COMP 152-1: Human Factors in Security and Privacy

Security Warnings

Lecture 15

Prof. Daniel Votipka
Fall 2023

(some slides courtesy of Michelle Mazurek, Rob Reeder, Blasé Ur, and Adam Aviv)

Administrivia

- IRB Applications are due on Thursday (10/26)
- Homework 2 is due next Thursday (11/02)
- Guest Lecture next Tuesday (10/31):
  - Johanna Gunawan, Northeastern University (IoT Privacy)
- Tomorrow CSPP Talk:
  - Lily Hay Newman, Senior Technology Writer @ WIRED
    - 12pm in Cabot 205
- Example of Qualitative Coding/IRR Calculation

- I figured out how to create a public key by looking at StackOverflow

C1: Forum
C2: Forum

C1: Generate key
C2: Generate key

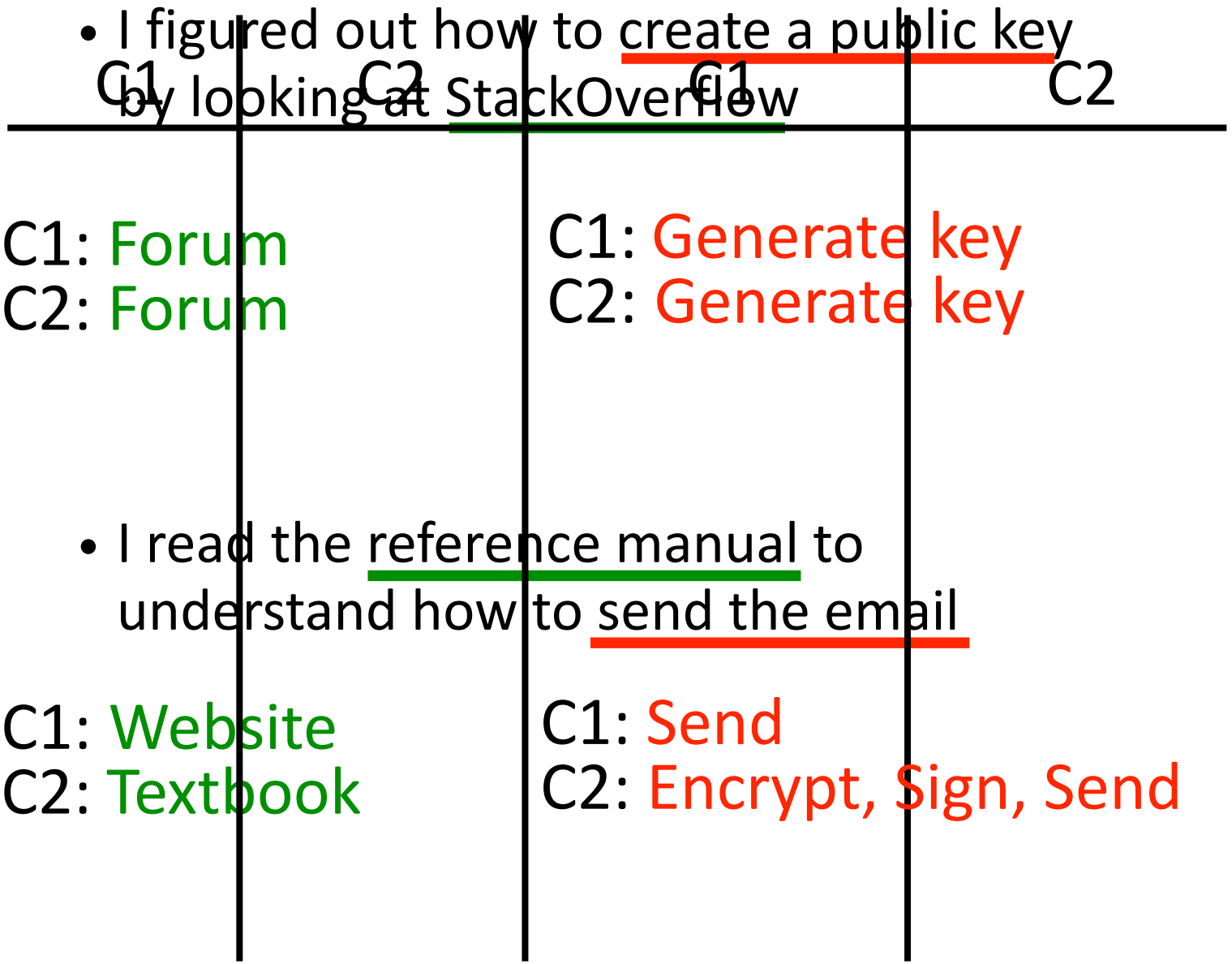
- I read the reference manual to understand how to send the email

C1: Website
C2: Textbook

C1: Send
C2: Encrypt, Sign, Send

Resource
- Textbook
- Forum
- Website

Steps
- Generate key
- Get receiver key
- Encrypt
- Sign
- Send



Resource

- Textbook (1)
- Forum (2)
- Website (3)

Steps

- Generate key (1)
- Get receiver key (2)
- Encrypt (3)
- Sign (4)
- Send (5)

C1	C2	C1	C2
2	2	1	1
3	1	5	5
2	2	0	4
2	2	0	3
1	1	1	1
3	1	4	3
		5	4
		3	3

Resource

- Textbook (1)
- Forum (2)
- Website (3)

Steps

- Generate key (1)
- Get receiver key (2)
- Encrypt (3)
- Sign (4)
- Send (5)

What we did last time!

- Android permissions overview
- Evolution of the permission model
  - Context matters!
- Privacy managers

What are we doing today?

- NEAT/SPRUCE Guidelines
- Wogalter Communication-Human Interaction Process
  - Getting the users' attention
- Nudges

Developer’s Perspective

User’s Perspective

Users swat away warning dialogs

- RQ: How can we get users to pay attention?
  - *Should we even require them to pay attention?*
- RQ: How do we get users to understand the warning?
  - *Do they even need to understand to do the right thing?*

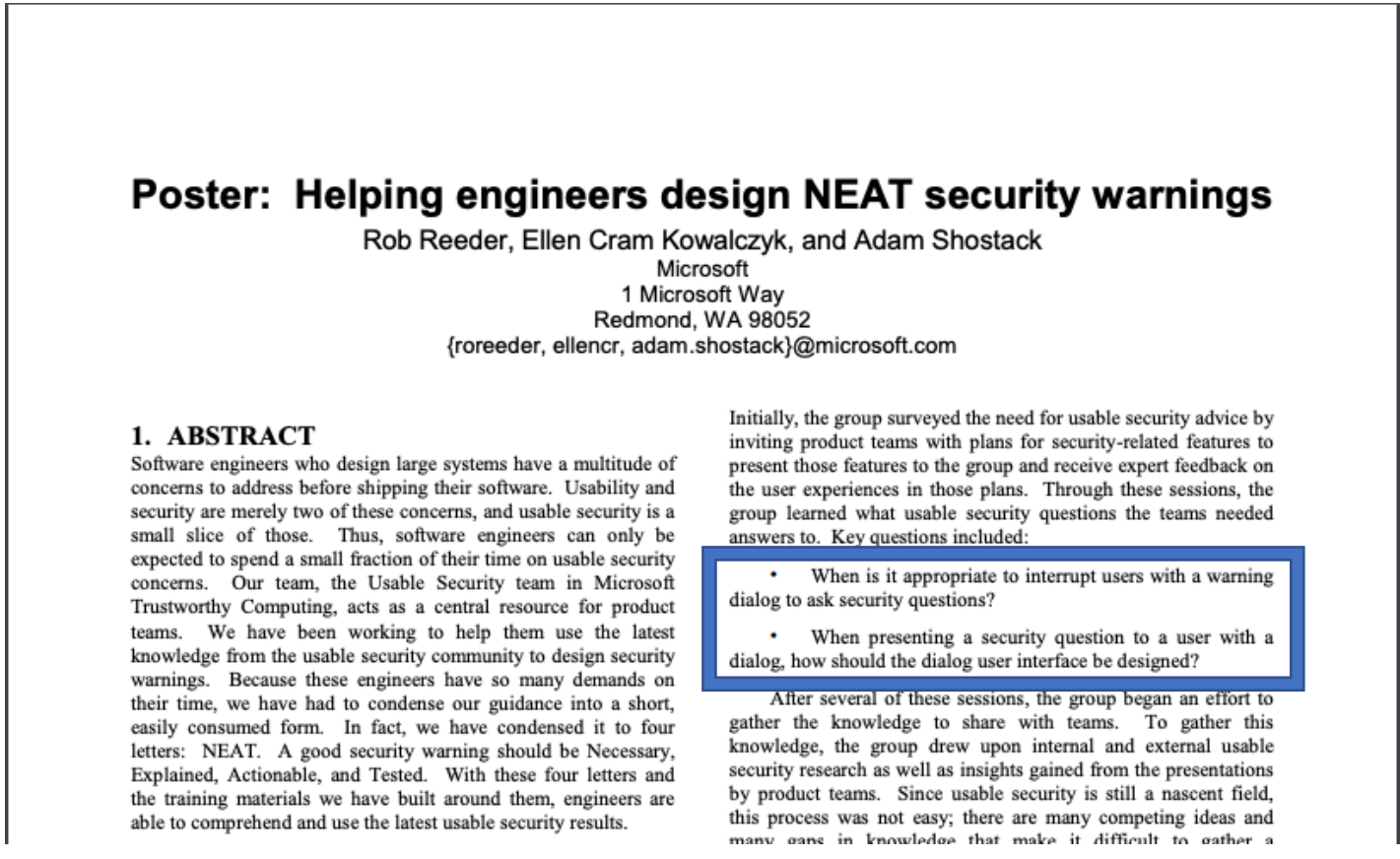
Warnings and the themes of the class

- Unmotivated user
  - “All I want is to do this thing”
- Uninformed user
  - Security fatigue
  - So many warnings, which one should I pay attention to?
- User workflow
  - Interruptions and annoyances
- And also: ***Users are not the enemy***
  - Showing a warning may not be enough
  - Can’t blame a user for “clicking through” a warning when bad things happen: **we should design better warning systems**

Designing NEAT security warnings

- When is it appropriate to interrupt users with a warning dialog to ask security questions?
- When presenting a security question to a user with a dialog, how should the dialog user interface be designed?

SOUPS Poster 2011



Poster: Helping engineers design NEAT security warnings

Rob Reeder, Ellen Cram Kowalczyk, and Adam Shostack
Microsoft
1 Microsoft Way
Redmond, WA 98052
{roreeder, ellencr, adam.shostack}@microsoft.com

1. ABSTRACT

Software engineers who design large systems have a multitude of concerns to address before shipping their software. Usability and security are merely two of these concerns, and usable security is a small slice of those. Thus, software engineers can only be expected to spend a small fraction of their time on usable security concerns. Our team, the Usable Security team in Microsoft Trustworthy Computing, acts as a central resource for product teams. We have been working to help them use the latest knowledge from the usable security community to design security warnings. Because these engineers have so many demands on their time, we have had to condense our guidance into a short, easily consumed form. In fact, we have condensed it to four letters: NEAT. A good security warning should be Necessary, Explained, Actionable, and Tested. With these four letters and the training materials we have built around them, engineers are able to comprehend and use the latest usable security results.

Initially, the group surveyed the need for usable security advice by inviting product teams with plans for security-related features to present those features to the group and receive expert feedback on the user experiences in those plans. Through these sessions, the group learned what usable security questions the teams needed answers to. Key questions included:

- When is it appropriate to interrupt users with a warning dialog to ask security questions?
- When presenting a security question to a user with a dialog, how should the dialog user interface be designed?

After several of these sessions, the group began an effort to gather the knowledge to share with teams. To gather this knowledge, the group drew upon internal and external usable security research as well as insights gained from the presentations by product teams. Since usable security is still a nascent field, this process was not easy; there are many competing ideas and many gaps in knowledge that make it difficult to gather a

Good Warnings

- Helps users determine whether they are actually at risk
- Stops users from doing something dangerous in risky context
- Doesn’t interfere with non-risky contexts

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**

Is this NEAT/SPRUCE? (IE 6)

NEAT

- Necessary
- Explained
- Actionable
- Tested

SPRUCE

- Source
- Process
- Risk
- Unique Knowledge
- Choices
- Evidence

In pairs/small groups: Make a warning!

- Flash drives can be dangerous
  - Left around with malware on them
  - Spread malware across machines
- Design a warning: USB autorun detected, option to prevent or continue.
- Use the NEAT and SPRUCE guidelines as you develop your design: http://cups.cs.cmu.edu/soups/2011/posters/soups_posters-Reeder.pdf

Wogalter Model

- Identify reasons that a particular warning is ineffective

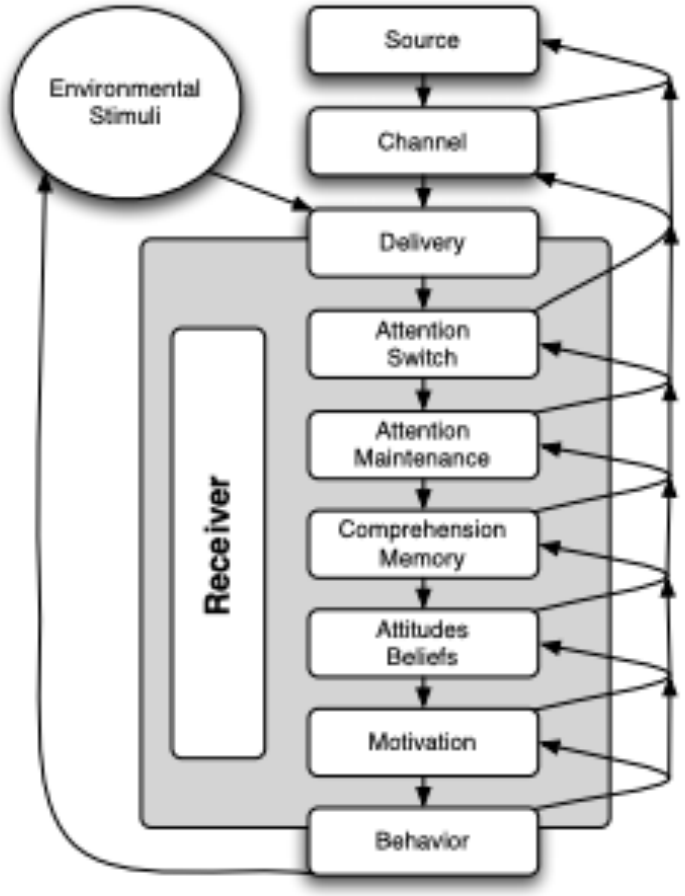


Figure 4. Diagram of the different phases of the C-HIP model [21].

We can ask the following questions to examine the different steps in Wogalter's model:

1. Attention Switch and Maintenance - Do users notice the indicators?
2. Comprehension/Memory - Do users know what the indicators mean?
3. Comprehension/Memory - Do users know what they are supposed to do when they see the indicators?
4. Attitudes/Beliefs - Do they believe the indicators?
5. Motivation - Are they motivated to take the recommended actions?
6. Behavior - Will they actually perform those actions?
7. Environmental Stimuli - How do the indicators interact with other indicators and other stimuli?

Alice in Warning Land

USENIX Security 2013

- Observe “warning impressions” *in situ* using In-browser telemetry
  - No need for deceptions
- Warning message types
  - Malware/Phishing
  - SSL Warnings

Alice in Warningland:
A Large-Scale Field Study of Browser Security Warning Effectiveness

Devdatta Akhawe
*University of California, Berkeley**
devdatta@cs.berkeley.edu

Adrienne Porter Felt
Google, Inc.
felt@google.com

Abstract

We empirically assess whether browser security warnings are as ineffective as suggested by popular opinion and previous literature. We used Mozilla Firefox and Google Chrome’s in-browser telemetry to observe over 25 million warning impressions *in situ*. During our field study, users continued through a tenth of Mozilla Firefox’s malware and phishing warnings, a quarter of Google Chrome’s malware and phishing warnings, and a third of Mozilla Firefox’s SSL warnings. This demonstrates that security warnings can be effective in practice; security experts and system architects should not dismiss the goal of communicating security information to end users. We also find that user behavior varies across warnings. In contrast to the other warnings, users continued through 70.2% of Google Chrome’s SSL warnings. This indicates that the user experience of a warning can have a significant impact on user behavior. Based on our findings, we make recommendations for warning designers and researchers.

The security community’s perception of the “oblivious” user evolved from the results of a number of laboratory studies on browser security indicators [5, 11, 13, 15, 27, 31, 35]. However, these studies are not necessarily representative of the current state of browser warnings in 2013. Most of the studies evaluated warnings that have since been deprecated or significantly modified, often in response to criticisms in the aforementioned studies. Our goal is to investigate whether modern browser security warnings protect users in practice.

We performed a large-scale field study of user decisions after seeing browser security warnings. Our study encompassed 25,405,944 warning impressions in Google Chrome and Mozilla Firefox in May and June 2013. We collected the data using the browsers’ telemetry frameworks, which are a mechanism for browser vendors to collect pseudonymous data from end users. Telemetry allowed us to unobtrusively measure user behavior during normal browsing activities. This design provides realism: our data reflects users’ actual behavior when presented with security warnings.

Data Collection --- huge data collection!

Sample Sizes. In Google Chrome, we recorded 6,040,082 malware warning impressions, 386,350 phishing warning impressions, and 16,704,666 SSL warning impressions. In Mozilla Firefox, we recorded 2,163,866 malware warning impressions, 100,004 phishing warning impressions, and 10,976 SSL warning impressions. Appendix A further breaks downs these sample sizes by OS and channel.

Number of Users. For Mozilla Firefox, we recorded warning impressions from the approximately 1% of Firefox users who opt in to share data with Mozilla via telemetry. In Google Chrome, we observed malware, phishing, and SSL warning impressions on 2,148,026; 204,462; and 4,491,767 clients (i.e., browser installs), respectively.

Malware Warning Messages (2012/2013)

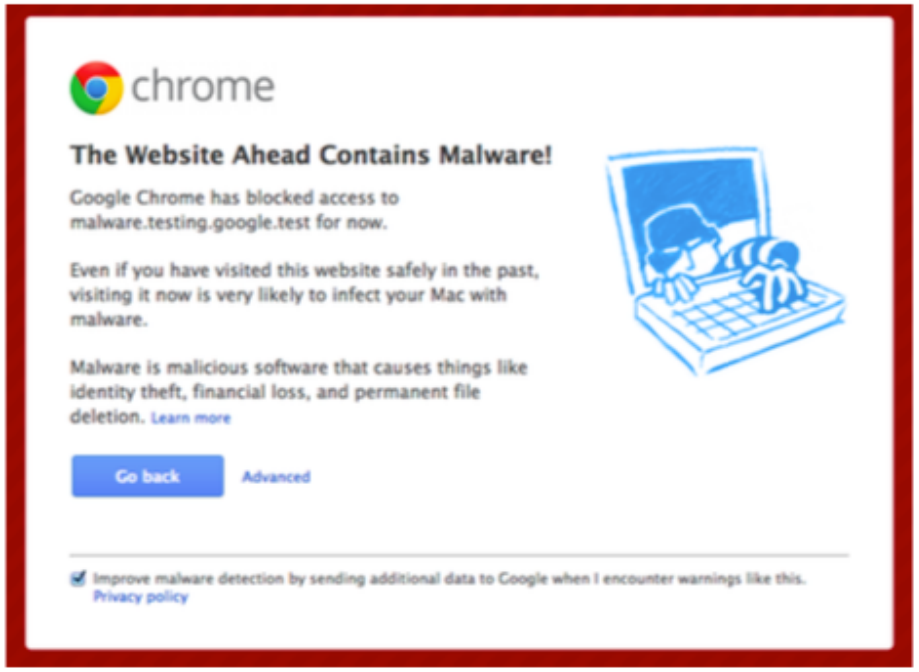


Figure 1: Malware warning for Google Chrome

Figure 2: Malware warning for Mozilla Firefox

SSL Warning Messages (2012/2013)

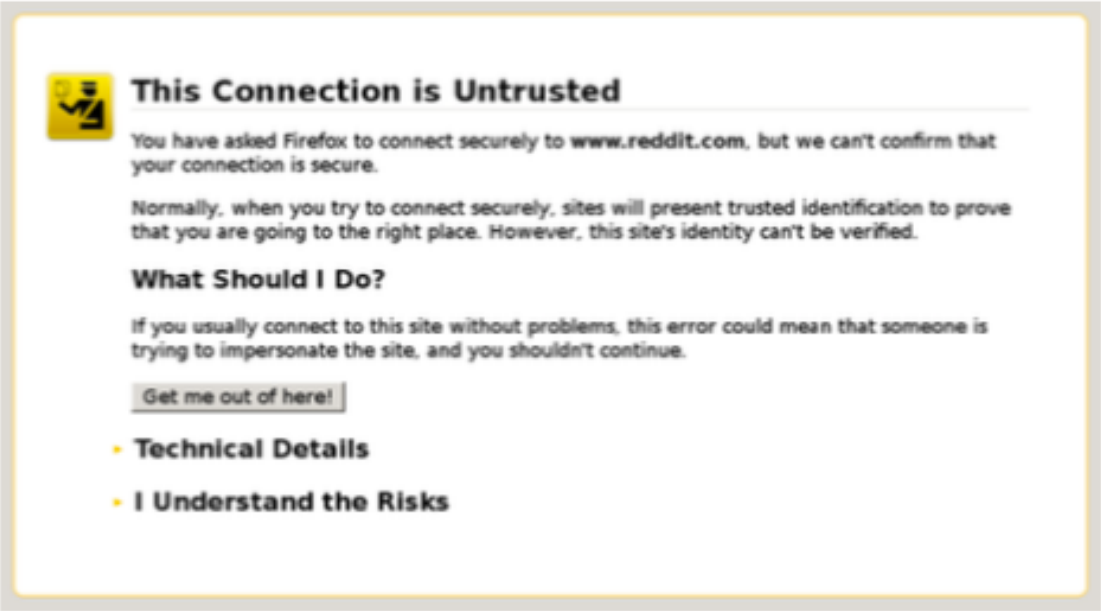


Figure 4: SSL warning for Mozilla Firefox

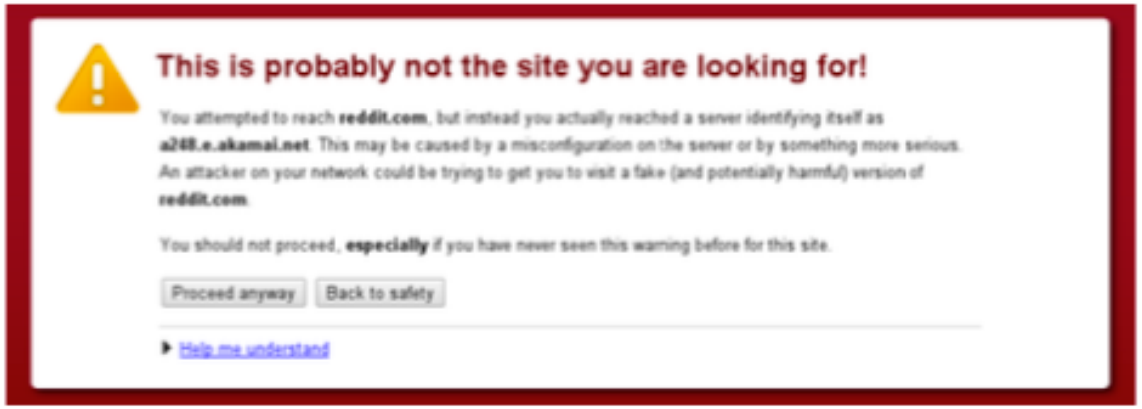


Figure 3: SSL warning for Google Chrome. The first paragraph changes depending on the specific SSL error.

Some Results

Some warnings seem to work well, others work very poorly.

What is the difference between Malware and SSL?

Operating System	Malware		Phishing	
	Firefox	Chrome	Firefox	Chrome
Windows	7.1%	23.5%	8.9%	17.9%
MacOS	11.2%	16.6%	12.5%	17.0%
Linux	18.2%	13.9%	34.8%	31.0%

Table 1: User operating system vs. clickthrough rates for malware and phishing warnings. The data comes from stable (i.e., release) versions.

# of clicks doesn't impact clickthrough

- Hiding "proceed" button doesn't do much

Operating System	SSL Warnings	
	Firefox	Chrome
Windows	32.5%	71.1%
MacOS	39.3%	68.8%
Linux	58.7%	64.2%
Android	NC	64.6%

Table 3: User operating system vs. clickthrough rates for SSL warnings. The Google Chrome data is from the stable channel, and the Mozilla Firefox data is from the beta channel.

Chrome Warnings (2019)

Your connection is not private

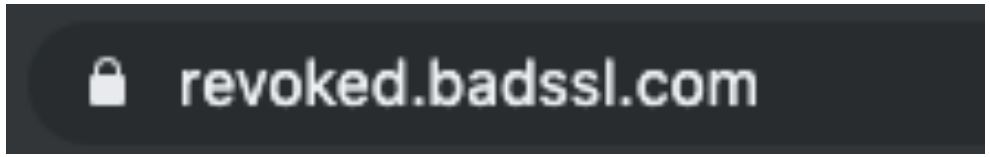
Attackers might be trying to steal your information from **self-signed.badssl.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

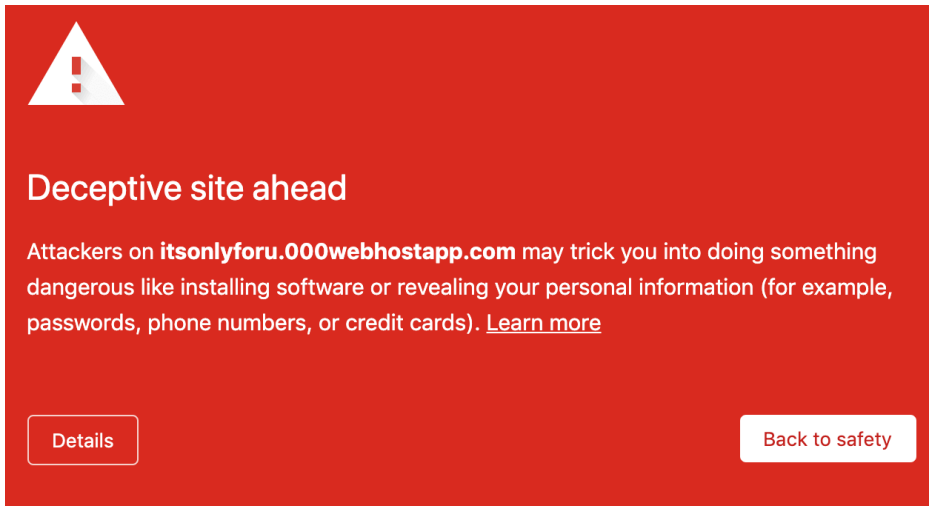
☐ Help improve Safe Browsing by sending some system information and page content to Google.
Privacy policy

Advanced Back to safety

Self Signed/Invalid Authority



Revoked Certificate



Deceptive site ahead

Attackers on **itsonlyforu.000webhostapp.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more

Details Back to safety

Malware Warning

Is it possible to focus users' attention on key information?

SOUPS 2013

- Use **ATTRACTORS** to draw attention to the publisher's name
- Force delay before users can install
- Force interaction before users can install
- Force users to read publisher name

Your Attention Please

Designing security-decision UIs to make genuine risks harder to ignore

Cristian Bravo-Lillo
cbravo@cmu.edu

Lorrie Faith Cranor
lorrie@cmu.edu

Julie Downs
downs@cmu.edu

Saranga Komanduri
sarangak@cmu.edu

Robert W. Reeder
reeder@cs.cmu.edu

Stuart Schechter
stus@microsoft.com

Manya Sleeper
msleeper@cmu.edu

ABSTRACT

We designed and tested *attractors* for computer security dialogs: user-interface modifications used to draw users' attention to the most important information for making decisions. Some of these modifications were purely visual, while others temporarily inhibited potentially-dangerous behaviors to redirect users' attention to salient information. We conducted three between-subjects experiments to test the effectiveness of the attractors.

In the first two experiments, we sent participants to perform a task on what appeared to be a third-party site that required installation of a browser plugin. We presented them with what appeared to be an installation dialog from their operating system. Participants who saw dialogs that employed inhibitive attractors were significantly less likely than those in the control group to ignore clues that installing this software might be harmful.

In the third experiment, we attempted to habituate participants to dialogs that they knew were part of the experiment. We used attractors to highlight a field that was of no value during habituation trials and contained critical information after the habituation period. Participants exposed to inhibitive attractors were two to three times more likely to make an informed decision than those in the control condition.

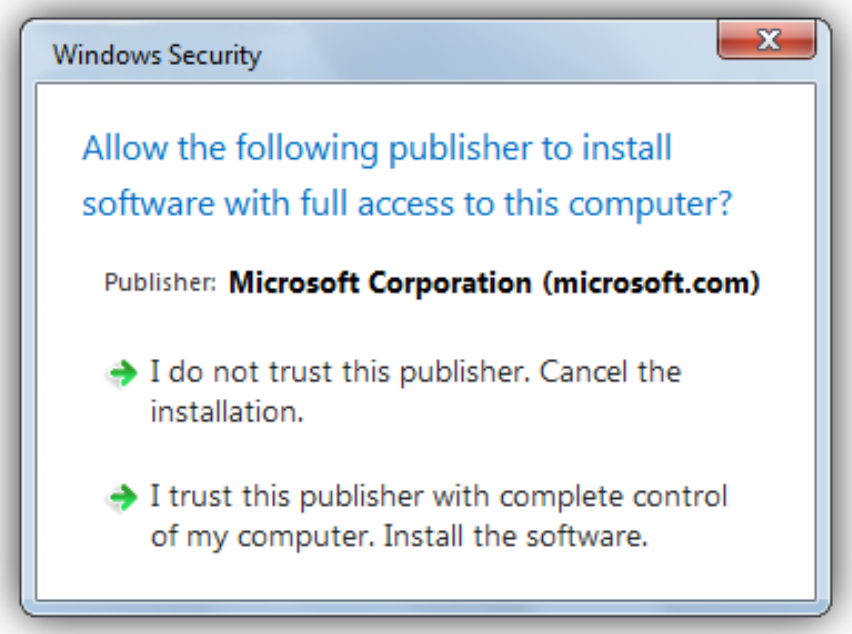
1. INTRODUCTION

Like the boy who cried wolf from Aesop's Fables, today's computer systems perpetually cry for attention in the name of safety, and hundreds of cries may be heard without a real threat. *Did you want to open a file in a legacy file format? Is it OK that this certificate is out of date? Do you want to view content that was sent insecurely?* The inevitable result is that, like Aesop's villagers, users stop paying attention. When a security dialog does contain information that could alert users to a real risk, they are less likely to notice it.

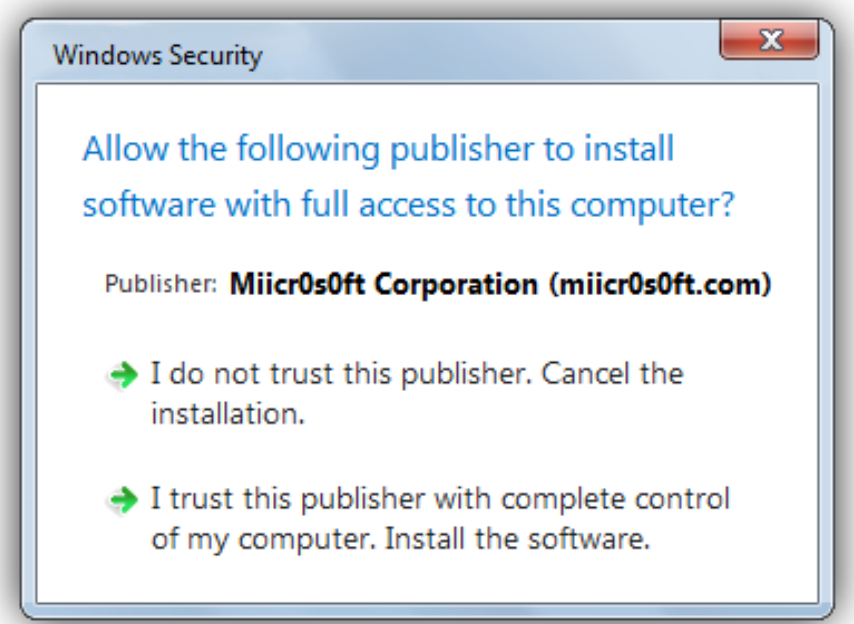
Reducing the onslaught of interrupting security warning dialogs might help reduce the strain on users' attention. Some warnings can be removed by re-architecting systems to reduce the potential for harm, such as by building file parsers in type-safe languages or sandboxing unsafe code.

Yet inevitably, some decisions must eventually be made by users. One type of unavoidable decision is the choice to take a risk that some users may embrace and others may reject. For example, some users may want to share their location with an application that others would not share their location with. In other cases, users have knowledge, which the system does not have, that is essential to making a correct choice. For example, the user may know that a particular wireless network is operated by somebody they trust.

The experiment: Can you spot the difference?



benign

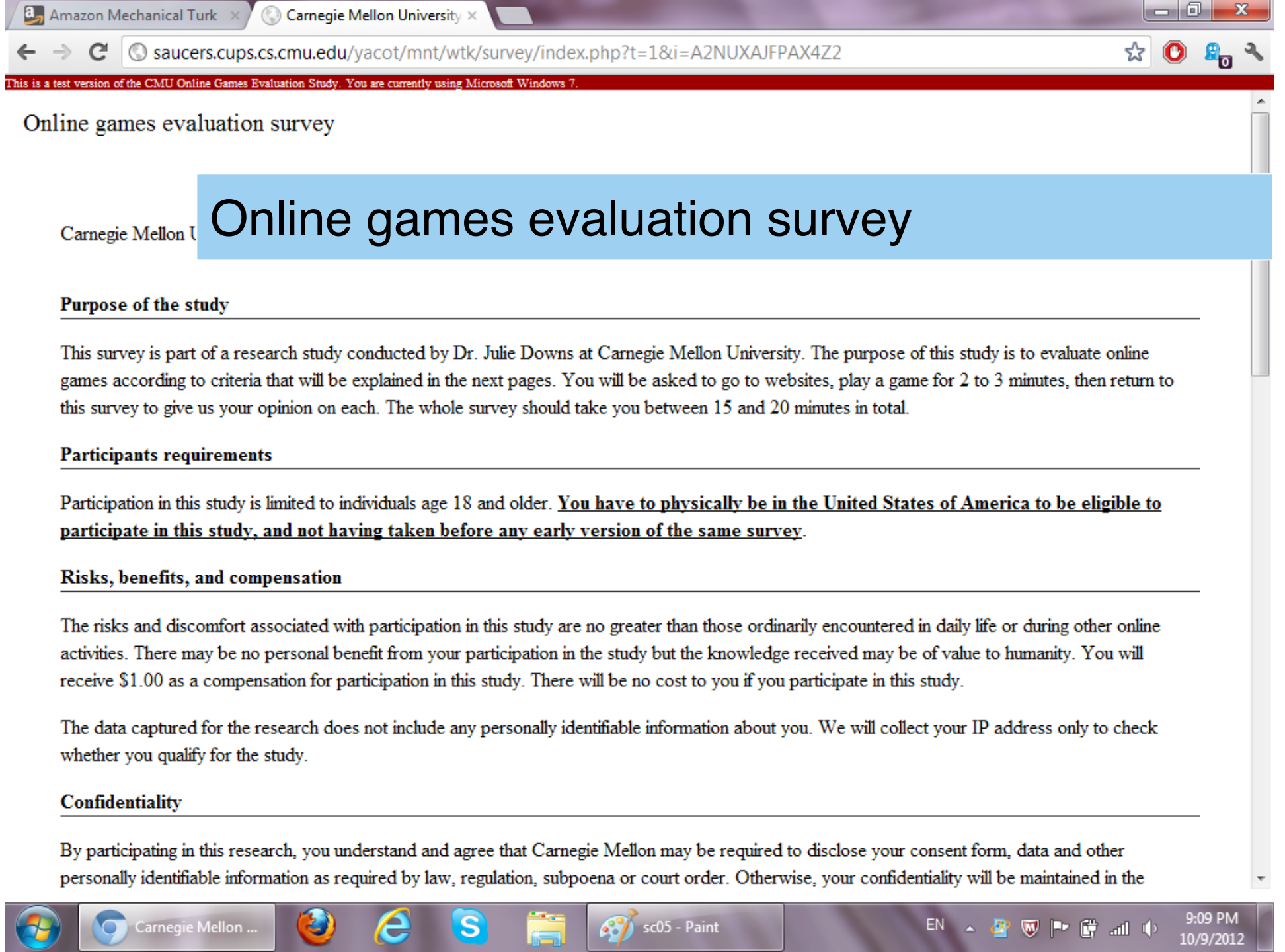


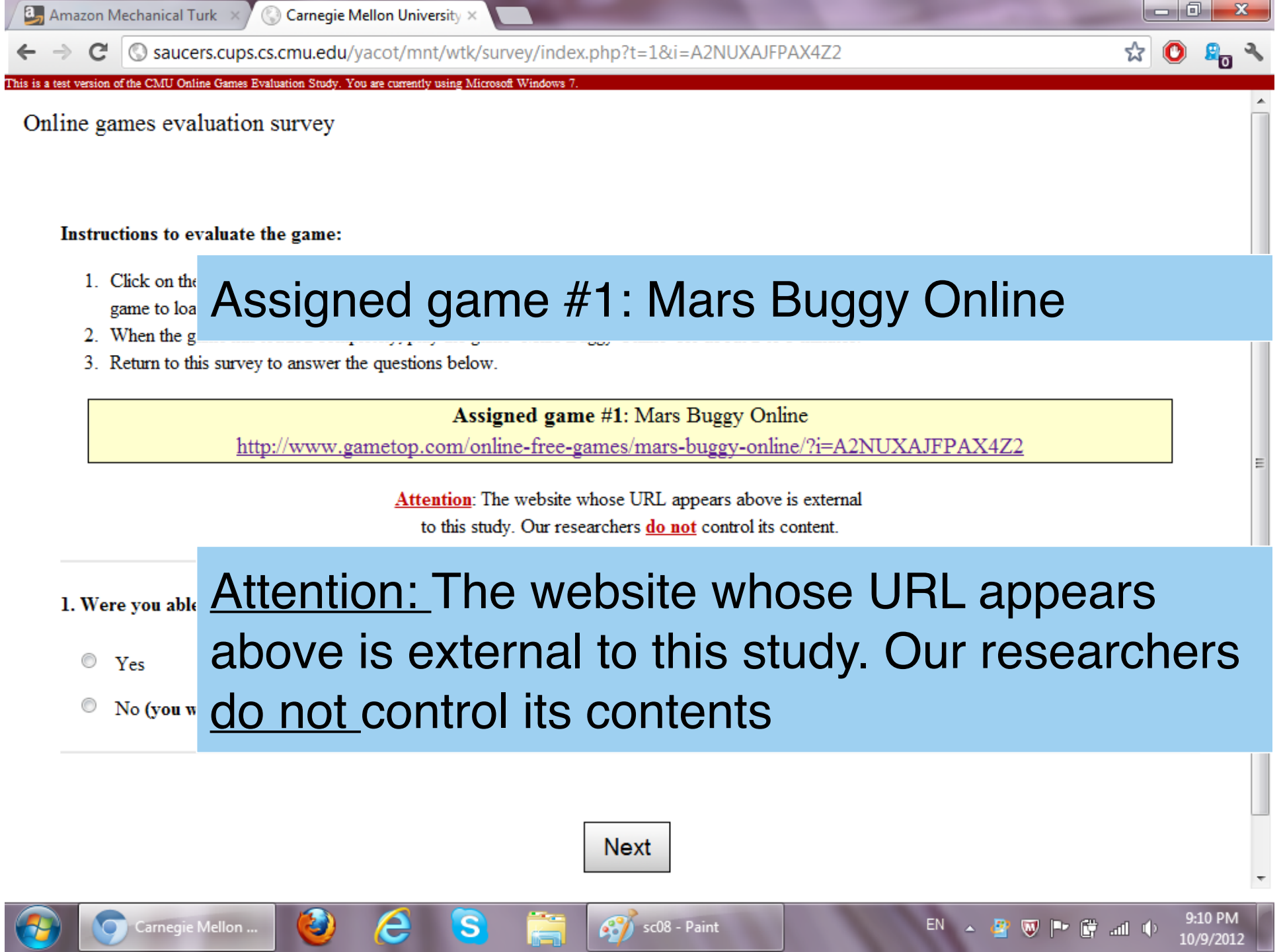
suspicious

The Task

- Participants were asked to evaluate three online games
  - Form contained a link to the game
  - Participants must install the game

- Ecological Validity
  - “By clicking on this link you acknowledge that the website you will be directed to is in no way affiliated with Carnegie Mellon University, and that CMU is in no way responsible for the content of this website.”


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

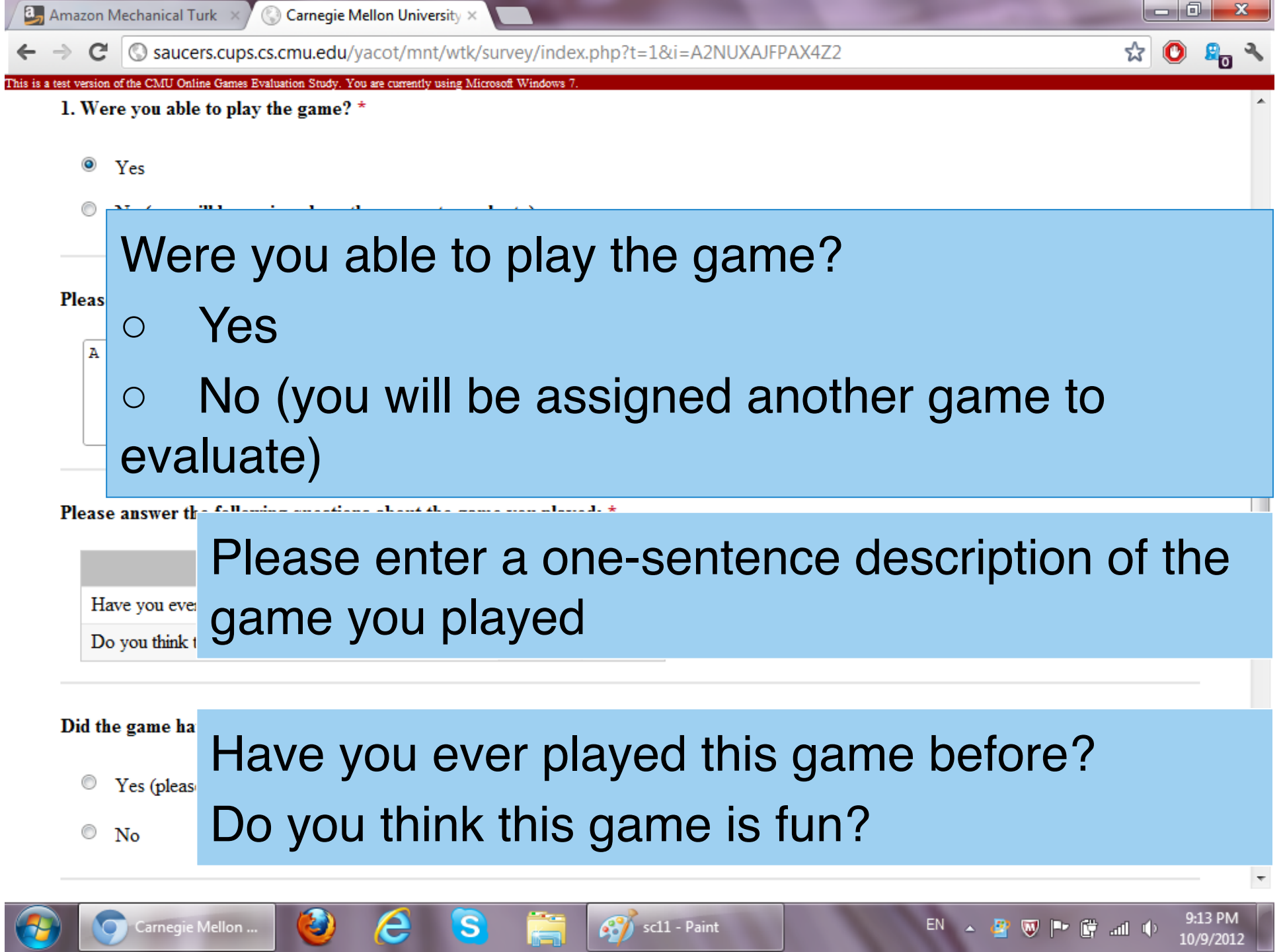
www.gametop.com/online-free-games/mars-buggy-online/?i=A2NUXAJFPAX4Z2

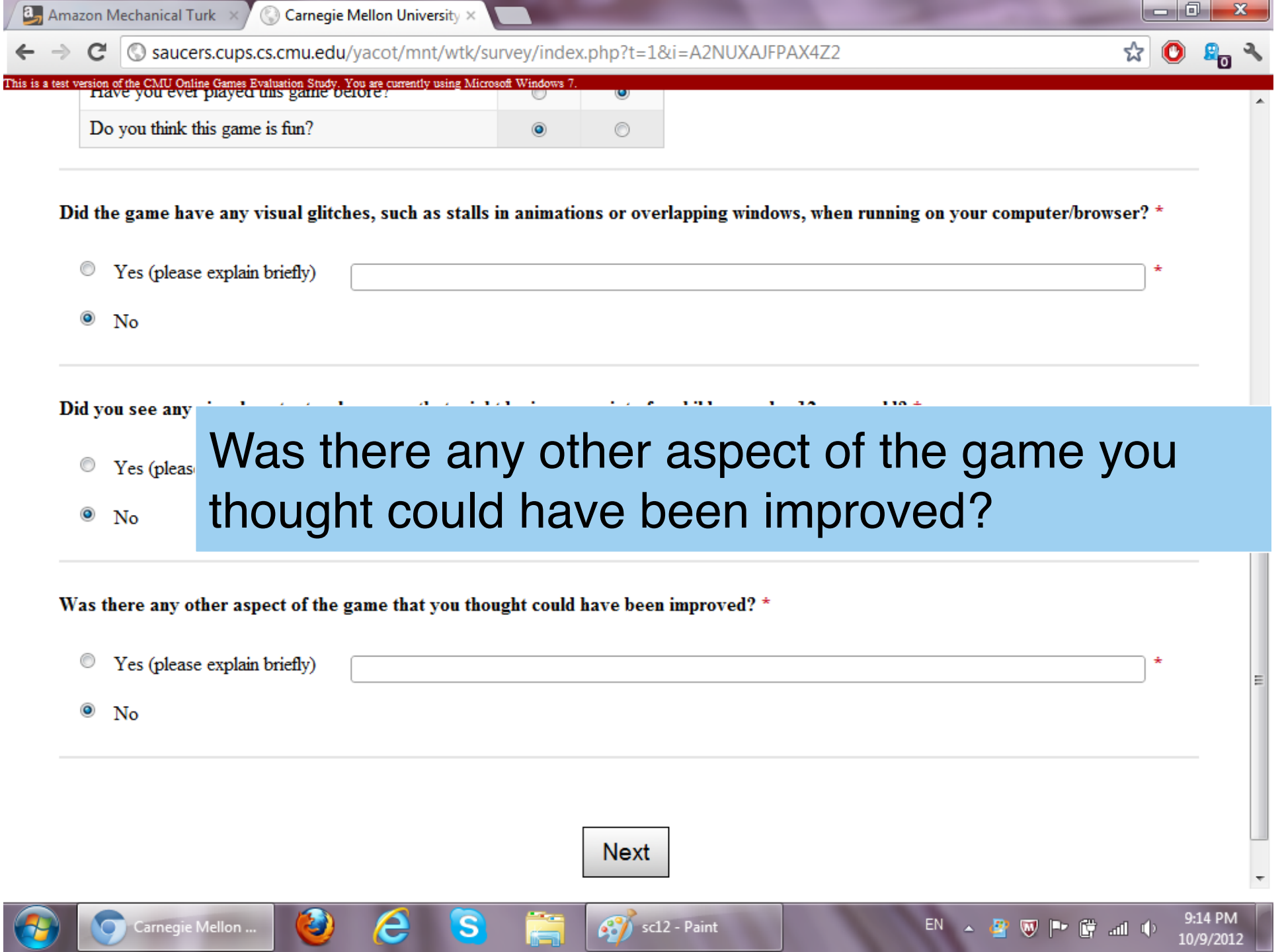
need to be rescued.

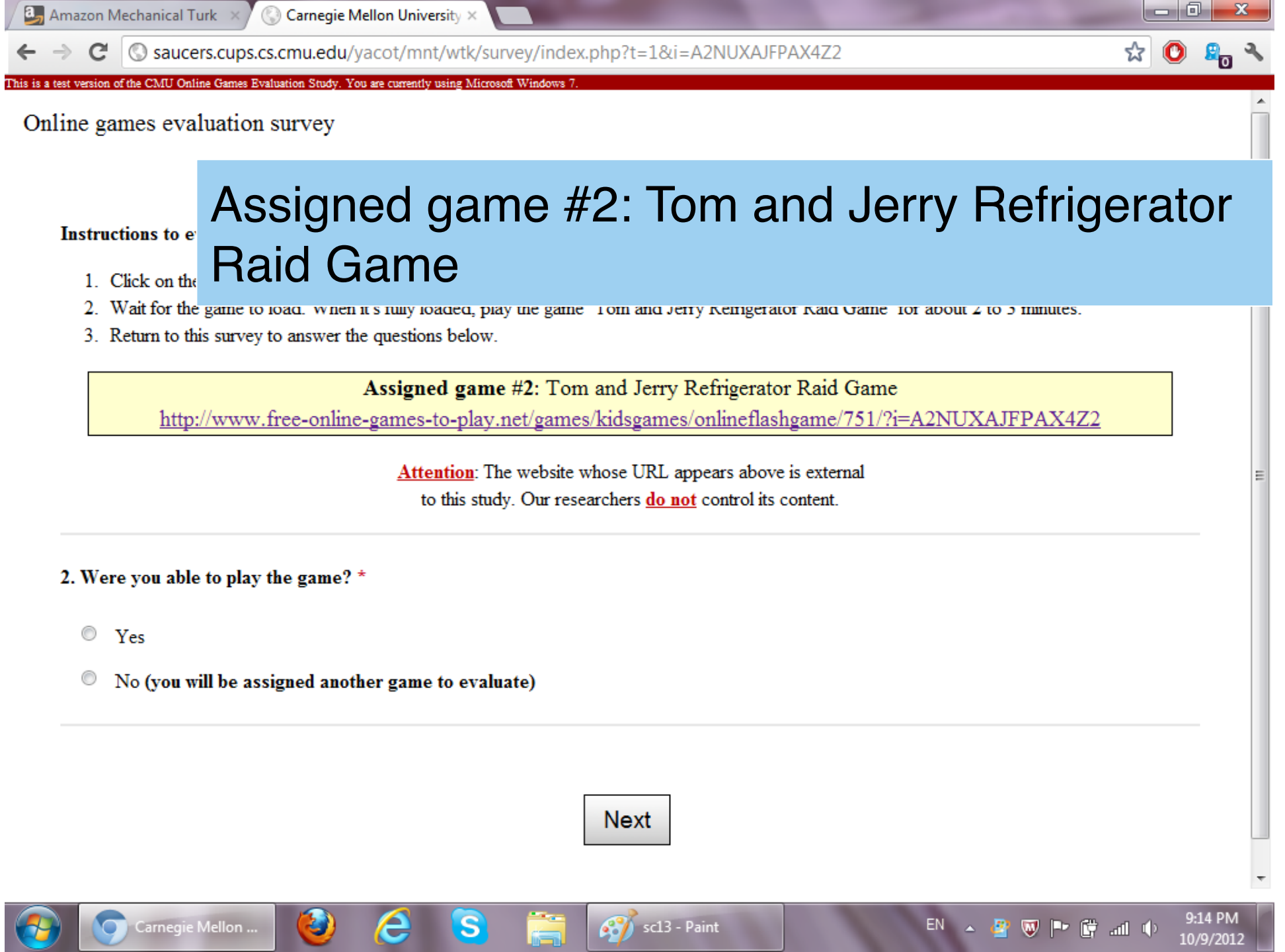
Play this free online game today and bring your crew back to earth.

Do you like this game? Tweet

Mars Buggy


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
Were you able to play the game?
○ Yes
○ No (you will be assigned another game to evaluate)
Please enter a one-sentence description of the game you played
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



Assigned game #2: Tom and Jerry Refrigerator Raid Game

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

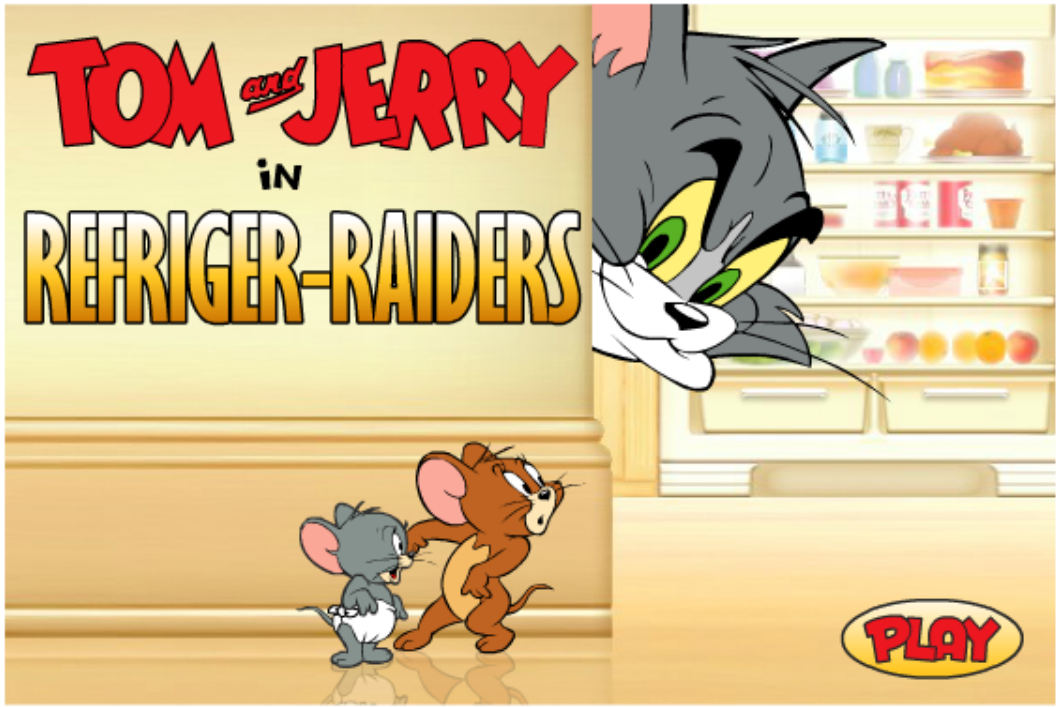
www.free-online-games-to-play.net/games/kidsgames/onlineflashgame/751/?i=A2NUXAJFPAX4Z2/

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.

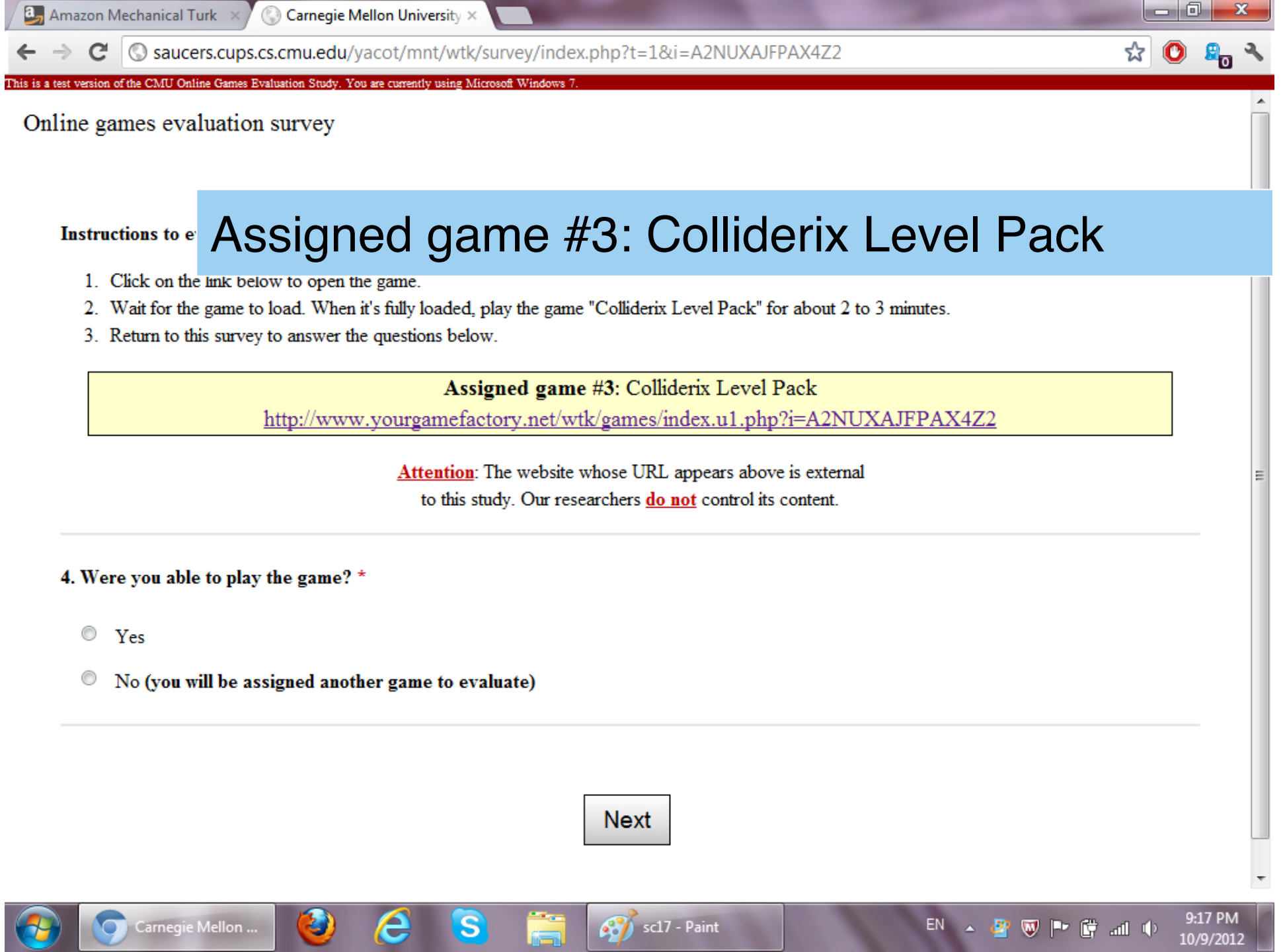
Please answer the following questions about the game you played: *

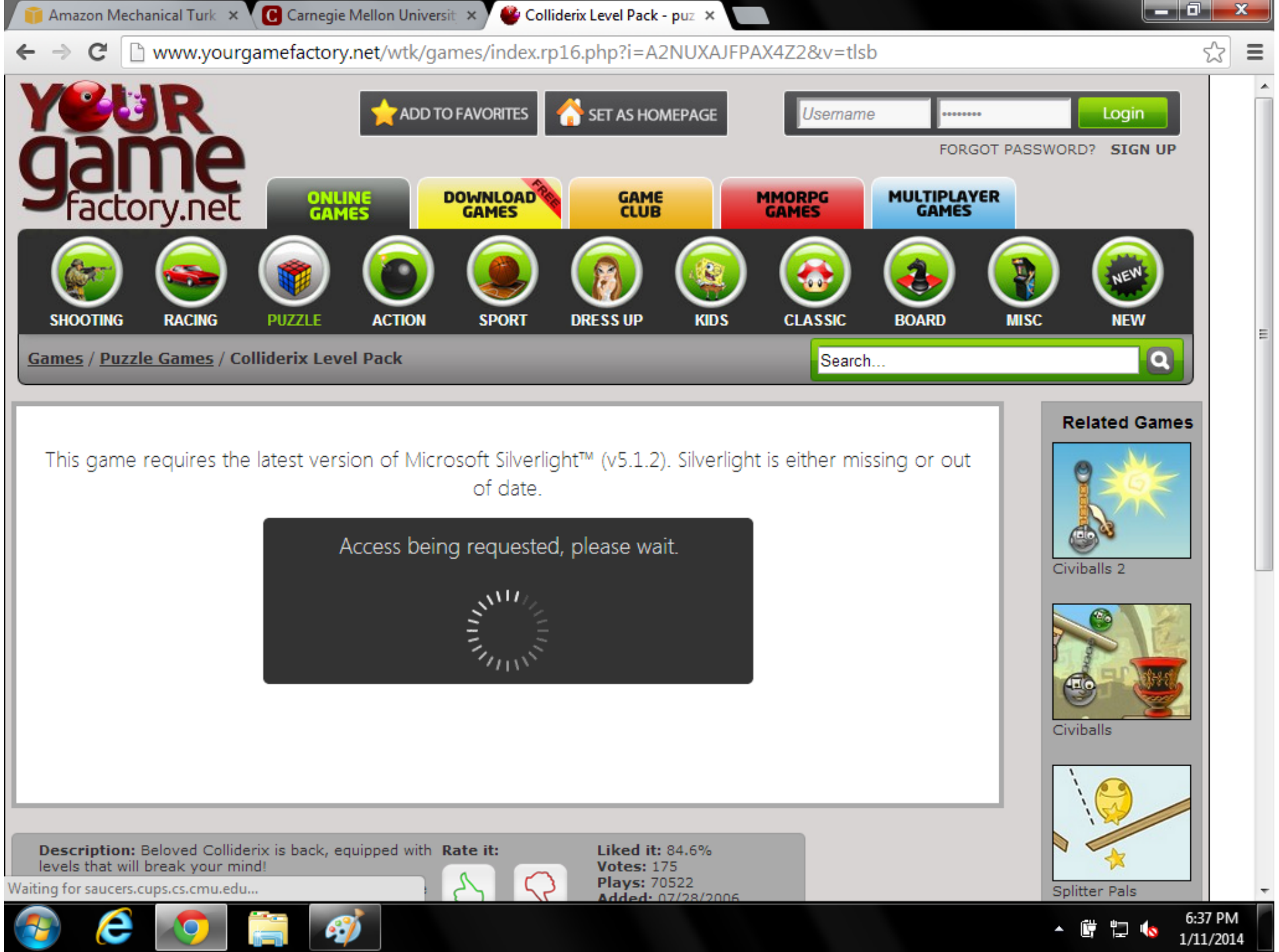
	Yes	No
Have you ever played this game before?	( )	(•)
Do you think this game is fun?	( )	(•)

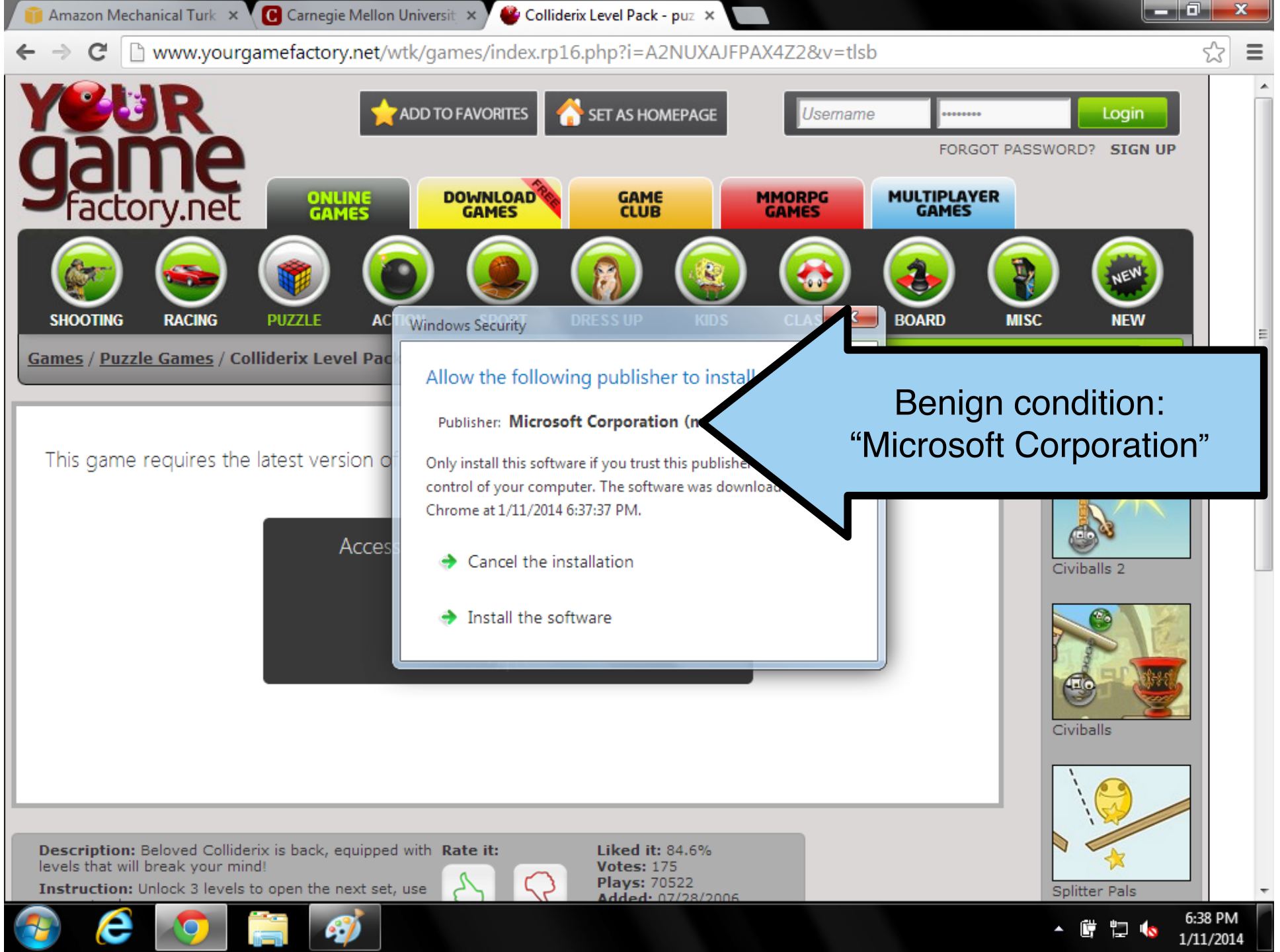
Did the game have any visual glitches, such as stalls in animations or overlapping windows, when running on your computer/browser? *

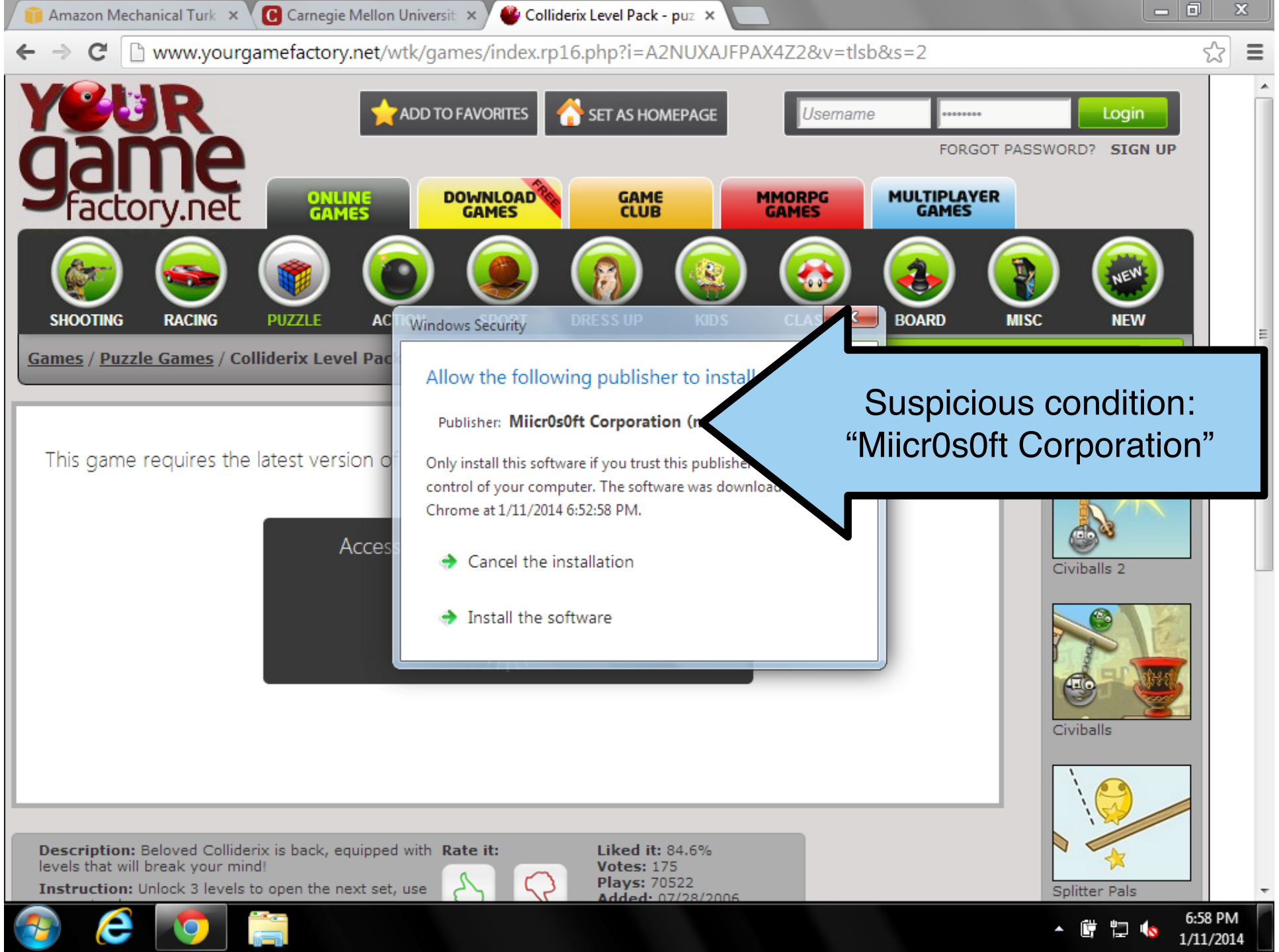
- ( ) Yes (please explain briefly) [ ] *
- ( ) No

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 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
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.
Related Games
Civiballs 2
Civiballs
Splitter Pals
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...
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
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 downloa
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
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
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

Participant Decision Design

- Amazon Mechanical Turk
  - Must complete the task they accept (otherwise, don't earn money)
    - Incentivized to finish an accepted task
  - Want to minimize the time and effort on each task
    - Opportunity cost

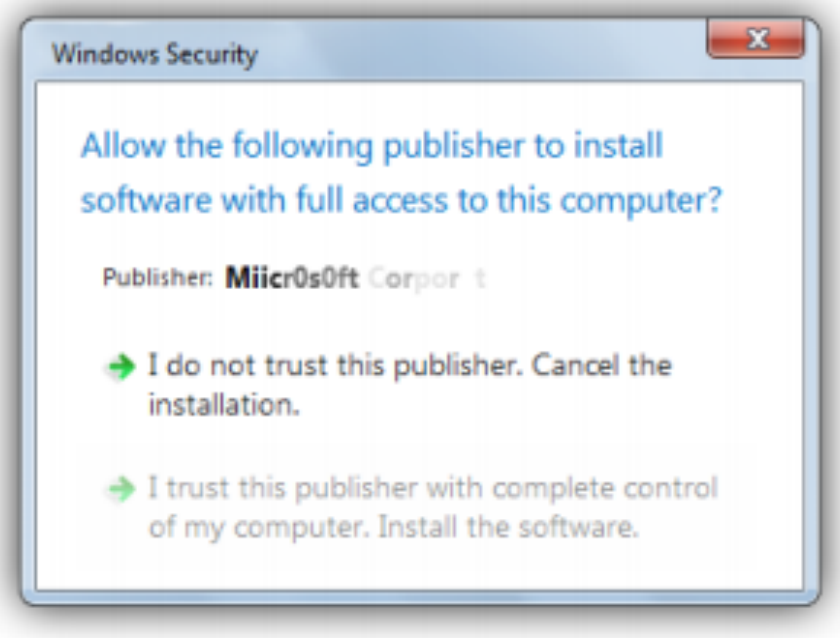
- "You can skip a game. If you do, we will assign you another."
  - It was ok to say NO but may be longer to complete

- Time/Money vs. Security
  - Install -> Take small risk, play the game, finish sooner
  - Not Install -> No risk, but waste time doing another game

- All participants were **DEBRIEFED** after the study

Delay and Focus: Animation and Reveal

(b) *Animated Connector (AC)*



(c) *Progressive Reveal*

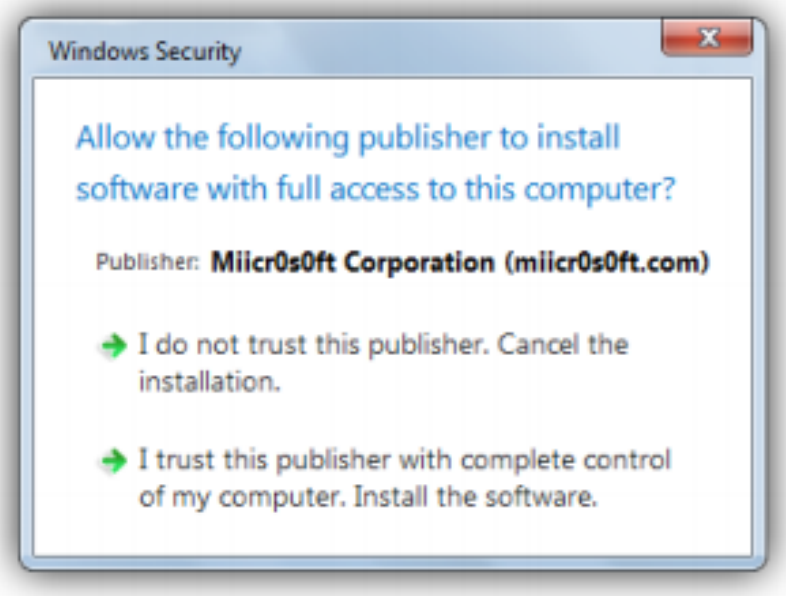
Force Interaction

(d) *Swipe* (e) *Type* (f) *Request*

ANSI Standard Warnings

(g) *ANSI*

Different Messaging



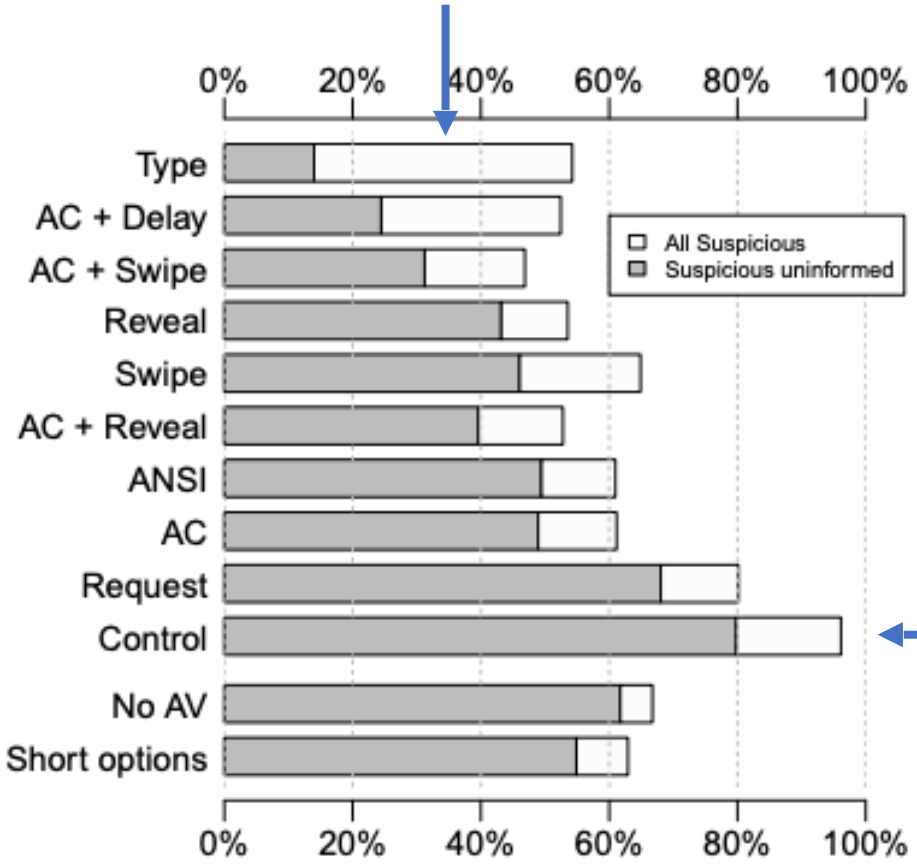
(a) *Control*

(h) *No Antivirus*

(i) *Short options*

Some Results

Participants noticed when they had to type the name



(a) Exp. 1: Suspicious install rate / benign install rate

All attractors work well

Control

Nudges

- Soft paternalistic interventions nudging users toward more secure behaviors
  - Seeks to influence decisions without actually limiting choices

Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online

ALESSANDRO ACQUISTI, Carnegie Mellon University
IDRIS ADJERID, University of Notre Dame
REBECCA BALEBAKO, Carnegie Mellon University
LAURA BRANDIMARTE, University of Arizona
LORRIE FAITH CRANOR, Carnegie Mellon University
SARANGA KOMANDURI, Civis Analytics
PEDRO GIOVANNI LEON, Banco de Mexico
NORMAN SADEH, Carnegie Mellon University
FLORIAN SCHAUB, University of Michigan
MANYA SLEEPER, Carnegie Mellon University
YANG WANG, Syracuse University
SHOMIR WILSON, University of Cincinnati

Advancements in information technology often task users with complex and consequential privacy and security decisions. A growing body of research has investigated individuals' choices in the presence of privacy and information security tradeoffs, the decision-making hurdles affecting those choices, and ways to mitigate such hurdles. This article provides a multi-disciplinary assessment of the literature pertaining to privacy and security decision making. It focuses on research on assisting individuals' privacy and security choices with soft paternalistic interventions that nudge users toward more beneficial choices. The article discusses potential benefits of those interventions, highlights their shortcomings, and identifies key ethical, design, and research challenges.

CCS Concepts: • **Security and privacy** → **Human and societal aspects of security and privacy**; • **Human-centered computing** → *Human computer interaction (HCI); Interaction design;*

Additional Key Words and Phrases: Privacy, security, nudge, soft paternalism, behavioral economics

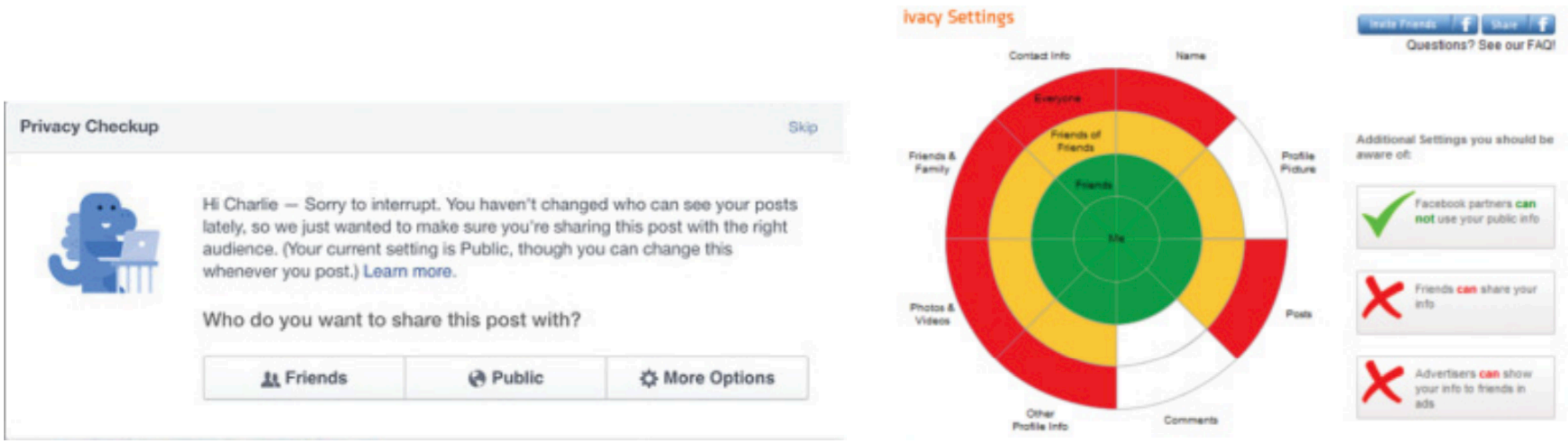


Fig. 3. Facebook-related privacy nudges. Facebook's privacy dinosaur (*left*) reminds users that they are about to post publicly and nudges them to check their privacy settings. PrivacyDefender (*right*) visualizes the audience of information on Facebook.

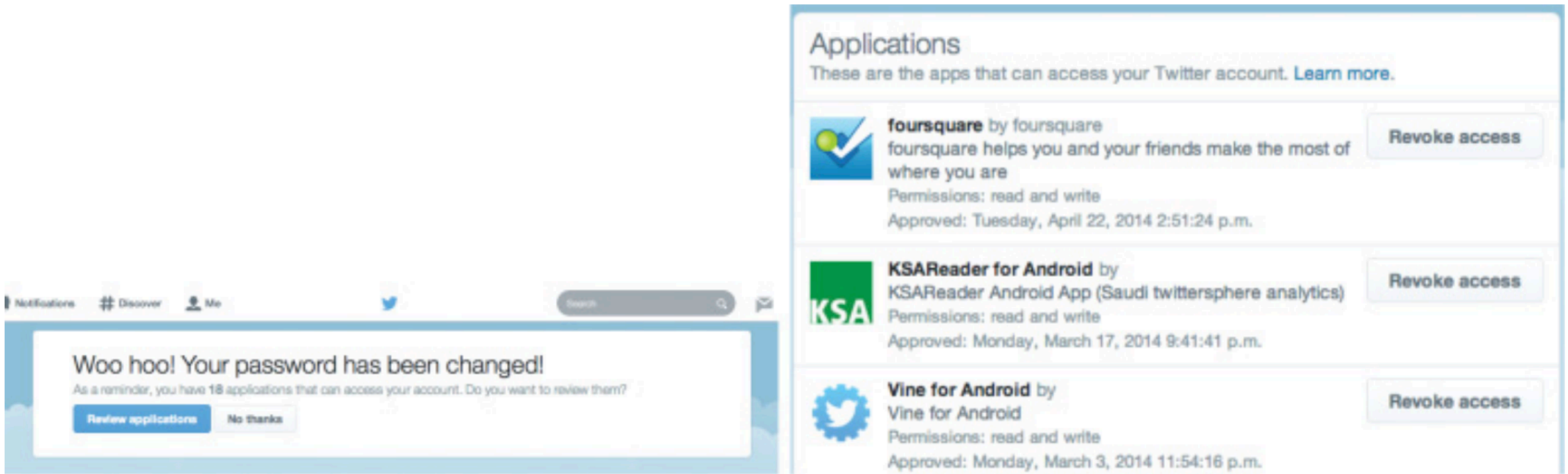


Fig. 4. Twitter nudges users to check their application access settings, right after they change their password—making it more likely for users to act on the nudge.

What we did today!

- NEAT/SPRUCE Guidelines
- Wogalter Communication-Human Interaction Process
  - Getting the users' attention
- Nudges

What’s next?

- Online Tracking and Compliance