Lecture 14: Security Warnings

CS 181W

Fall 2022

What to do about hazards?

Best solution: Remove hazard

Next best: guard against hazard

If all else fails: warn

Text-based Warnings

Icon-based warnings


CAUTION
LOOK UP

VILLE DE LYON

Chenilles processionnaires du chêne et du pin :

attention aux poils

Ces chenilles provoquent des réactions allergiques

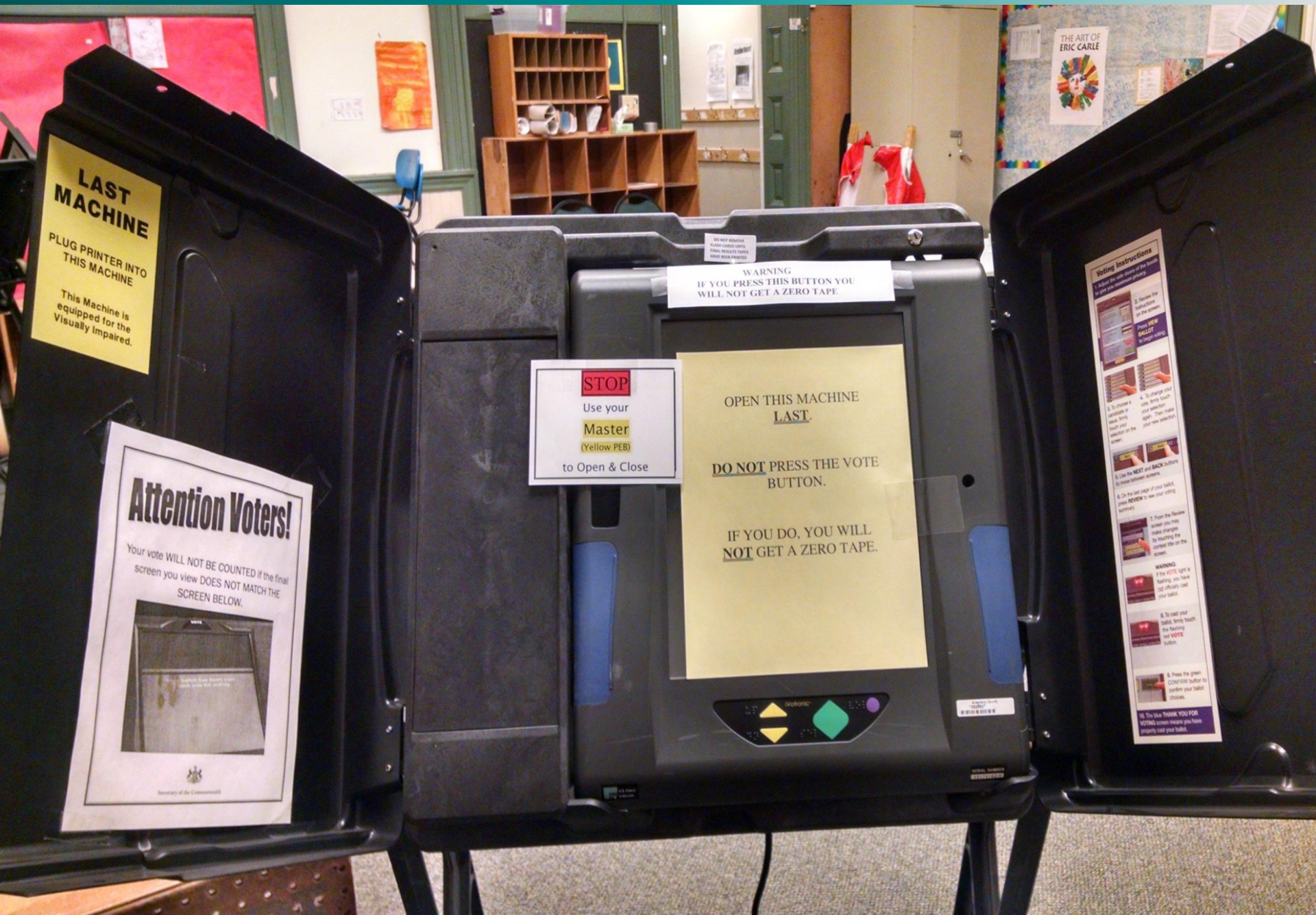
Je ne m'approche pas et je ne touche pas les chenilles ou leur nid

ars Agence Régionale de Santé Rhône-Alpes

La ville comme on l'aime, **attentive**

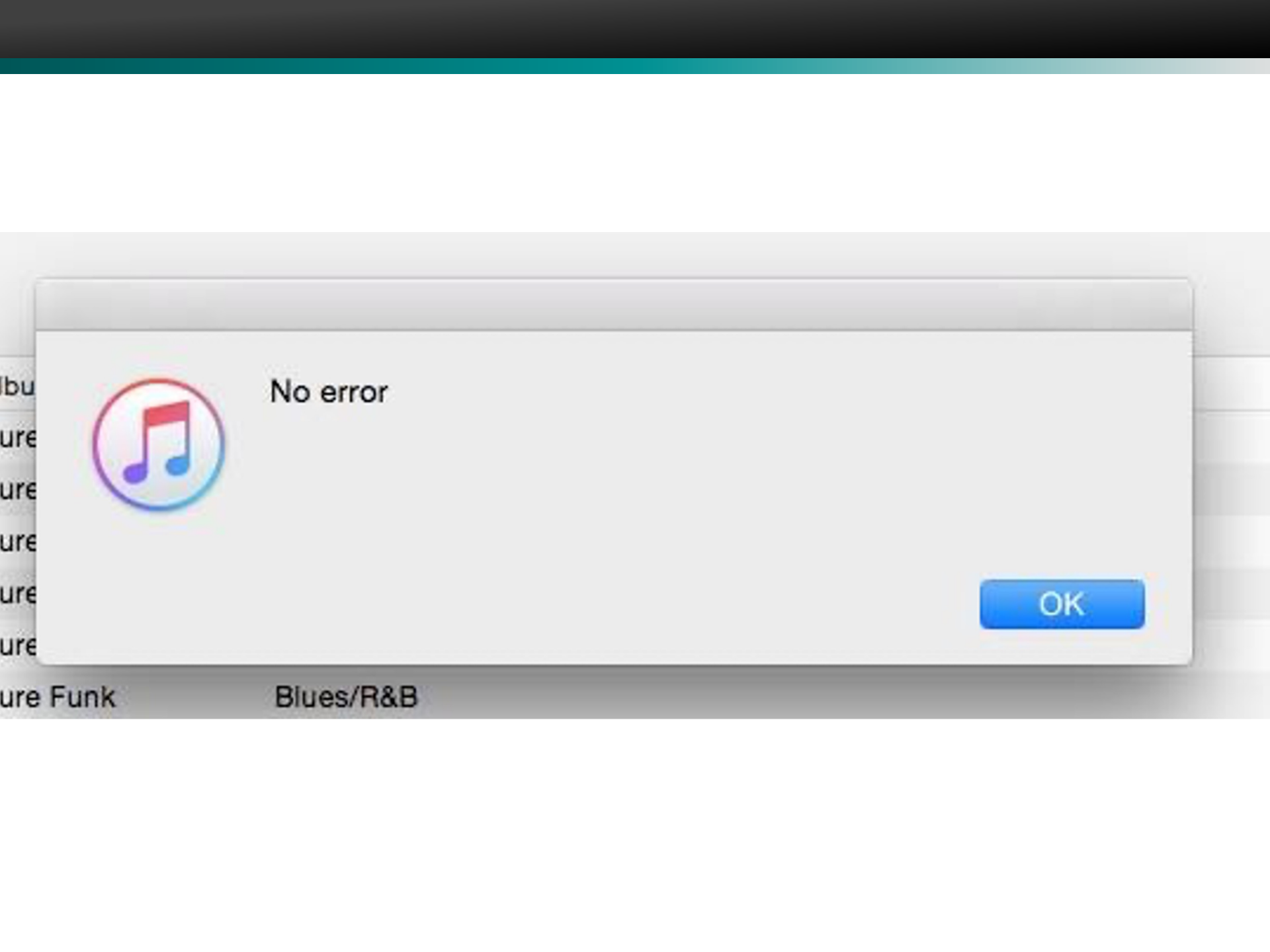

Caution!
Ravens may bite
Attention! Les corbeaux peuvent mordre
Vorsicht! Raben können zuschnappen
Precaución! Los cuervos pueden picar
Fare attenzione ai corvi: possono beccare
Digniin! Shimbirahu waxaa laga yaabaa inay wax qaniinaan
Осторожно! Вороны клюются
カラスに注意!噛み付くことがあります
주의! 까마귀가 물 수 있습니다
小心！ 烏鴉可能咬人
সতর্ক হোন! দাঁড়কাক ঠোকরাতে পারে


Leland
97 TO CLAYTON TC
Go Ape
LIVE LIFE ADVENTUROUSLY


LAST MACHINE
PLUG PRINTER INTO THIS MACHINE
This Machine is equipped for the Visually Impaired.
Attention Voters!
Your vote WILL NOT BE COUNTED if the final screen you view DOES NOT MATCH THE SCREEN BELOW.
WARNING
IF YOU PRESS THIS BUTTON YOU WILL NOT GET A ZERO TAPE
STOP
Use your
Master
(Yellow PEB)
to Open & Close
OPEN THIS MACHINE LAST.
DO NOT PRESS THE VOTE BUTTON.
IF YOU DO, YOU WILL NOT GET A ZERO TAPE.
THE ART OF ERIC CARLE
Voting Instructions


CVS
pharmacy
24 HOURS


ATTENTION VALUED
CVS/pharmacy® CUSTOMERS:
To protect your privacy, please do not throw
any materials containing your personal
information into this trash container.

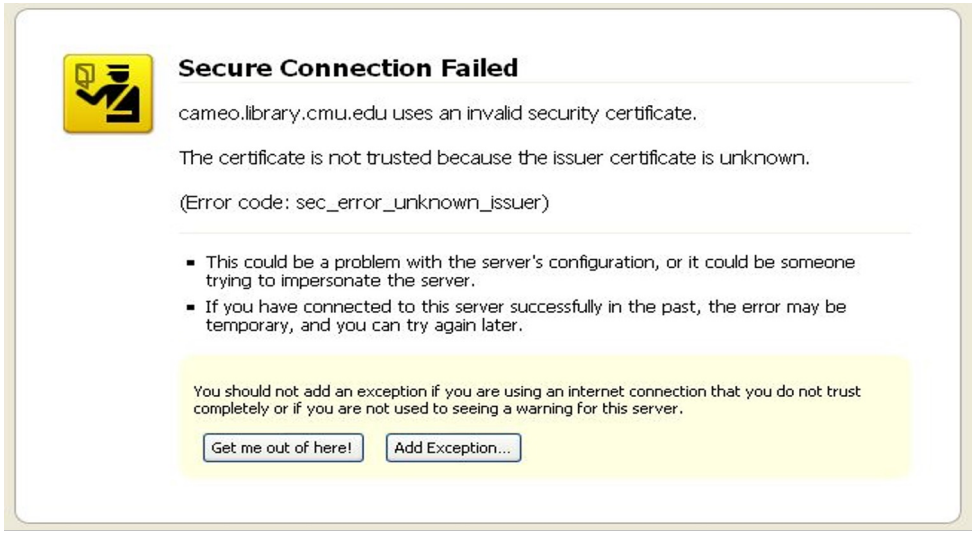

No error
OK
ure Funk
Blues/R&B

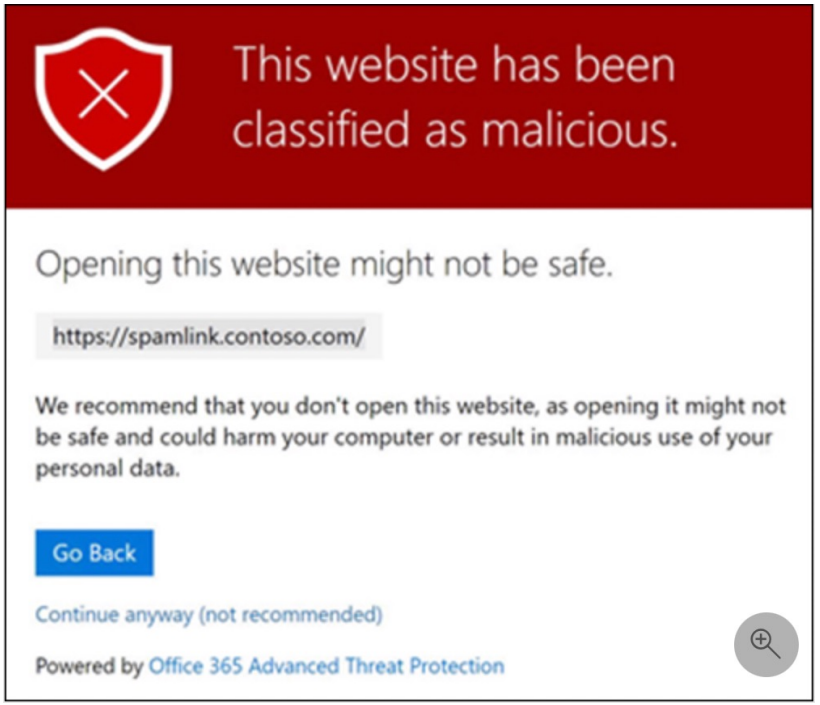

GREATERLONDONAUTHORITY

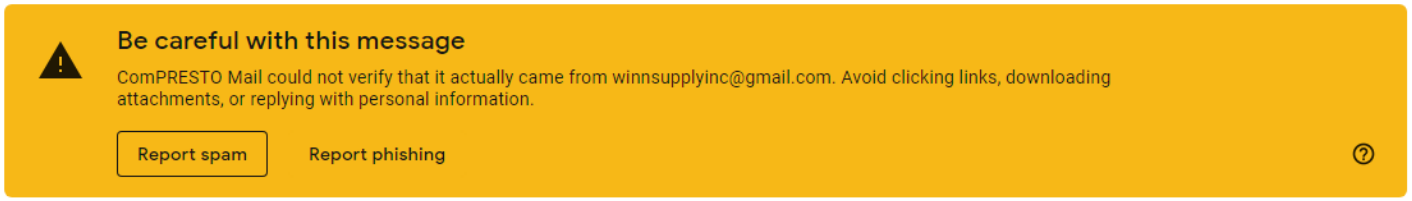

KEEP
OFF
MEDIAN
BMC # 14.32.040
Epicurious Garden
Kirala
1513 A
ALEGIO
Lush GELATO & CAFÉ
Imperial Tea
KITCHEN FIRE
Picoso
SOOP

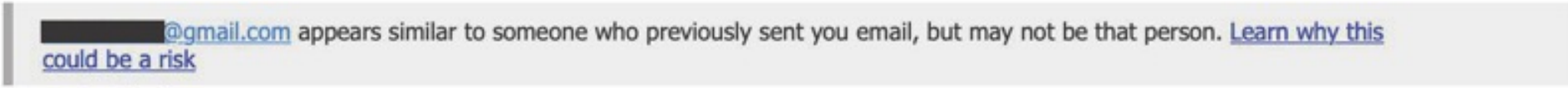

IN CASE OF FIRE
EXIT BUILDING
BEFORE TWEETING
ABOUT IT

Security Warnings







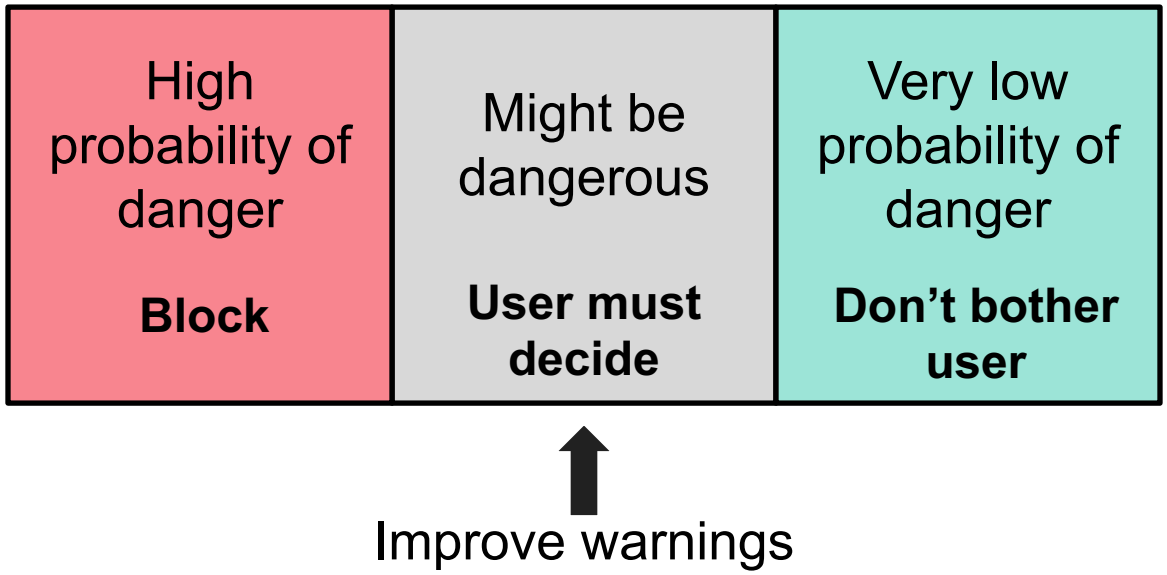


Security dialogs context dependent

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

Support user decision

- Use automated analysis to determine probability of danger

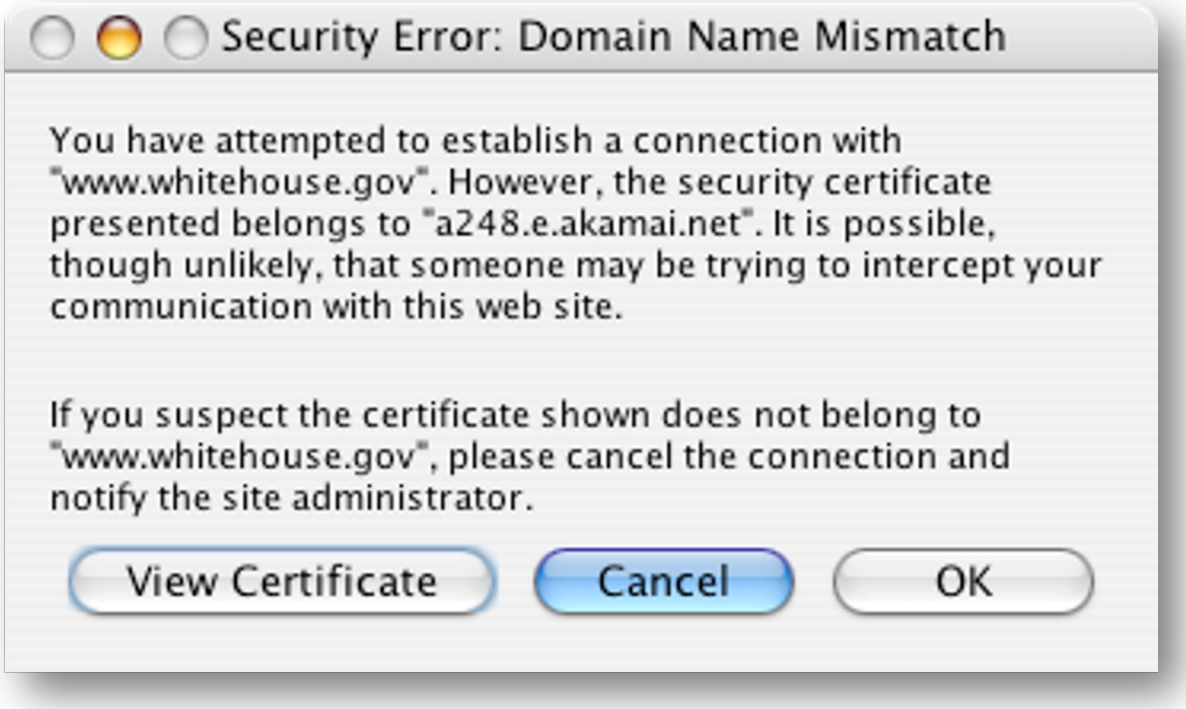


Help user decide by asking question user is qualified to answer

Good warnings

- Help users determine whether they are at risk
- Stop users from doing something dangerous in risky context
- Don’t interfere with non-risky contexts

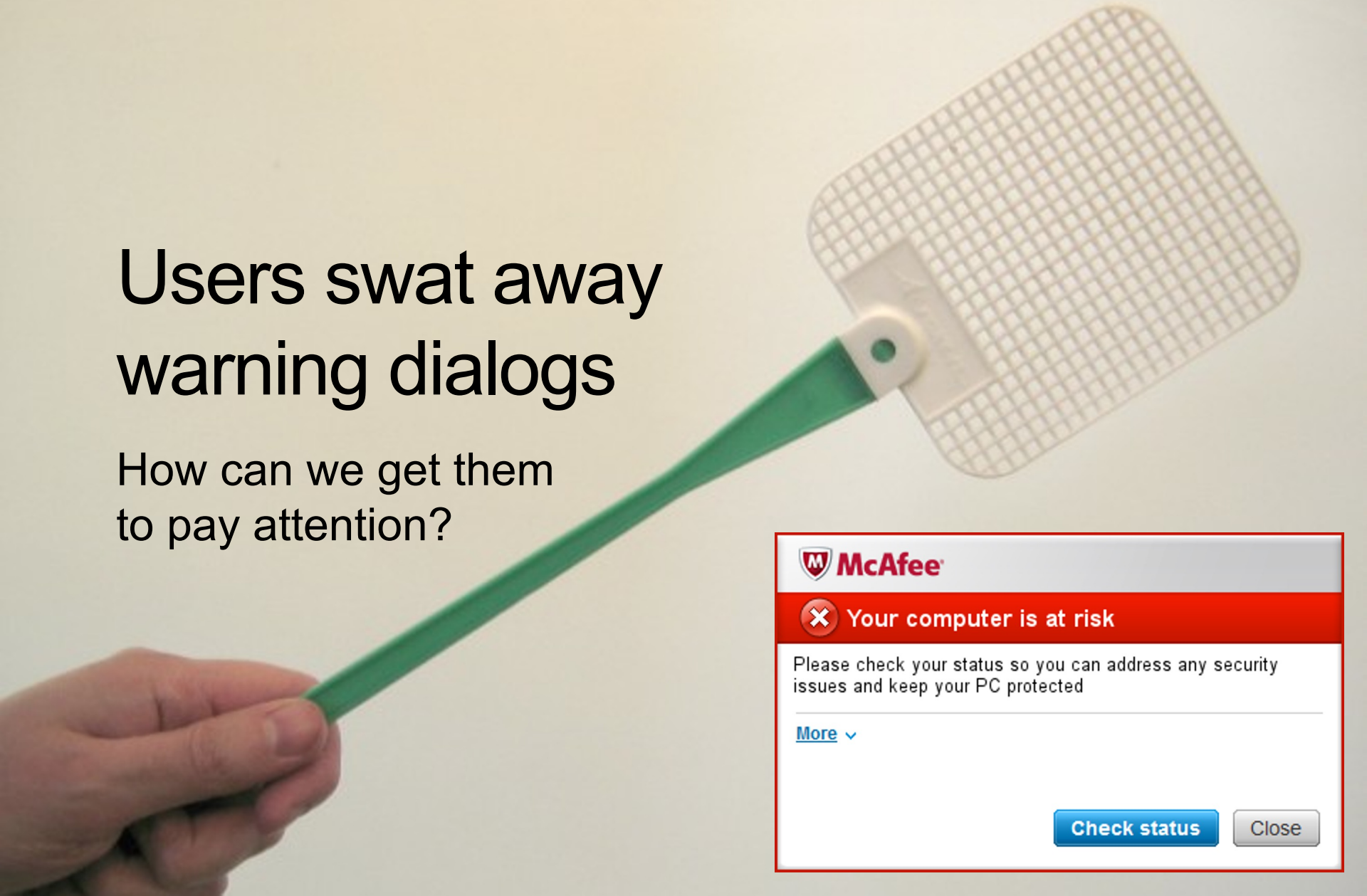
Bad Warnings



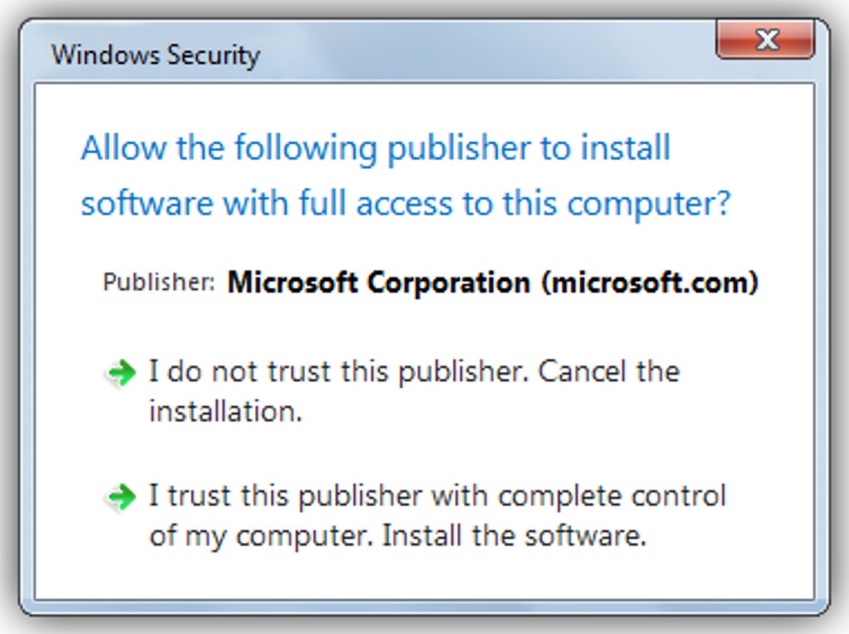
Bad Warnings

Users swat away warning dialogs

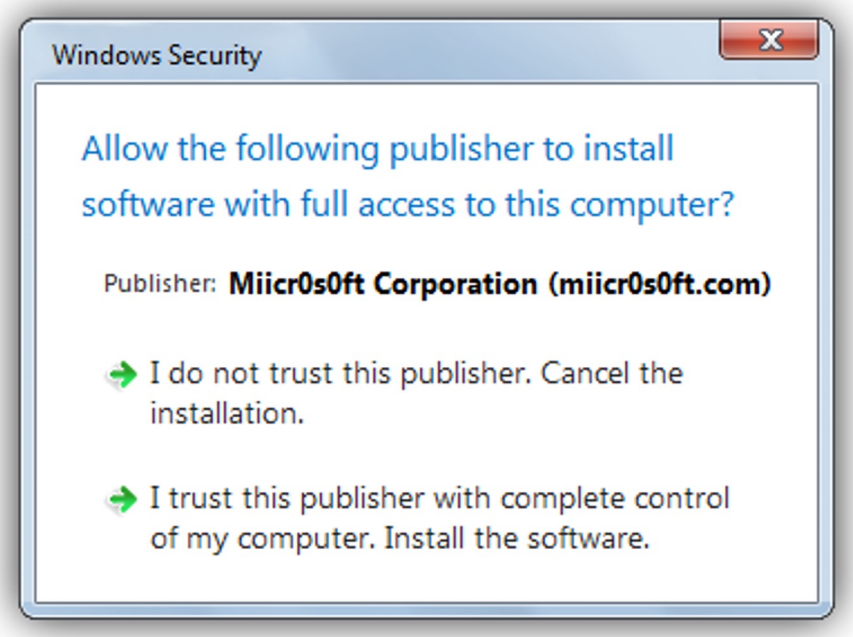
How can we get them to pay attention?



Can you spot the suspicious software?



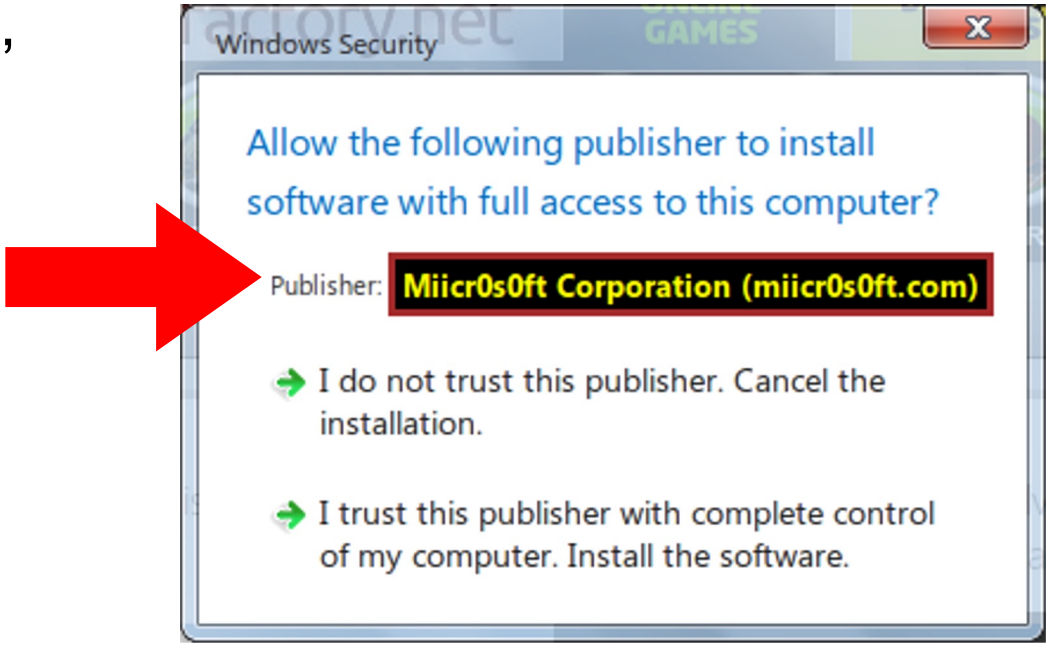
benign



suspicious

Attracting users' attention

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

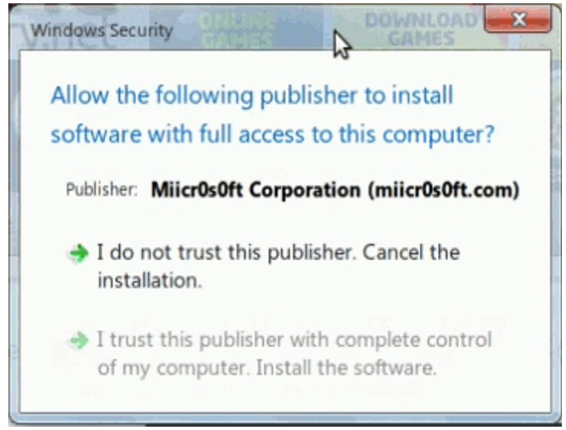


C. Bravo-Lillo, L.F. Cranor, J. Downs, S. Komanduri, R.W. Reeder, S. Schechter, and M. Sleeper. Your Attention Please: Designing security-decision UIs to make genuine risks harder to ignore. SOUPS 2013.

How can we get users to notice suspicious publishers?

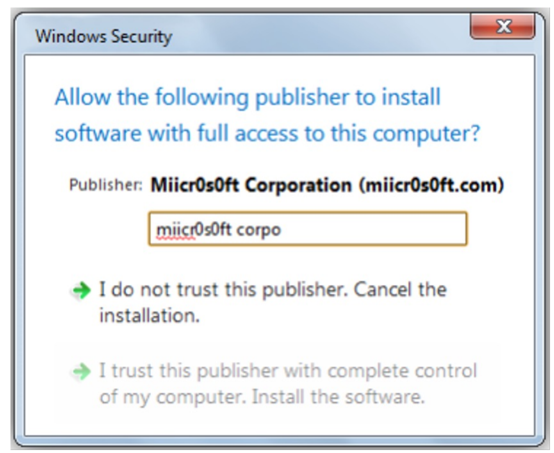
- Use **attractors** to draw attention to publisher name
- Force delay before users can install
- Force interaction before users can install
- Force users to read publisher name


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.


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.

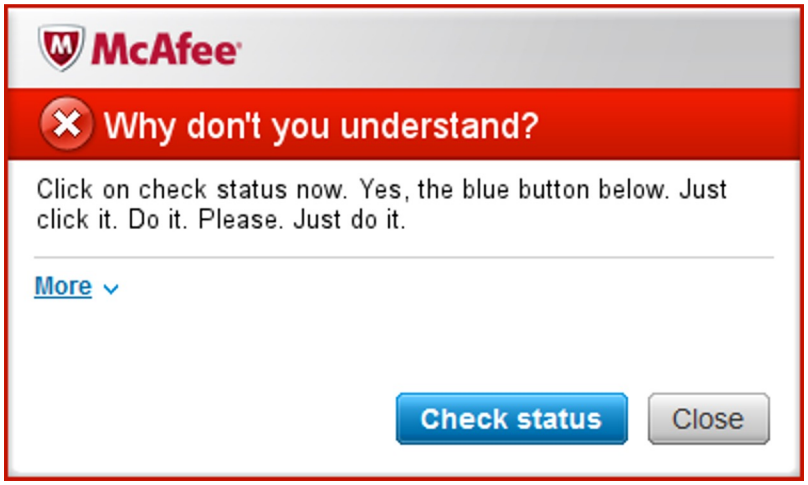

Windows Security
Allow the following publisher to install software with full access to this computer?
Publisher: Miicr0s0ft Corporation (miicr0s0ft.com)
I do not trust this publisher. Cancel the installation.
I trust this publisher with complete control of my computer. Install the software.


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.


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

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

real non-security tasks

simulated risk

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

Carn 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

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 #1: Mars Buggy Online

Instr

1.

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

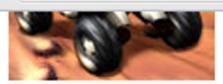
Attention: The website whose URL appears above is external to this study. Our researchers **do not** control its content.

Attention: The website whose URL appears above is external to this study. Our researchers do not control its contents

1. W

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

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

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? *

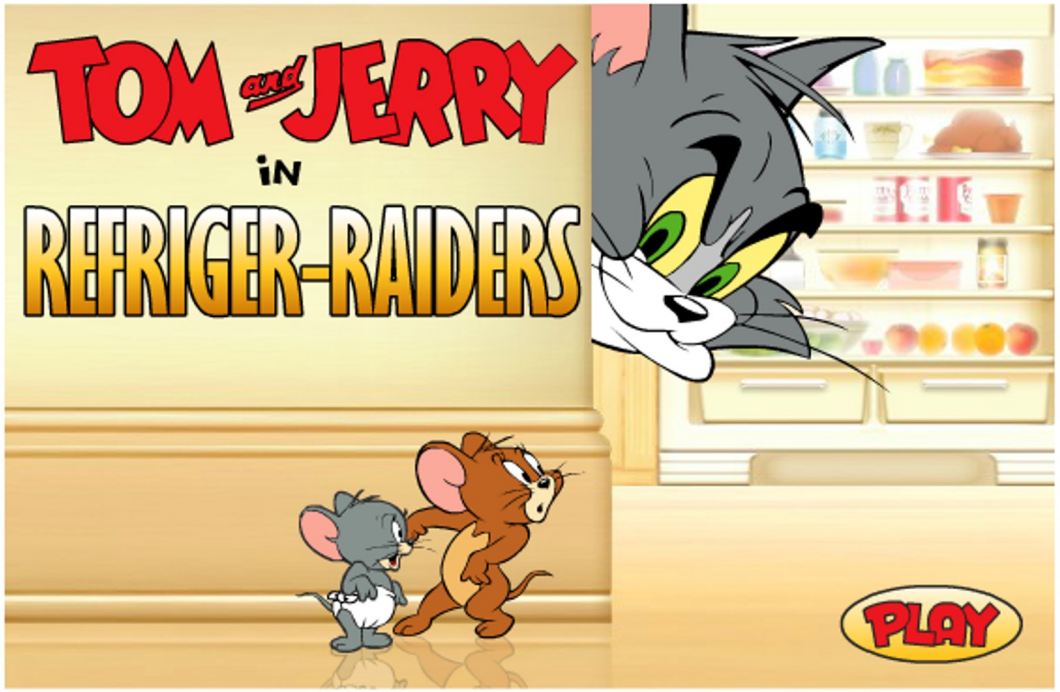
- ○ Yes
- ○ No **(you will be assigned another game to evaluate)**

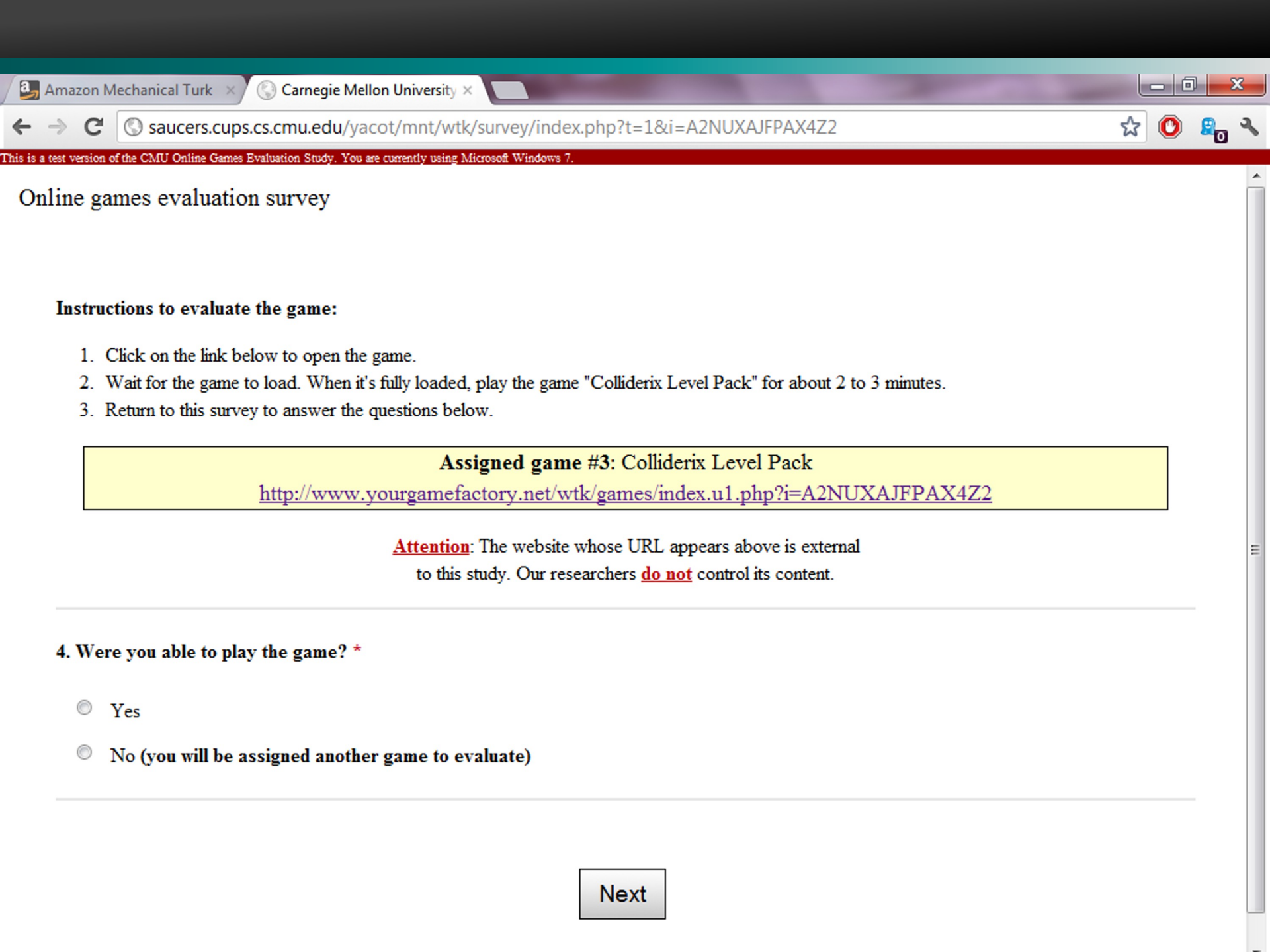
Next

Add to Favorites

Tom and Jerry Refrigerator Raid Game

stars (3973)




Amazon Mechanical Turk
Carnegie Mellon University
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

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

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

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&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 | ACTION | SPORT | DRESS UP | KIDS | CLAS | BOARD | MISC | NEW

Games / Puzzle Games / Colliderix Level Pac

This game requires the latest version of ... ng or out

Acces...

Windows Security

Allow the following publisher to install software?

Publisher: **Miicr0s0ft Corporation (miicr0s0ft.com)**

Only install this software if you trust this publisher with complete control of your computer. The software was downloaded by Chrome at 1/11/2014 6:52:58 PM.

Cancel the installation

Install the software

Related Games

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

Participant decision design

- Workers in Amazon's Mechanical Turk aim to:
  - Complete tasks they accept (otherwise, don't earn money)
  - Minimize time and effort (so they can complete more tasks)
- Our message to participants:
  - “You may skip a game. If you do, we will assign you another”
- Decision 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

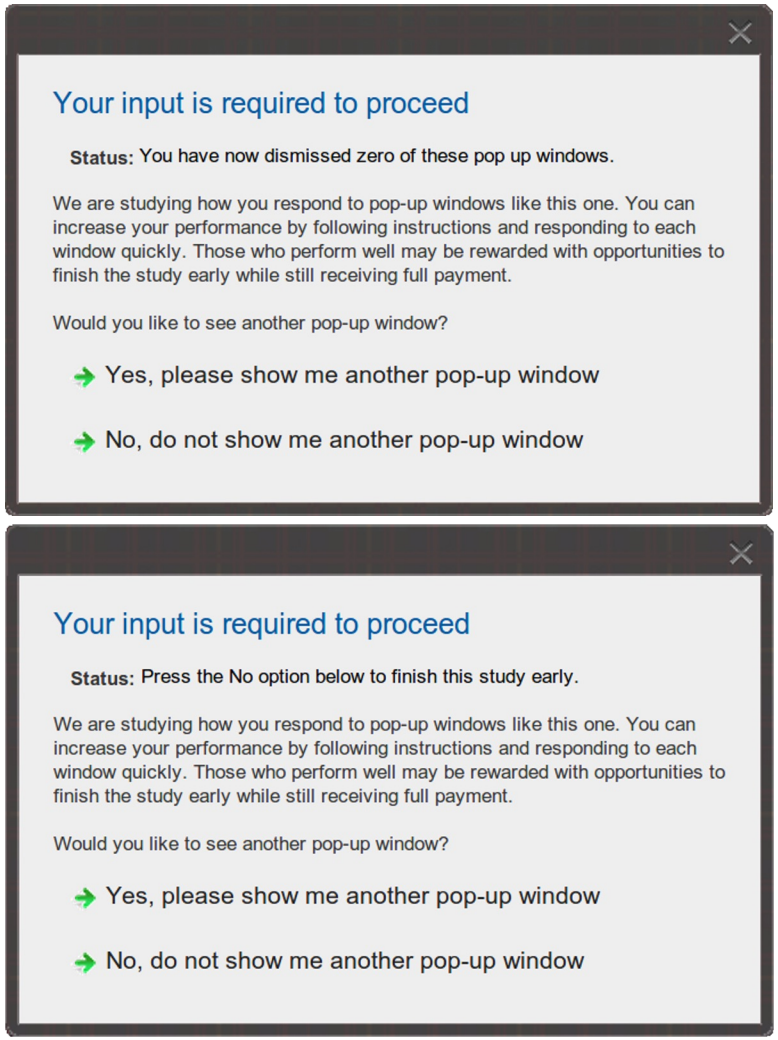
- 2,227 participants encountered dialogs
- Benign scenario
  - Installation not prevented
  - But some approaches slowed people down
- Suspicious scenario
  - Our new dialogs reduced installations
  - Swipe, type, and delay were particularly effective

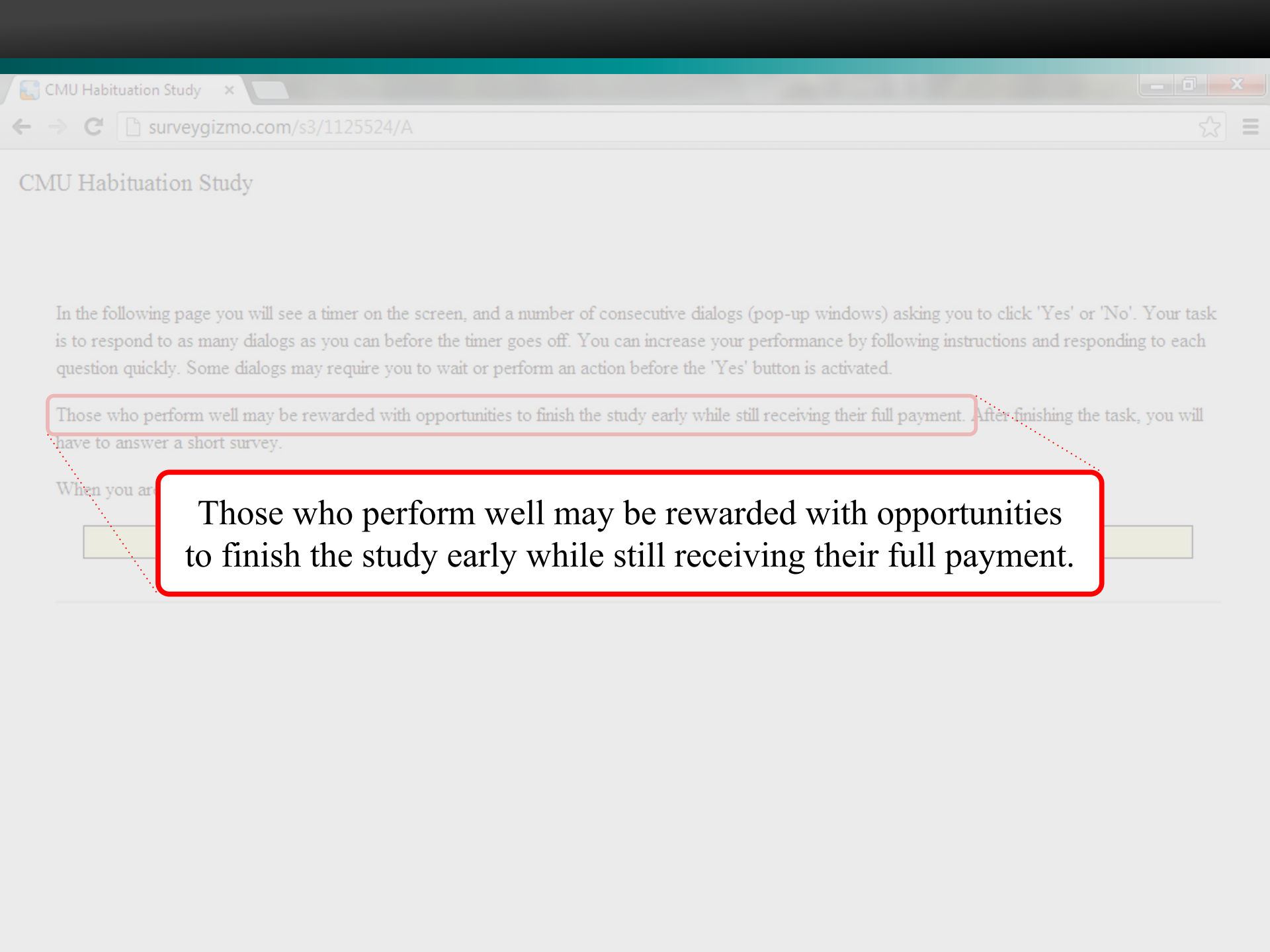
What if they saw attractors repeatedly?

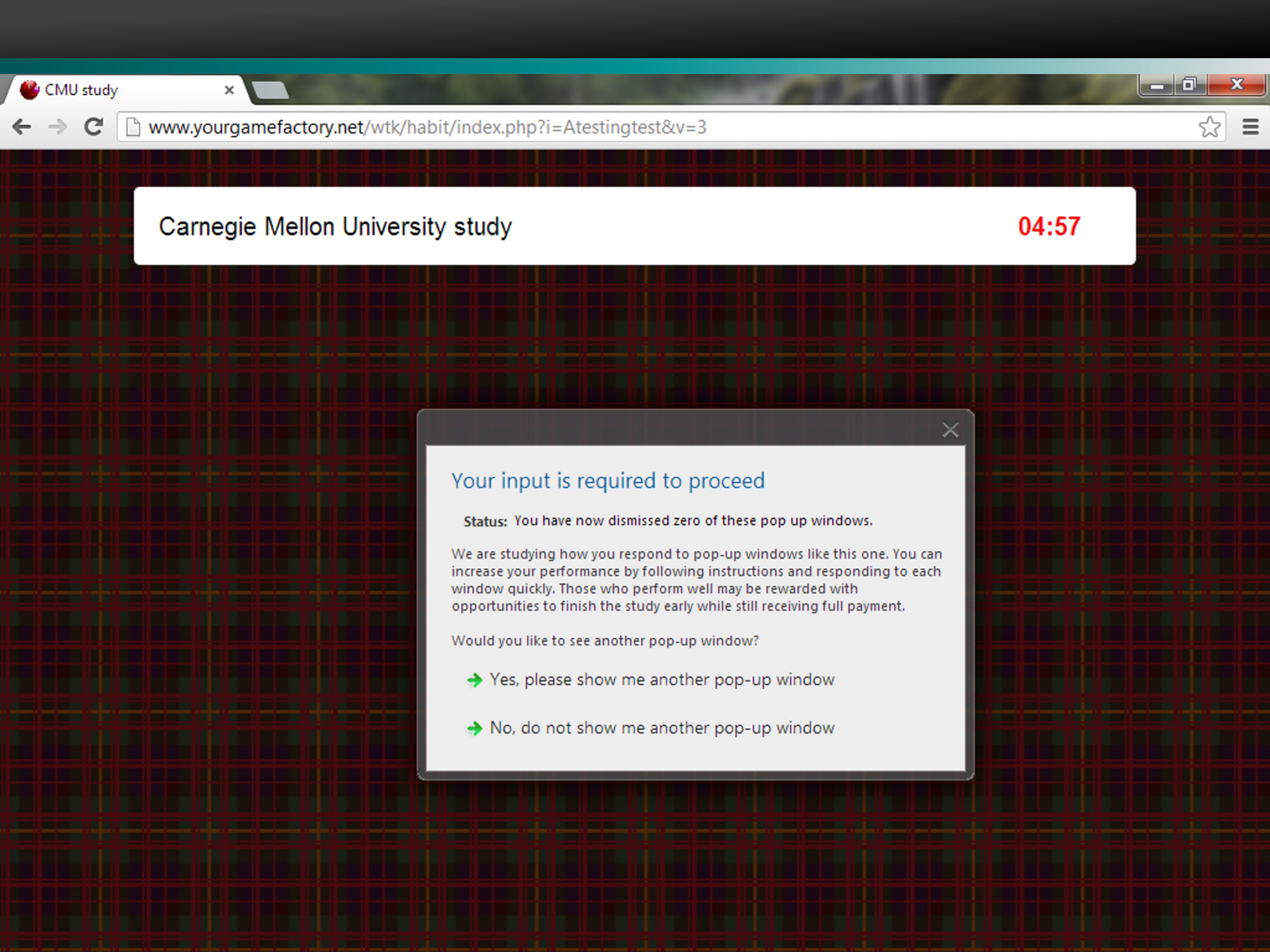
- Conducted more experiments
- Scenario in which participants had to dismiss a dialog repeatedly for several minutes until the dialog changed
- Measured rate of compliance with changed dialog
- Showed that some attractors performed better than control in presence of **habituation**

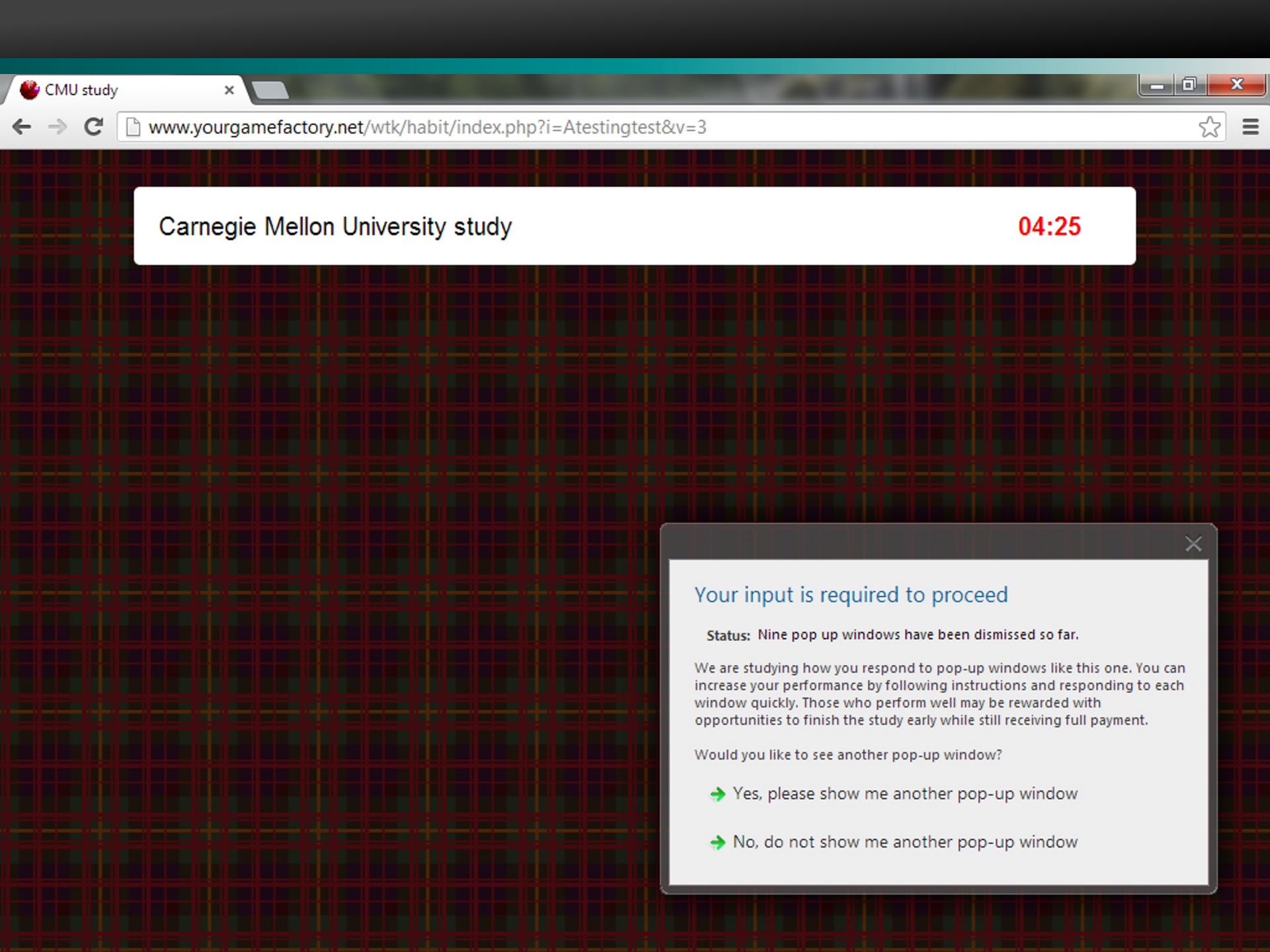
Habituation experiment

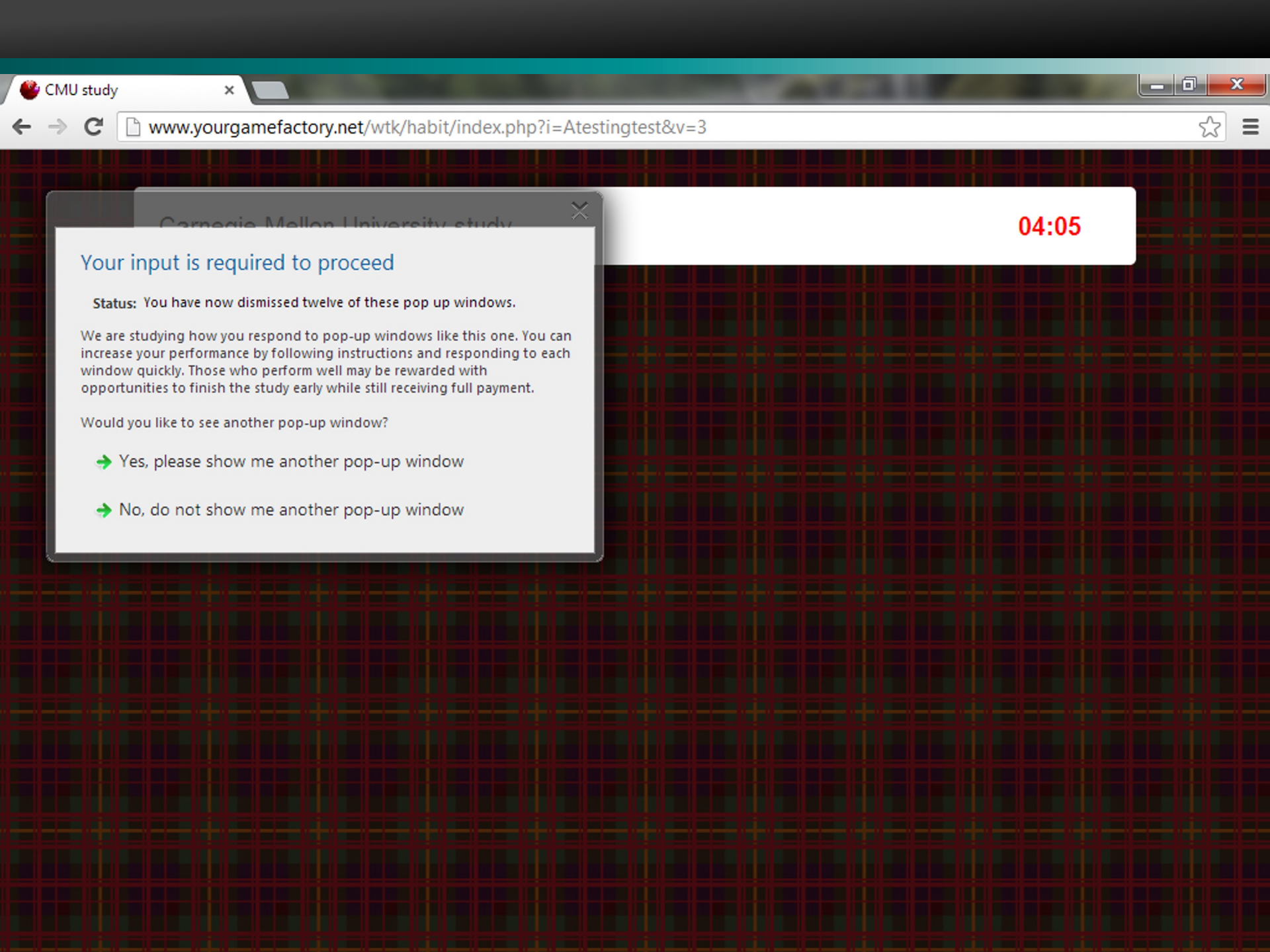
- Show dialog repeatedly with irrelevant message
- Ask participants to click “Yes”
- Change salient field to “Click on No”
- Check if participants notice the change and click “No”

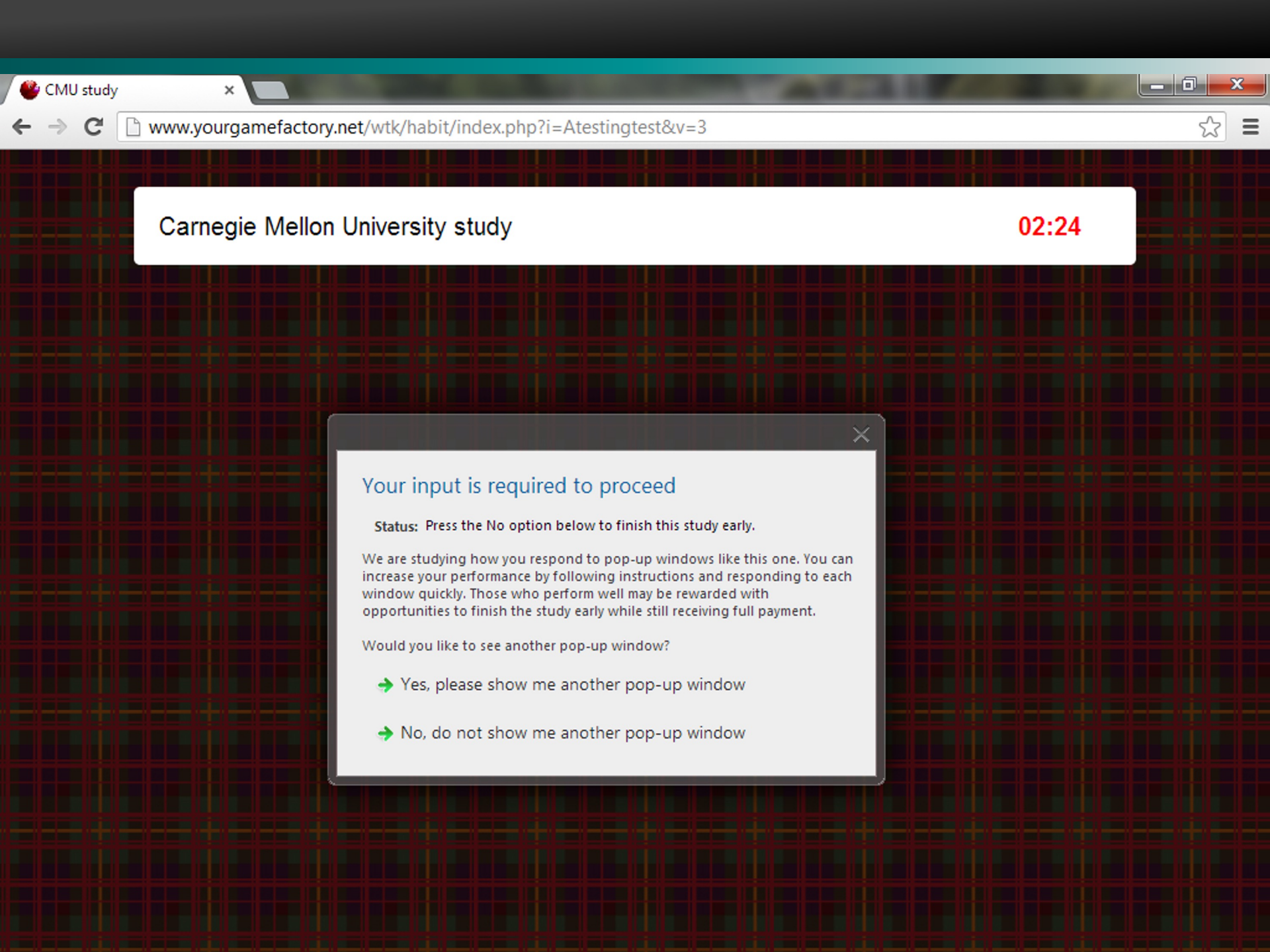


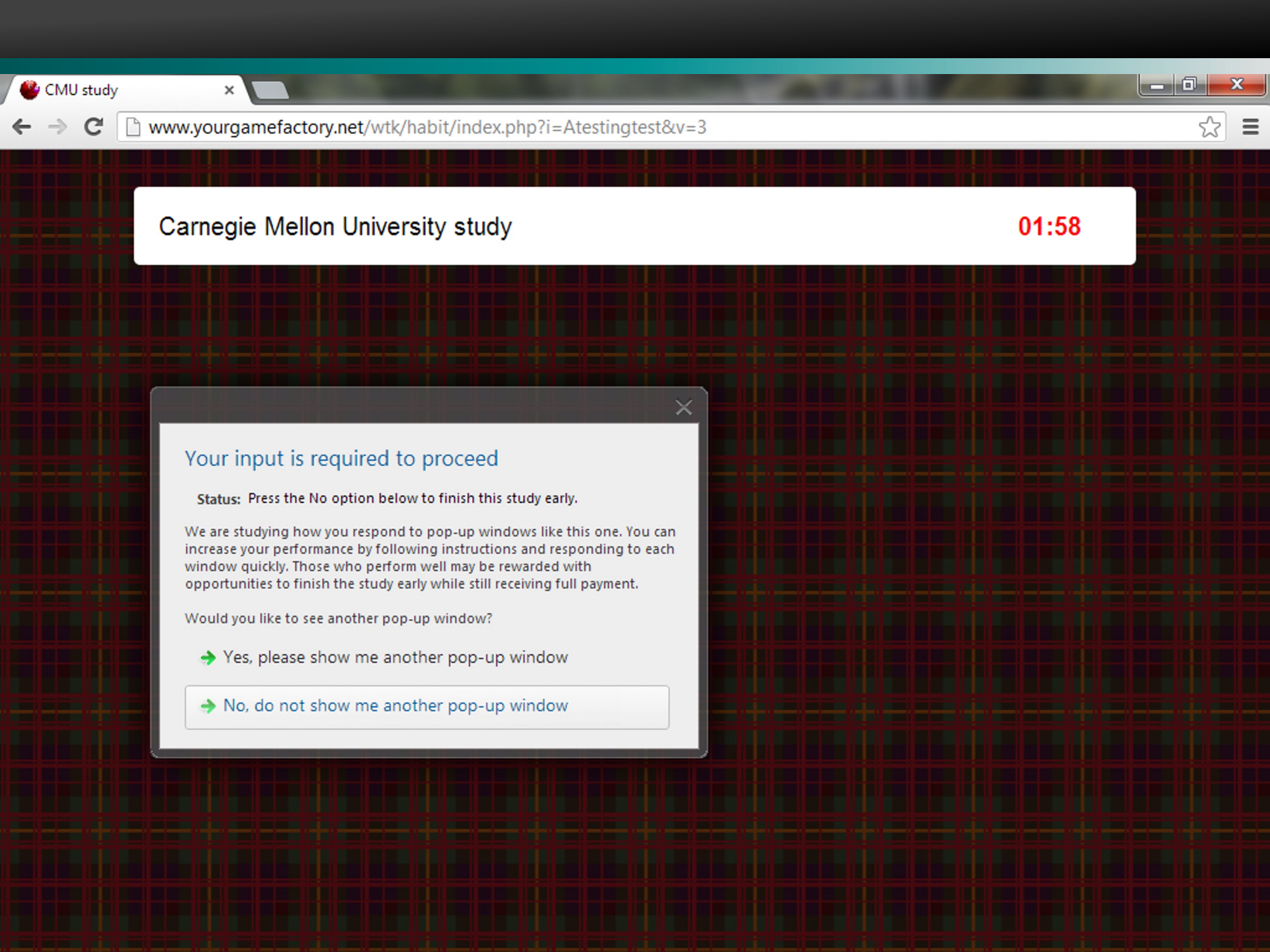

CMU Habituation Study
surveygizmo.com/s3/1125524/A
CMU Habituation Study
In the following page you will see a timer on the screen, and a number of consecutive dialogs (pop-up windows) asking you to click 'Yes' or 'No'. Your task is to respond to as many dialogs as you can before the timer goes off. You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

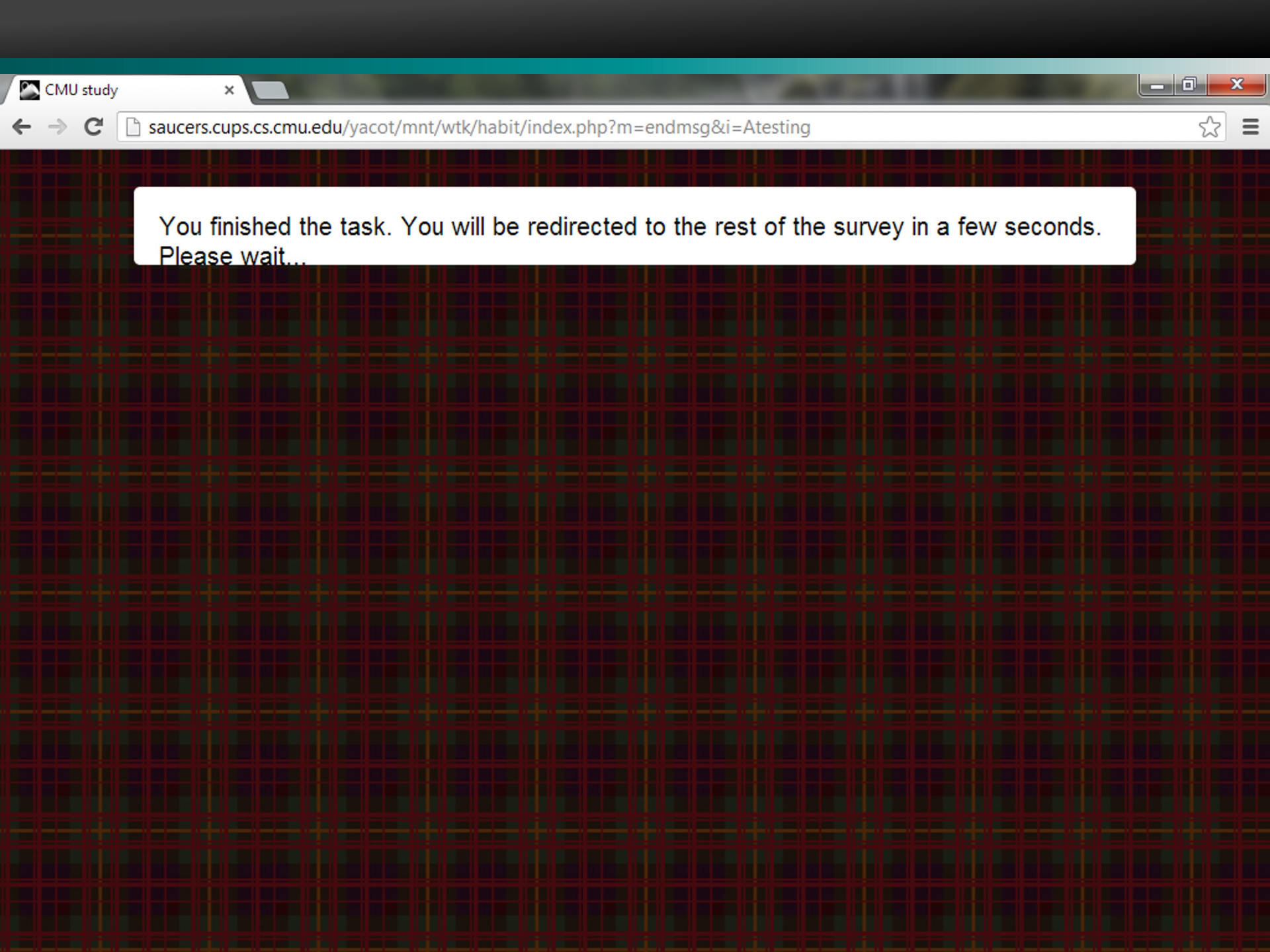

CMU study
www.yourgamefactory.net/wtk/habit/index.php?i=Atestingtest&v=3
Carnegie Mellon University study
04:57
Your input is required to proceed
Status: You have now dismissed zero of these pop up windows.
We are studying how you respond to pop-up windows like this one. You can increase your performance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


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


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


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


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

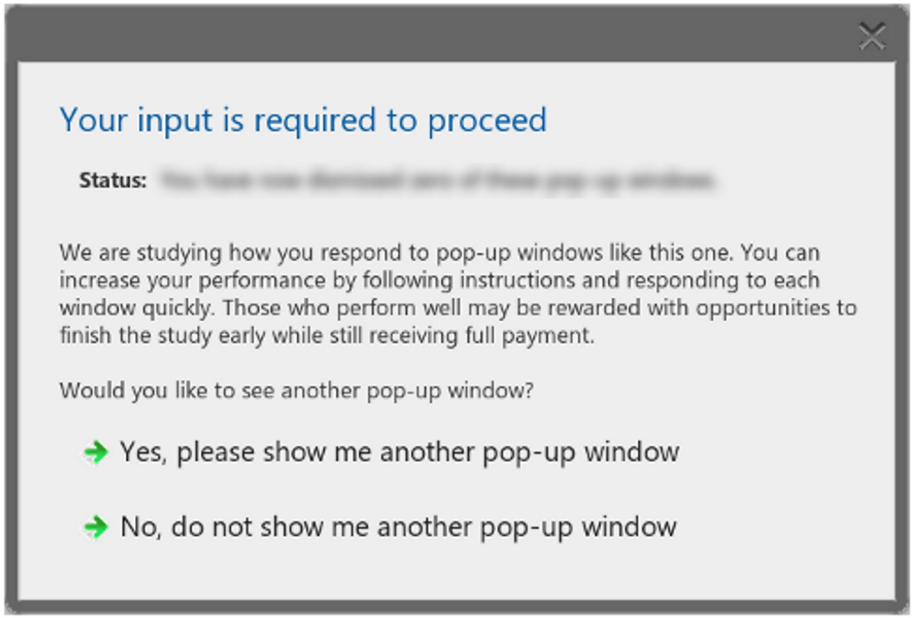

CMU study
saucers.cups.cs.cmu.edu/yacot/mnt/wtk/habit/index.php?m=endmsg&i=Atesting
You finished the task. You will be redirected to the rest of the survey in a few seconds. Please wait...

CMU Pop-up dialogs stud ×

www.surveygizmo.com/s3/1126212/B

CMU Pop-up dialogs study

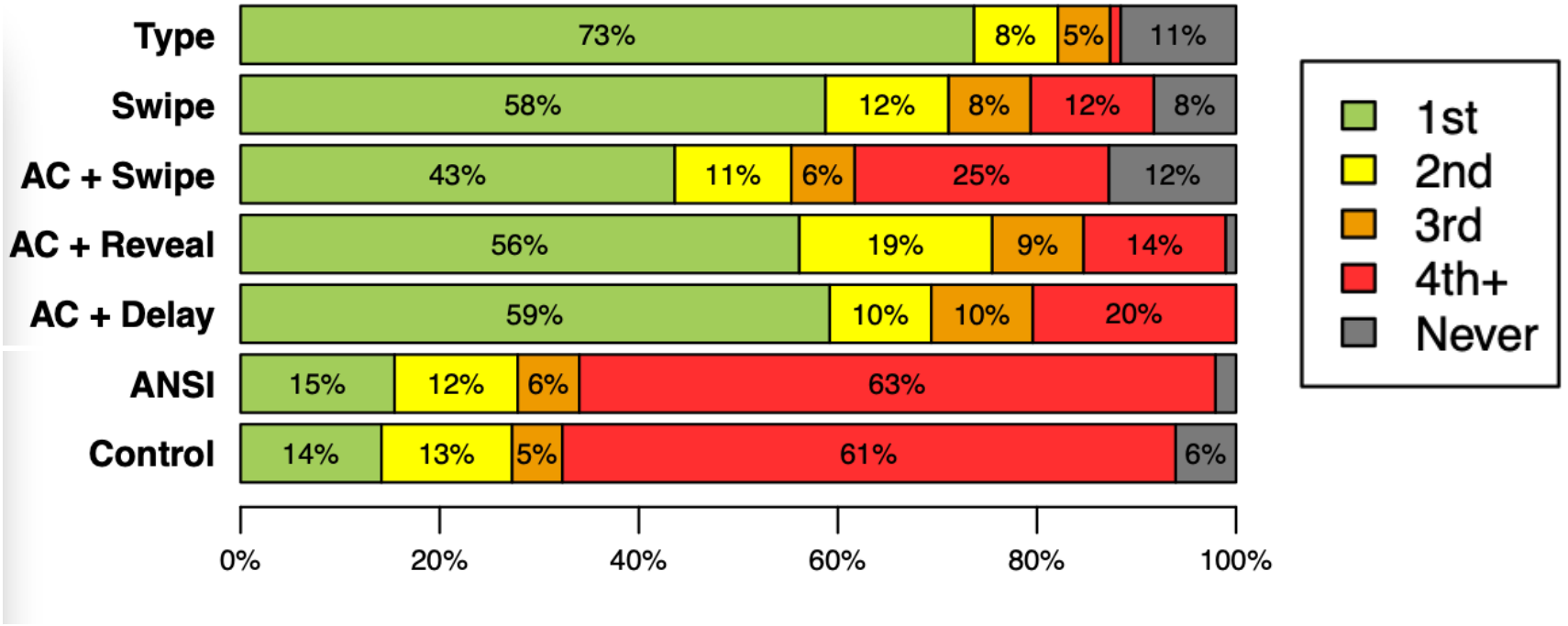
The image below corresponds to one of the dialogs you saw during this study:



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

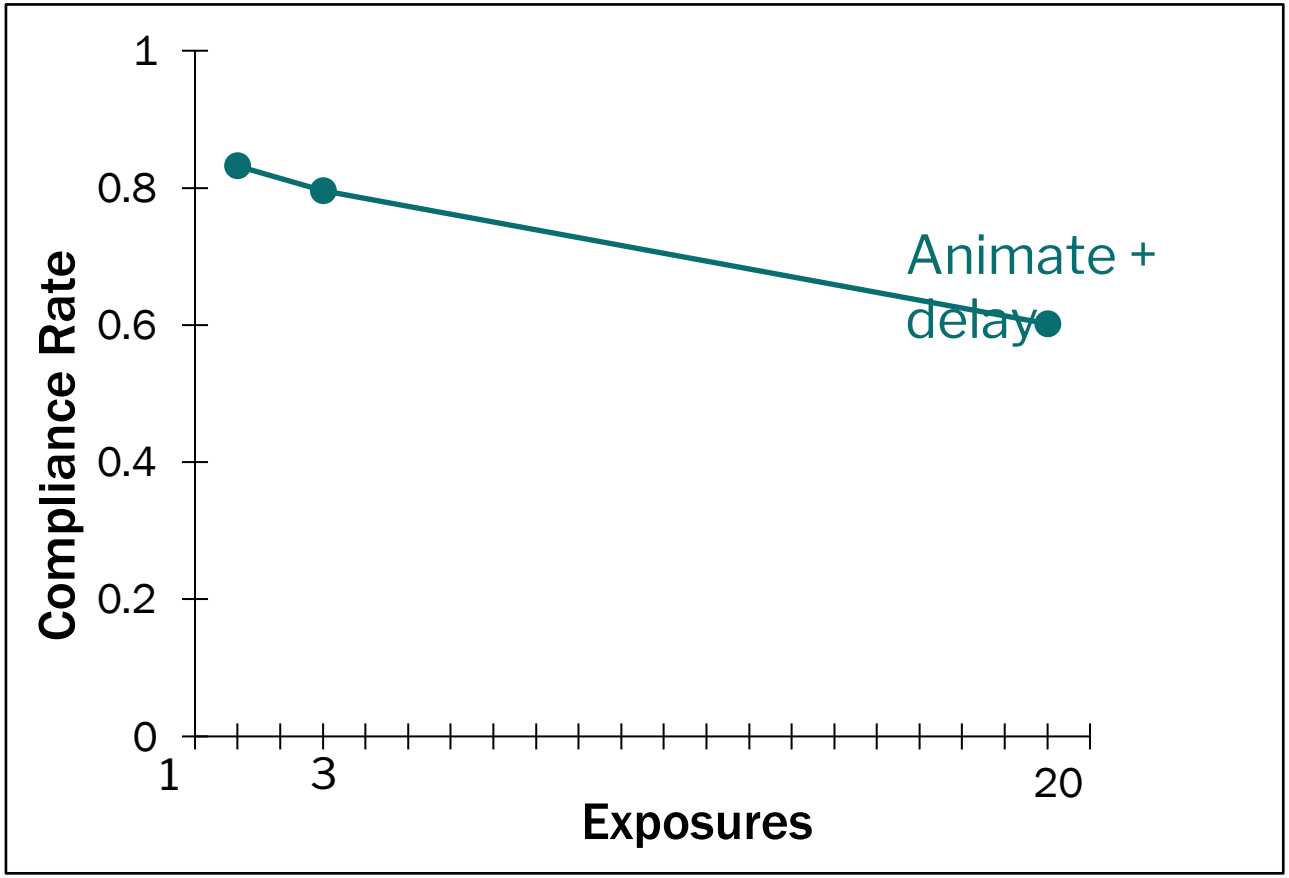
Habituation Results

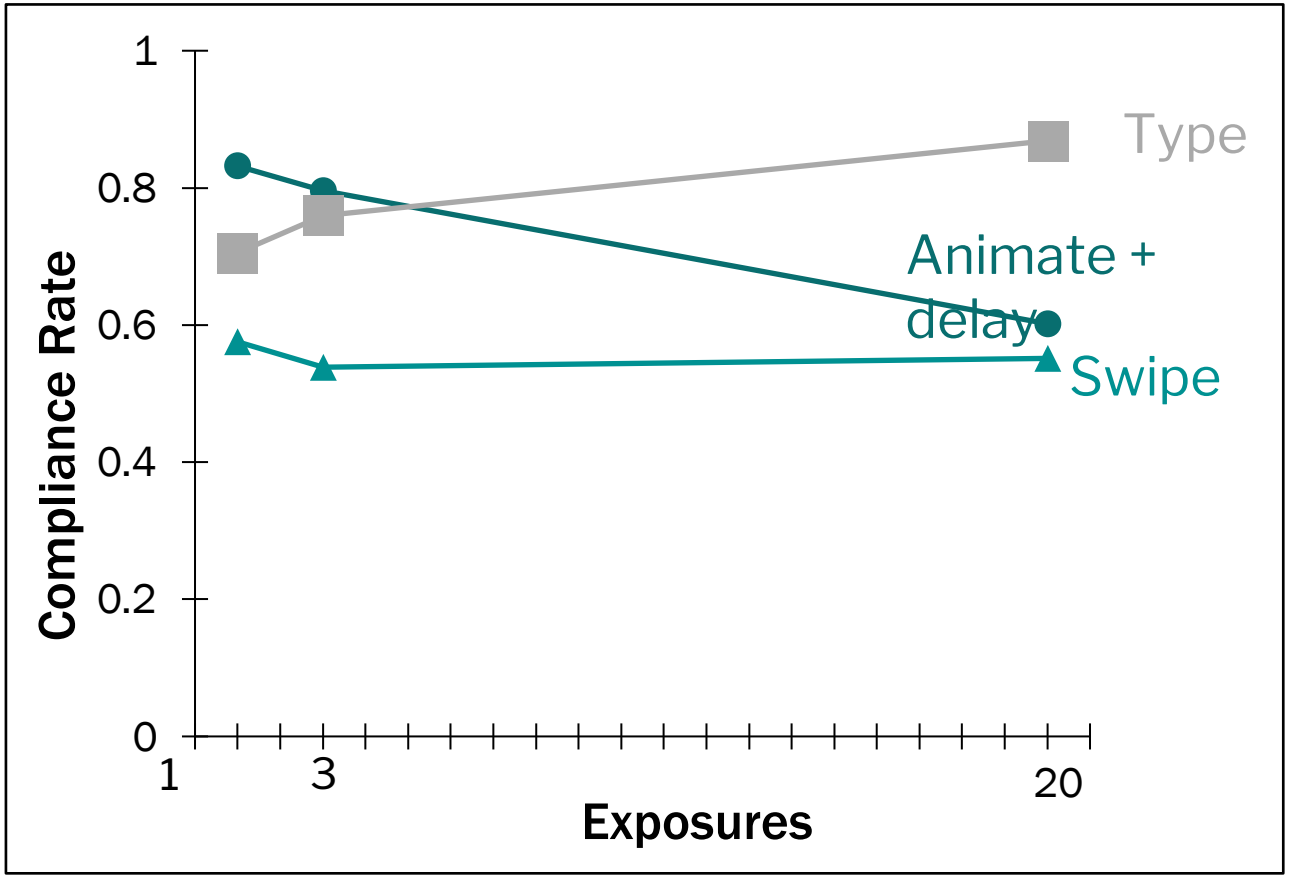


“Harder to ignore” experimental design

- {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”

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.


Compliance Rate
1
0.8
0.6
0.4
0.2
0
1
3
20
Exposures
Animate + delay


1
0.8
0.6
0.4
0.2
0
Compliance Rate
1
3
20
Exposures
Type
Animate + delay
Swipe

Experience sampling warnings study

- Participants expressed a variety of reasons for choosing to adhere to or proceed past a given warning
- Warnings have improved from prior work and additional improvements may require refinements on a case-by-case basis
- Habituation may play a smaller role than previously thought

---

R. Reeder, A. Felt, S. Consolvo, N. Malkin, C. Thompson, and S. Egelman. An Experience Sampling Study of User Reactions to Browser Warnings in the Field. CHI 2018.

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

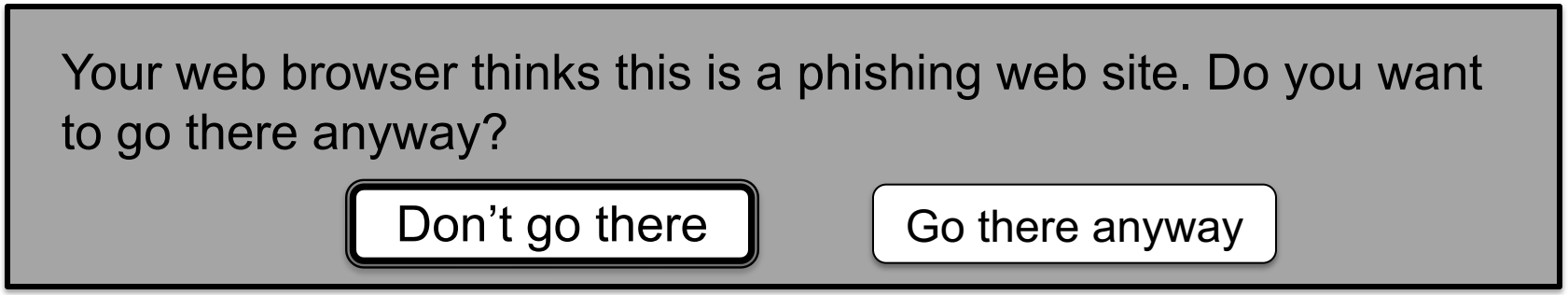
CHOICES: List available options and clearly recommend one

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

Exercise: Warning design

- 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 from 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. Design the warning.
- In a group, sketch a warning design

Security Warnings