11 – Security Warnings

Lorrie Cranor, Blase Ur, and Rich Shay

February 17, 2015

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

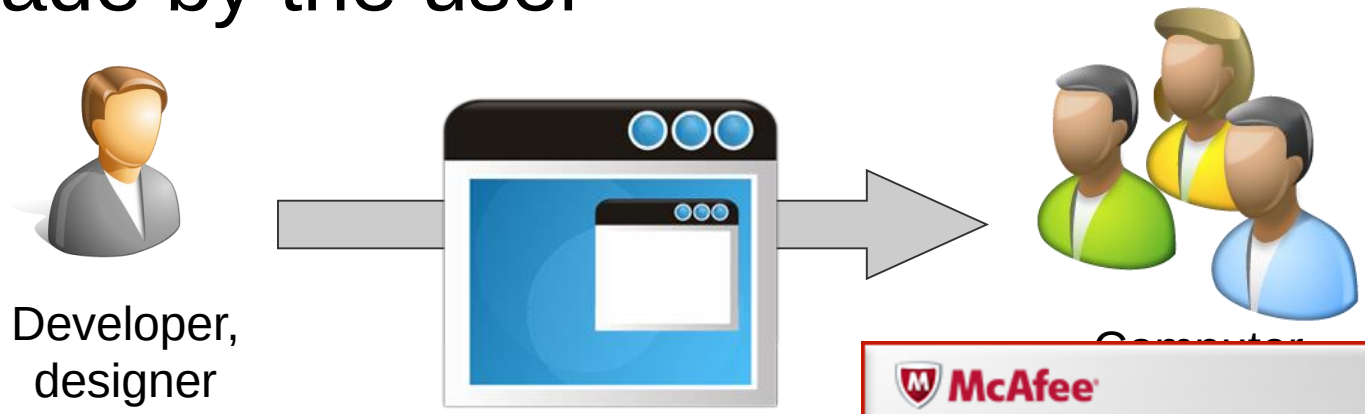
Carnegie Mellon University
CyLab

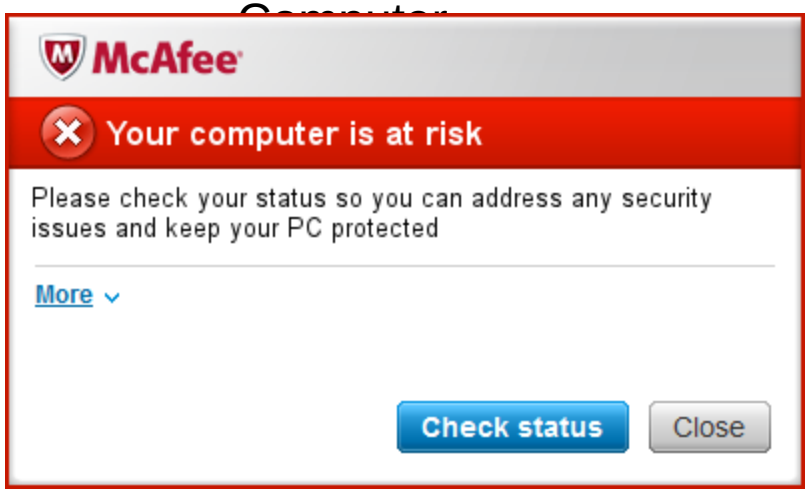
institute for SOFTWARE RESEARCH

Engineering & Public Policy

Computer security dialogs

- Small pop-up windows that interrupt the user to present a security decision to be made by the user





What is the problem?

- Dialogs communicate risks; if ignored, people expose themselves to avoidable harm

- Studying computer user reactions to security dialogs is extremely difficult

Participants behave differently in studies

- Schechter et al. (2007) showed participants behave differently when role playing
- Authors emphasized the importance of:
  - Ecological validity
  - Ethical concerns:
    - Researchers are obligated to minimize harm
    - Yet harm must be credible

Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. The Emperor's New Security Indicators: An evaluation of website authentication and

Lab studies are effective but costly

- Egelman et al. (2008) studied effectiveness of browser phishing dialogs:
  - Participants bought items with their credit cards, and were sent spear phishing emails
  - Experiment was effective but expensive, much effort, ethically challenging
  - Interesting observations about mental models associated with phishing warnings

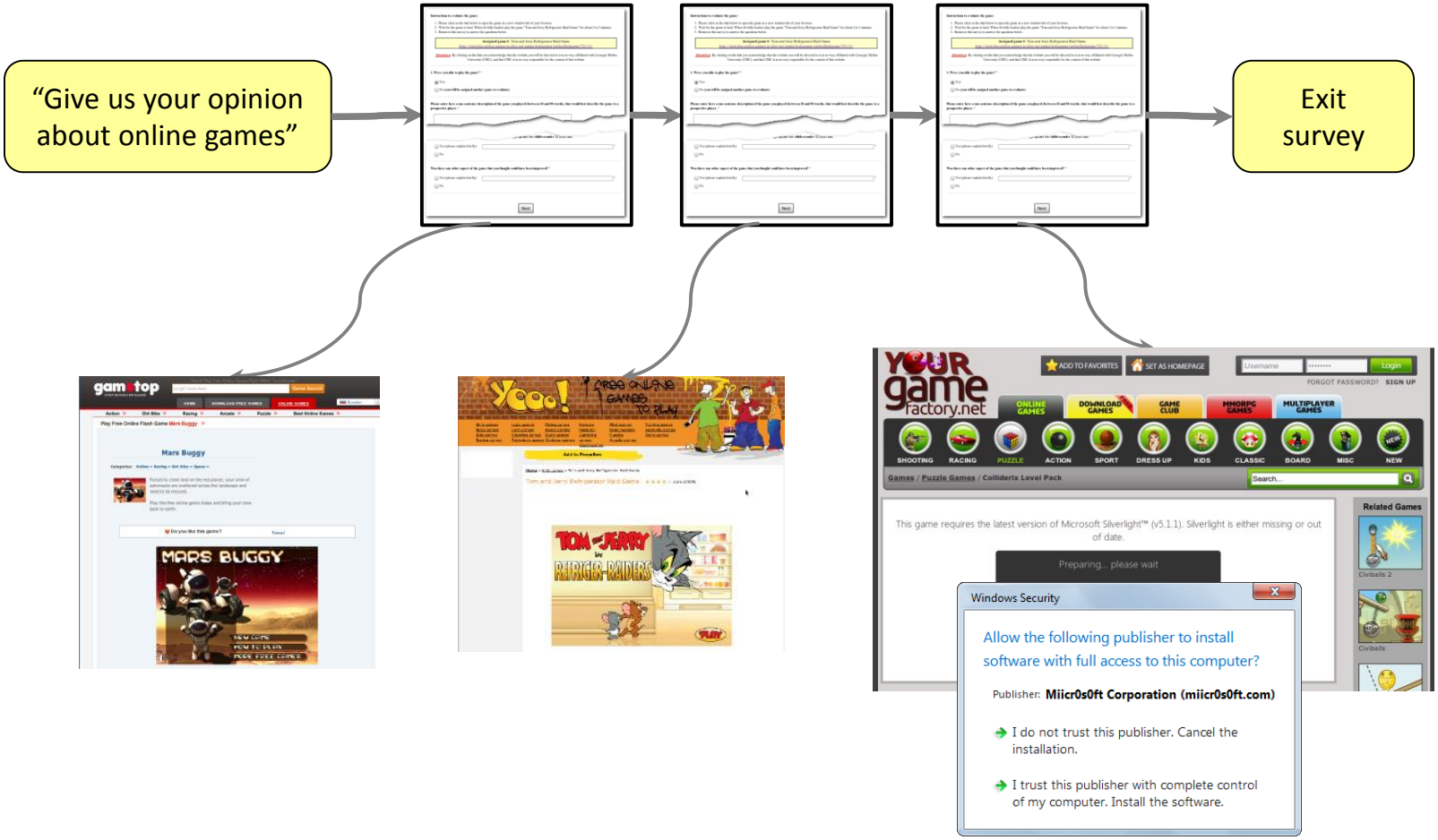
Ecological validity is crucial

- Sunshine et al. (2009) studied effectiveness of SSL certificate dialogs:
  - Realistic tasks with simulated man-in-the-middle attack, but:
    - Participants used lab computer
    - Browser choice was imposed on users
  - Required much negotiation with university lawyers

Methodology requirements

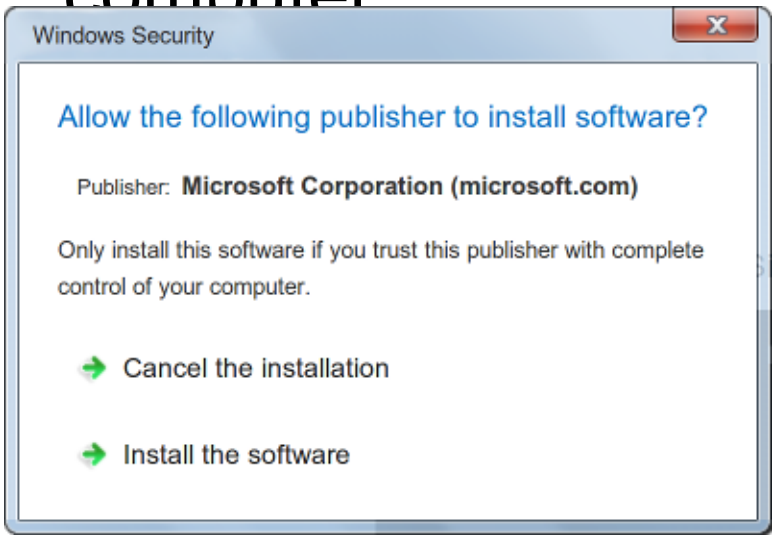
- Desired
  - Massive, inexpensive, quick data collection
  - Remote observation/recording/replay of user behavior
  - Flexibility to conduct different between-subjects experiments
- Avoid
  - Perceived safety due to “participation in experiment”
  - Incentives to behave differently than in real life
  - Risk higher than in real life

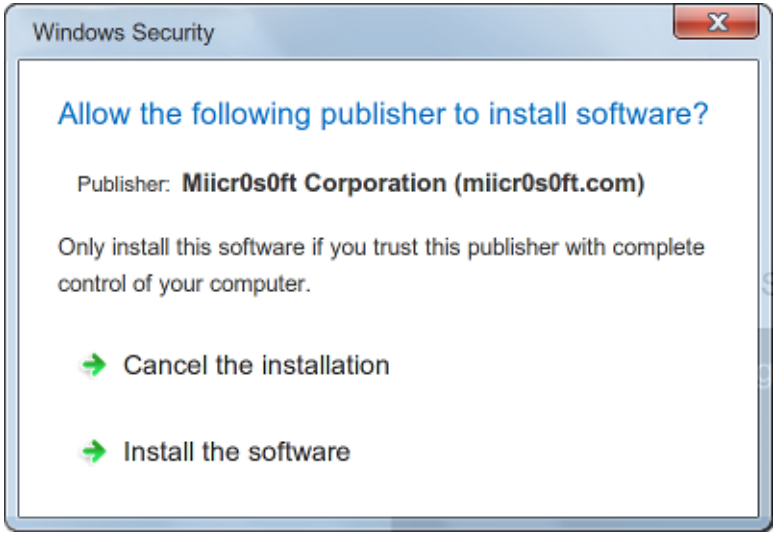
Online game ruse methodology



A software installation decision

- Triggered by OS when user installs an application
- Security advice: “Only install this software if you trust this publisher with complete control of your computer”





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

10

Online games evaluation survey

Carnegie Mellon University is conducting a study about online games evaluation. Please read the online consent below to participate in this study.

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

Online games evaluation survey

Instructions to evaluate the game:

1. Click on the link below to open the game. When the page loads, click on the button "Click to play online" on the left of your screen. Wait for the game to load.
2. When the game has loaded completely, play the game "Mars Buggy Online" for about 2 to 3 minutes.
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 to play the game? *

- ○ Yes
- ○ No **(you will be assigned another game to evaluate)**

Next

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

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

1. 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 buggy on mars has to collect astronauts.

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

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 visual content or language that might be inappropriate for children under 12 years old? *

- ○ Yes (please explain briefly) _____ *
- ◉ No

Was there any other aspect of the game that you thought could have been improved? *

- ○ Yes (please explain briefly) _____ *
- ◉ No

Next

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 link below to open the game.
2. Wait for the game to load. When it's fully loaded, play the game "Tom and Jerry Refrigerator Raid Game" for about 2 to 3 minutes.
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

Add to Favorites

Tom and Jerry Refrigerator Raid Game

stars (3973)

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)

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

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 link below to open the game.
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

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:

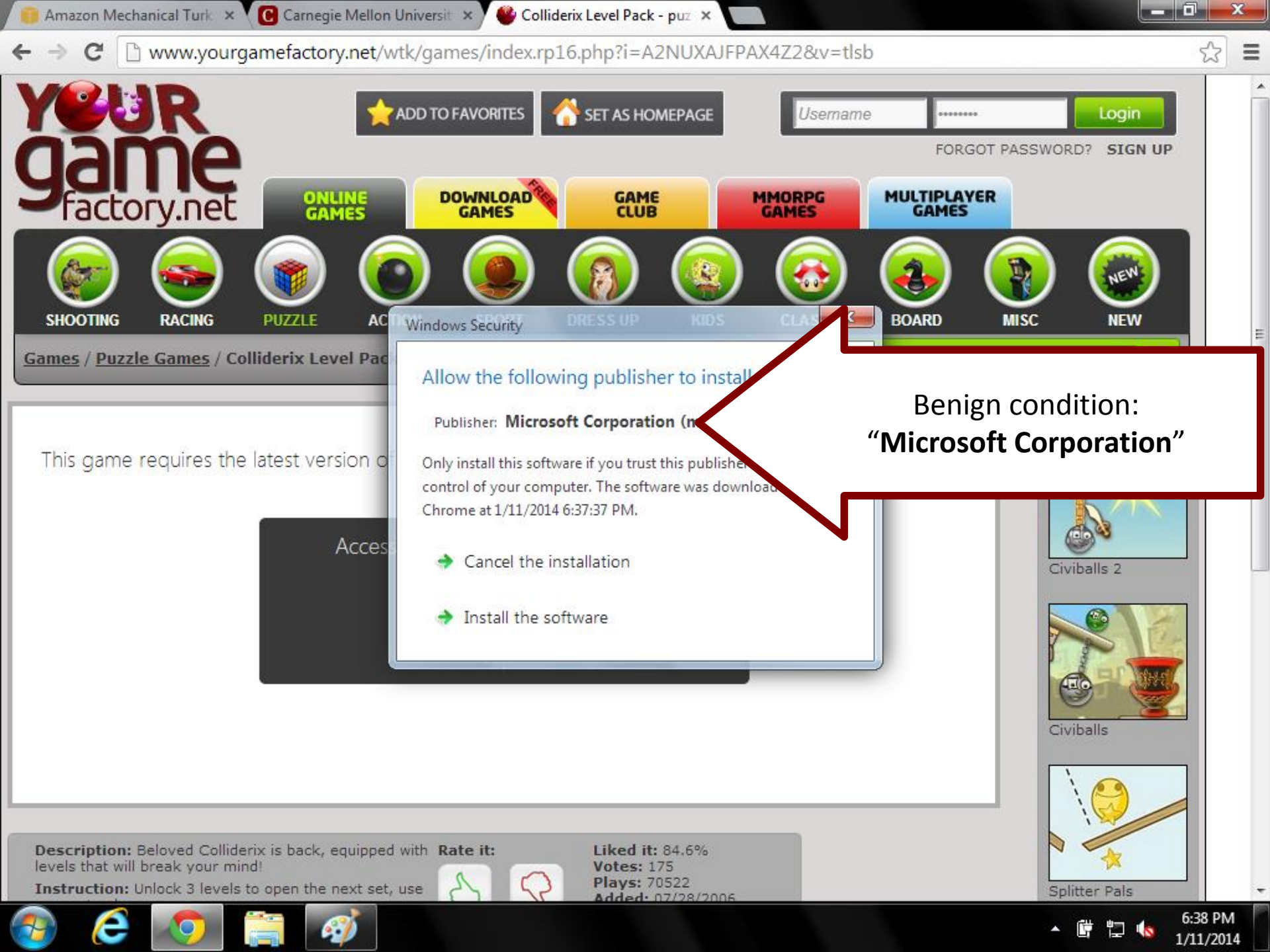
Liked it: 84.6%
Votes: 175
Plays: 70522
Added: 07/28/2006

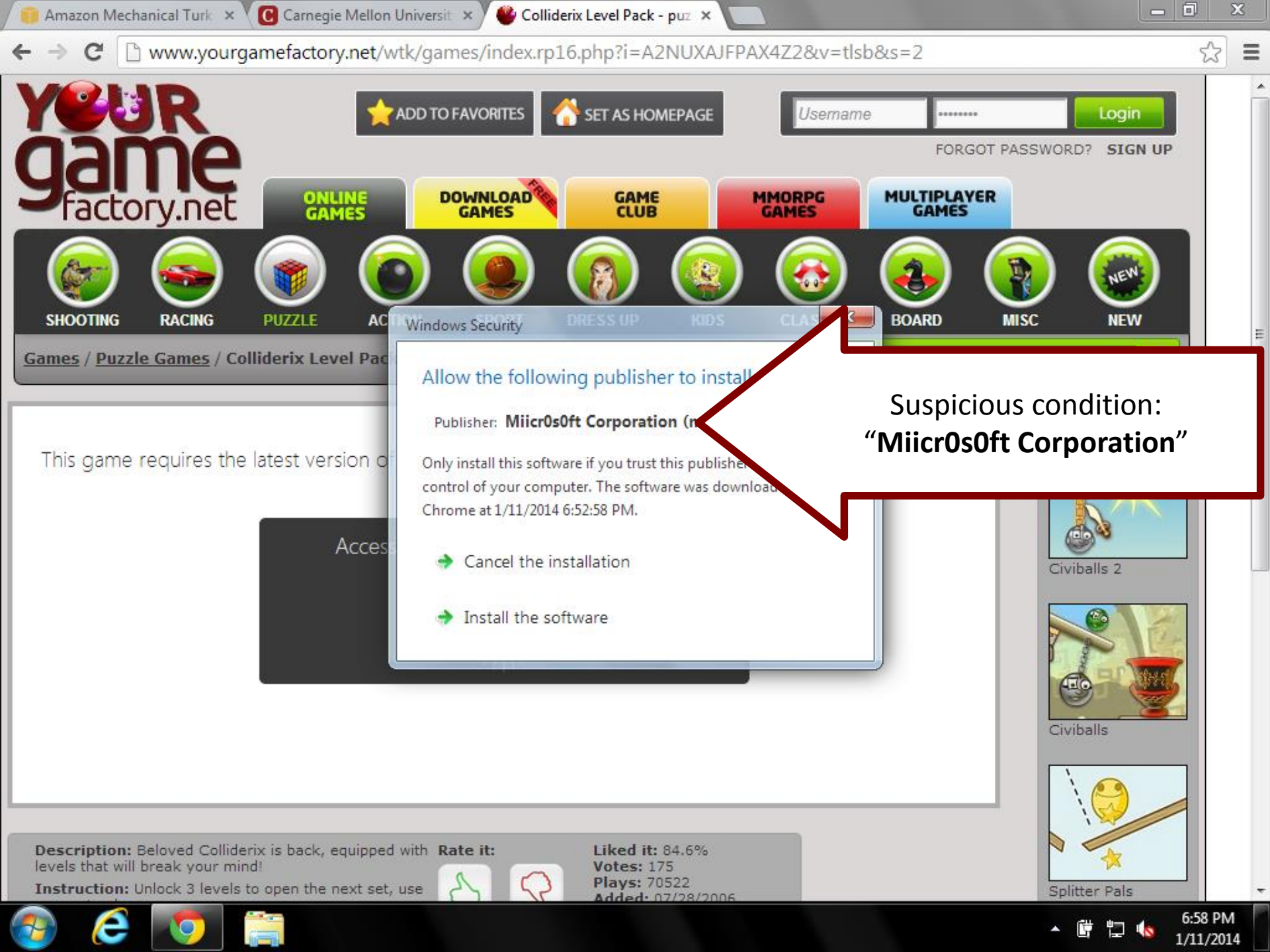
Related Games


Civiballs 2


Civiballs


Splitter Pals


Amazon Mechanical Turk
Carnegie Mellon Universit
Colliderix Level Pack - puz
www.yourgamefactory.net/wtk/games/index.rp16.php?i=A2NUXAJFPAX4Z2&v=tlsb
ADD TO FAVORITES
SET AS HOMEPAGE
Username
Login
FORGOT PASSWORD?
SIGN UP
ONLINE GAMES
DOWNLOAD GAMES
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
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
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

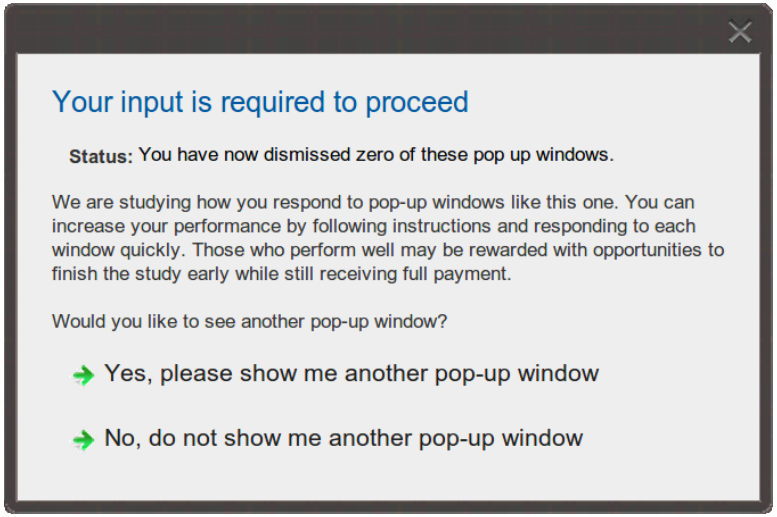

Amazon Mechanical Turk
Carnegie Mellon Universit
Colliderix Level Pack - puz
www.yourgamefactory.net/wtk/games/index.rp16.php?i=A2NUXAJFPAX4Z2&v=tlsb&s=2
ADD TO FAVORITES
SET AS HOMEPAGE
Username
Login
FORGOT PASSWORD?
SIGN UP
ONLINE GAMES
DOWNLOAD GAMES
GAME CLUB
MMORPG GAMES
MULTIPLAYER GAMES
SHOOTING
RACING
PUZZLE
BOARD
MISC
NEW
Games / Puzzle Games / Colliderix Level Pac
This game requires the latest version o
Windows Security
Allow the following publisher to install
Publisher: Miicr0s0ft Corporation (n
Only install this software if you trust this publisher
control of your computer. The software was downloa
Chrome at 1/11/2014 6:52:58 PM.
Cancel the installation
Install the software
Suspicious condition:
“Miicr0s0ft Corporation”
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
6:58 PM
1/11/2014

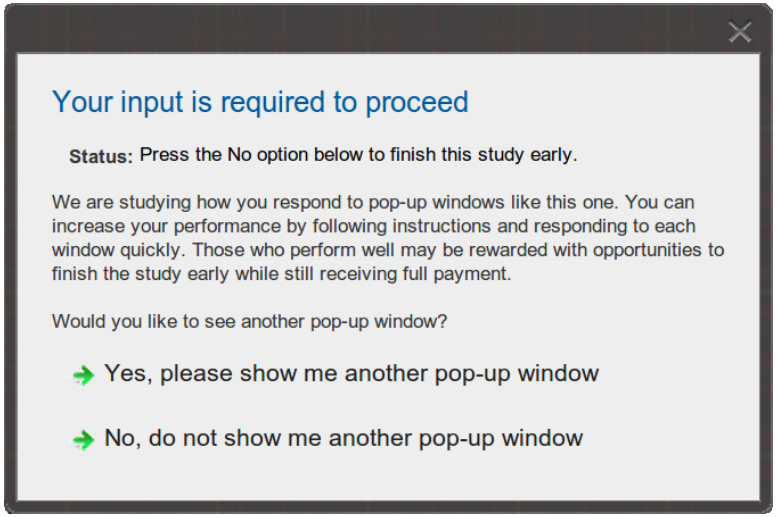
Habituation experiments

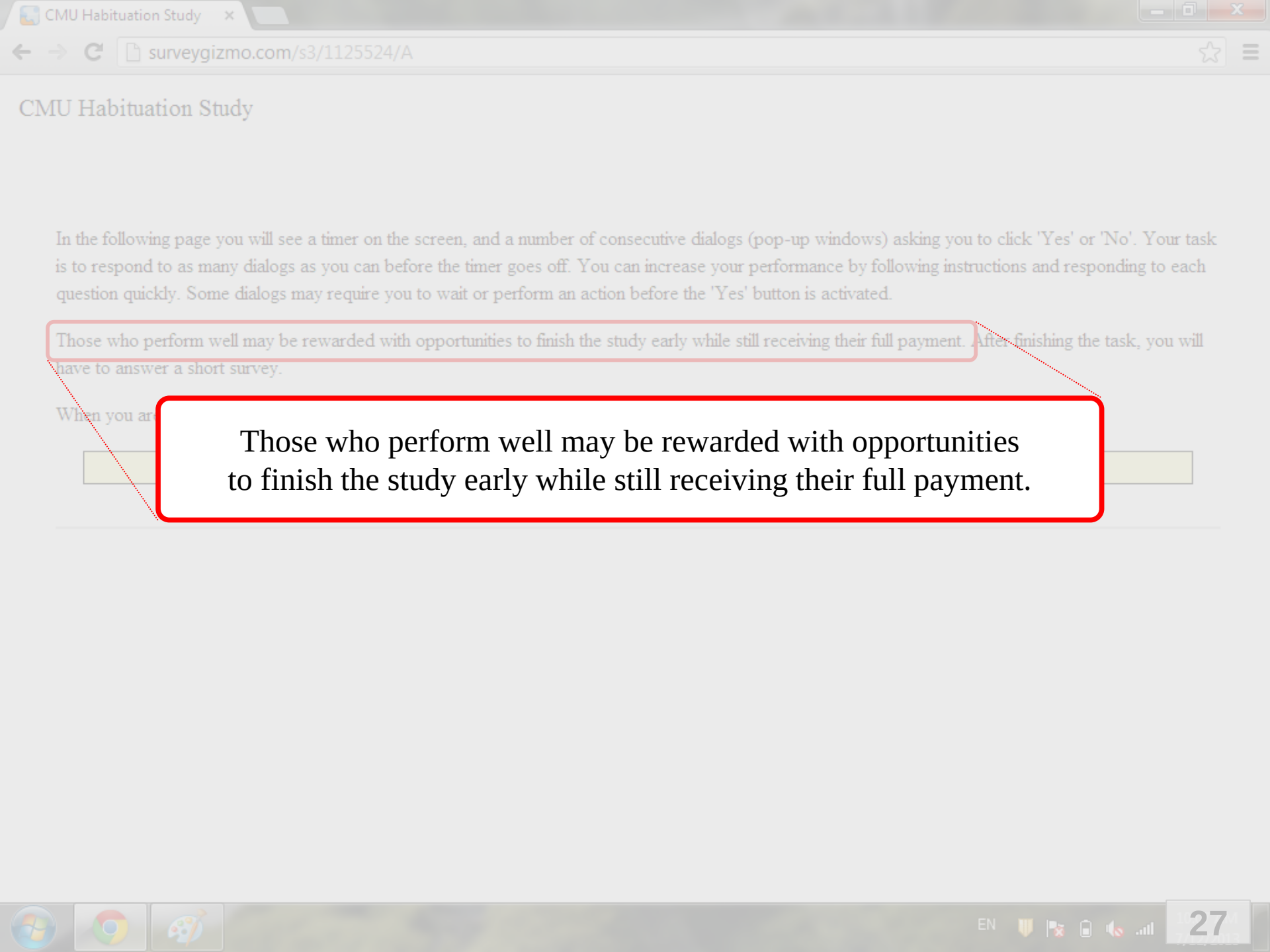
- “Your Attention Please” paper showed that some attractors performed better than control in presence of habituation
  - But those attractors also performed better without habituation
- Can attractors actually eliminate or reduce effects of habituation?
  - How can we test this

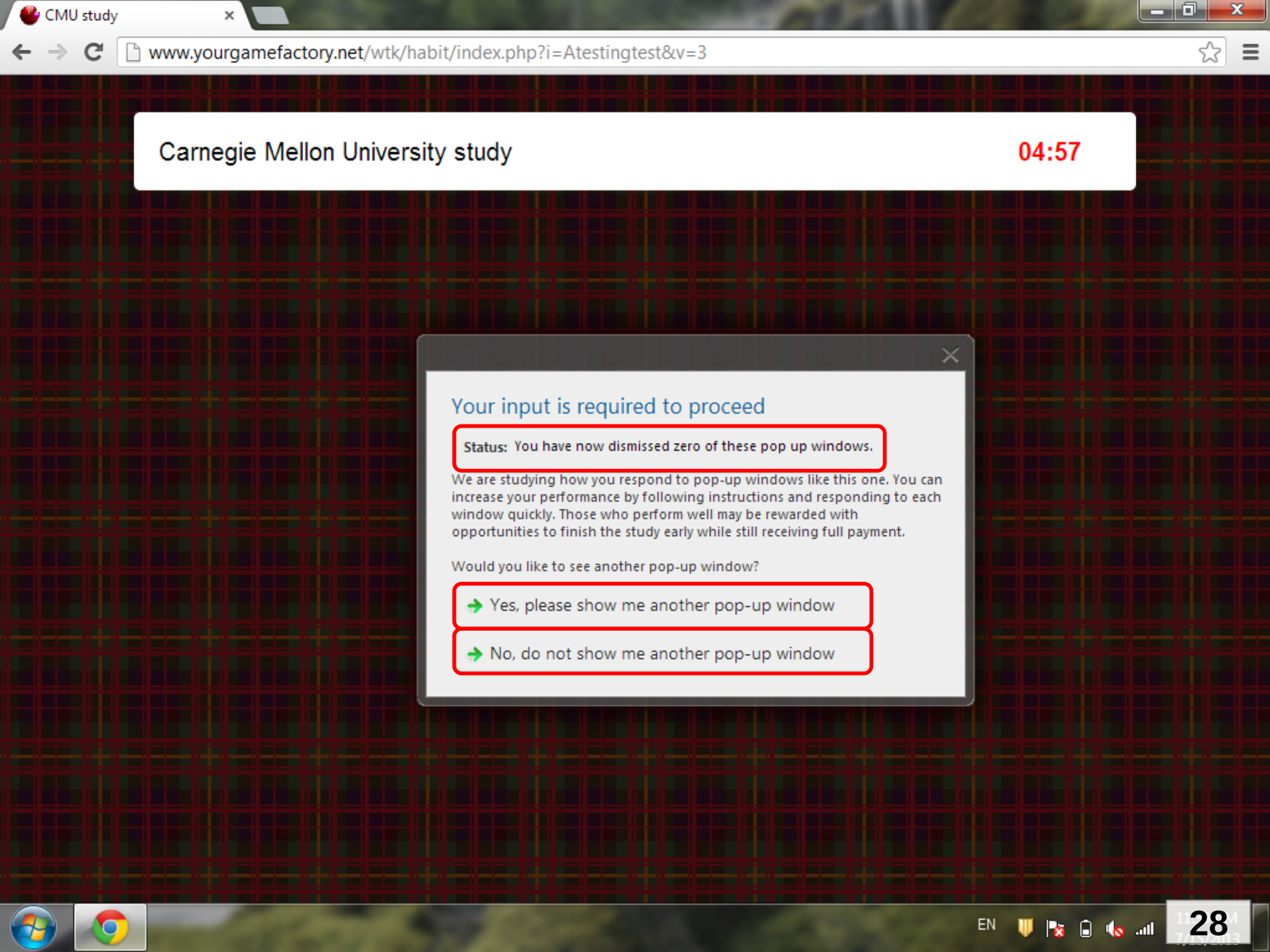
Habituation experiment

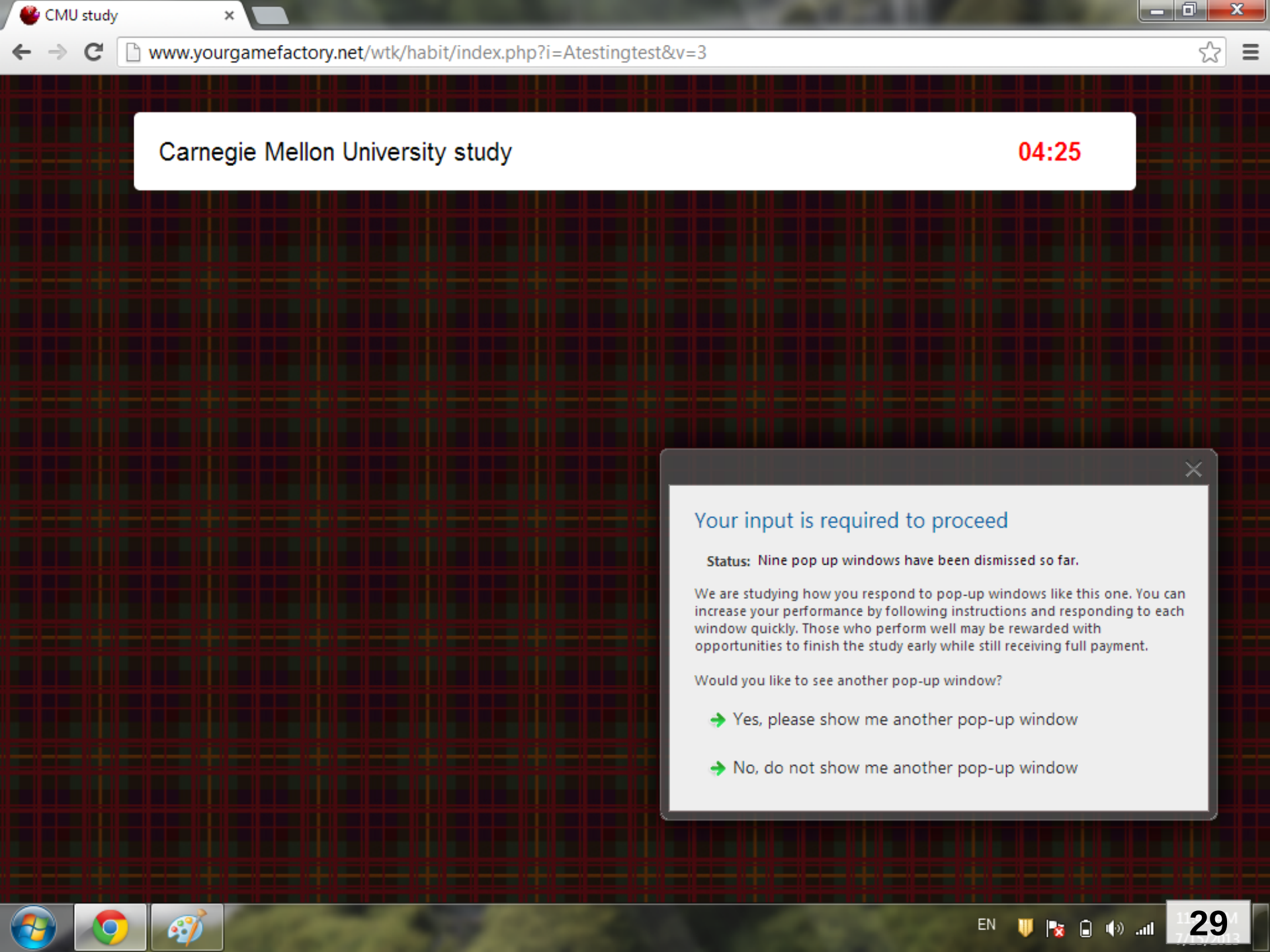
- Show a dialog repeatedly with irrelevant message
- Ask participants to click “Yes”
- Change salient field to “Click on No”
- Check if participants notice the change and click “No”

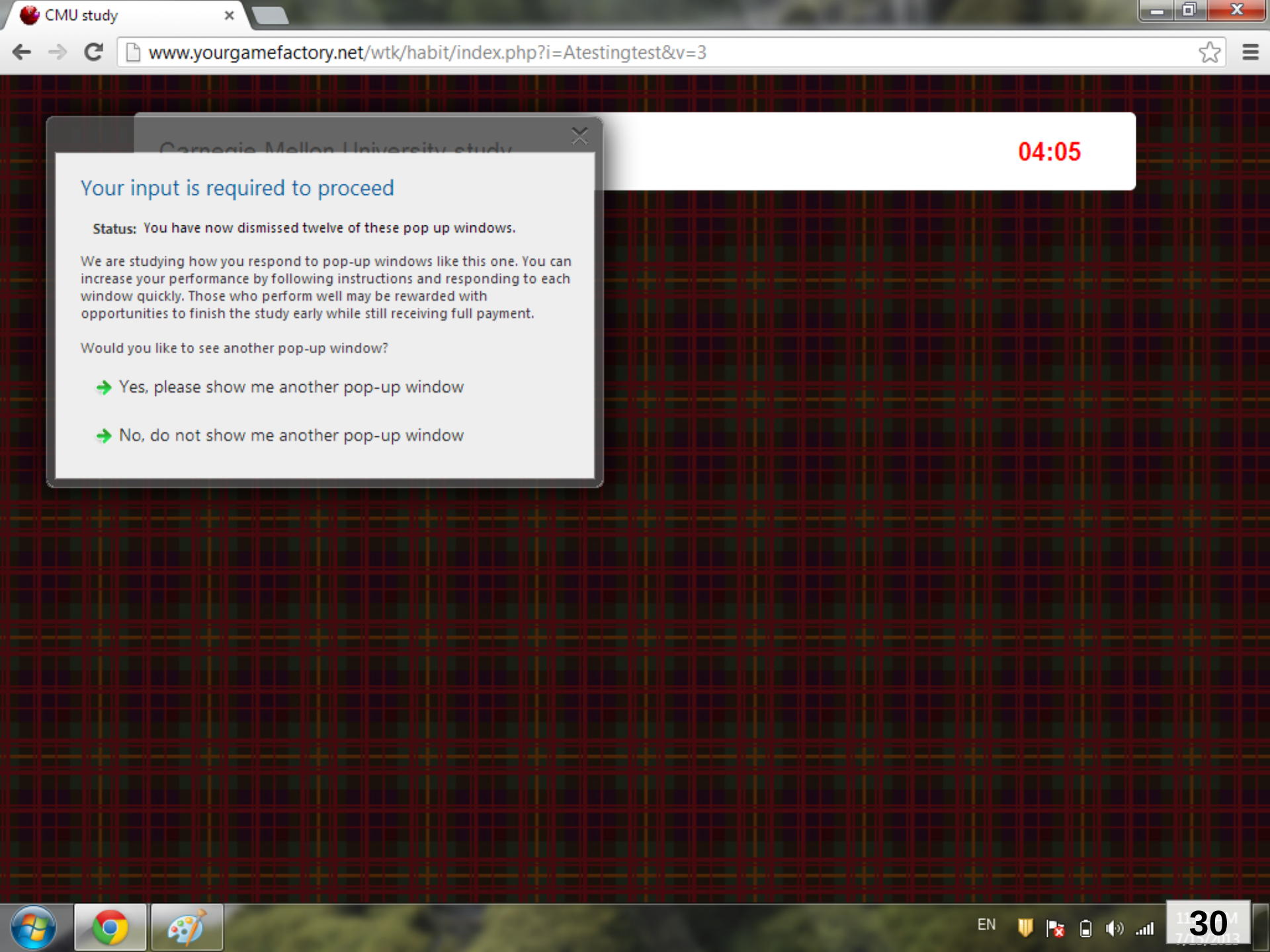


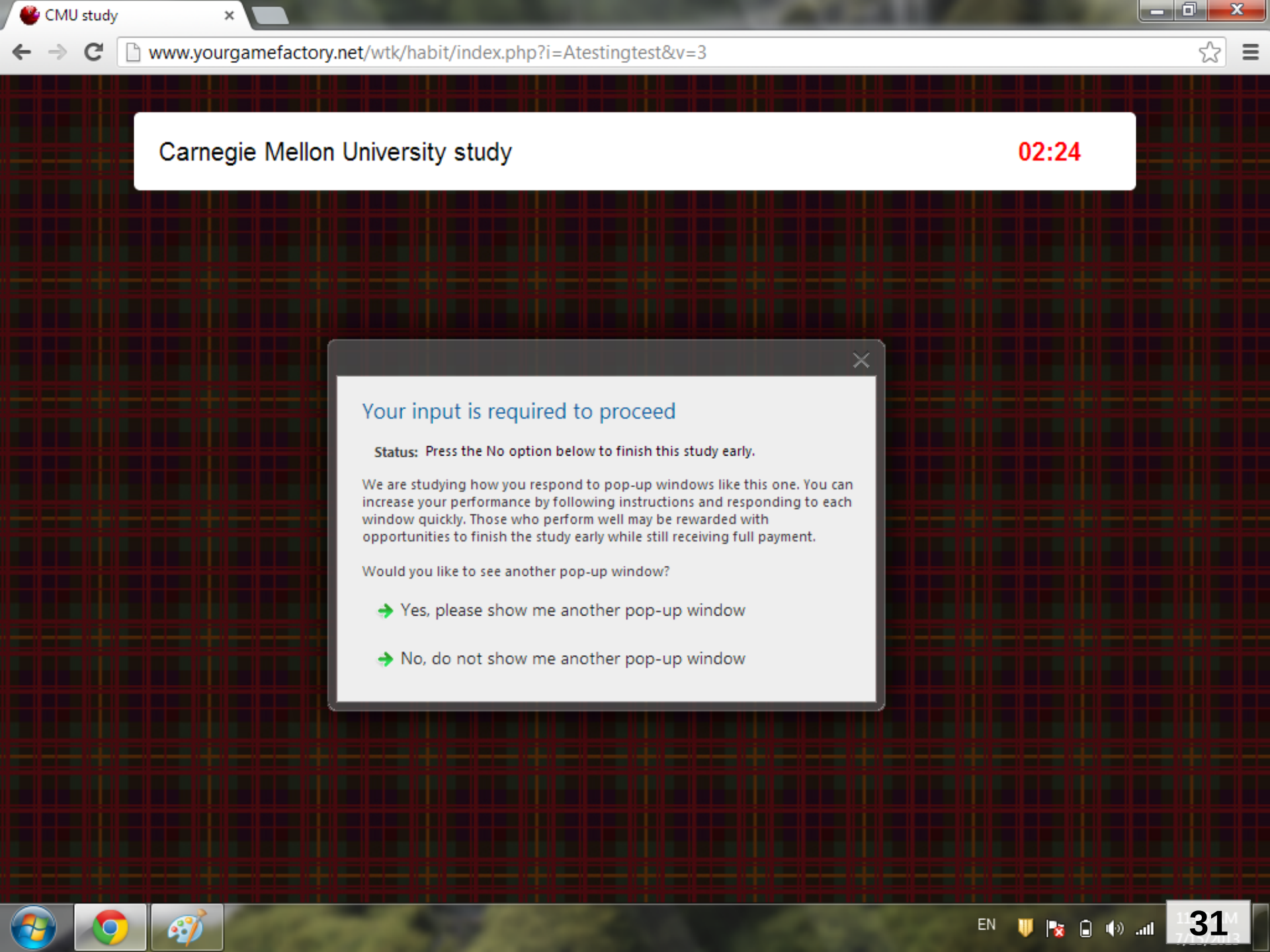


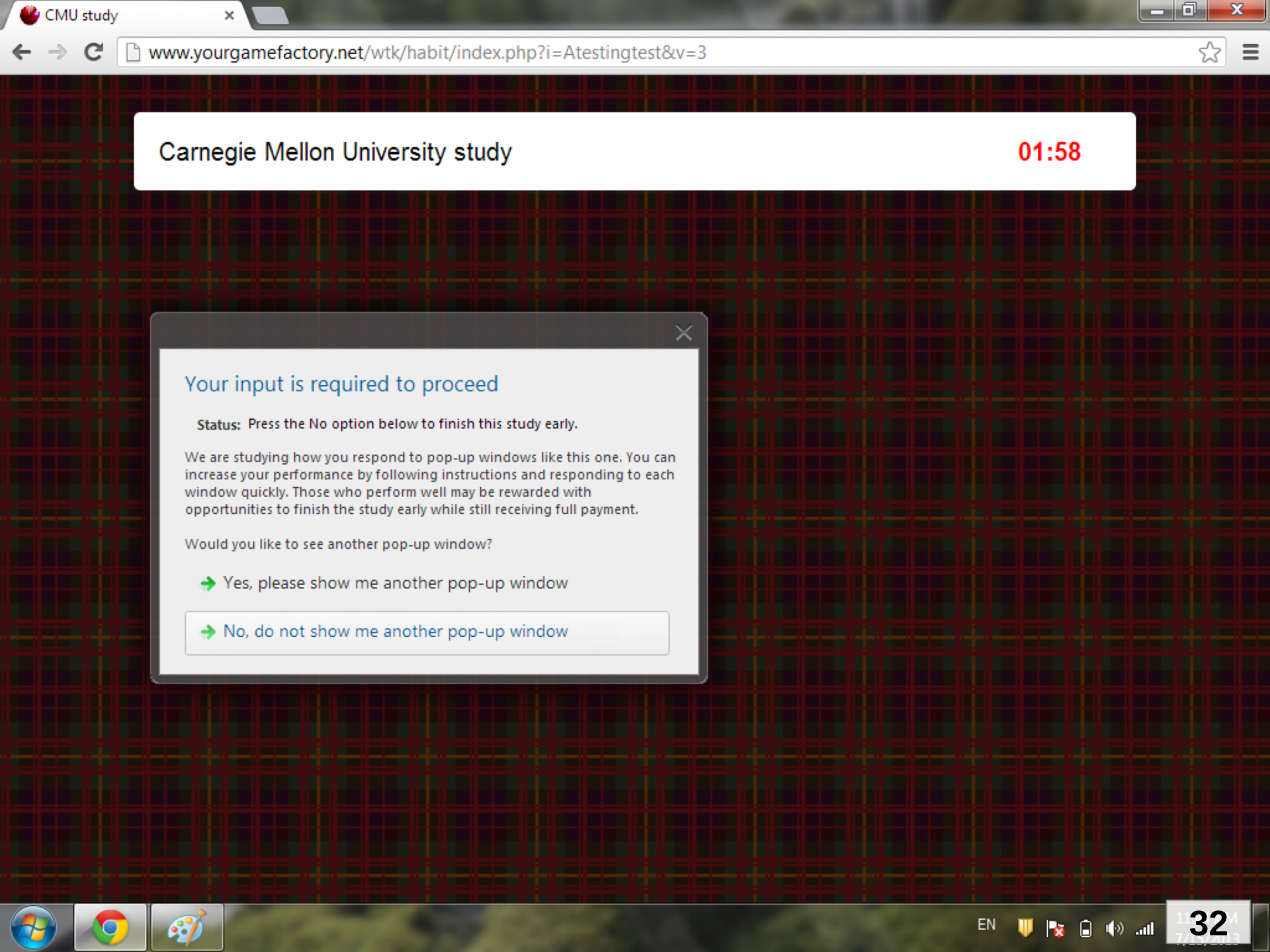

CMU Habituation Study
surveygizmo.com/s3/1125524/A
CMU Habituation Study
In the following page you will see a timer on the screen, and a number of consecutive dialogs (pop-up windows) asking you to click 'Yes' or 'No'. Your task is to respond to as many dialogs as you can before the timer goes off. You 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
27

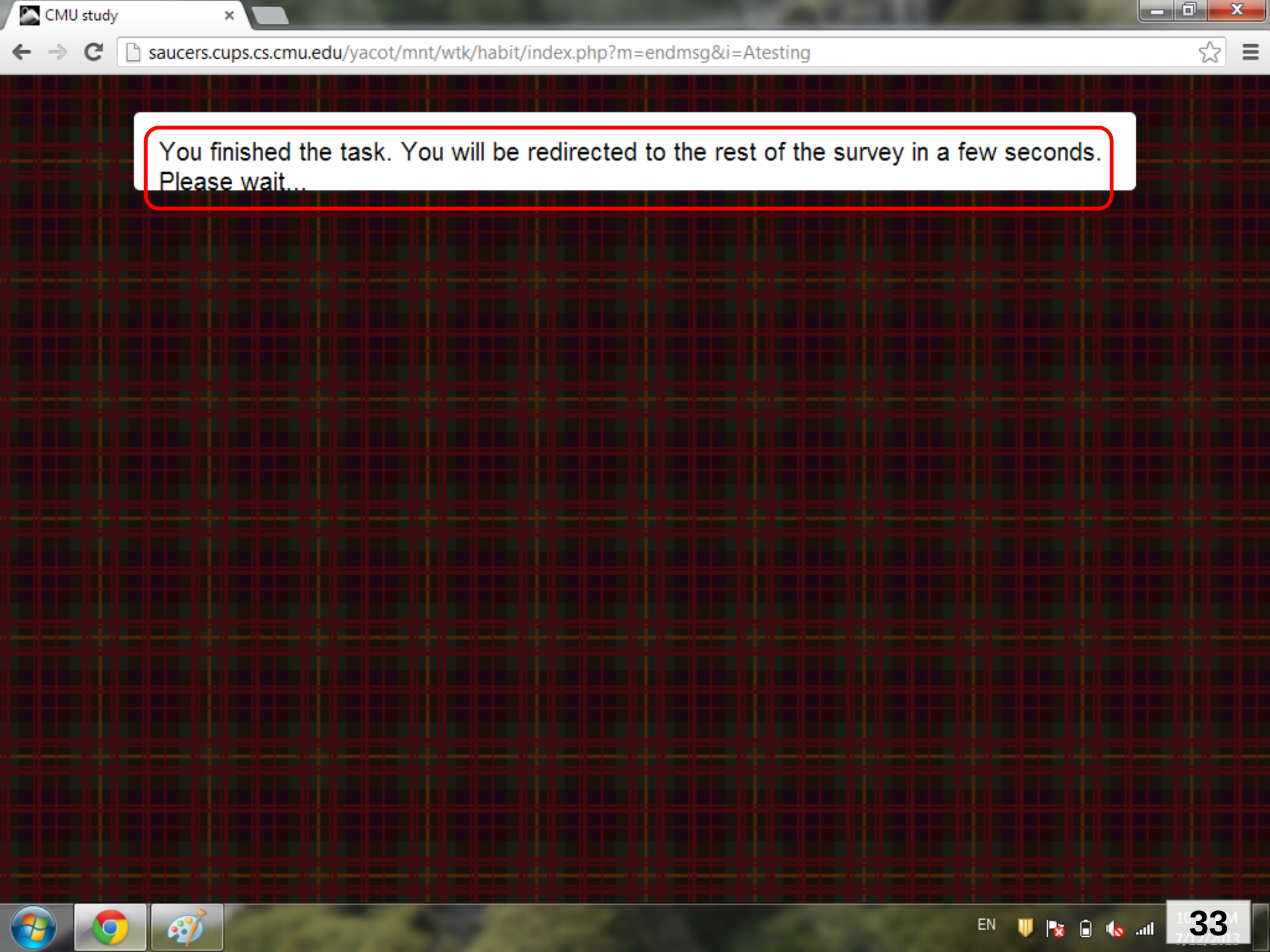

CMU study
www.yourgamefactory.net/wtk/habit/index.php?i=Atestingtest&v=3
Carnegie Mellon University study
04:57
Your input is required to proceed
Status: You have now dismissed zero of these pop up windows.
We are studying how you respond to pop-up windows like this one. You can increase your performance 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
28


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
29


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
30


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
31


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
32

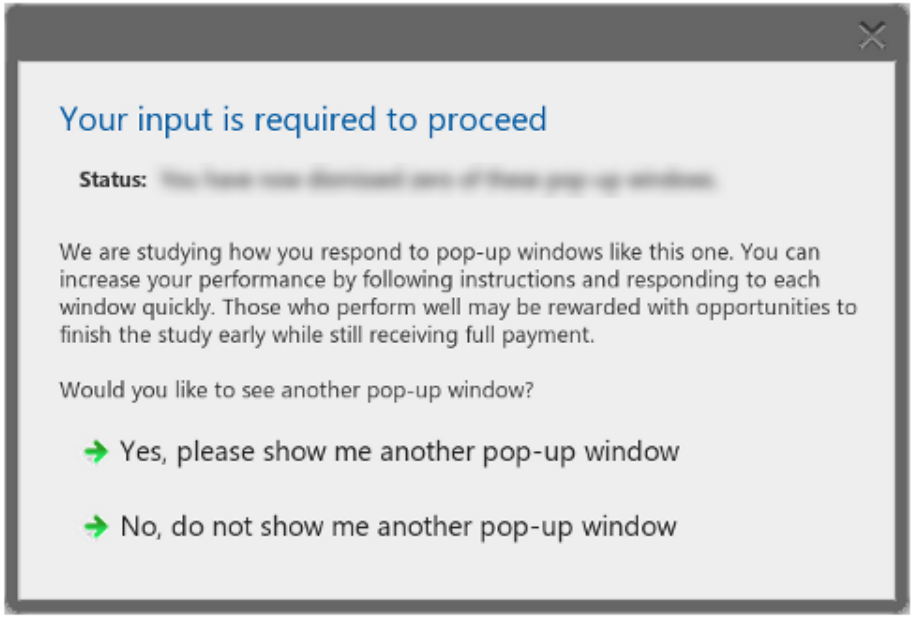

CMU study
saucers.cups.cs.cmu.edu/yacot/mnt/wtk/habit/index.php?m=endmsg&i=Atesting
You finished the task. You will be redirected to the rest of the survey in a few seconds. Please wait...
EN
33

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": *

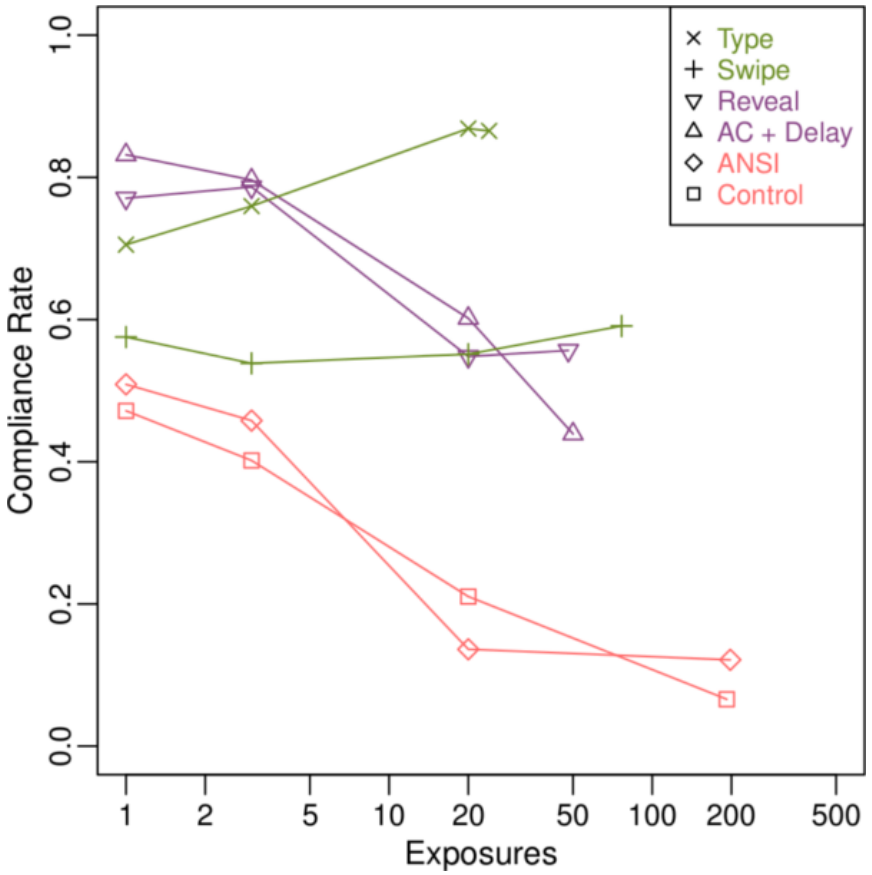
None

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”

Swipe and Type are resilient to habituation

- Control and ANSI (red) are not significantly different
- Reveal and AC+Delay (purple) have same performance of Control and ANSI, but with higher compliance rate
- Swipe and Type (green) show steady or increasing compliance rates



N=2,567 participants, 29.4 years old (SD=10.1), 55% male, 77% caucasian. Top two reported occupations: 'student' (25%), 'unemployed' (15%).

36

NEAT and SPRUCE

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

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**

Class assignment

- USB flash drives can spread infections in a number of ways. Seehttp://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/~cbravo/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 designhttp://cups.cs.cmu.edu/soups/2011/posters/soups_posters-Reeder.pdf

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/~cbravo/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.