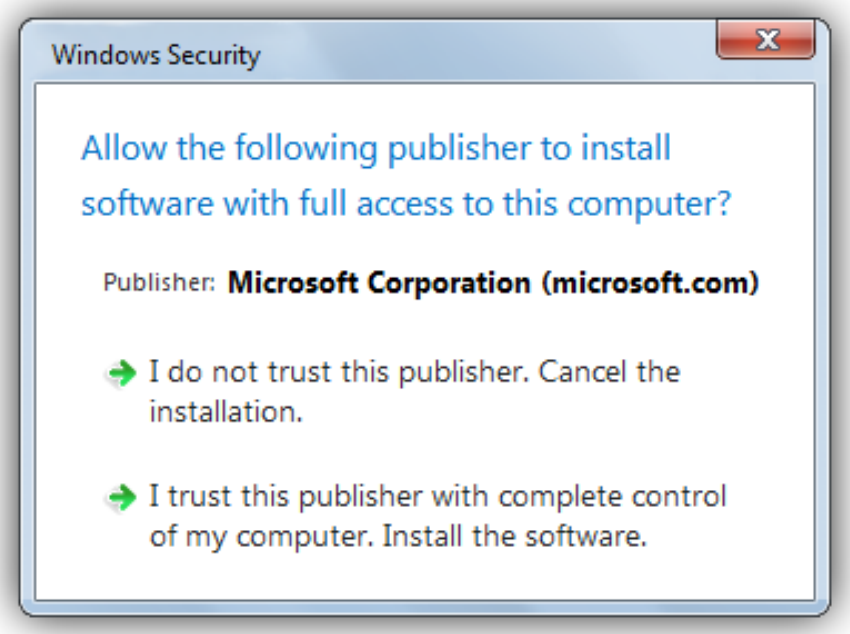
- 100 users tested FF2, FF3, IE7 + 2 new warnings
- **IE7 and FF2:** Most users ignored all warnings
- **FF3:** Most users heeded all warnings, couldn't figure out 4-step override process
- **New warnings:** Most users ignored warnings at library, about half heeded warnings at bank
  - Big improvement but still failed to keep users safe half the time

Security-decision UI study

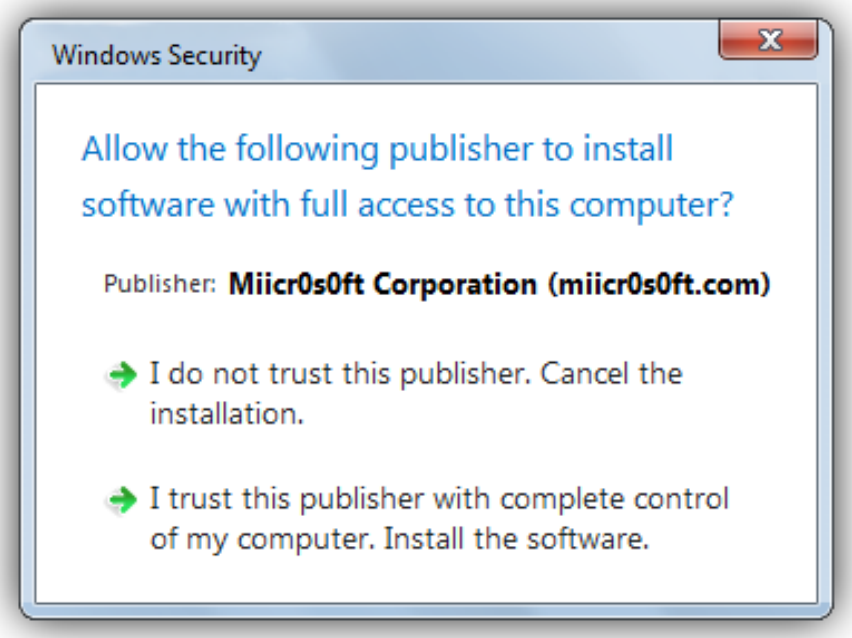
- How can we focus users' attention on key information they need to make informed decisions?

C. Bravo-Lillo, L.F. Cranor, J. Downs, S. Komanduri, R.W. Reeder, S. Schechter, and M. Sleeper. **Your Attention Please: Designing security-decision UIs to make genuine risks harder to ignore**. SOUPS 2013.

Can you spot the suspicious software?



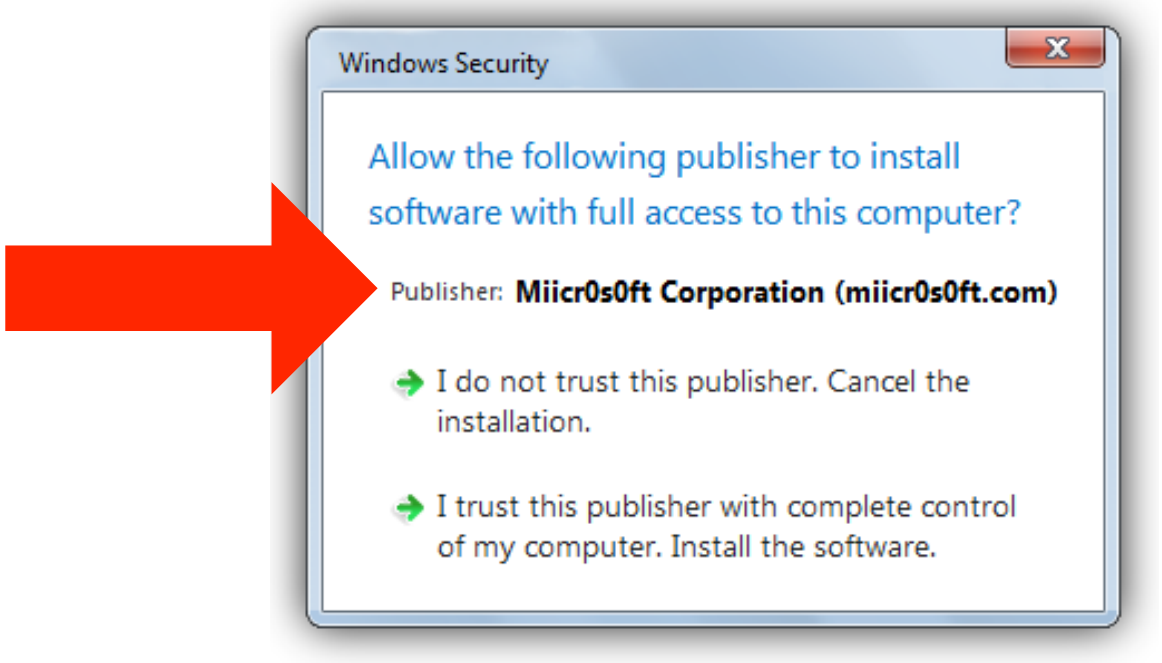
benign



suspicious

Key question: Do you trust publisher?

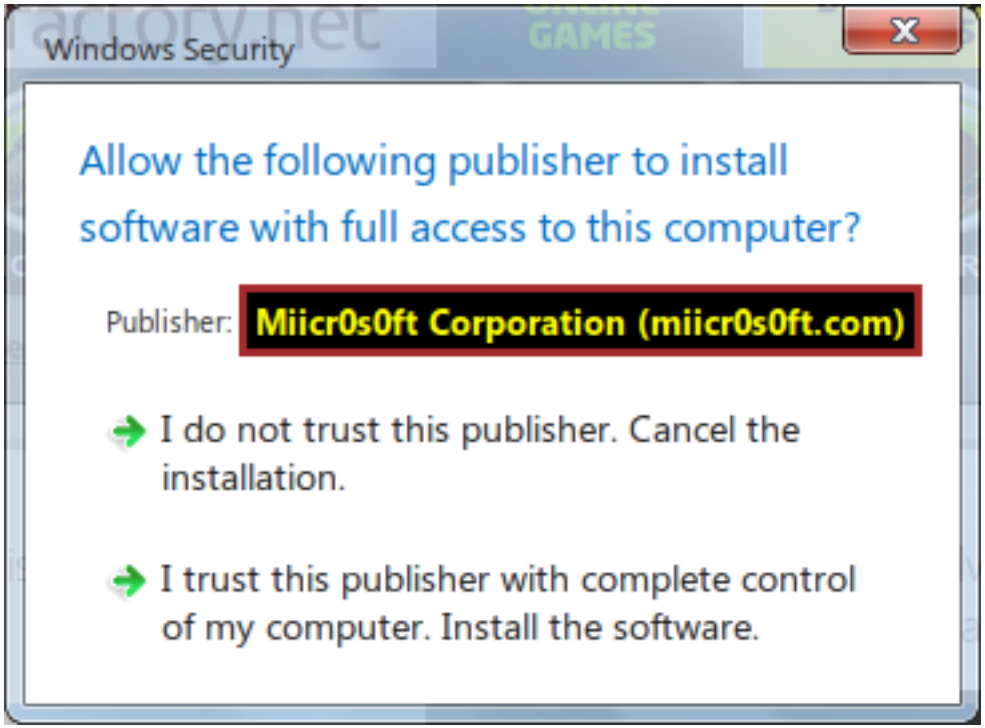
Name of publisher is critical information in trust decision



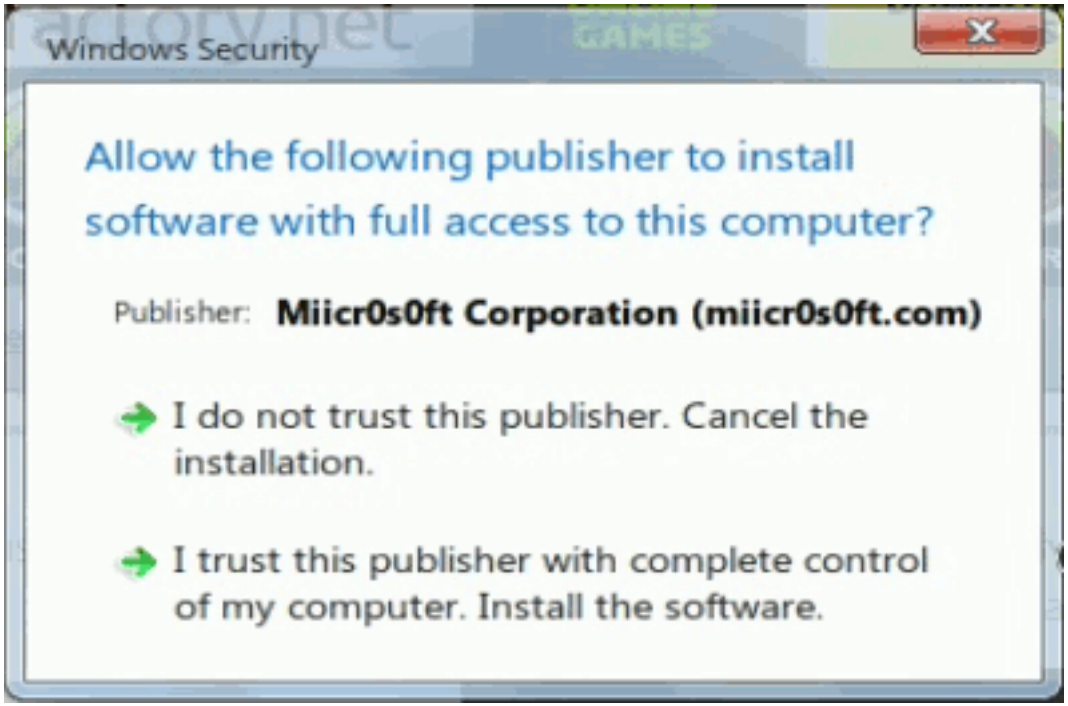
How can we get users to notice suspicious publishers?

- Use **attractors** to draw attention to publisher name
- Force delay before users can install
- Force interaction before users can install
- Force users to read publisher name

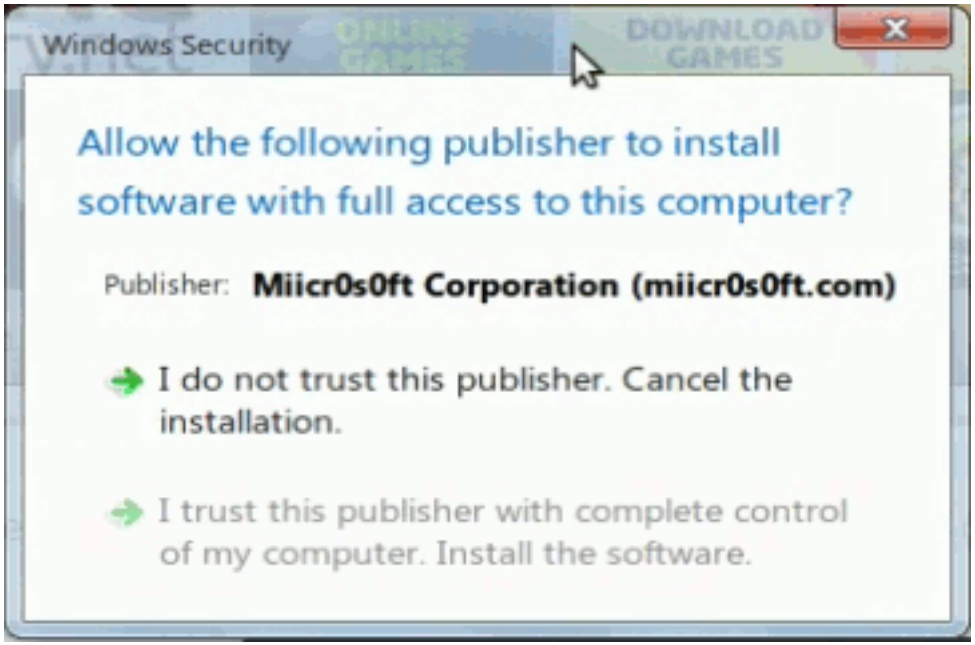
ANSI standard warning colors



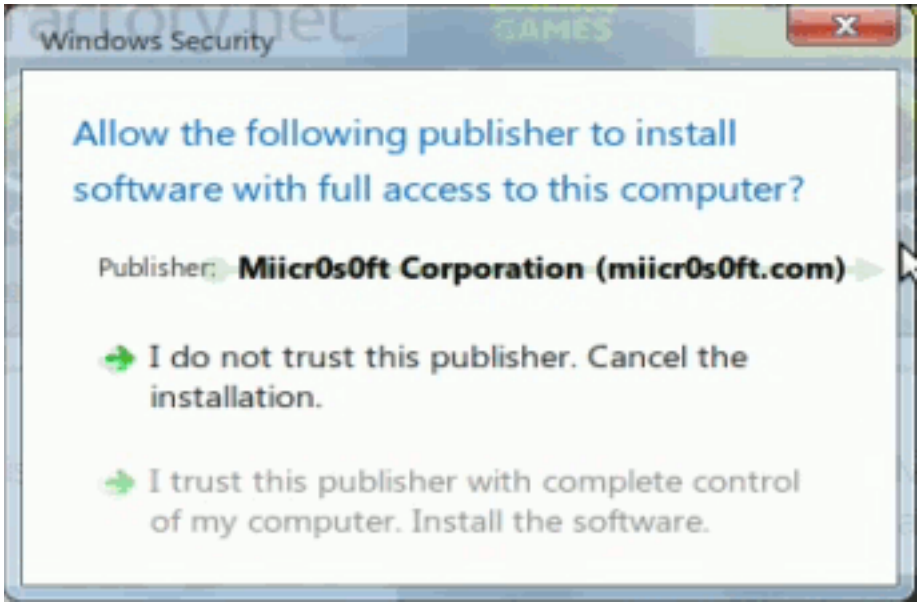
Animated connector



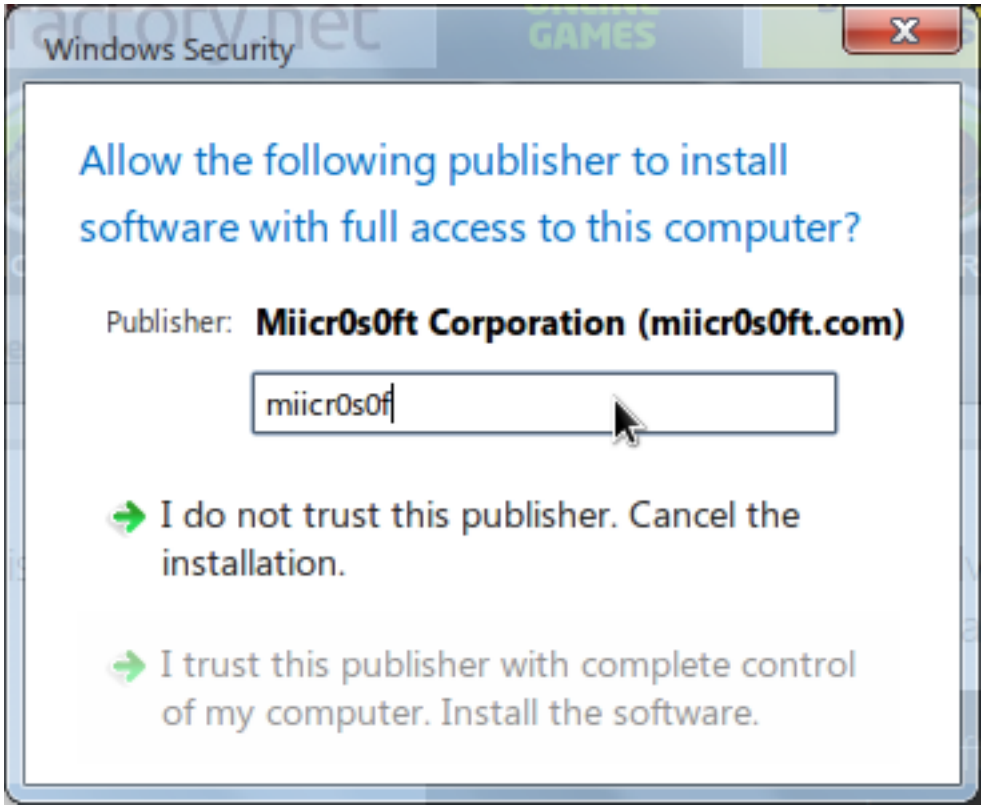
Slow reveal


Windows Security
Allow the following publisher to install software with full access to this computer?
Publisher: Miicr0s0ft Corporation (miicr0s0ft.com)
I do not trust this publisher. Cancel the installation.
I trust this publisher with complete control of my computer. Install the software.

Obstruct install button until user swipes mouse over publisher name

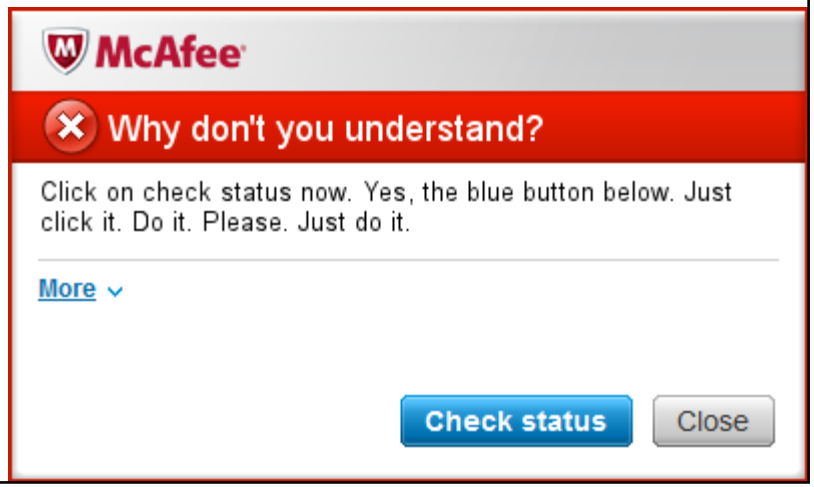


Obstruct install button until user types publisher name



Do any of these work?

- Do attractors and other techniques prevent suspicious installs without preventing benign installs?
- How much do attractors delay benign installs?

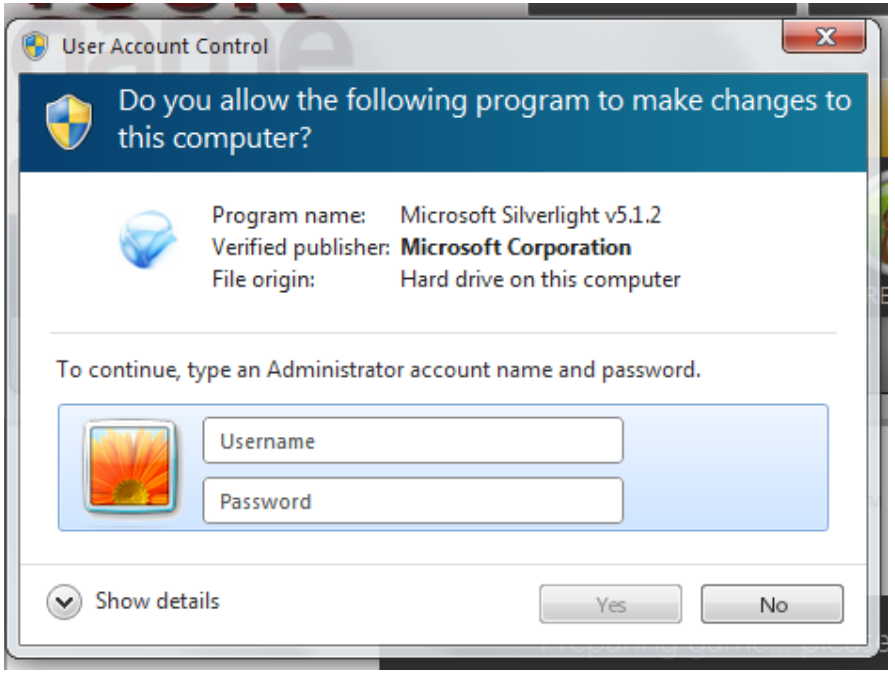


Methodology requirements

- Massive, inexpensive, quick
- Remote observation/recording of behavior
- Participants should feel safety/risk and behave as they would in real life
- But should not actually be at increased risk through participation in experiment

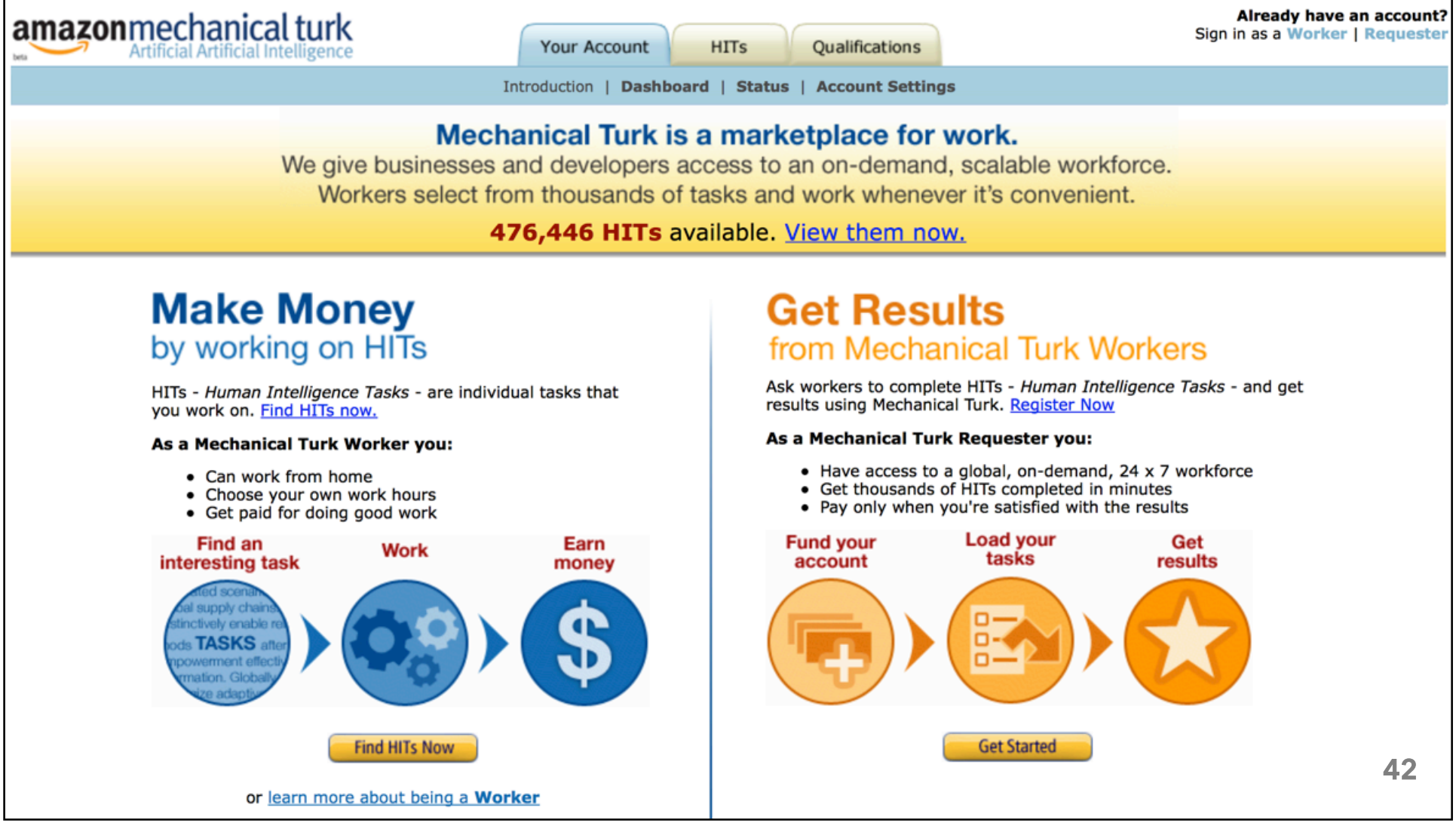
Use Mturk game ruse

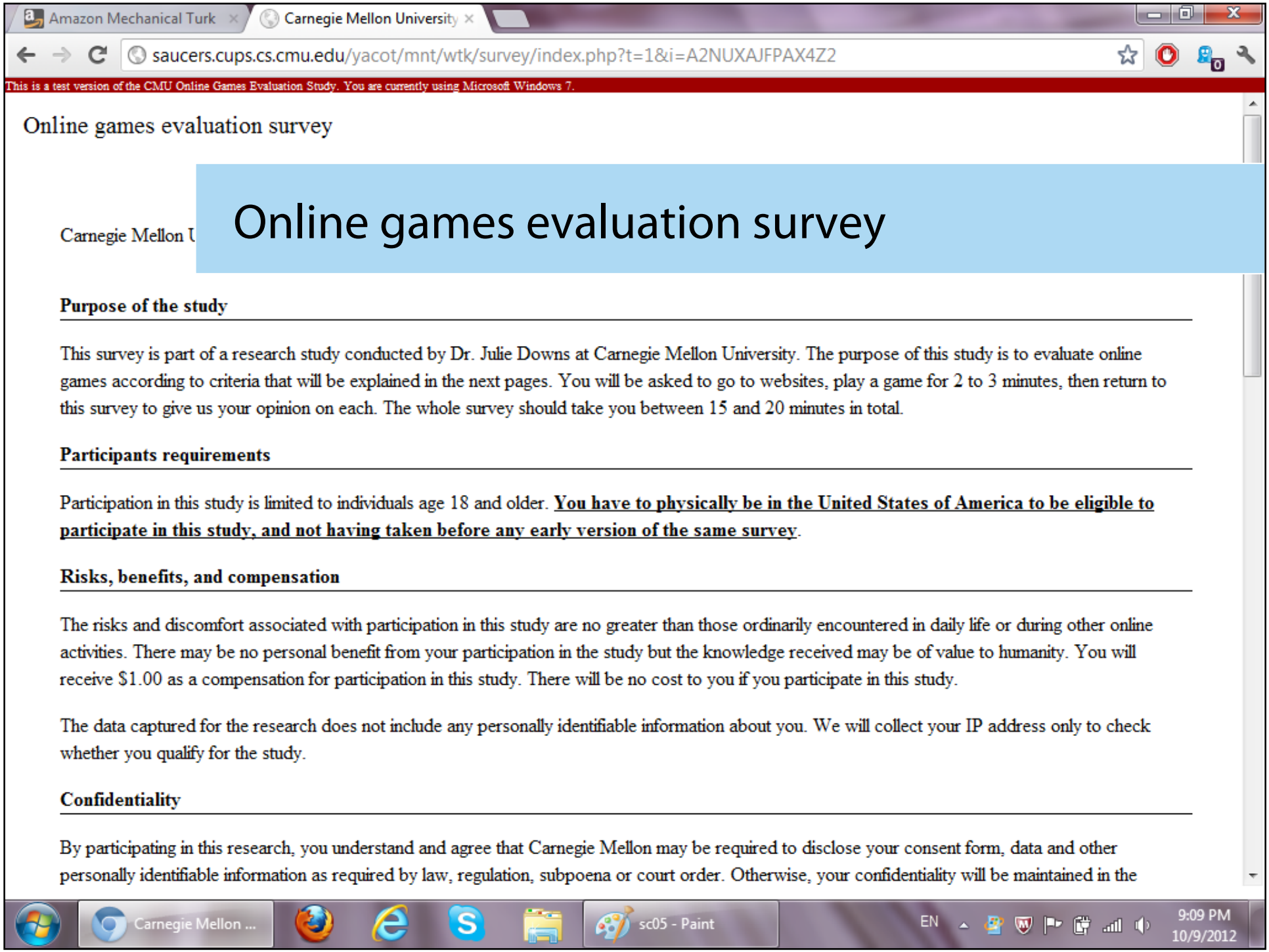
- Ruse previously developed for study of whether users would fall for fake OS password dialogs

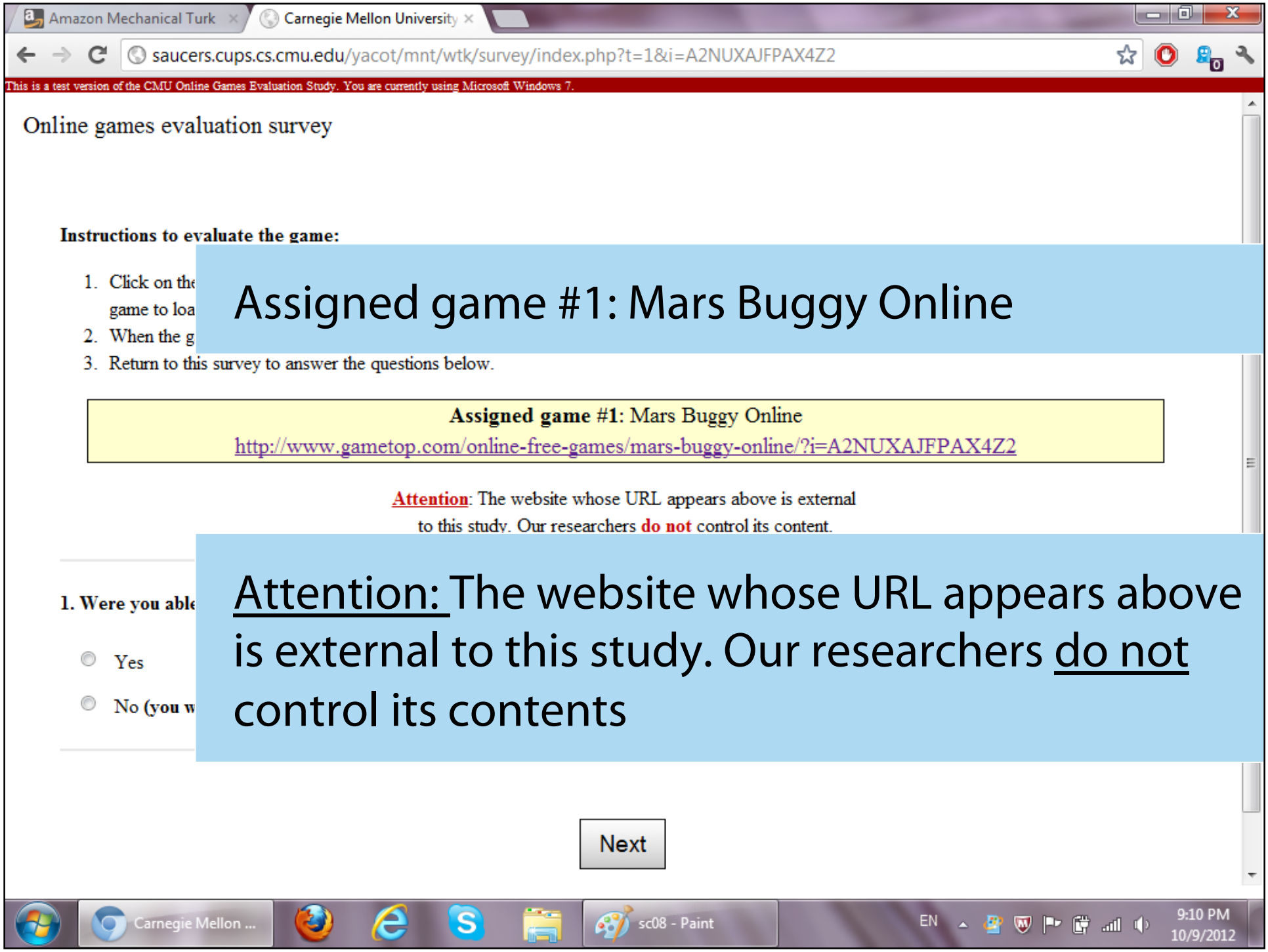


Operating System Framed in Case of Mistaken Identity: Measuring the success of web-based spoofing attacks on OS password-entry (ACM CCS 2012)

Amazon Mechanical Turk




Amazon Mechanical Turk
Carnegie Mellon University
saucers.cups.cs.cmu.edu/yacot/mnt/wtk/survey/index.php?t=1&i=A2NUXAJFPAX4Z2
This is a test version of the CMU Online Games Evaluation Study. You are currently using Microsoft Windows 7.
Online games evaluation survey
Carnegie Mellon U
Online games evaluation survey
Purpose of the study
This survey is part of a research study conducted by Dr. Julie Downs at Carnegie Mellon University. The purpose of this study is to evaluate online games according to criteria that will be explained in the next pages. You will be asked to go to websites, play a game for 2 to 3 minutes, then return to this survey to give us your opinion on each. The whole survey should take you between 15 and 20 minutes in total.
Participants requirements
Participation in this study is limited to individuals age 18 and older. You have to physically be in the United States of America to be eligible to participate in this study, and not having taken before any early version of the same survey.
Risks, benefits, and compensation
The risks and discomfort associated with participation in this study are no greater than those ordinarily encountered in daily life or during other online activities. There may be no personal benefit from your participation in the study but the knowledge received may be of value to humanity. You will receive $1.00 as a compensation for participation in this study. There will be no cost to you if you participate in this study.
The data captured for the research does not include any personally identifiable information about you. We will collect your IP address only to check whether you qualify for the study.
Confidentiality
By participating in this research, you understand and agree that Carnegie Mellon may be required to disclose your consent form, data and other personally identifiable information as required by law, regulation, subpoena or court order. Otherwise, your confidentiality will be maintained in the
Carnegie Mellon ...
sc05 - Paint
EN
9:09 PM
10/9/2012


Amazon Mechanical Turk
Carnegie Mellon University
saucers.cups.cs.cmu.edu/yacot/mnt/wtk/survey/index.php?t=1&i=A2NUXAJFPAX4Z2
This is a test version of the CMU Online Games Evaluation Study. You are currently using Microsoft Windows 7.
Online games evaluation survey
Instructions to evaluate the game:
1. Click on the
game to loa
2. When the g
3. Return to this survey to answer the questions below.
Assigned game #1: Mars Buggy Online
http://www.gametop.com/online-free-games/mars-buggy-online/?i=A2NUXAJFPAX4Z2
Attention: The website whose URL appears above is external
to this study. Our researchers do not control its content.
1. Were you able
Yes
No (you w
Next
Assigned game #1: Mars Buggy Online
Attention: The website whose URL appears above is external to this study. Our researchers do not control its contents
Carnegie Mellon ...
sc08 - Paint
EN
9:10 PM
10/9/2012

Amazon Mechanical Turk | Carnegie Mellon University | Mars Buggy Free Game

www.gametop.com/online-free-games/mars-buggy-online/?i=A2NUXAJFPAX4Z2

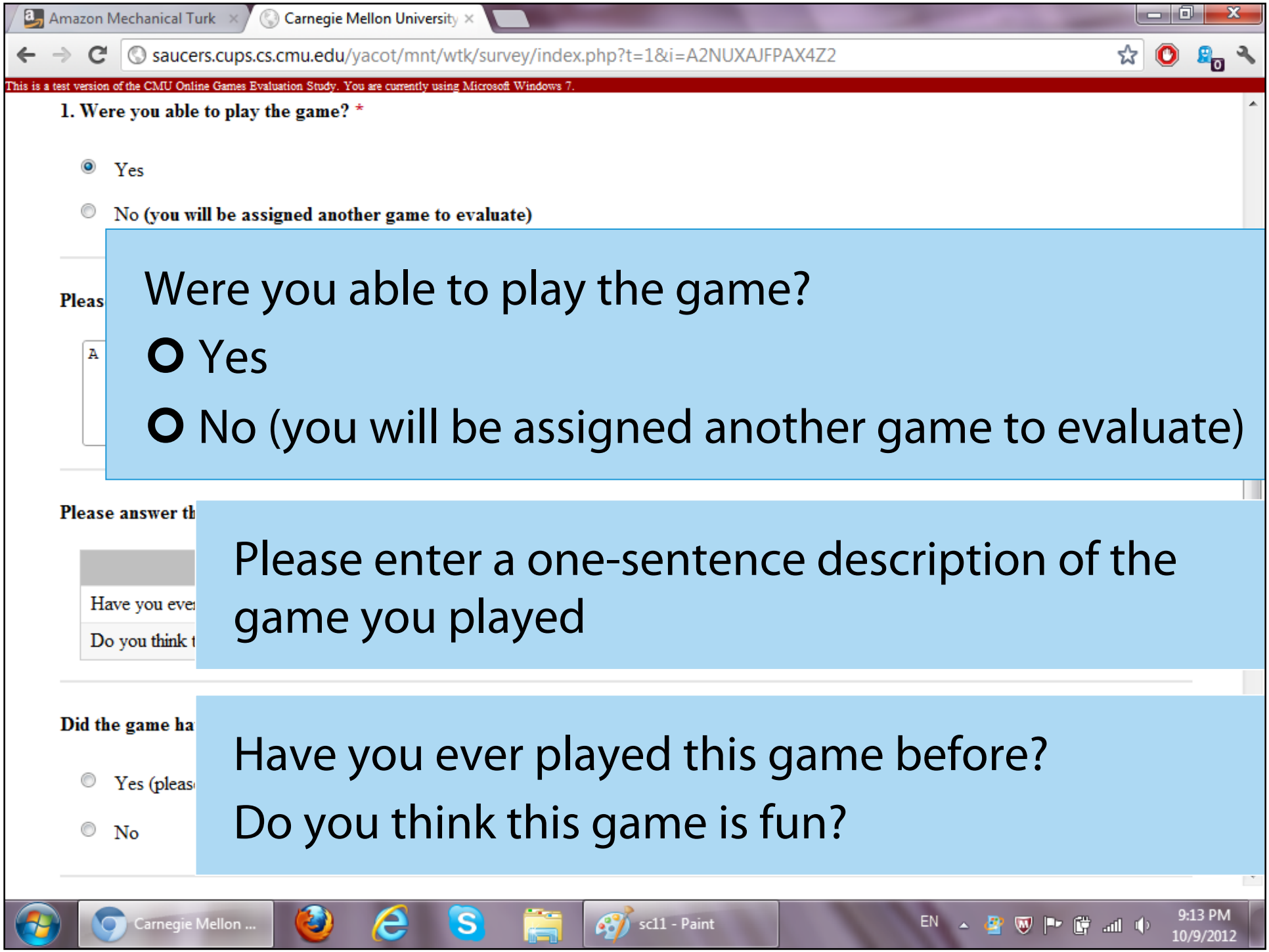
need to be rescued.

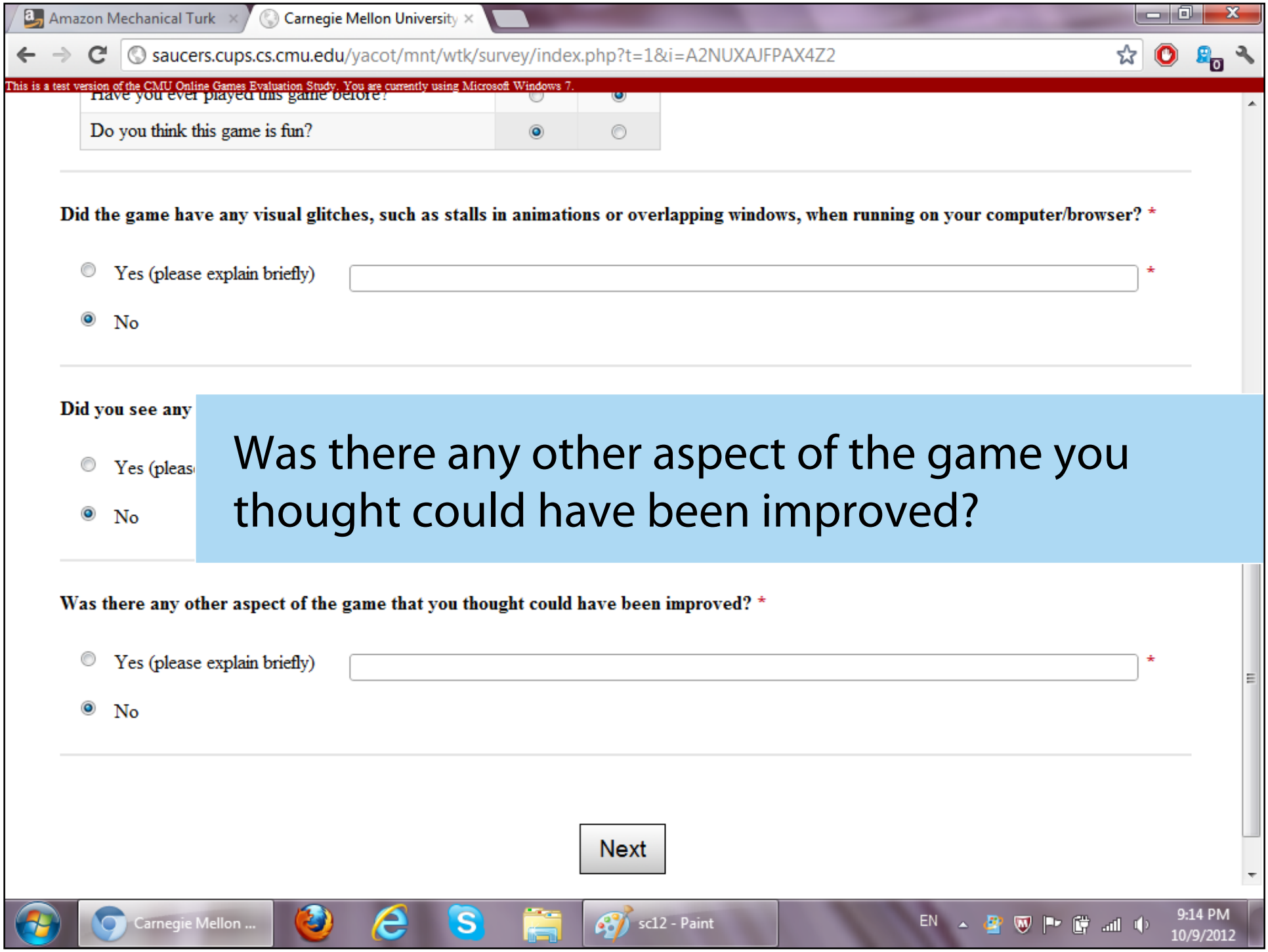
Play this free online game today and bring your crew back to earth.

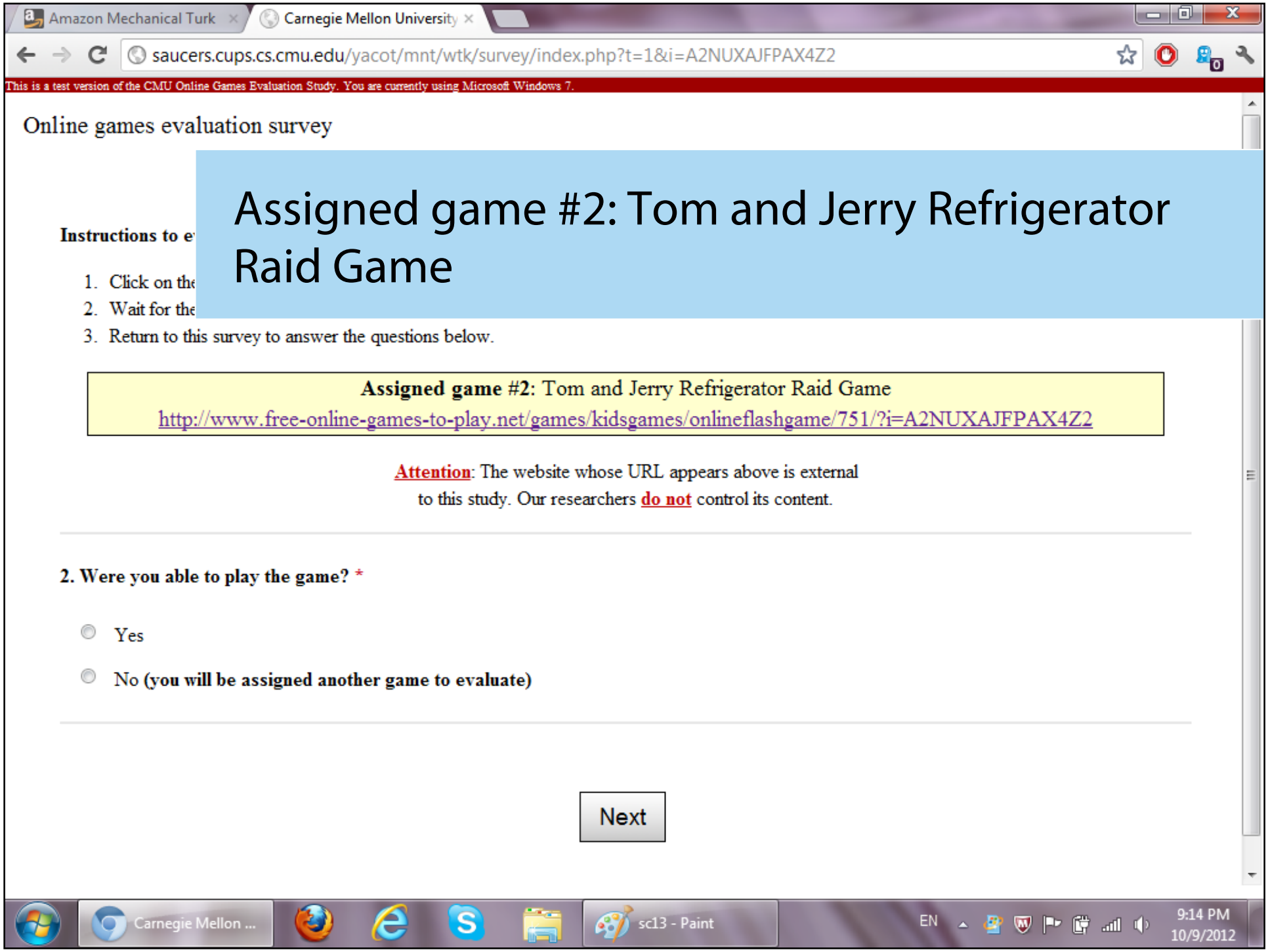
Do you like this game? Tweet

Mars Buggy

Mars Buggy Free ... | sc09 - Paint | EN | 9:11 PM 10/9/2012


Amazon Mechanical Turk
Carnegie Mellon University
saucers.cups.cs.cmu.edu/yacot/mnt/wtk/survey/index.php?t=1&i=A2NUXAJFPAX4Z2
This is a test version of the CMU Online Games Evaluation Study. You are currently using Microsoft Windows 7.
1. Were you able to play the game? *
Yes
No (you will be assigned another game to evaluate)
Were you able to play the game?
Yes
No (you will be assigned another game to evaluate)
Please answer th
Have you ever
Do you think t
Please enter a one-sentence description of the game you played
Did the game ha
Yes (pleas
No
Have you ever played this game before?
Do you think this game is fun?
Carnegie Mellon ...
sc11 - Paint
EN
9:13 PM
10/9/2012


Amazon Mechanical Turk
Carnegie Mellon University
saucers.cups.cs.cmu.edu/yacot/mnt/wtk/survey/index.php?t=1&i=A2NUXAJFPAX4Z2
This is a test version of the CMU Online Games Evaluation Study. You are currently using Microsoft Windows 7.
Have you ever played this game before?
Do you think this game is fun?
Did the game have any visual glitches, such as stalls in animations or overlapping windows, when running on your computer/browser? *
Yes (please explain briefly)
No
Did you see any
Yes (pleas
No
Was there any other aspect of the game you thought could have been improved?
Was there any other aspect of the game that you thought could have been improved? *
Yes (please explain briefly)
No
Next
Carnegie Mellon ...
sc12 - Paint
EN
9:14 PM
10/9/2012


Amazon Mechanical Turk
Carnegie Mellon University
saucers.cups.cs.cmu.edu/yacot/mnt/wtk/survey/index.php?t=1&i=A2NUXAJFPAX4Z2
This is a test version of the CMU Online Games Evaluation Study. You are currently using Microsoft Windows 7.
Online games evaluation survey
Assigned game #2: Tom and Jerry Refrigerator Raid Game
Instructions to e
1. Click on the
2. Wait for the
3. Return to this survey to answer the questions below.
Assigned game #2: Tom and Jerry Refrigerator Raid Game
http://www.free-online-games-to-play.net/games/kidsgames/onlineflashgame/751/?i=A2NUXAJFPAX4Z2
Attention: The website whose URL appears above is external to this study. Our researchers do not control its content.
2. Were you able to play the game? *
Yes
No (you will be assigned another game to evaluate)
Next
Carnegie Mellon ...
sc13 - Paint
EN
9:14 PM
10/9/2012

Amazon Mechanical Turk | Carnegie Mellon University | Tom and Jerry Refrigerator

www.free-online-games-to-play.net/games/kidsgames/onlineflashgame/751/?i=A2NUXAJFPAX4Z2/

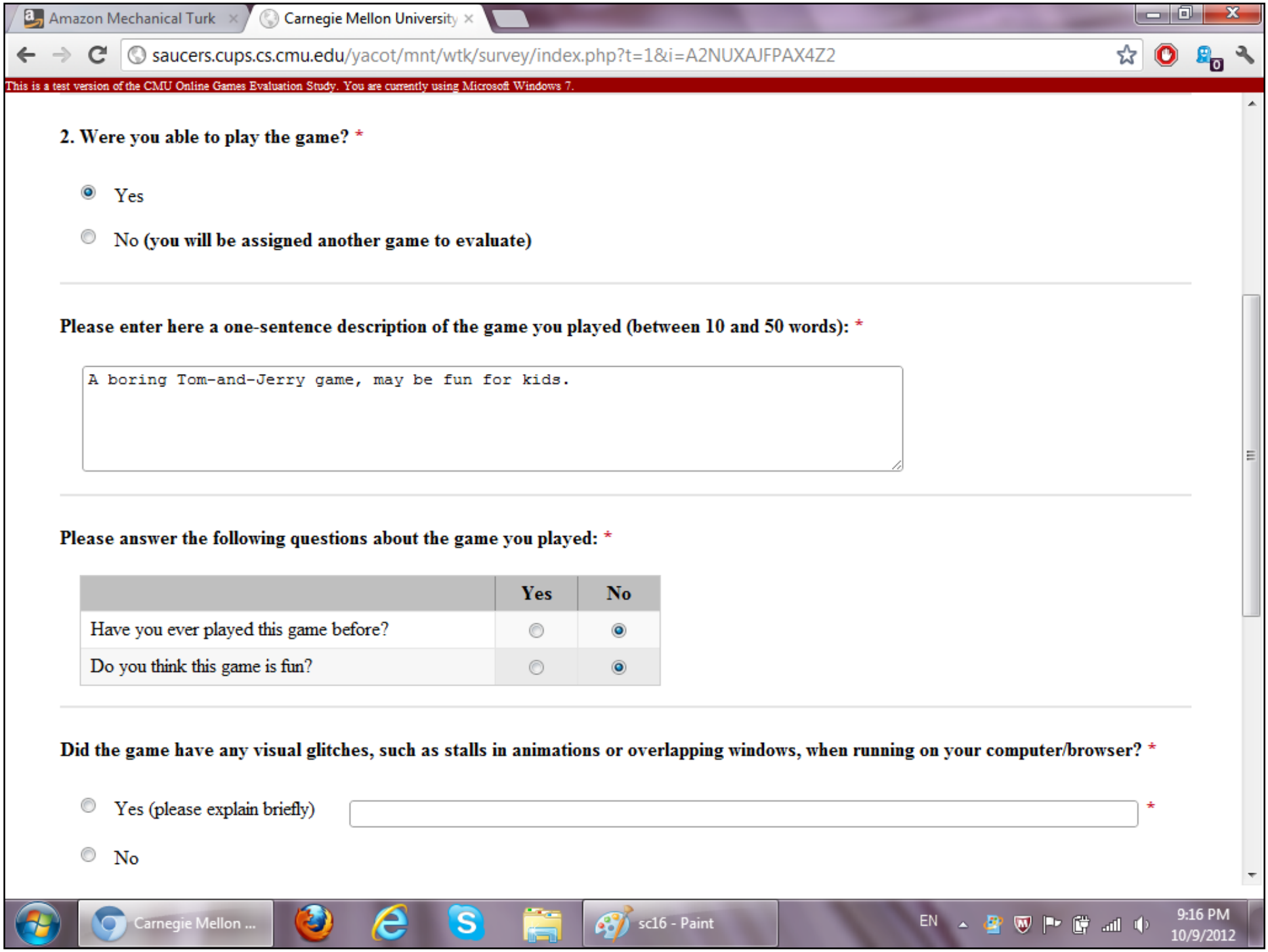
Add to Favorites

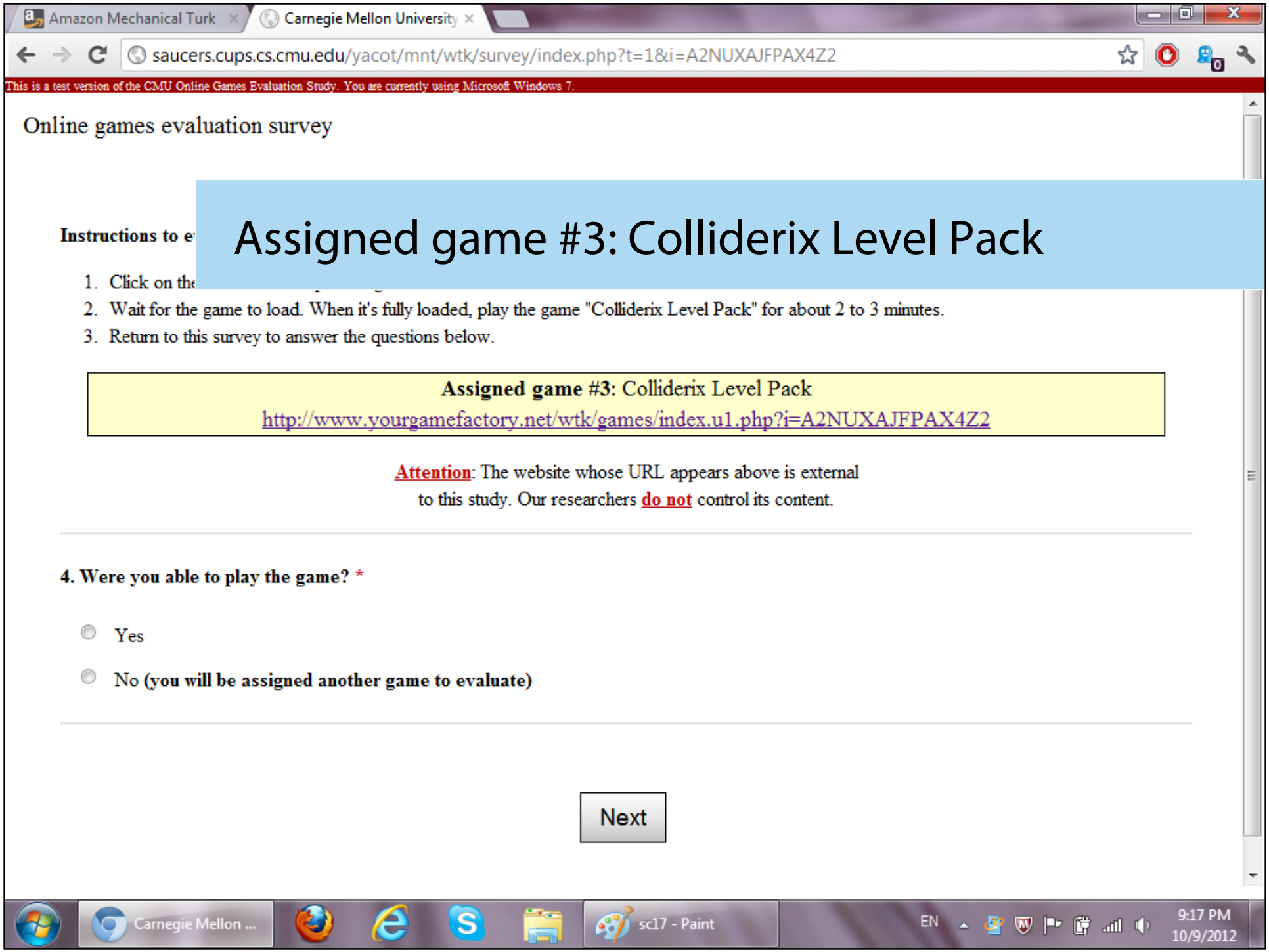
Home » Kids games » Tom and Jerry Refrigerator Raid Game

Tom and Jerry Refrigerator Raid Game

stars (3973)

Tom and Jerry Ref... | sc14 - Paint | EN | 9:14 PM 10/9/2012


Amazon Mechanical Turk
Carnegie Mellon University
saucers.cups.cs.cmu.edu/yacot/mnt/wtk/survey/index.php?t=1&i=A2NUXAJFPAX4Z2
This is a test version of the CMU Online Games Evaluation Study. You are currently using Microsoft Windows 7.
2. Were you able to play the game? *
Yes
No (you will be assigned another game to evaluate)
Please enter here a one-sentence description of the game you played (between 10 and 50 words): *
A boring Tom-and-Jerry game, may be fun for kids.
Please answer the following questions about the game you played: *
Yes
No
Have you ever played this game before?
Do you think this game is fun?
Did the game have any visual glitches, such as stalls in animations or overlapping windows, when running on your computer/browser? *
Yes (please explain briefly)
*
No
Carnegie Mellon ...
sc16 - Paint
EN
9:16 PM
10/9/2012


Amazon Mechanical Turk
Carnegie Mellon University
saucers.cups.cs.cmu.edu/yacot/mnt/wtk/survey/index.php?t=1&i=A2NUXAJFPAX4Z2
This is a test version of the CMU Online Games Evaluation Study. You are currently using Microsoft Windows 7.
Online games evaluation survey
Assigned game #3: Colliderix Level Pack
Instructions to e
1. Click on the
2. Wait for the game to load. When it's fully loaded, play the game "Colliderix Level Pack" for about 2 to 3 minutes.
3. Return to this survey to answer the questions below.
Assigned game #3: Colliderix Level Pack
http://www.yourgamefactory.net/wtk/games/index.u1.php?i=A2NUXAJFPAX4Z2
Attention: The website whose URL appears above is external
to this study. Our researchers do not control its content.
4. Were you able to play the game? *
Yes
No (you will be assigned another game to evaluate)
Next
Carnegie Mellon ...
sc17 - Paint
EN
9:17 PM
10/9/2012

Amazon Mechanical Turk | Carnegie Mellon Universit | Colliderix Level Pack - puz

www.yourgamefactory.net/wtk/games/index.rp16.php?i=A2NUXAJFPAX4Z2&v=tlsb

YOUR game factory.net

ADD TO FAVORITES | SET AS HOMEPAGE

Username ••••••••• Login

FORGOT PASSWORD? SIGN UP

ONLINE GAMES | DOWNLOAD GAMES FREE | GAME CLUB | MMORPG GAMES | MULTIPLAYER GAMES

SHOOTING | RACING | PUZZLE | ACTION | SPORT | DRESS UP | KIDS | CLASSIC | BOARD | MISC | NEW

Games / Puzzle Games / Colliderix Level Pack

Search...

This game requires the latest version of Microsoft Silverlight™ (v5.1.2). Silverlight is either missing or out of date.

Access being requested, please wait.

Description: Beloved Colliderix is back, equipped with levels that will break your mind!

Rate it:

Liked it: 84.6%
Votes: 175
Plays: 70522
Added: 07/28/2006

Waiting for saucers.cups.cs.cmu.edu...

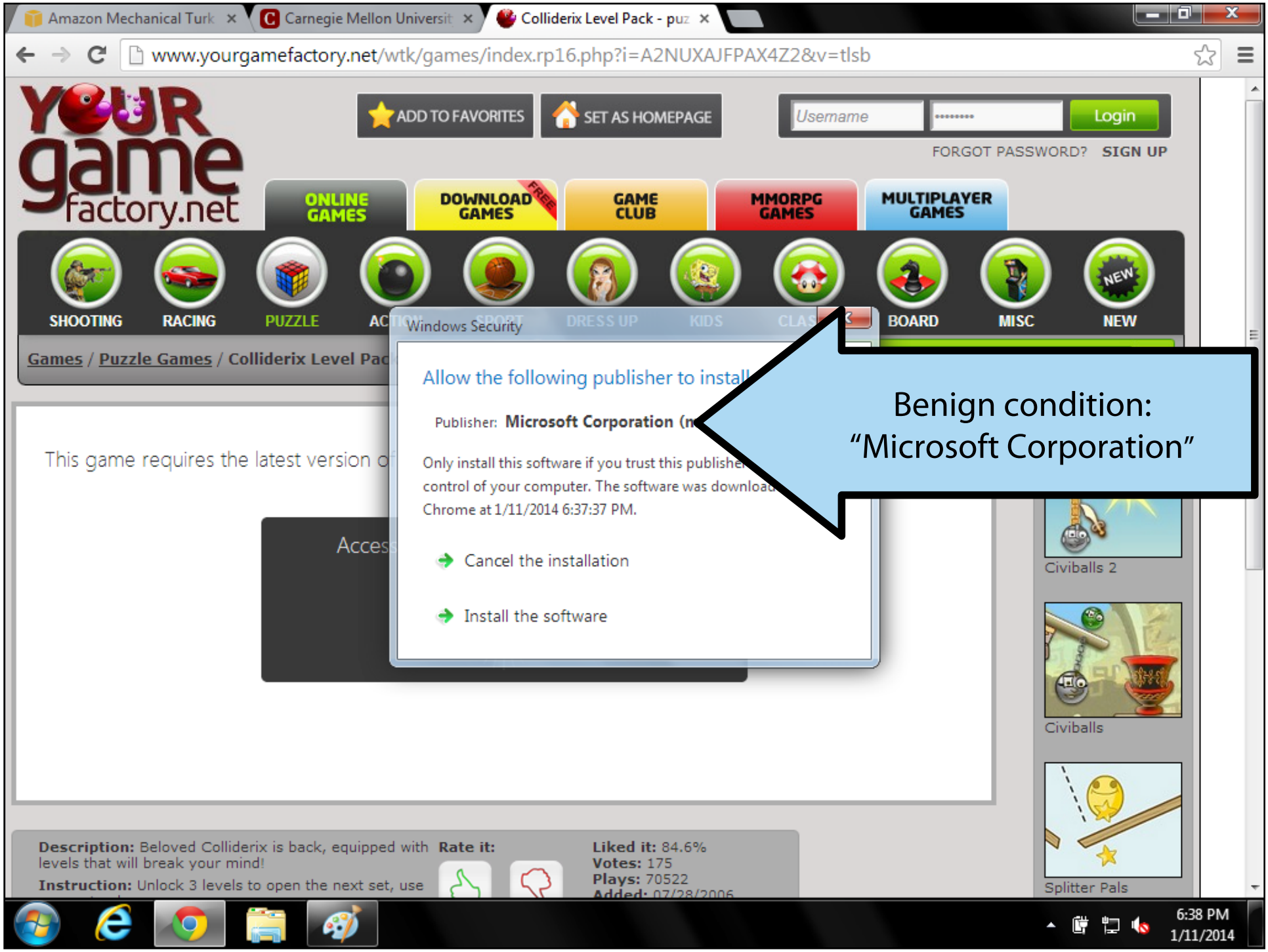
Related Games


Civiballs 2


Civiballs


Splitter Pals

6:37 PM
1/11/2014


Amazon Mechanical Turk
Carnegie Mellon Universit
Colliderix Level Pack - puz
www.yourgamefactory.net/wtk/games/index.rp16.php?i=A2NUXAJFPAX4Z2&v=tlsb
YOUR game factory.net
ADD TO FAVORITES
SET AS HOMEPAGE
Username
Login
FORGOT PASSWORD?
SIGN UP
ONLINE GAMES
DOWNLOAD GAMES
FREE
GAME CLUB
MMORPG GAMES
MULTIPLAYER GAMES
SHOOTING
RACING
PUZZLE
BOARD
MISC
NEW
Games / Puzzle Games / Colliderix Level Pac
Windows Security
Allow the following publisher to install
Publisher: Microsoft Corporation (n
Only install this software if you trust this publisher
control of your computer. The software was downloaded
Chrome at 1/11/2014 6:37:37 PM.
Cancel the installation
Install the software
Benign condition:
“Microsoft Corporation”
This game requires the latest version of
Civiballs 2
Civiballs
Splitter Pals
Description: Beloved Colliderix is back, equipped with levels that will break your mind!
Instruction: Unlock 3 levels to open the next set, use
Rate it:
Liked it: 84.6%
Votes: 175
Plays: 70522
Added: 07/28/2006
6:38 PM
1/11/2014


Amazon Mechanical Turk
Carnegie Mellon Universit
Colliderix Level Pack - puz
www.yourgamefactory.net/wtk/games/index.rp16.php?i=A2NUXAJFPAX4Z2&v=tlsb&s=2
YOUR game factory.net
ADD TO FAVORITES
SET AS HOMEPAGE
Username
Login
FORGOT PASSWORD?
SIGN UP
ONLINE GAMES
DOWNLOAD GAMES
FREE
GAME CLUB
MMORPG GAMES
MULTIPLAYER GAMES
SHOOTING
RACING
PUZZLE
BOARD
MISC
NEW
Games / Puzzle Games / Colliderix Level Pac
Windows Security
Allow the following publisher to install
Publisher: Miicr0s0ft Corporation
Only install this software if you trust this publisher
control of your computer. The software was downloaded
Chrome at 1/11/2014 6:52:58 PM.
Cancel the installation
Install the software
Suspicious condition:
“Miicr0s0ft Corporation”
This game requires the latest version
Description: Beloved Colliderix is back, equipped with levels that will break your mind!
Instruction: Unlock 3 levels to open the next set, use
Rate it:
Liked it: 84.6%
Votes: 175
Plays: 70522
Added: 07/28/2006
Civiballs 2
Civiballs
Splitter Pals
6:58 PM
1/11/2014

Participant decision design

- Workers in Amazon's Mechanical Turk aim to:
  - Complete the tasks they accept (otherwise, don't earn money)
  - Minimize the time and effort in each task (each accepted task has an opportunity cost)
- Our message to participants:
  - “You may skip a game. If you do, we will assign you another”
- The decision was designed to gamble time/money for security:
  - Install → Take small risk, play the game, finish sooner
  - Not install → Not take any risks, not play the game, waste time

Results are encouraging

- 2,227 participants encountered dialogs
- Benign scenario
  - Installation not prevented
  - But some approaches slowed people down
- Suspicious scenario
  - Our new dialogs reduced installations
  - Swipe, type, and delay were particularly effective

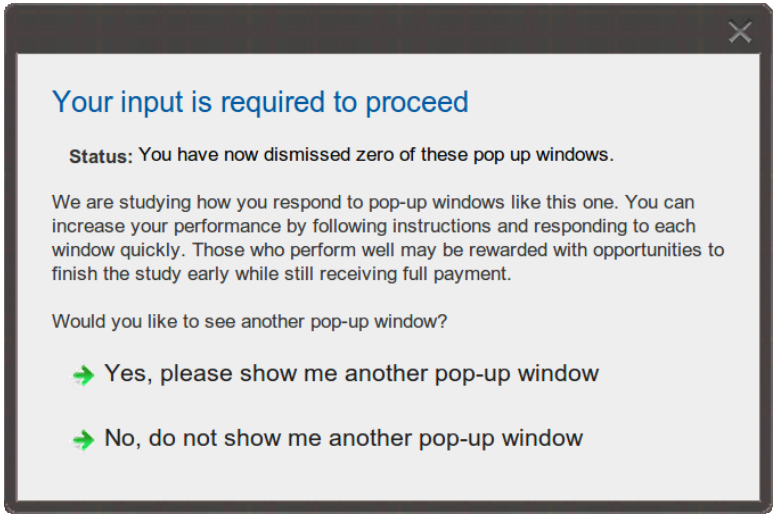
But what would happen if users saw these attractors repeatedly?

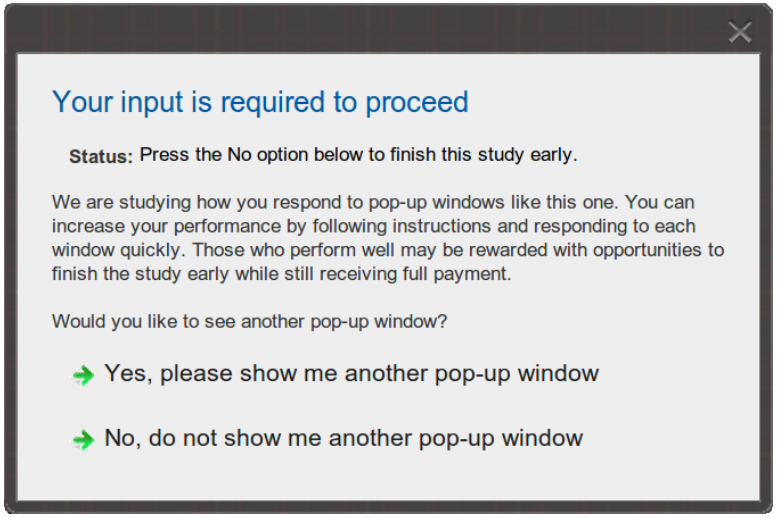
- Conducted more experiments
- Scenario in which participants had to dismiss a dialog repeatedly for several minutes until the dialog changed
- Measured rate of compliance with changed dialog
- Showed that some attractors performed better than control in presence of habituation
- "Harder to Ignore?" paper: Can attractors actually eliminate or reduce effects of habituation?

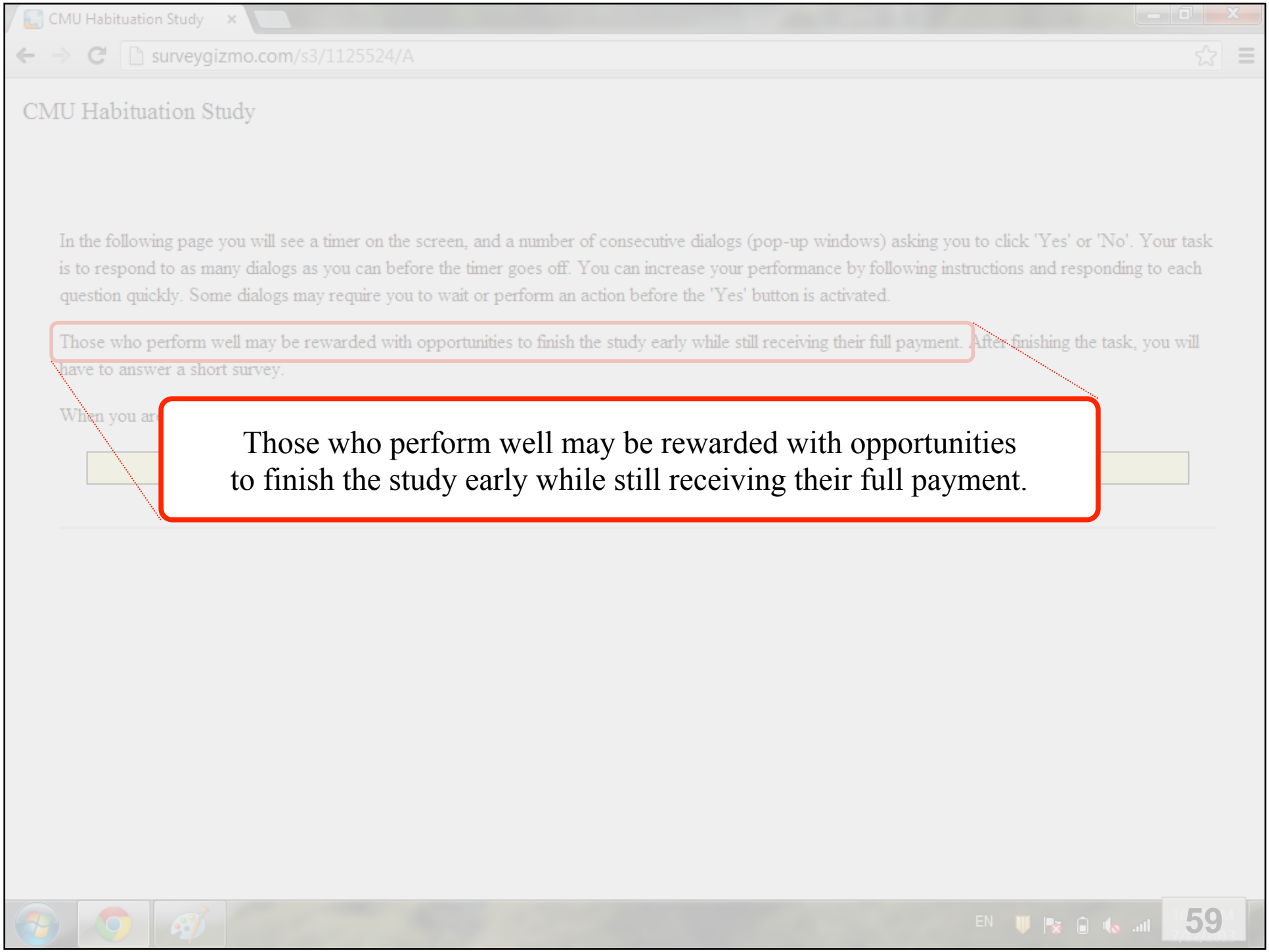
C. Bravo-Lillo, L. Cranor, S. Komanduri, S. Schechter, M. Sleeper. **Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It.** SOUPS 2014.

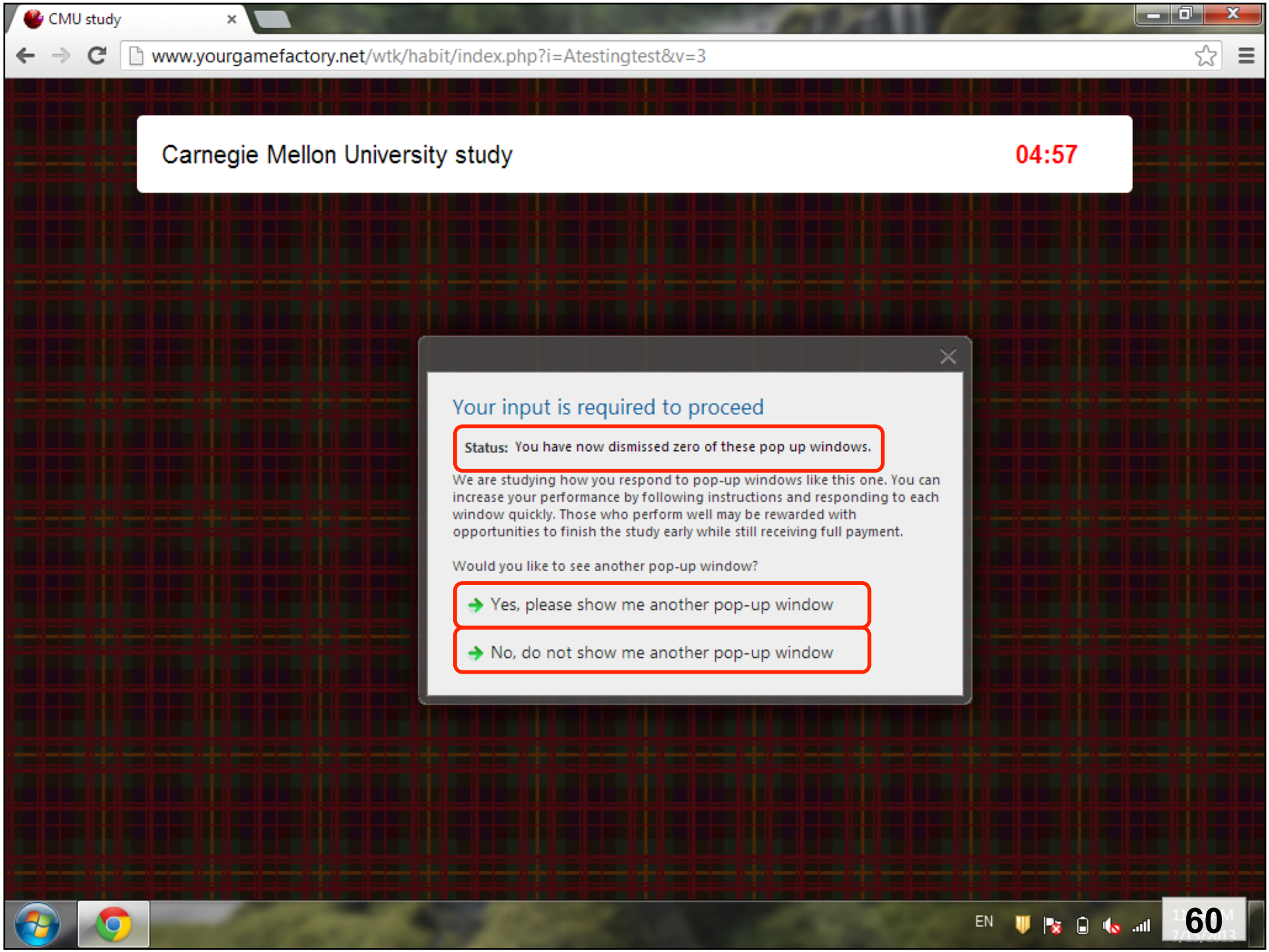
Habituation experiment

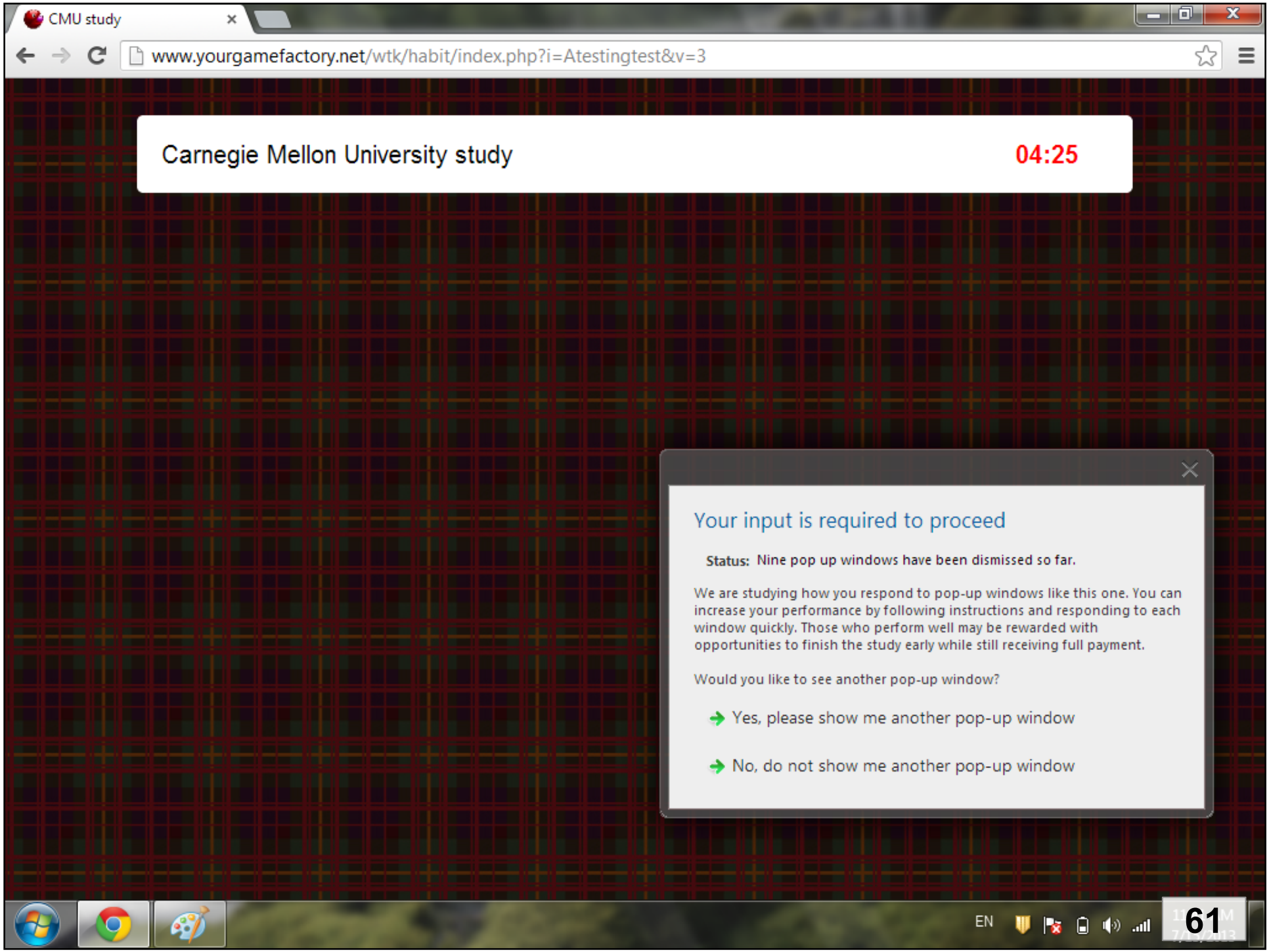
- Show a dialog repeatedly with irrelevant message
- Ask participants to click “Yes”
- Change salient field to “Click on No”
- Check if participants notice the change and click “No”

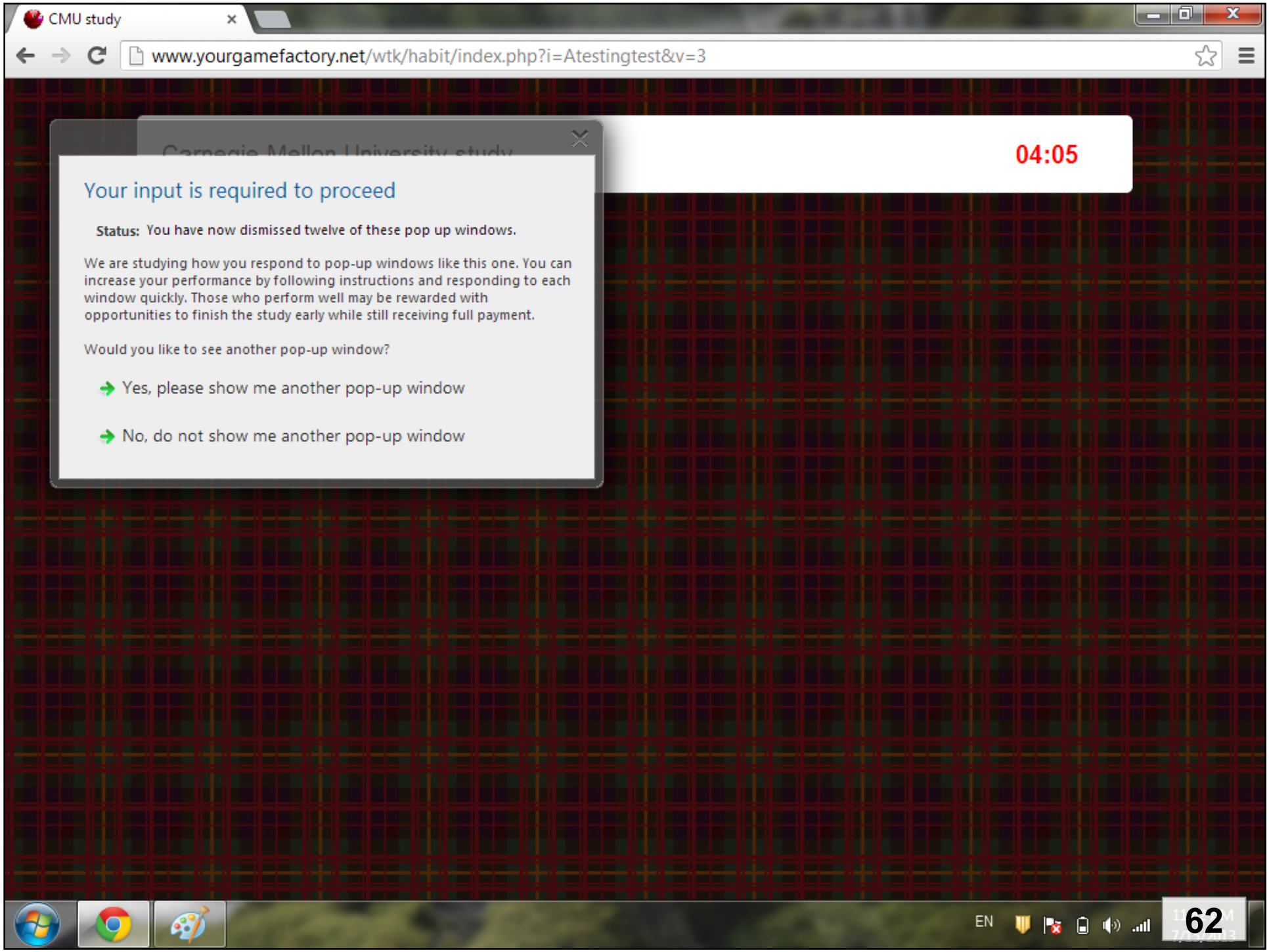


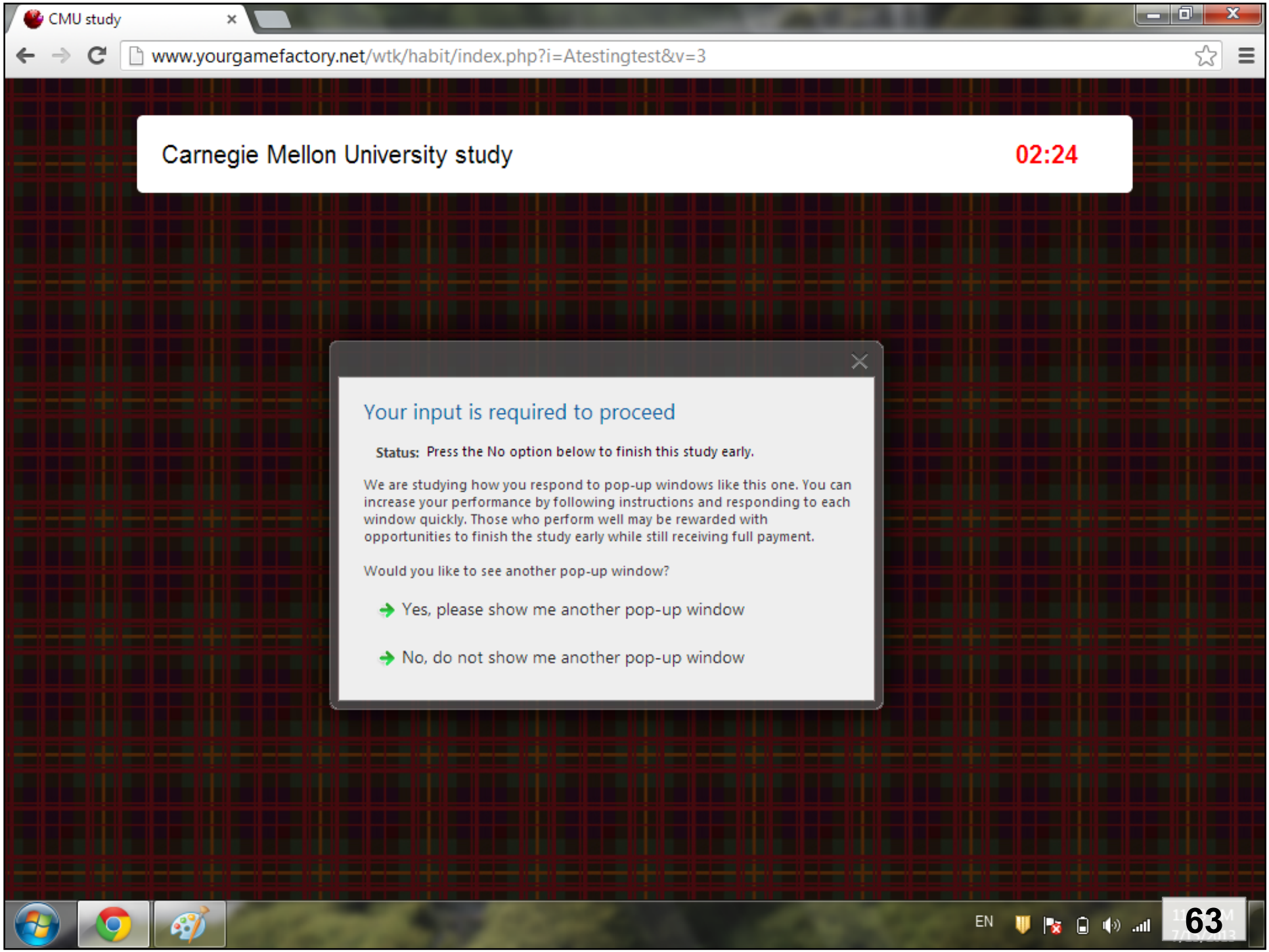


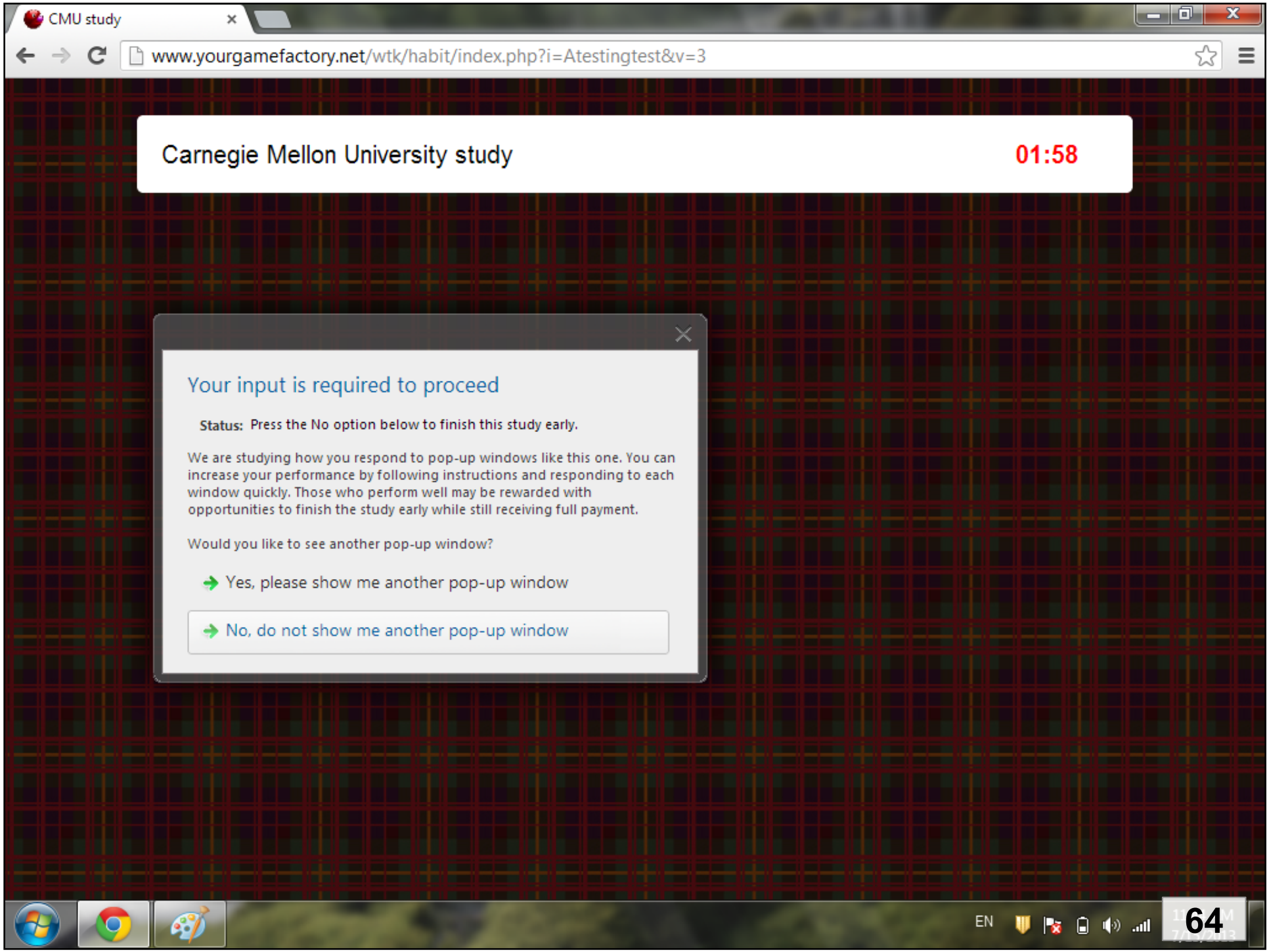

CMU Habituation Study
surveygizmo.com/s3/1125524/A
CMU Habituation Study
In the following page you will see a timer on the screen, and a number of consecutive dialogs (pop-up windows) asking you to click 'Yes' or 'No'. Your task is to respond to as many dialogs as you can before the timer goes off. You can increase your performance by following instructions and responding to each question quickly. Some dialogs may require you to wait or perform an action before the 'Yes' button is activated.
Those who perform well may be rewarded with opportunities to finish the study early while still receiving their full payment. After finishing the task, you will have to answer a short survey.
When you ar
Those who perform well may be rewarded with opportunities to finish the study early while still receiving their full payment.
EN
59

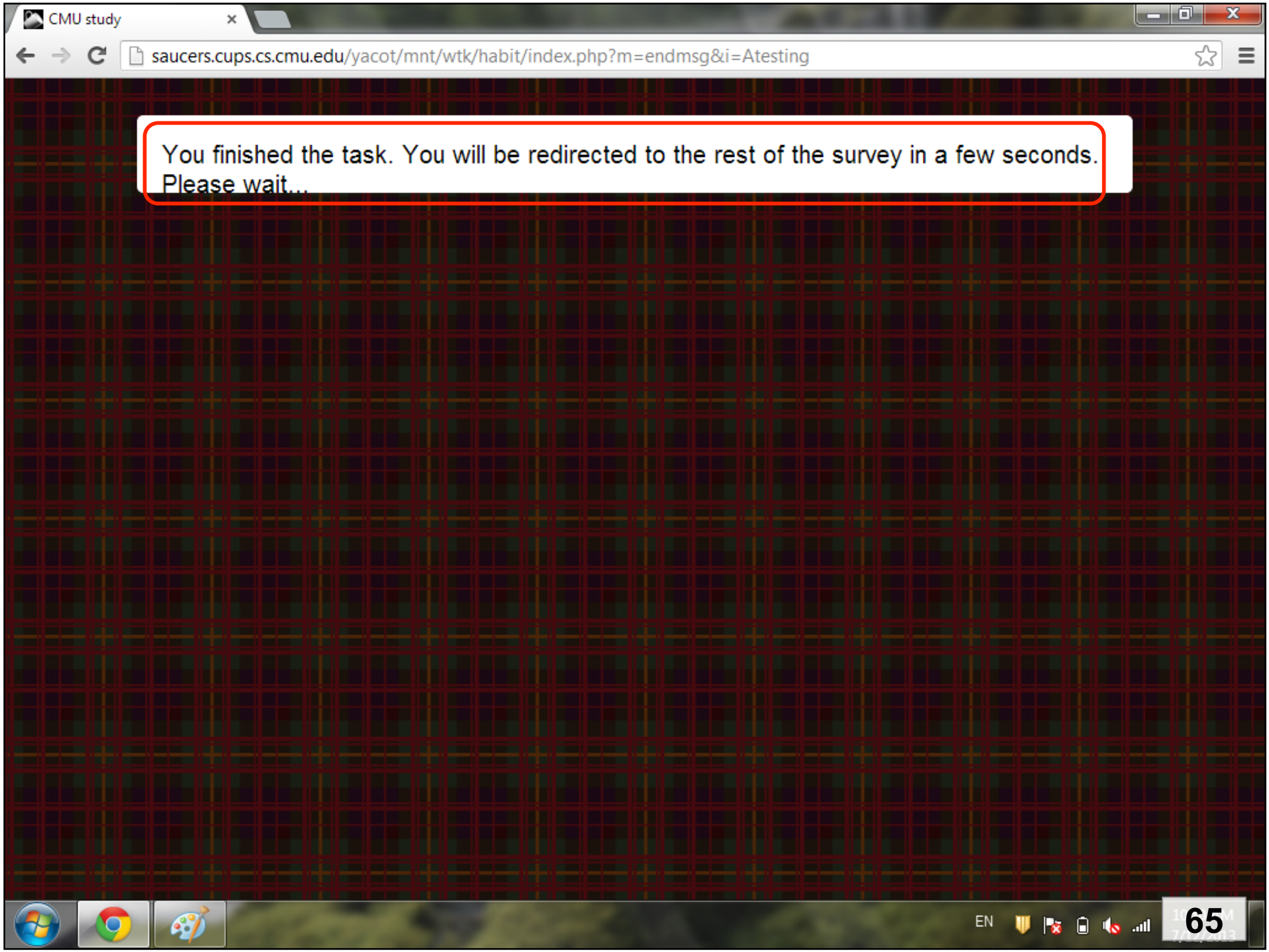

CMU study
www.yourgamefactory.net/wtk/habit/index.php?i=Atestingtest&v=3
Carnegie Mellon University study
04:57
Your input is required to proceed
Status: You have now dismissed zero of these pop up windows.
We are studying how you respond to pop-up windows like this one. You can increase your performance by following instructions and responding to each window quickly. Those who perform well may be rewarded with opportunities to finish the study early while still receiving full payment.
Would you like to see another pop-up window?
Yes, please show me another pop-up window
No, do not show me another pop-up window
EN


CMU study
www.yourgamefactory.net/wtk/habit/index.php?i=Atestingtest&v=3
Carnegie Mellon University study
04:25
Your input is required to proceed
Status: Nine pop up windows have been dismissed so far.
We are studying how you respond to pop-up windows like this one. You can increase your performance by following instructions and responding to each window quickly. Those who perform well may be rewarded with opportunities to finish the study early while still receiving full payment.
Would you like to see another pop-up window?
Yes, please show me another pop-up window
No, do not show me another pop-up window
EN


CMU study
www.yourgamefactory.net/wtk/habit/index.php?i=Atestingtest&v=3
04:05
Your input is required to proceed
Status: You have now dismissed twelve of these pop up windows.
We are studying how you respond to pop-up windows like this one. You can increase your performance by following instructions and responding to each window quickly. Those who perform well may be rewarded with opportunities to finish the study early while still receiving full payment.
Would you like to see another pop-up window?
Yes, please show me another pop-up window
No, do not show me another pop-up window
EN


CMU study
www.yourgamefactory.net/wtk/habit/index.php?i=Atestingtest&v=3
Carnegie Mellon University study
02:24
Your input is required to proceed
Status: Press the No option below to finish this study early.
We are studying how you respond to pop-up windows like this one. You can increase your performance by following instructions and responding to each window quickly. Those who perform well may be rewarded with opportunities to finish the study early while still receiving full payment.
Would you like to see another pop-up window?
Yes, please show me another pop-up window
No, do not show me another pop-up window
EN


CMU study
www.yourgamefactory.net/wtk/habit/index.php?i=Atestingtest&v=3
Carnegie Mellon University study
01:58
Your input is required to proceed
Status: Press the No option below to finish this study early.
We are studying how you respond to pop-up windows like this one. You can increase your performance by following instructions and responding to each window quickly. Those who perform well may be rewarded with opportunities to finish the study early while still receiving full payment.
Would you like to see another pop-up window?
Yes, please show me another pop-up window
No, do not show me another pop-up window
EN

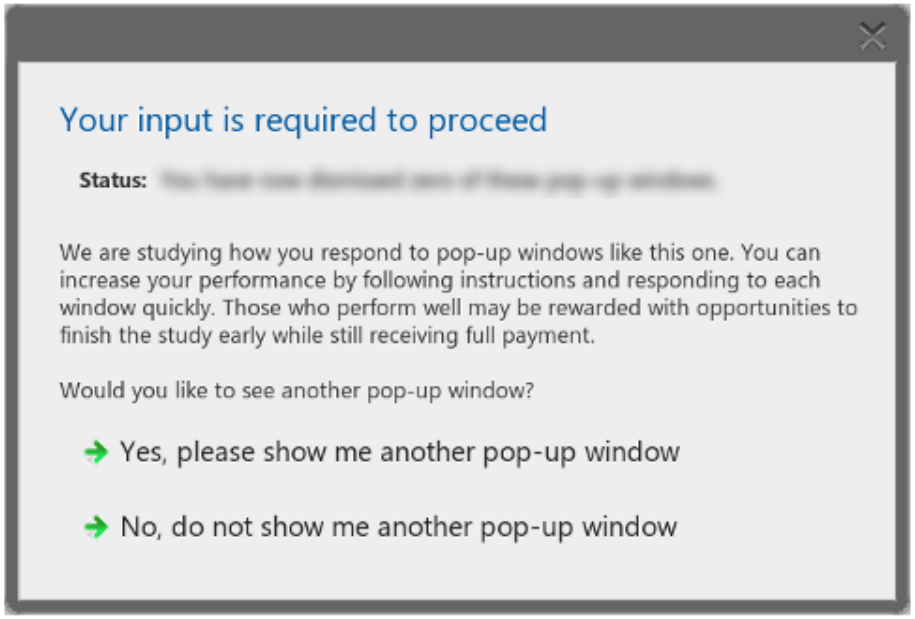

CMU study
saucers.cups.cs.cmu.edu/yacot/mnt/wtk/habit/index.php?m=endmsg&i=Atesting
You finished the task. You will be redirected to the rest of the survey in a few seconds. Please wait...
EN
65

CMU Pop-up dialogs stud ×

www.surveygizmo.com/s3/1126212/B

CMU Pop-up dialogs study

The image below corresponds to one of the dialogs you saw during this study:



1. Please type in the contents of the "Status:" field in the most-recently shown dialog, to the best of your memory. If you have no memory, please type "none": *

None

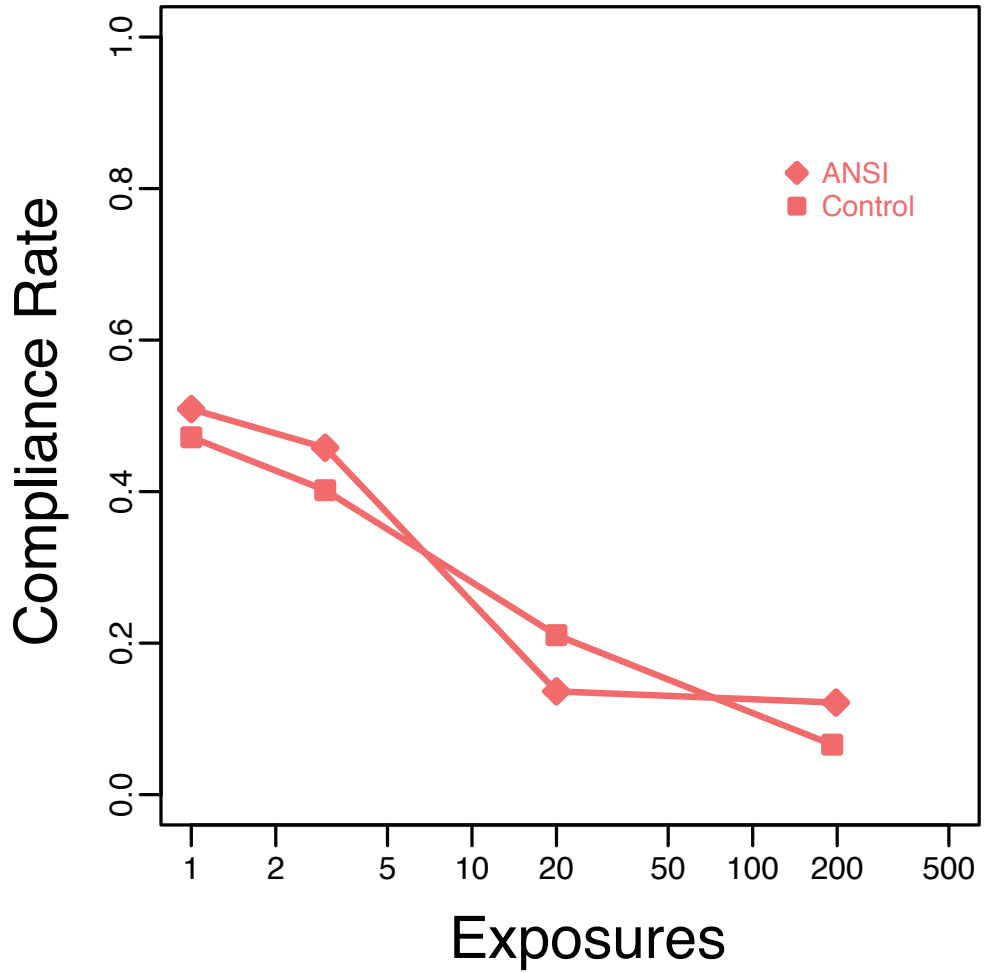
EN

“Harder to ignore” experimental design

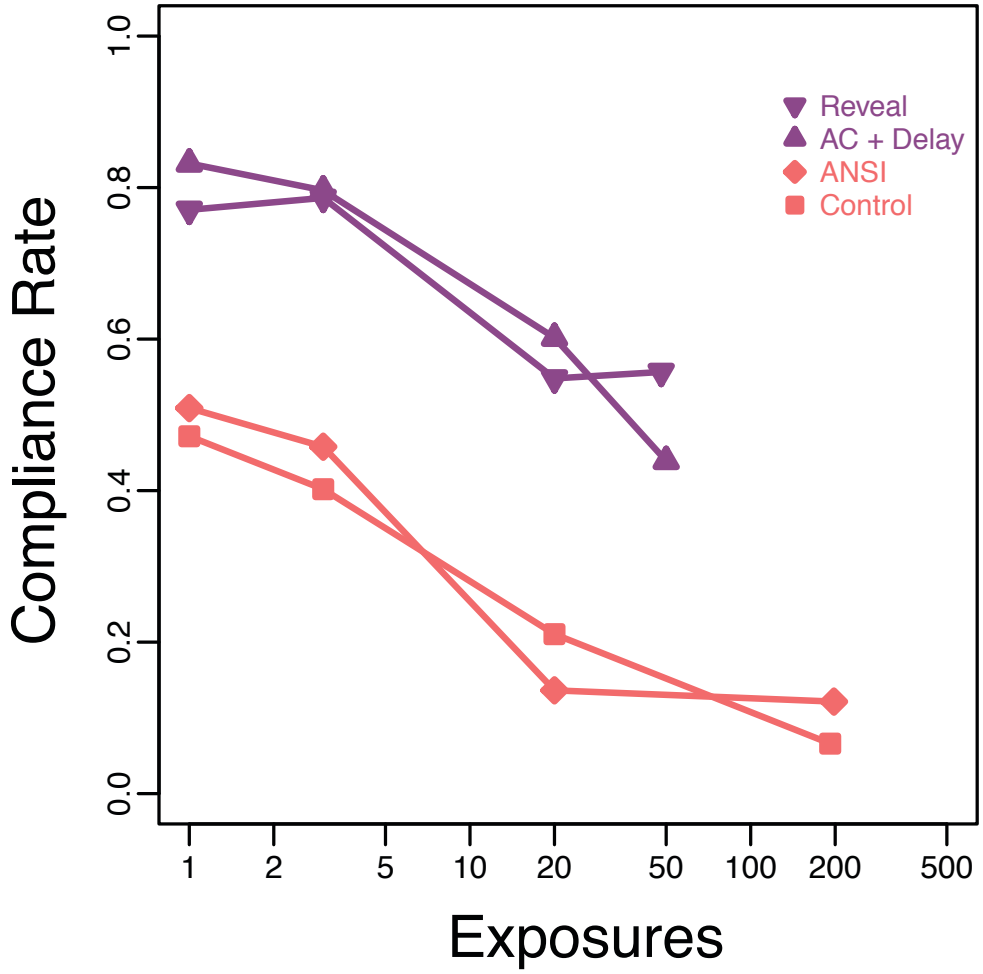
- {6 dialogs} x {4 exposure conditions} = 24 conditions
  - Dialogs: Control, Swipe, Type, AC + Delay, Reveal, ANSI
  - Exposure to 'irrelevant message': 1 exposure, 3 exposures, 20 exposures, 150 sec. of exposure
- Two phases:
  - Habituation phase: participants are shown irrelevant message, they could only click on “Yes”
  - Test phase: participants are asked to click “No”

Cristian Bravo-Lillo, Lorrie Faith Cranor, Saranga Komanduri, Stuart Schechter, and Manya Sleeper. Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It. SOUPS '14.

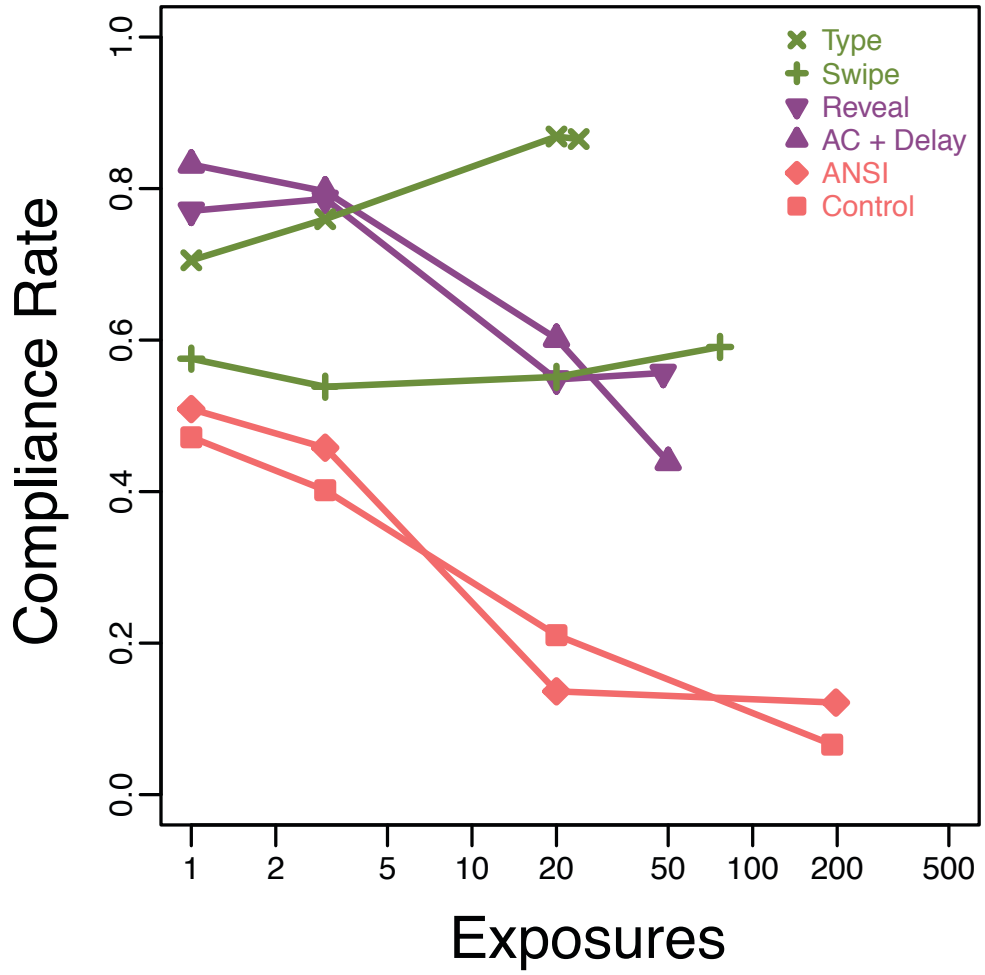
Control and ANSI decline with habituation



Reveal and AC+Delay start out better, decline with habituation



Swipe and Type are resilient to habituation



Could not predict difference between green and purple lines from previous experiments

NEAT and SPRUCE (from Microsoft)

Rob Reeder, Ellen Cram Kowalczyk, and Adam Shostack. Poster: Helping engineers design NEAT security warnings. SOUPS 2011.

http://cups.cs.cmu.edu/soups/2011/posters/soups_posters-Reeder.pdf

- NEAT – 4 questions to ask when you design a security or privacy UX
- SPRUCE – 6 elements to include in a security or privacy UX
  - Good advice, but sometimes it may be better to keep it short and simple rather than include all 6 elements

Microsoft

Ask yourself: Is your security or privacy UX:

NECESSARY? Can you change the architecture to eliminate or defer this user decision?

EXPLAINED? Does your UX present all the information the user needs to make this decision? **Have you followed SPRUCE? (see back)**

ACTIONABLE? Have you determined a set of steps the user will realistically be able to take to make the decision correctly?

TESTED? Have you checked that your UX is NEAT for all scenarios, both benign and malicious?

NEAT

When you involve the user in a NEAT security or privacy decision, explain the decision using these 6 elements:

SOURCE: State who or what is asking the user to make a decision

PROCESS: Give the user actionable steps to follow to make a good decision

RISK: Explain what bad thing could happen if the user makes the wrong decision

UNIQUE KNOWLEDGE user has: Tell the user what information they bring to the decision

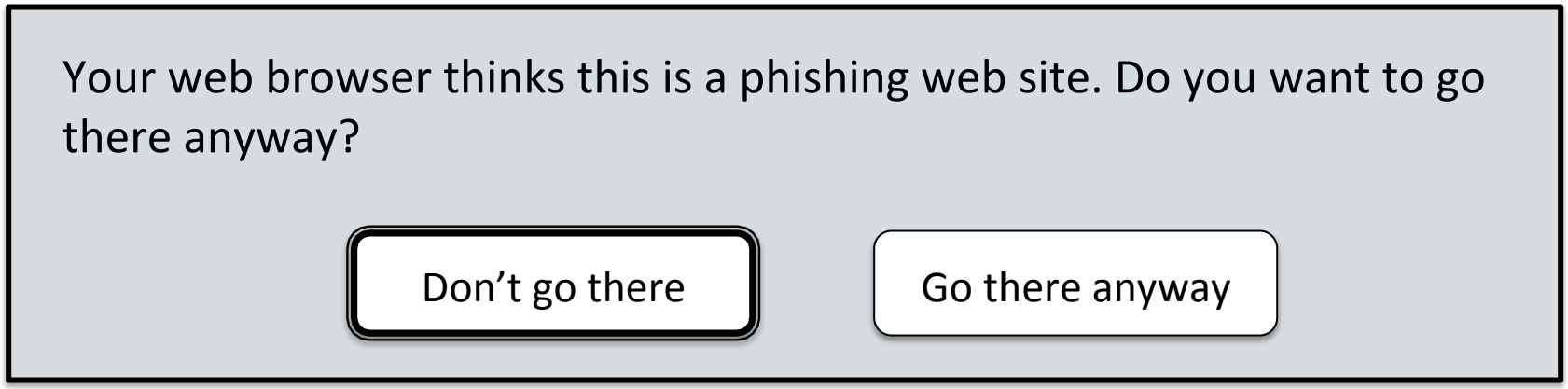
CHOICES: List available options and clearly recommend one

EVIDENCE: Highlight information the user should factor in or exclude in making the decision

SPRUCE

For more info, contact **neatux@microsoft.com**

Analyze with NEAT SPRUCE



- Necessary
- Explained
- Actionable
- Tested

- Source
- Process
- Risk
- Unique knowledge
- Choices
- Evidence

Class assignment

- USB flash drives can spread infections in a number of ways. See http://www.cioinsight.com/security/the-dangers-of-unsecured-usb-drives
- Attackers may distribute infected flash drives by leaving them around where employees of a target company are likely to pick them up. In addition, a user who uses a flash drive to exchange files with another user whose machine is already infected, may pick up the infection on the flash drive and bring it to their own machine. Some companies are prohibiting their employees form using flash drives, but others are just asking their employees to be careful.
- Imagine a security tool that runs on a user's computer and monitors the USB ports, looking for programs that run automatically when a flash drive is plugged in. When an autorun program is detected it prevents it from running and displays a warning. The warning dialog offers users the option of letting the program run.
- Your first task (to be done in class) is to design the warning using the design tool at: http://saucers.cups.cs.cmu.edu/woda/
- You may do this yourself or work with someone else. If you are not in class, do this at home. Use the NEAT and SPRUCE guidelines as you develop your design.

Homework assignment

- Your next task (to be done at home and turned in with your homework) is to critique someone else's warning. Go to http://saucers.cups.cs.cmu.edu/woda/
- Critique the warning that was submitted immediately before yours. If you submitted the first one then critique the last warning submitted. Please write one bullet point addressing each of the NEAT and SPRUCE messages. Then briefly discuss any additional factors you think might be relevant that are not addressed by NEAT and SPRUCE.