06. Designing and Analyzing Quantitative Studies; Security Warnings

Blase Ur, April 12th, 2017
CMSC 23210 / 33210

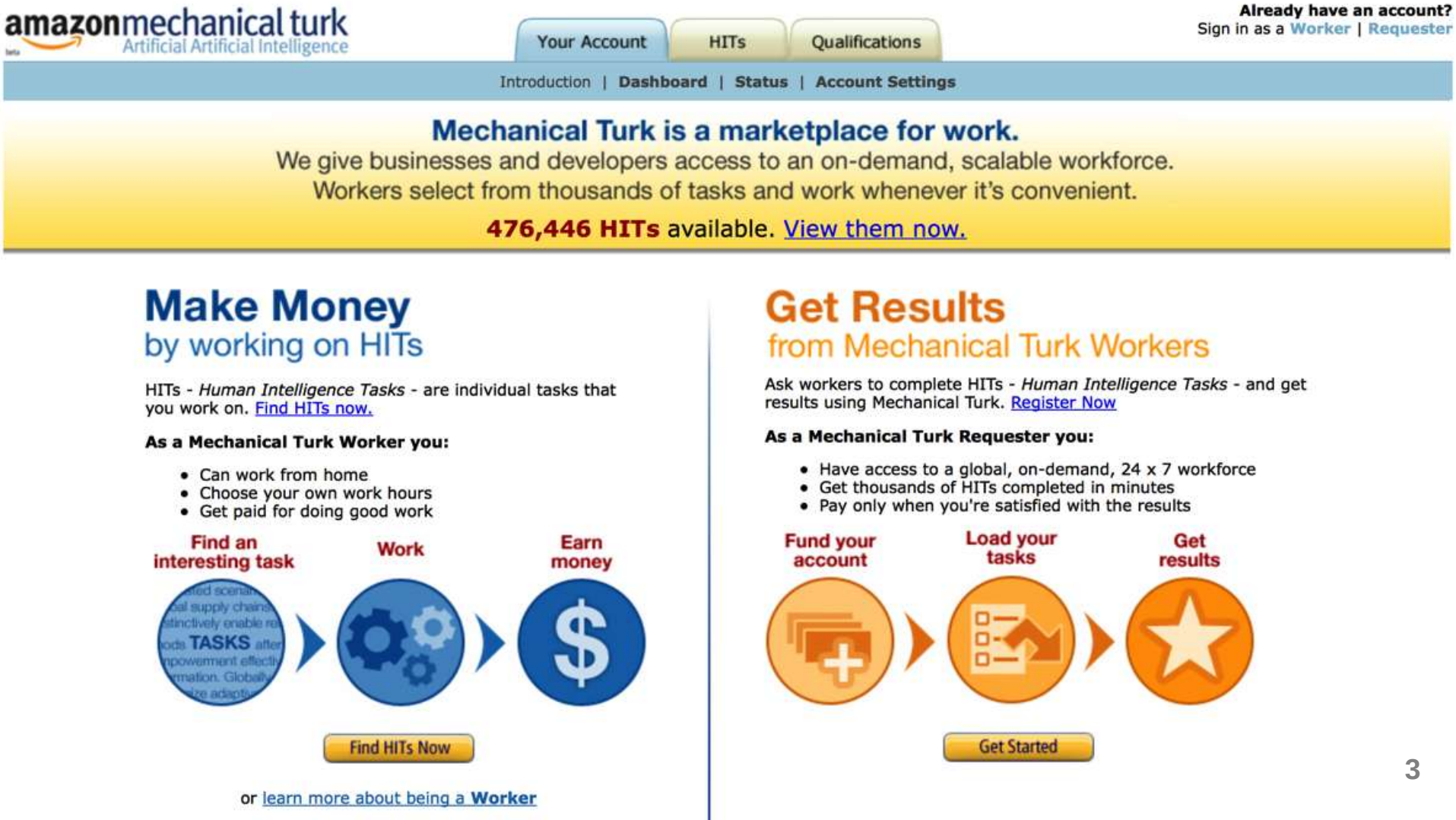
THE UNIVERSITY OF CHICAGO

Security, Usability, & Privacy Education & Research

Today's class

- PSET 1 Usability Studies
- MTurk
- Finish discussing ethical experiments
- **Quantitative studies about warnings!**

Amazon Mechanical Turk



Security Warnings

Image courtesy of Johnathan Nightingale

Users swat away warning dialogs

How can we get users to pay attention?

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

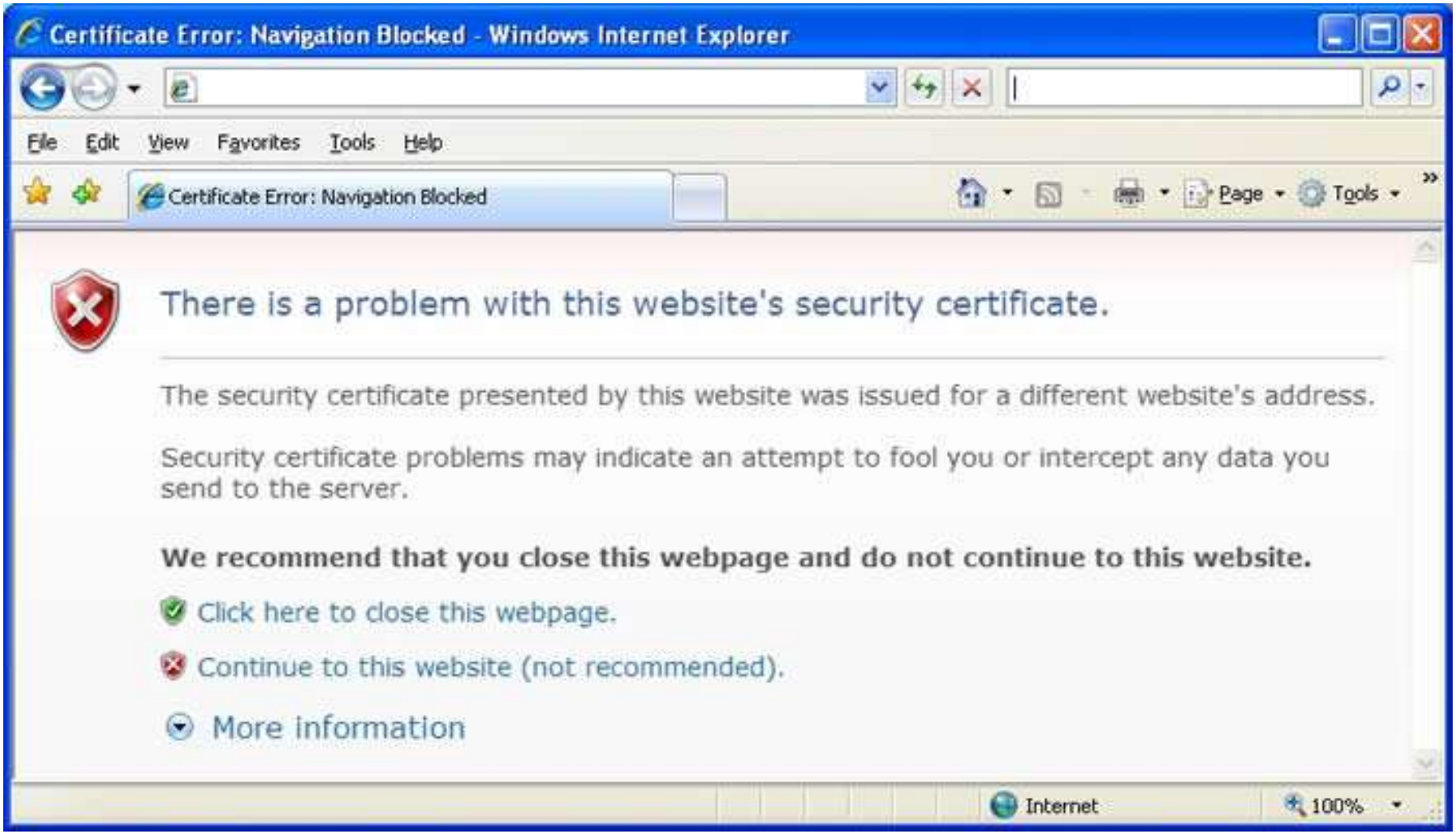
SPRUCE

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

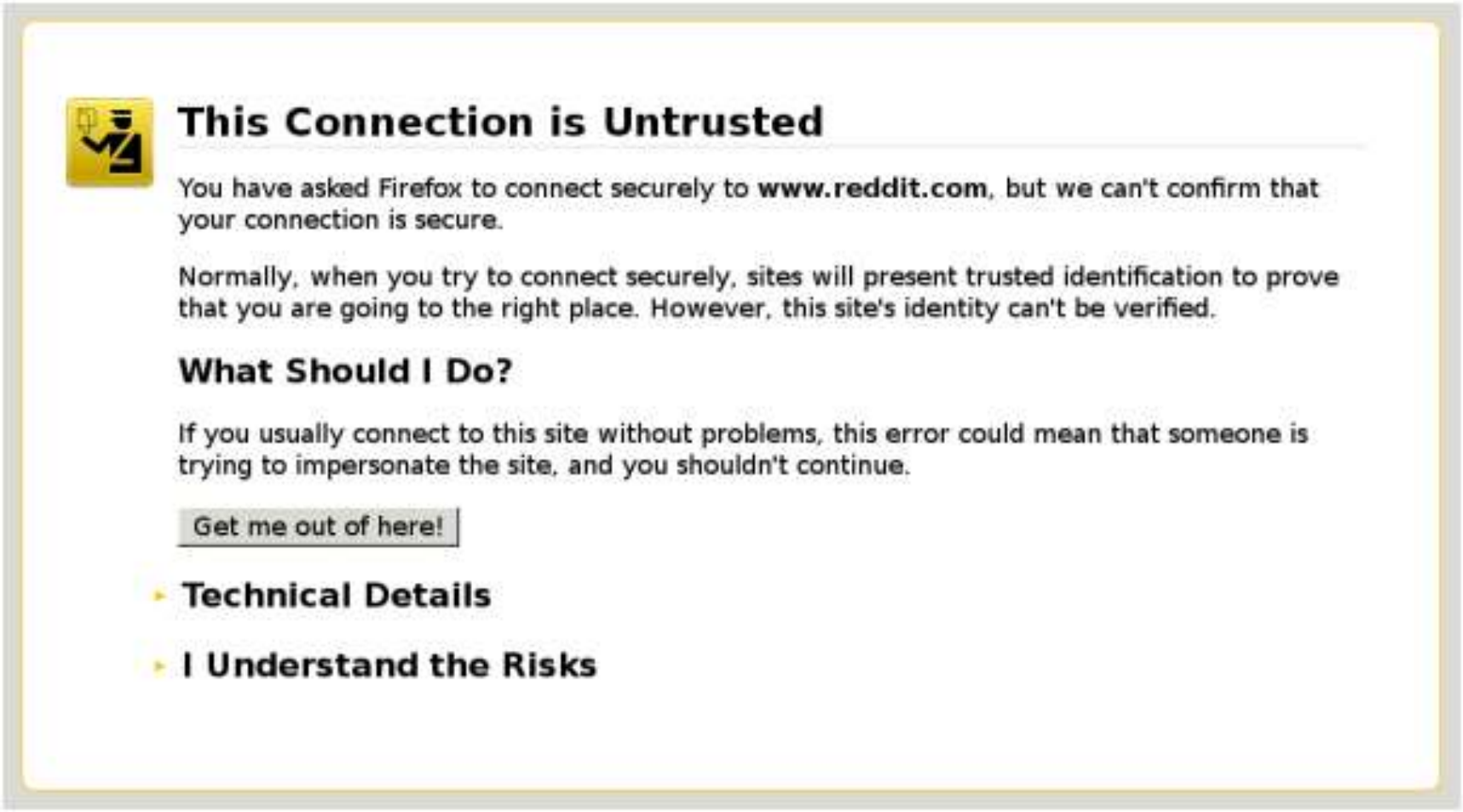
Alice in Warningland

Old Warning (IE 6)

Slightly Newer Warning (IE 7)

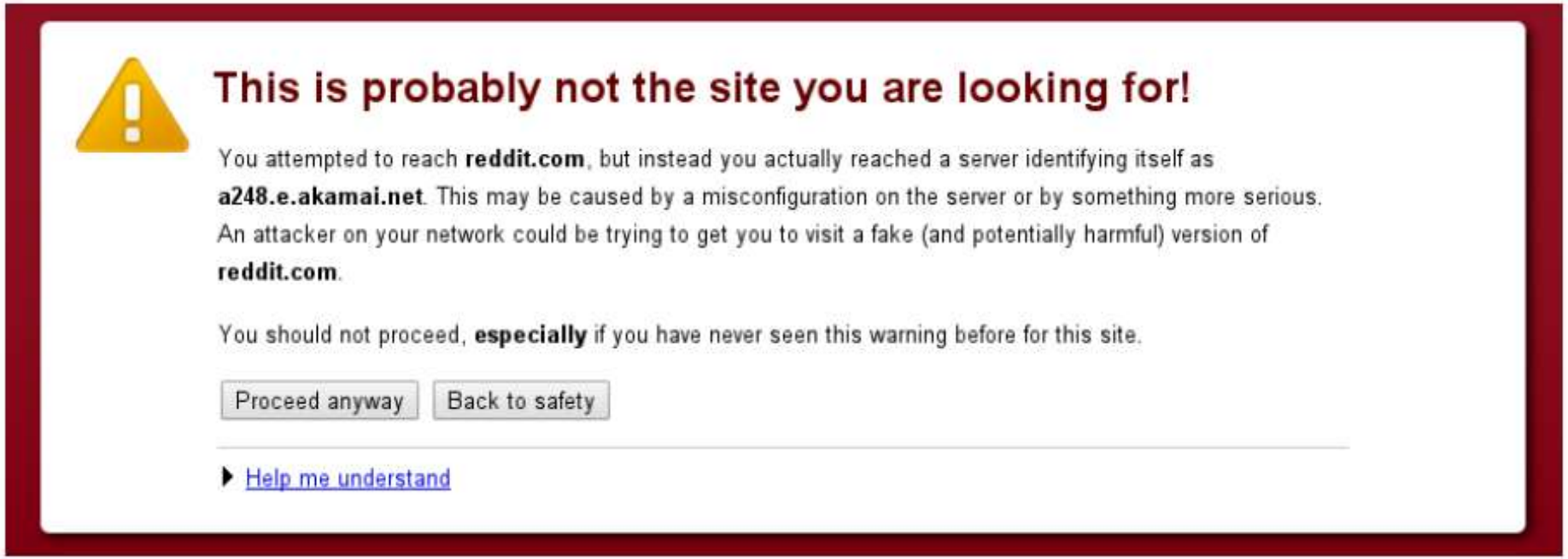


Newer Warning (Firefox)



Newer Warning (Firefox): Step 2

Newer Warning (Chrome)



Alice in Warningland takeaways

- Field study: correlation or causation?
- Is clicking through an SSL warnings always wrong?
  - Technically skilled users (e.g., Linux users) ignored warnings more often
- Comparison with lab studies
- Prior lab study using eye-tracking software (Whalen and Inkpen)

More takeaways

- Passive warnings vs. interstitial warnings
- Consent and ethics
- Sampling bias
- Dealing with noisy data
  - Differences between Chrome and Firefox
- Certificate pinning
- HSTS (HTTP Strict Transport Security)

How do you know when you are actually at risk?

Some hazards are ALWAYS dangerous

Some hazards are context dependent

Computer security dialogs are context dependent

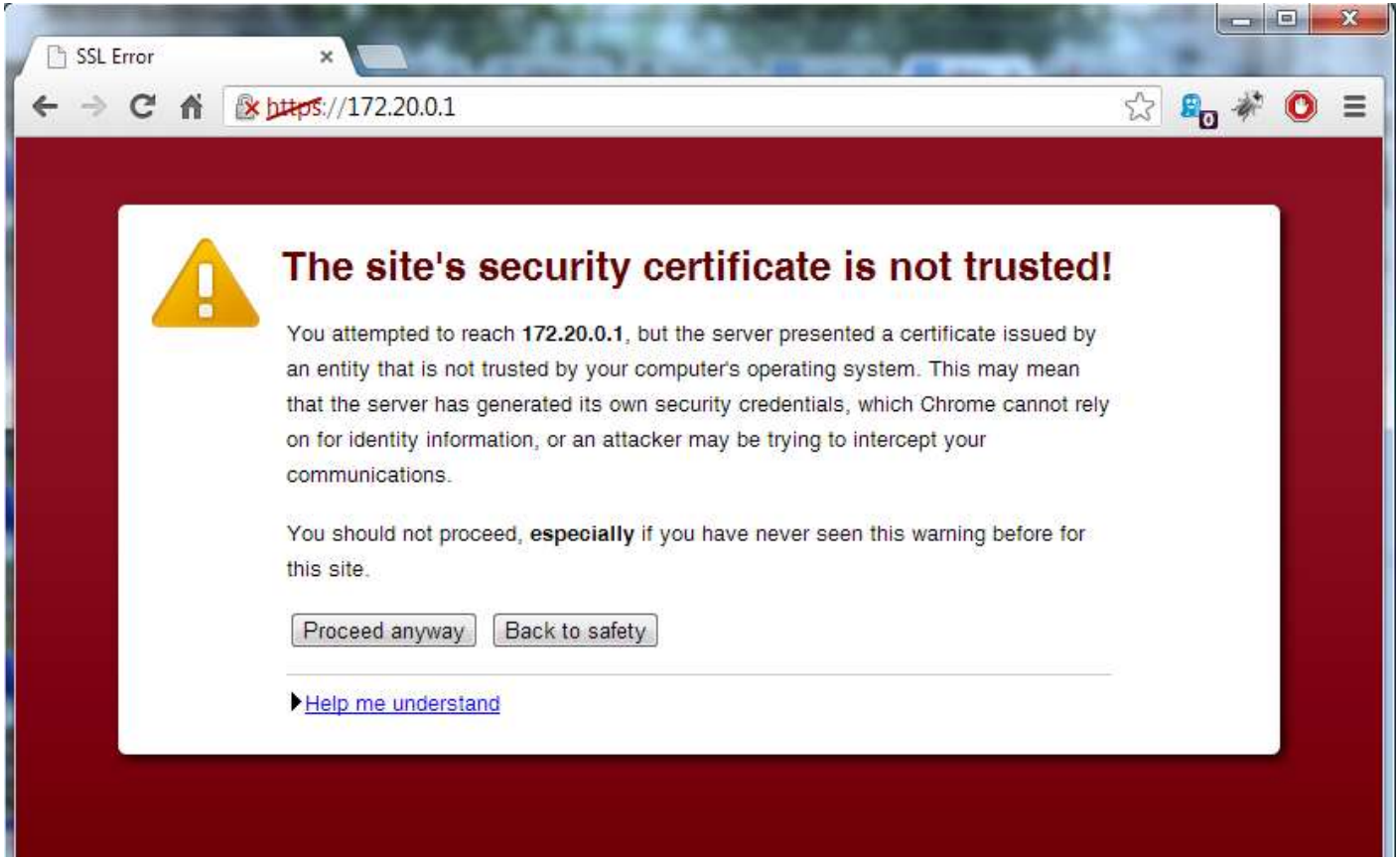
- Security warning dialogs more like warnings on wine than warnings on poison
- Software developers place burden of assessing risk on users

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

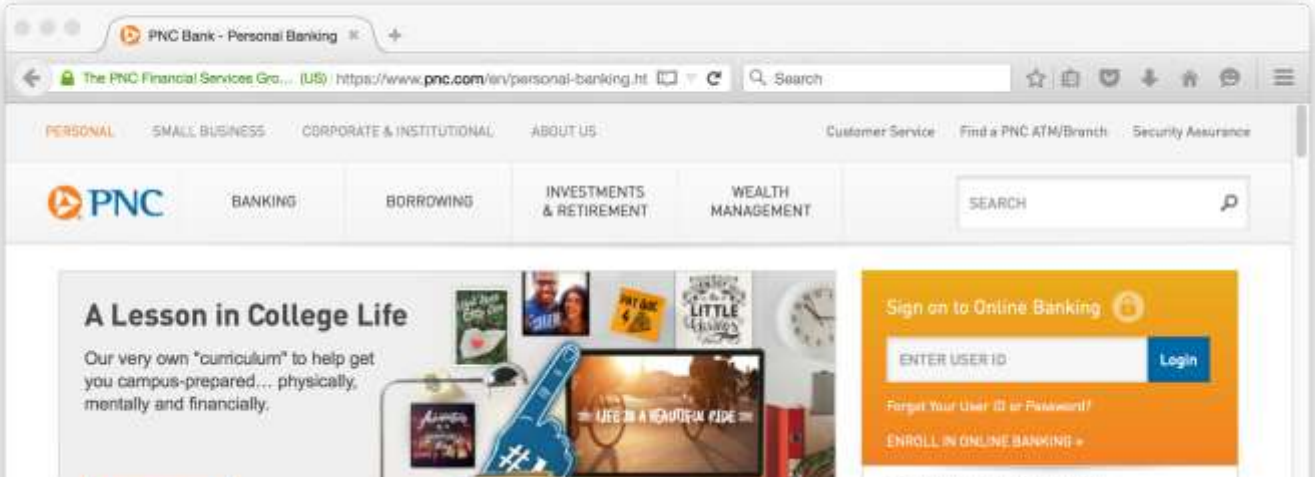
Non-risky context

- Encounter self-signed certificate (familiar experience for developers)



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

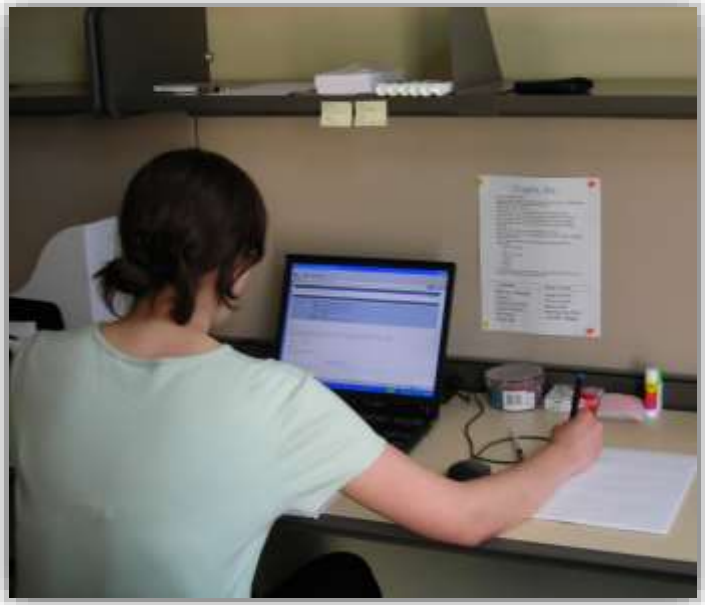


New plan

- 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



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.

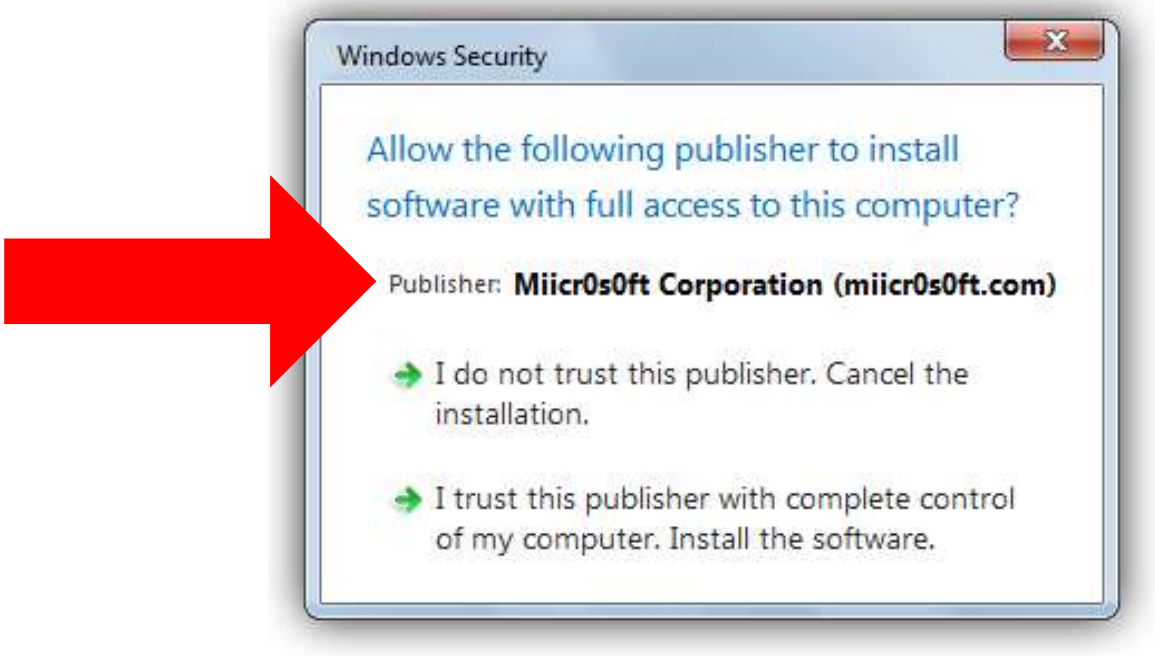
Can you spot the suspicious software?

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

Obstruct install button until user types publisher name

Do any of these work?

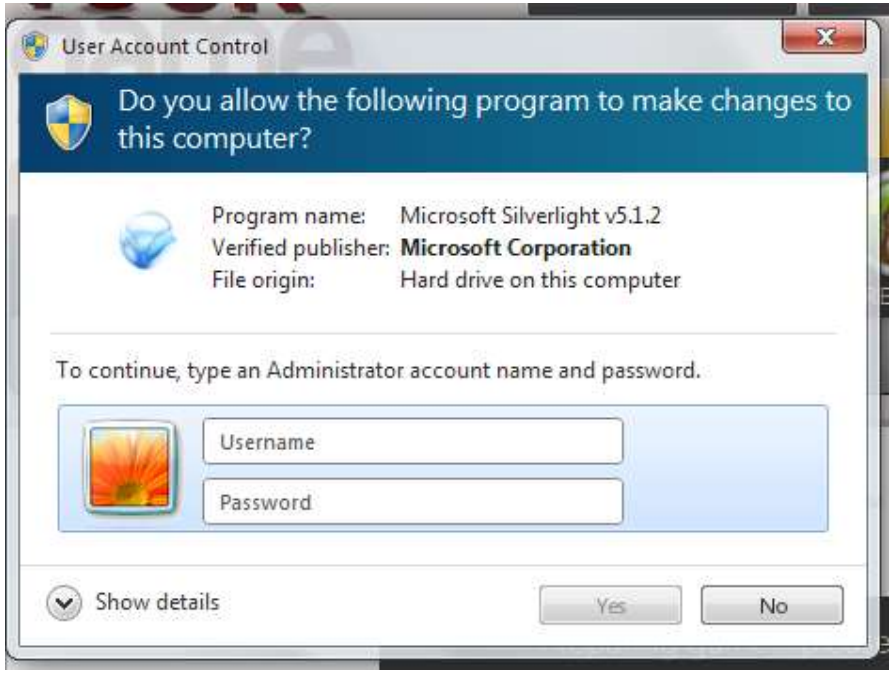
- Do attractors and other techniques prevent suspicious installs without preventing benign installs?
- How much do attractors delay benign installs?

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 | 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

Online games evaluation survey

Carnegie Mellon U

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

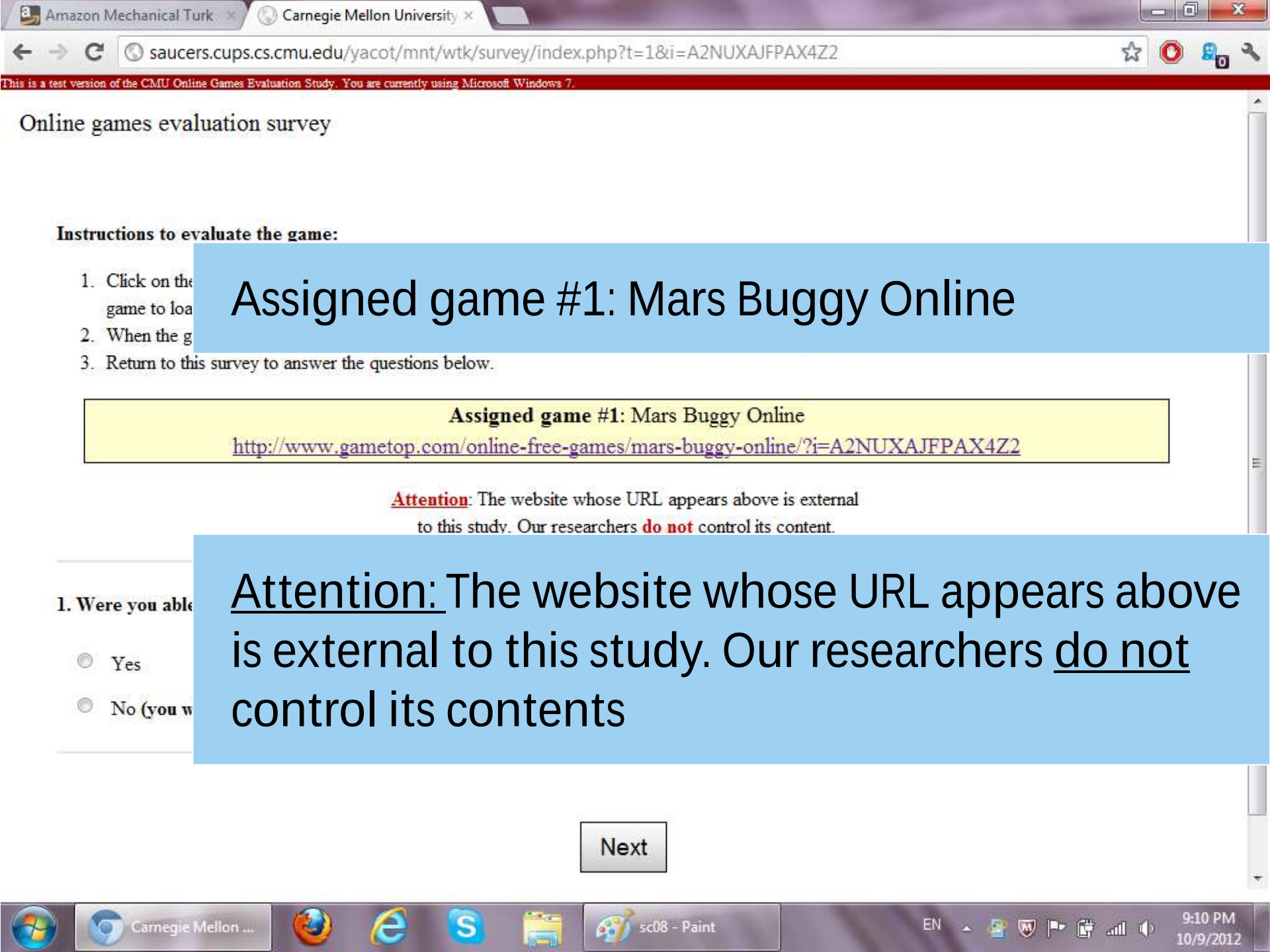
The risks and discomfort associated with participation in this study are no greater than those ordinarily encountered in daily life or during other online activities. There may be no personal benefit from your participation in the study but the knowledge received may be of value to humanity. You will 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

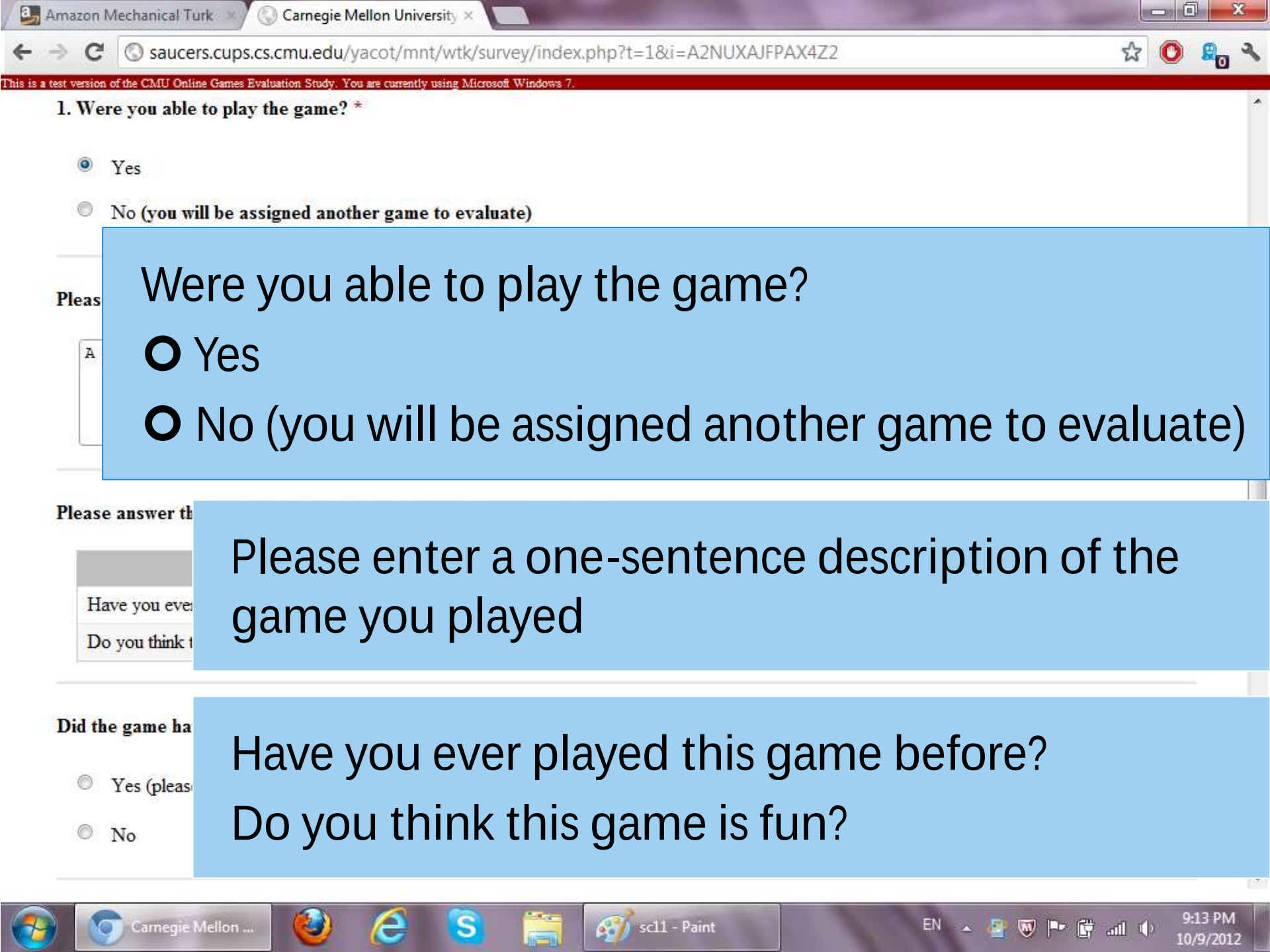

Amazon Mechanical Turk
Carnegie Mellon University
saucers.cups.cs.cmu.edu/yacot/mnt/wtk/survey/index.php?t=1&i=A2NUXAJFPAX4Z2
This is a test version of the CMU Online Games Evaluation Study. You are currently using Microsoft Windows 7.
Online games evaluation survey
Instructions to evaluate the game:
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
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
Attention: The website whose URL appears above is external to this study. Our researchers do not control its contents
Next
Carnegie Mellon ...
sc08 - Paint
EN
9:10 PM
10/9/2012

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
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 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 ...
scl1 - 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

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.

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

Related Games

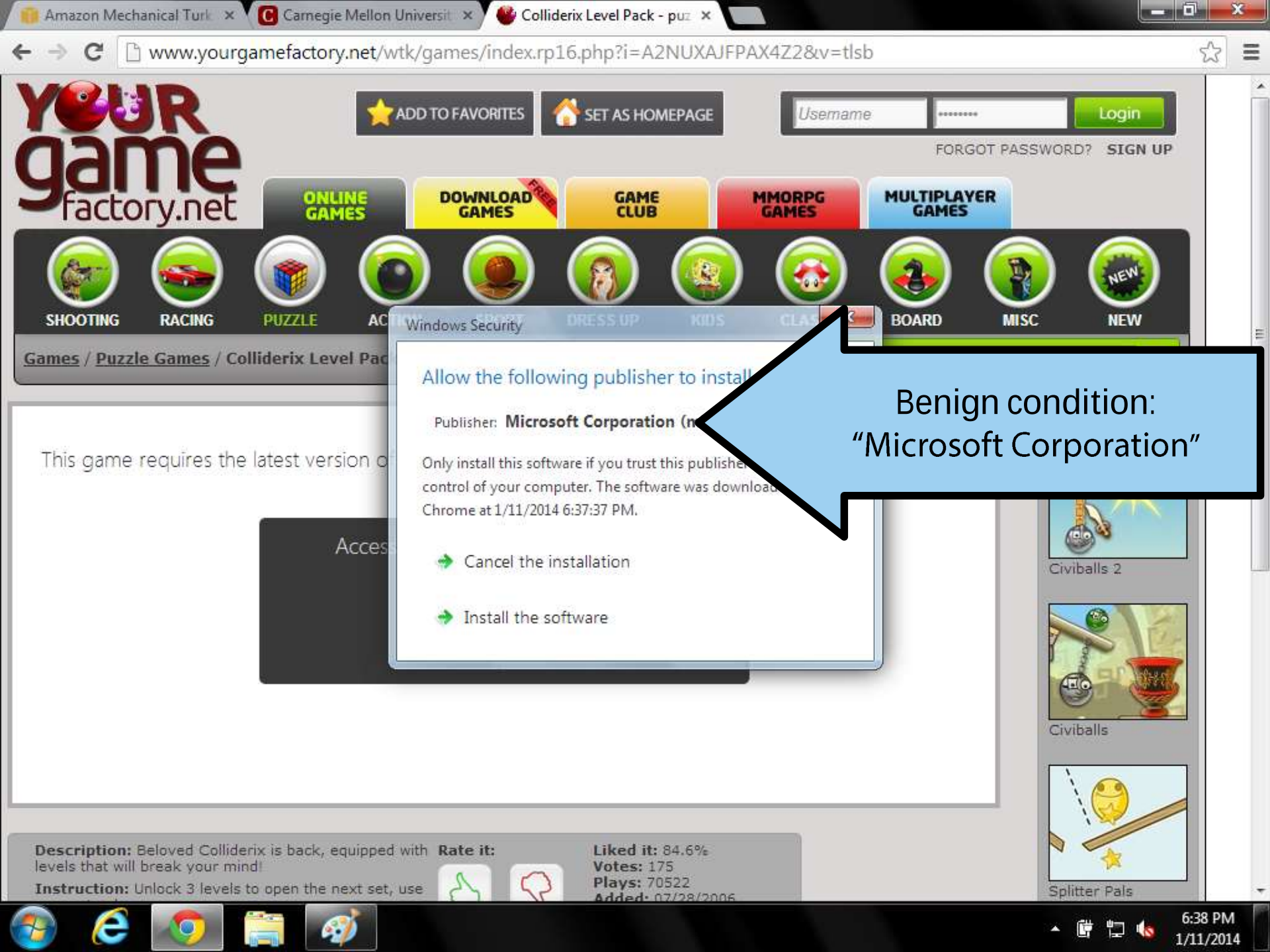
Civiballs 2

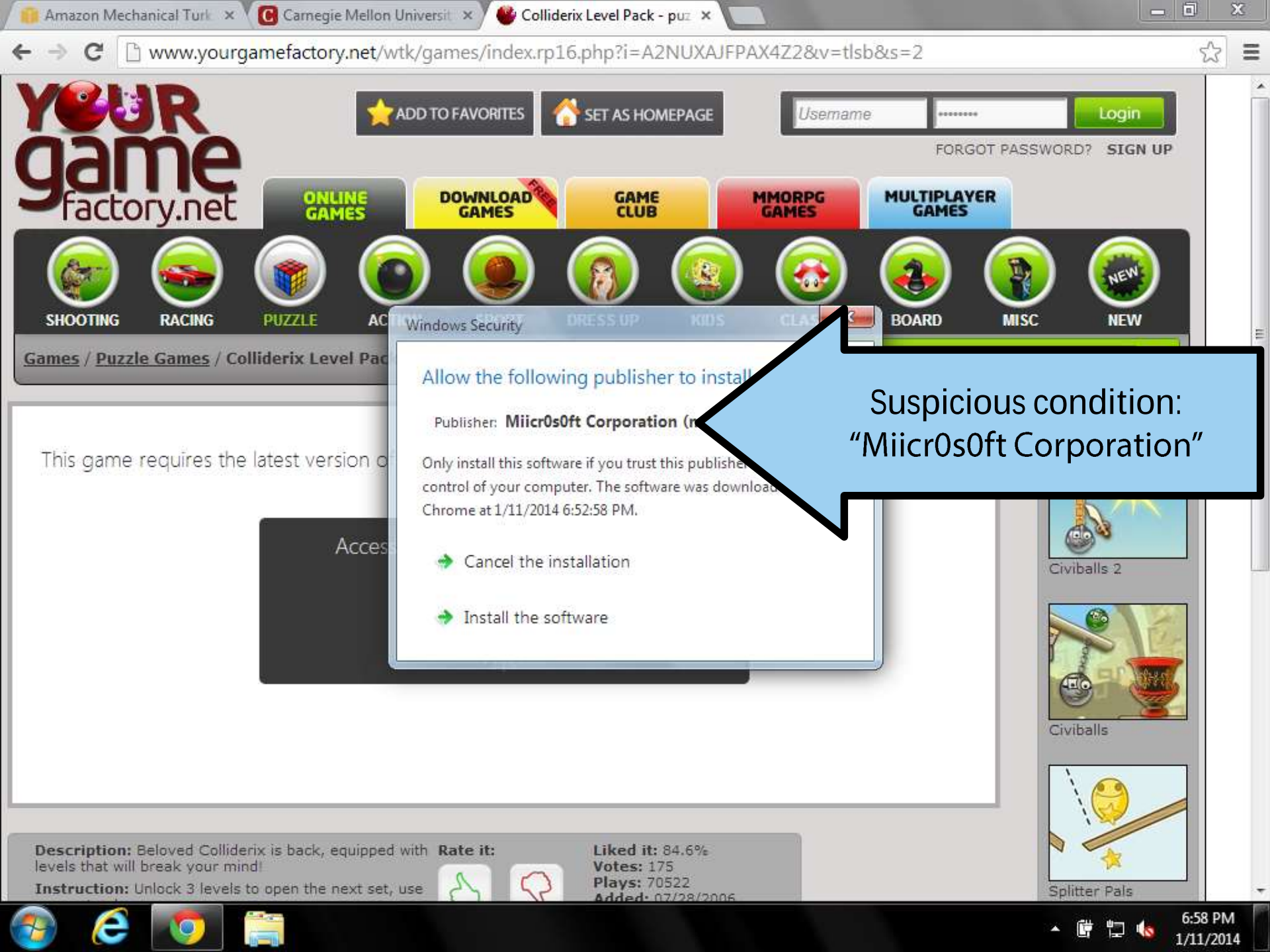
Civiballs

Splitter Pals

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
YOUR game factory.net
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: Microsoft Corporation (n
Only install this software if you trust this publisher
control of your computer. The software was downloa
Chrome at 1/11/2014 6:37:37 PM.
Cancel the installation
Install the software
Benign condition:
“Microsoft 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
6:38 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
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
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

Debrief is crucial for ethics!

- Explain what the actual purpose of the study was