Conducting Usable Security Studies

IT'S COMPLICATED!

Lorrie Faith Cranor

Carnegie Mellon University
CyLab

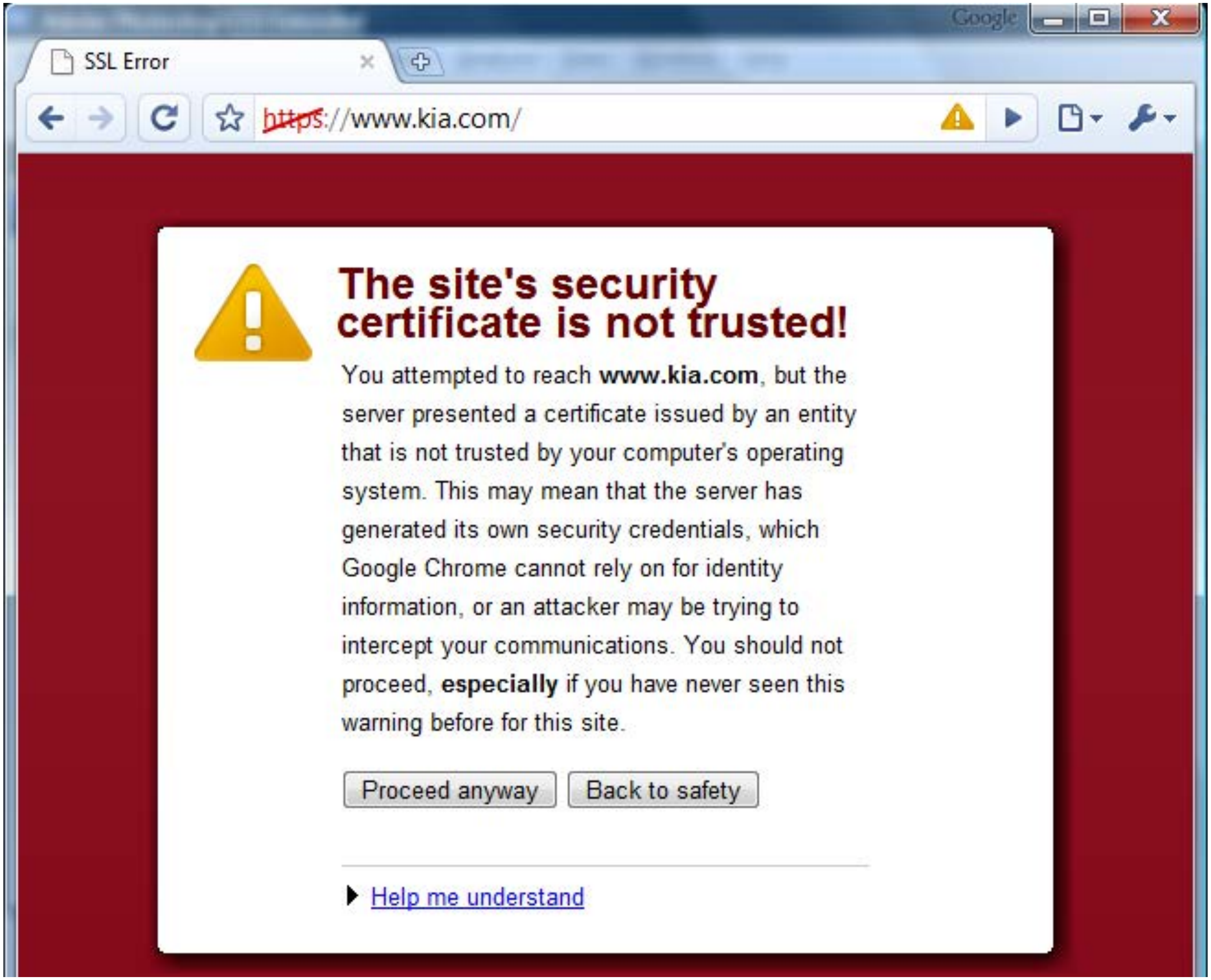
isr institute for SOFTWARE RESEARCH

Engineering & Public Policy

privacy ENGINEERING

CyLab Usable Privacy & Security Laboratory
HTTP://CUPS.CS.CMU.EDU

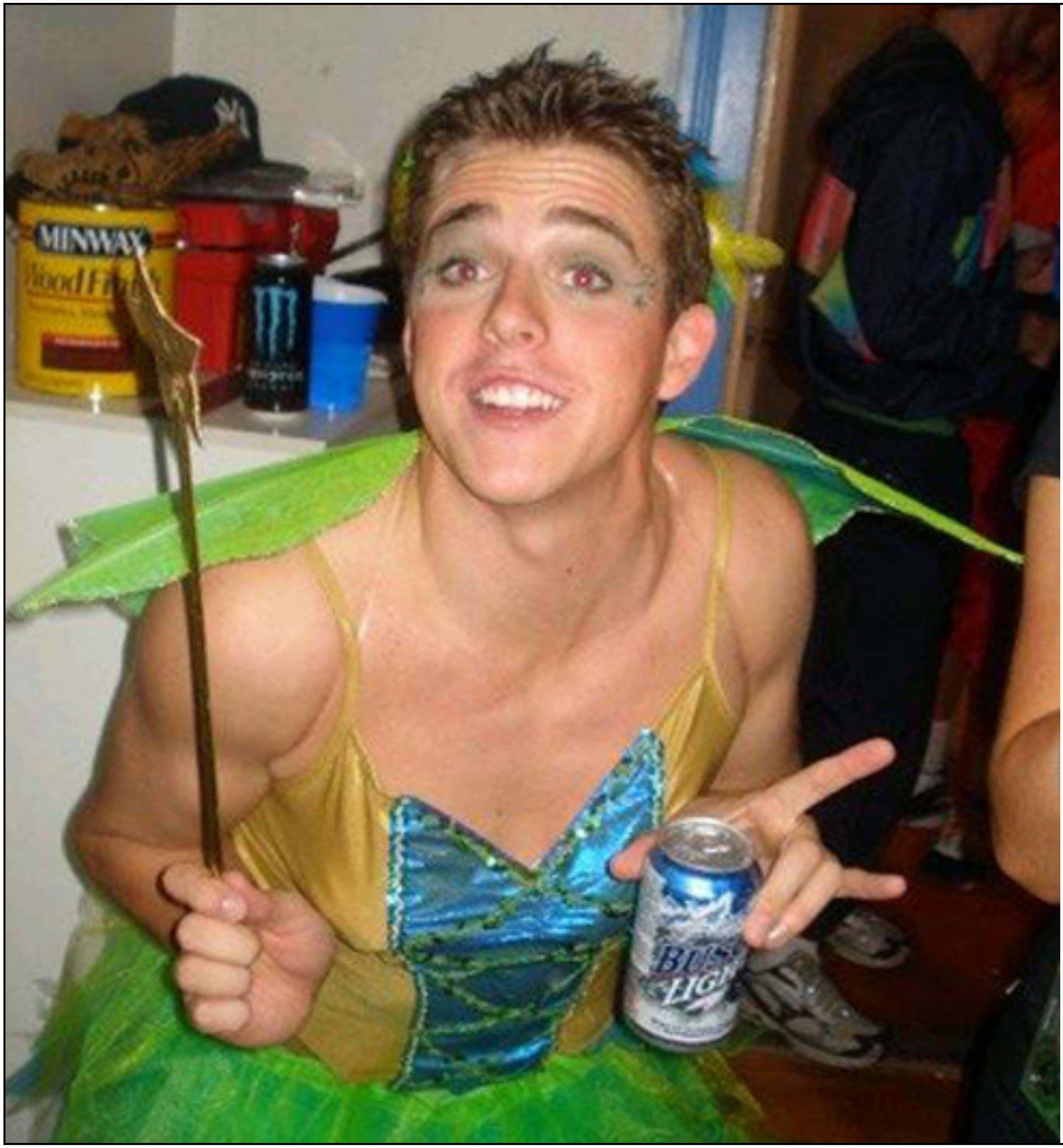
Have you ever wondered…



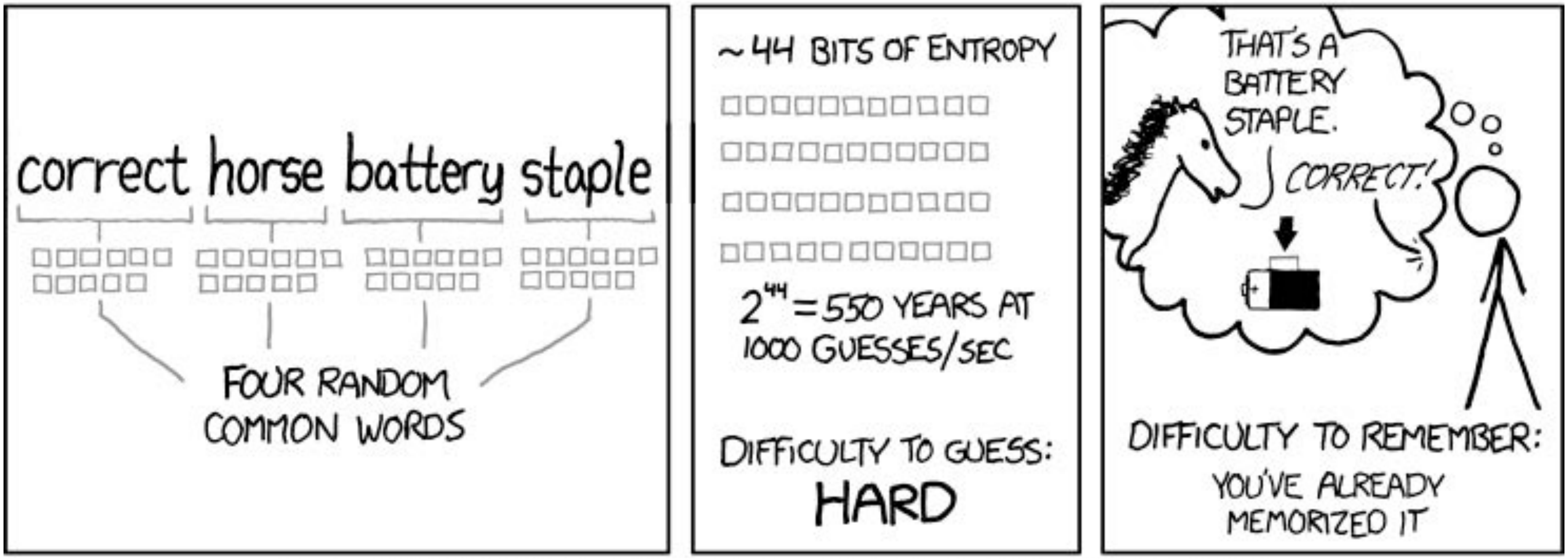
The site's security certificate is not trusted!

You attempted to reach **www.kia.com**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, **especially** if you have never seen this warning before for this site.

Credit Card
0001 4492 0781 7376
Bank

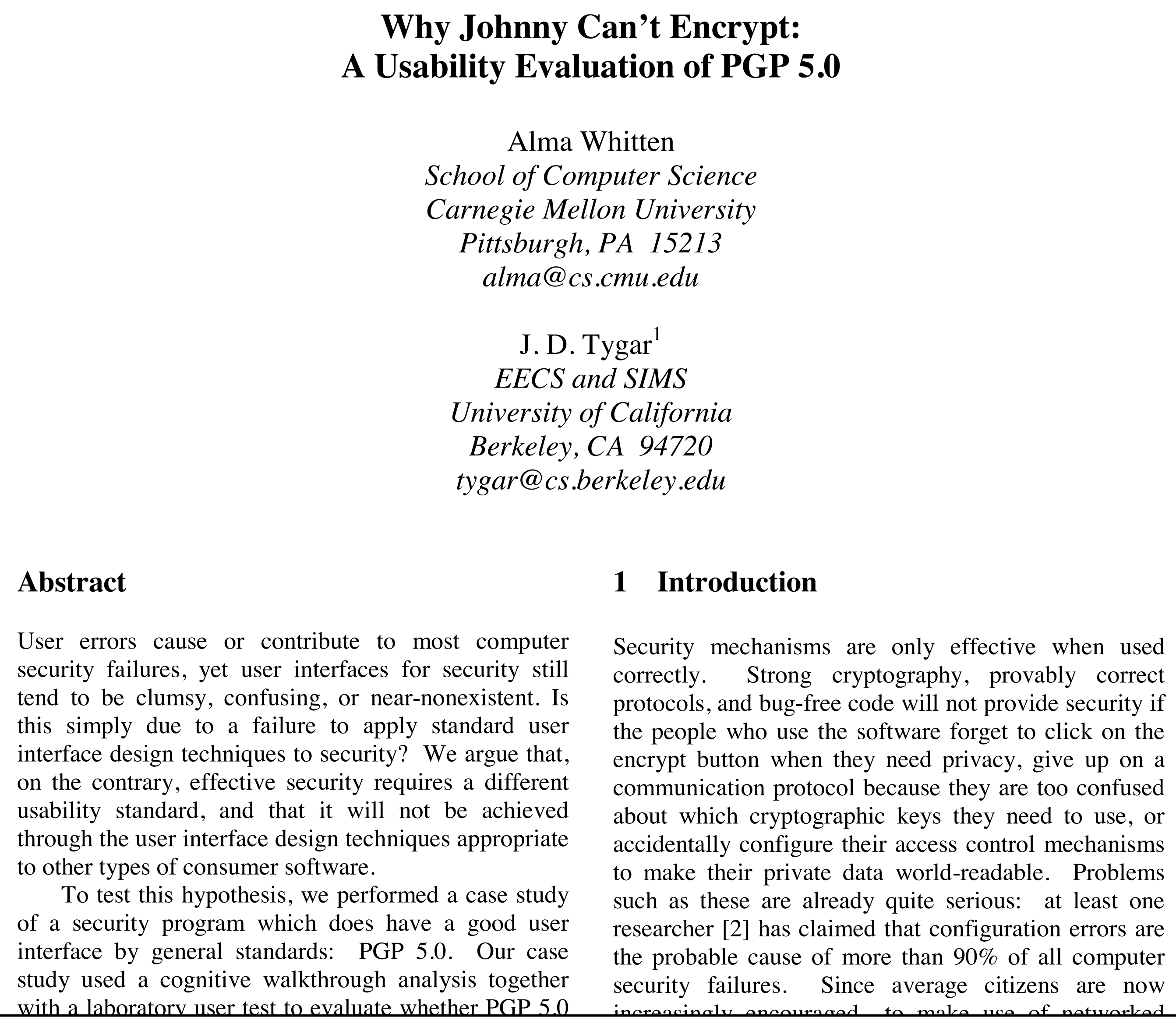


Kevin Colvin's Facebook photo that got him fired for missing work


correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^{44} = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

http://xkcd.com/936/

USENIX Security 1999



Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0

Alma Whitten
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu

J. D. Tygar[1]
EECS and SIMS
University of California
Berkeley, CA 94720
tygar@cs.berkeley.edu

Abstract

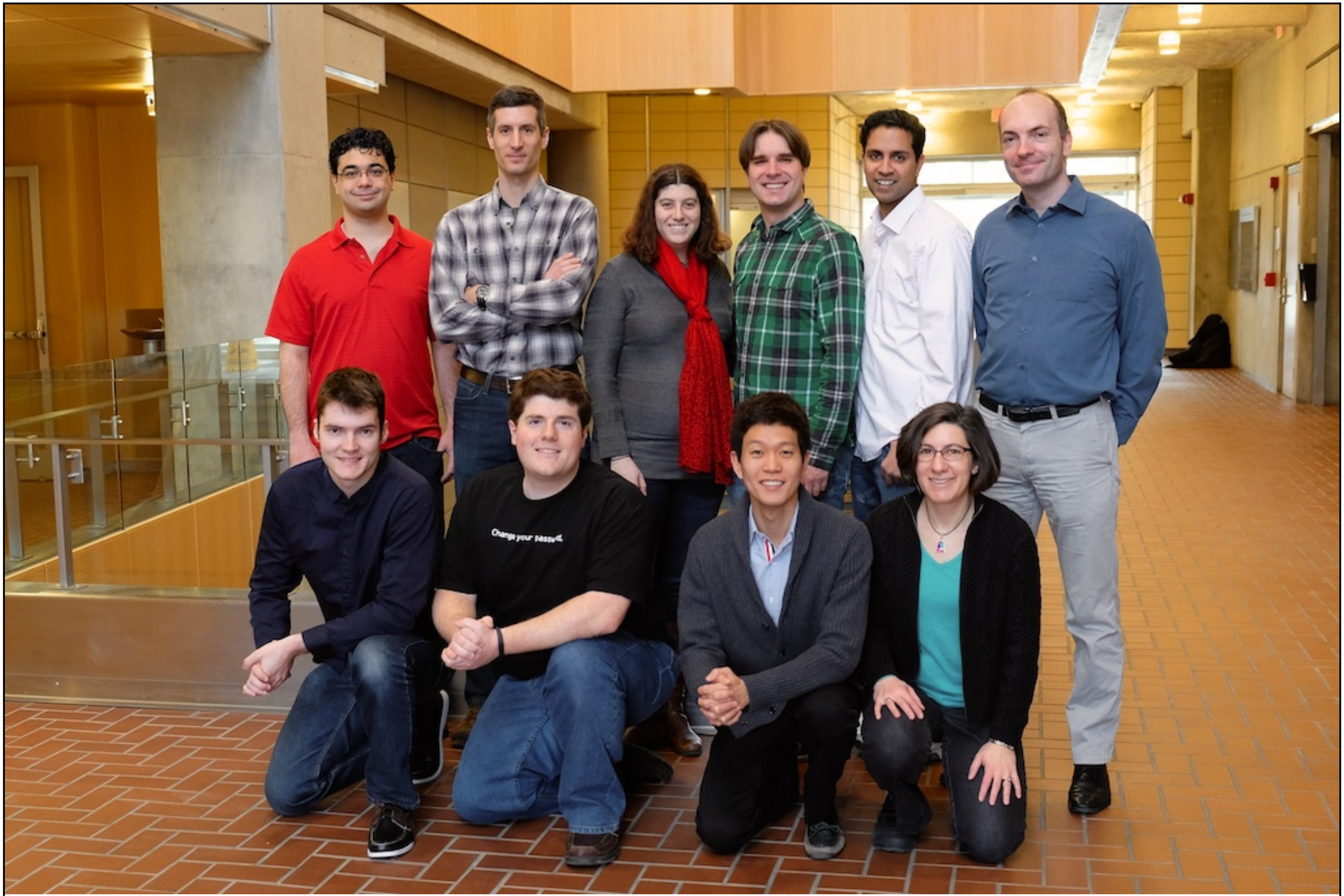
User errors cause or contribute to most computer security failures, yet user interfaces for security still tend to be clumsy, confusing, or near-nonexistent. Is this simply due to a failure to apply standard user interface design techniques to security? We argue that, on the contrary, effective security requires a different usability standard, and that it will not be achieved through the user interface design techniques appropriate to other types of consumer software.

To test this hypothesis, we performed a case study of a security program which does have a good user interface by general standards: PGP 5.0. Our case study used a cognitive walkthrough analysis together with a laboratory user test to evaluate whether PGP 5.0

1 Introduction

Security mechanisms are only effective when used correctly. Strong cryptography, provably correct protocols, and bug-free code will not provide security if the people who use the software forget to click on the encrypt button when they need privacy, give up on a communication protocol because they are too confused about which cryptographic keys they need to use, or accidentally configure their access control mechanisms to make their private data world-readable. Problems such as these are already quite serious: at least one researcher [2] has claimed that configuration errors are the probable cause of more than 90% of all computer security failures. Since average citizens are now increasingly encouraged to make use of networked

CUPS Lab 2007



CUPS passwords research team 2014

CUPS people + alumni at CHI 2014

Roadmap

- Usable security studies 101
- Evaluating security warnings
- Privacy indicators and willingness to pay for privacy
- Designing and evaluating privacy nudges
- Investigating the XKCD passphrase assertion

Usable security studies 101

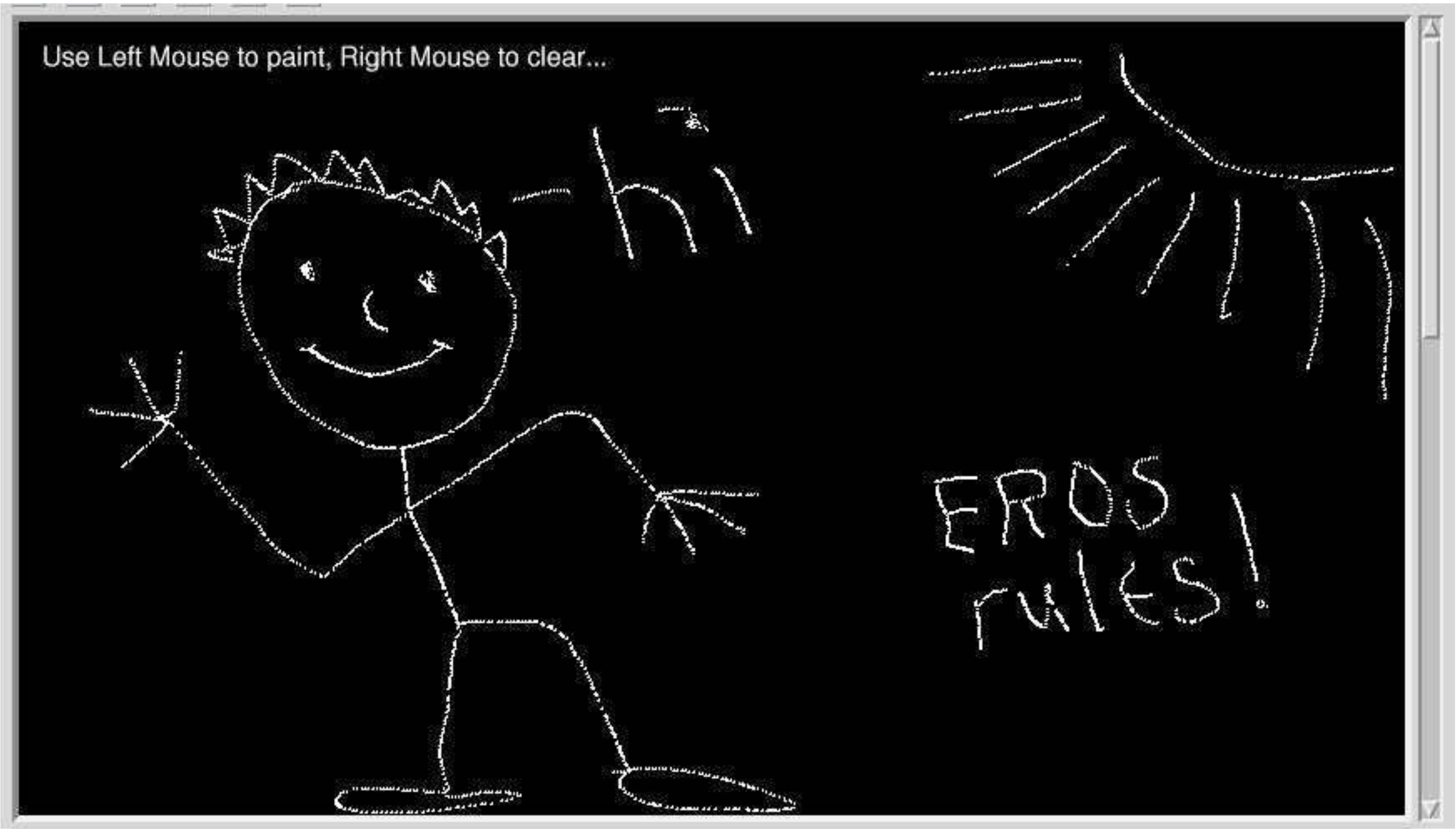
Why do usable security studies?

Purpose	Useful to…
Assess needs	Decide what to build
Evaluate	Determine whether system meets requirements and what needs to be improved
Understand tradeoffs	Decide which features/approaches/systems best fit particular needs
Find root causes	Determine where redesigns or new approaches are needed

Excuses for not doing usable security studies

- If people weren't so lazy/stupid/careless the system would work just fine
- I'm a cryptographer, not a usability expert
- I already know what people want
- I find the system easy to use so it must be usable
- My kids can use the system so it definitely must be usable

Your kids are not typical users

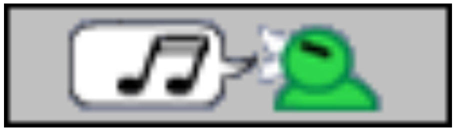


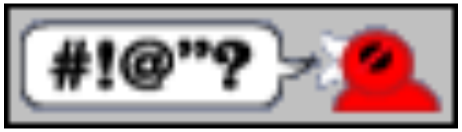
Use Left Mouse to paint, Right Mouse to clear...

J. Shaprio, J. Vanderburgh, E. Northrup, D. Chizmadia. **Design of the EROS Trusted Window System.** USENIX Security 2004.

You are not a typical user

2002 Privacy Bird study





Privacy policy matches user's privacy preferences

Privacy policy does not match user's privacy preferences

L. Cranor, P. Guduru and M. Arjula. **User Interfaces for Privacy Agents.** ACM ToCHI June 2006.

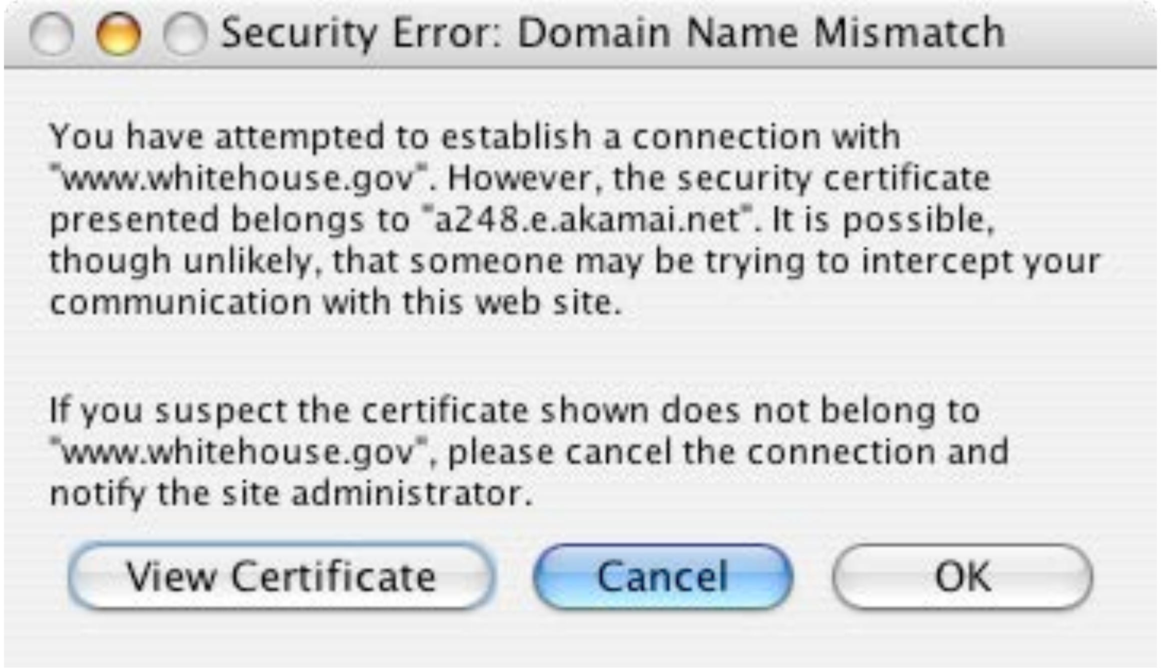
User study steps

- Identify research questions, metrics, and use cases
- Decide on type of study and design study protocol
- Develop detailed scripts, surveys, scenarios, incentives, instrumentation, prototypes, recruiting materials, etc.
- Obtain ethics approval
- Pilot and iterate on study design
- Collect data
- Analyze Results
- Repeat some or all of these steps as needed

Usable security study challenges

- Keeping it real (ecological validity)
  - Create realistic sense of risk **(but not real risk)**
  - Provide realistic incentives
  - Don’t bias participants
- Measuring the right thing
  - Design the right protocol
  - Control the variables
  - Instrument
- Observing infrequent events and small differences
- Legal, ethical, and practical issues

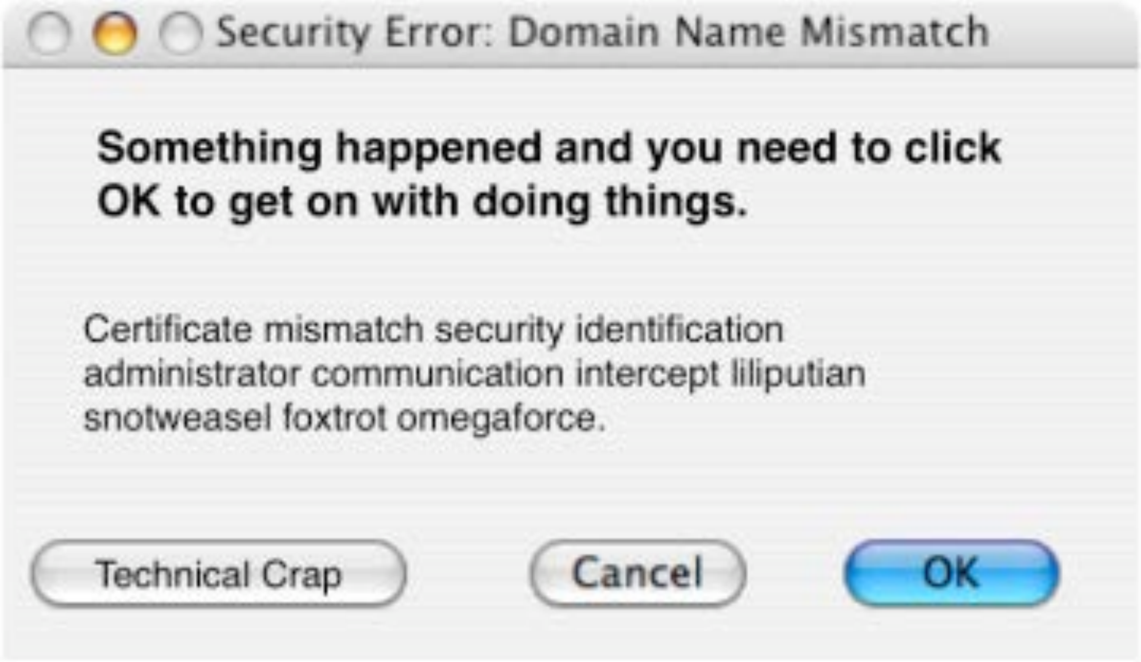
Evaluating security warnings



Security Error: Domain Name Mismatch

You have attempted to establish a connection with "www.whitehouse.gov". However, the security certificate presented belongs to "a248.e.akamai.net". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.

If you suspect the certificate shown does not belong to "www.whitehouse.gov", please cancel the connection and notify the site administrator.



Security Error: Domain Name Mismatch

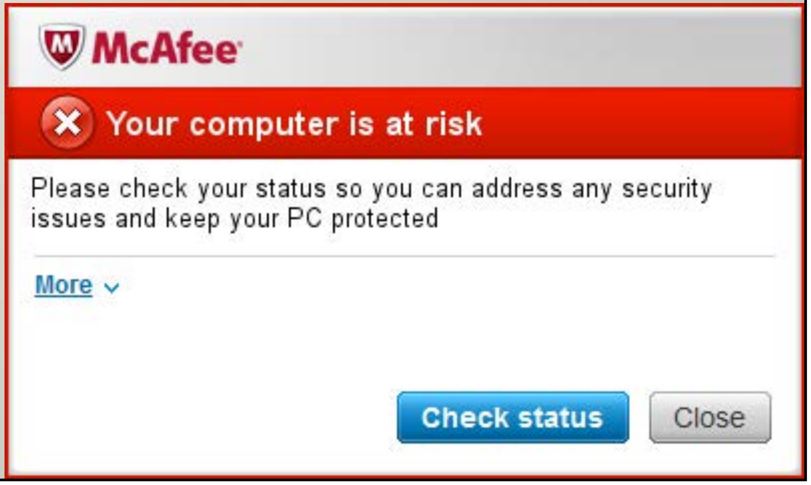
Something happened and you need to click OK to get on with doing things.

Certificate mismatch security identification administrator communication intercept liliputian snotweasel foxtrot omegaforce.

Image courtesy of Johnathan Nightingale

Users swat away warning dialogs

How can we get users to pay attention?

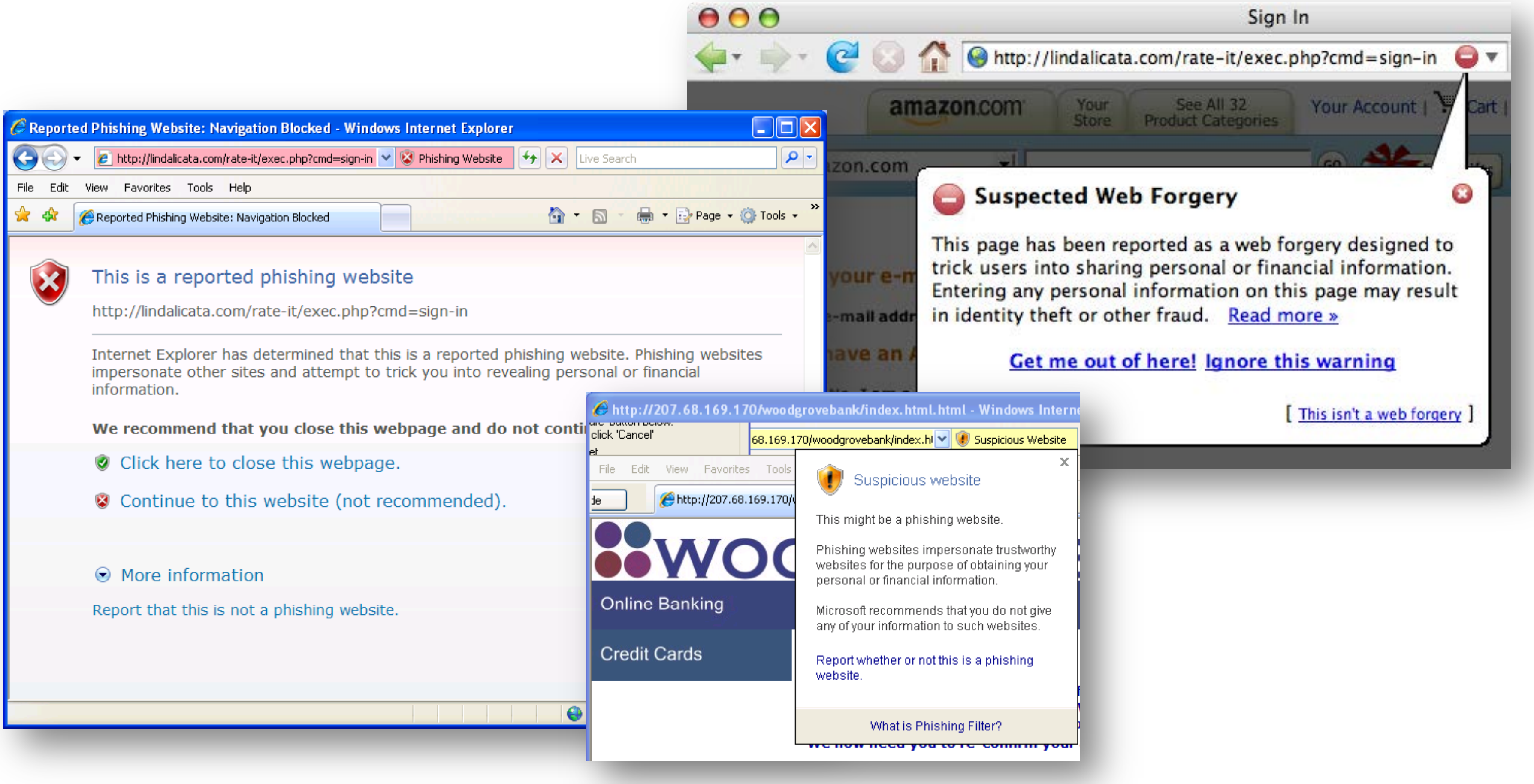


McAfee

Your computer is at risk

Please check your status so you can address any security issues and keep your PC protected

2007 Phishing warnings study



Reported Phishing Website: Navigation Blocked - Windows Internet Explorer

http://lindalicata.com/rate-it/exec.php?cmd=sign-in

Phishing Website
Live Search
File Edit View Favorites Tools Help
Reported Phishing Website: Navigation Blocked
Page
Tools

This is a reported phishing website

http://lindalicata.com/rate-it/exec.php?cmd=sign-in

Internet Explorer has determined that this is a reported phishing website. Phishing websites impersonate other sites and attempt to trick you into revealing personal or financial information.

We recommend that you close this webpage and do not conti

Click here to close this webpage.

Continue to this website (not recommended).

More information

Report that this is not a phishing website.

Sign In

http://lindalicata.com/rate-it/exec.php?cmd=sign-in

Suspected Web Forgery

This page has been reported as a web forgery designed to trick users into sharing personal or financial information. Entering any personal information on this page may result in identity theft or other fraud. Read more »

Get me out of here! Ignore this warning

[This isn't a web forgery]

http://207.68.169.170/woodgrovebank/index.html.html - Windows Interne

Suspicious website

This might be a phishing website.

Phishing websites impersonate trustworthy websites for the purpose of obtaining your personal or financial information.

Microsoft recommends that you do not give any of your information to such websites.

Report whether or not this is a phishing website.

What is Phishing Filter?

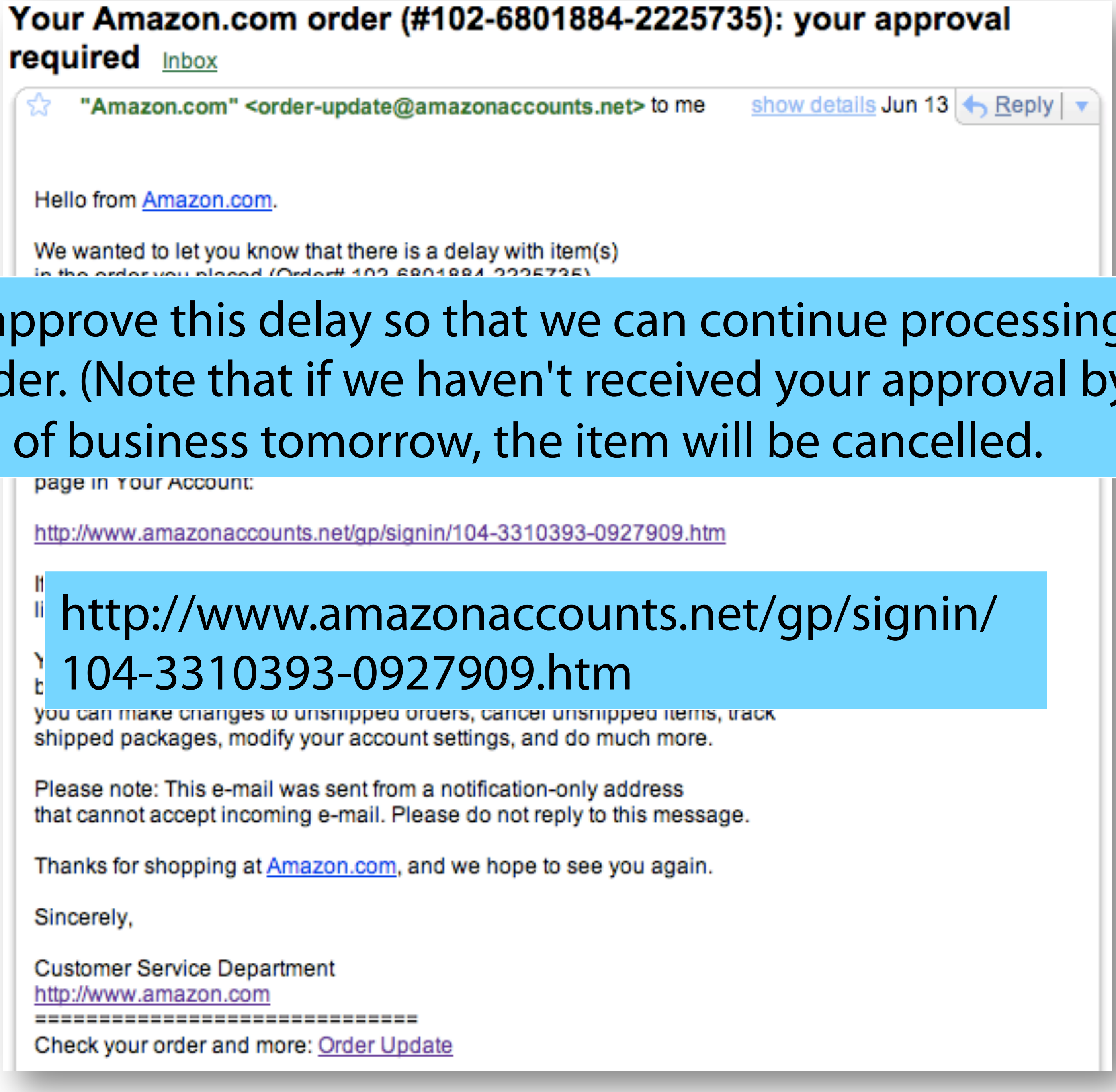
S. Egelman, L. Cranor, and J. Hong. **You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings**. CHI 2008.

Study design challenges

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

Required a little deception

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



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

"Amazon.com" <order-update@amazonaccounts.net> to me

Hello from Amazon.com.

We wanted to let you know that there is a delay with item(s)
in the order you placed (Order# 102-6801884-2225735)

page in Your Account:

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

If
li

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

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

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

Sincerely,

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

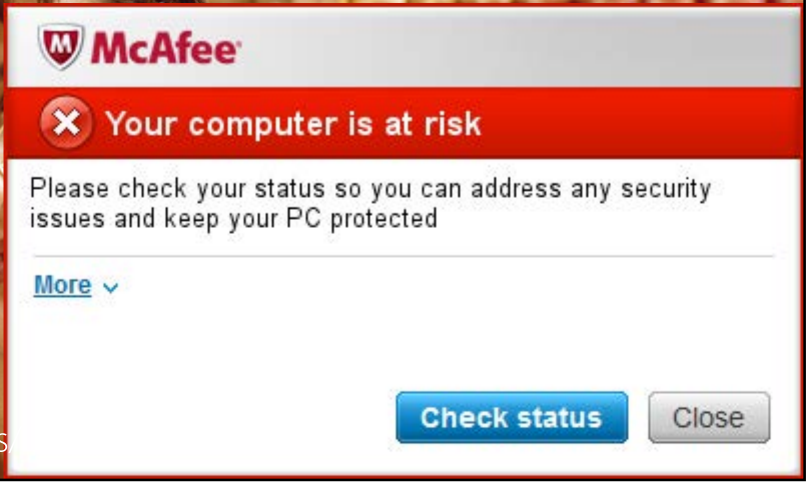
Please approve this delay so that we can continue processing your order. (Note that if we haven't received your approval by the end of business tomorrow, the item will be cancelled.

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

More issues to address

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

http://special-ism.com/before-you-call-that-attorney-what-is-due-process/

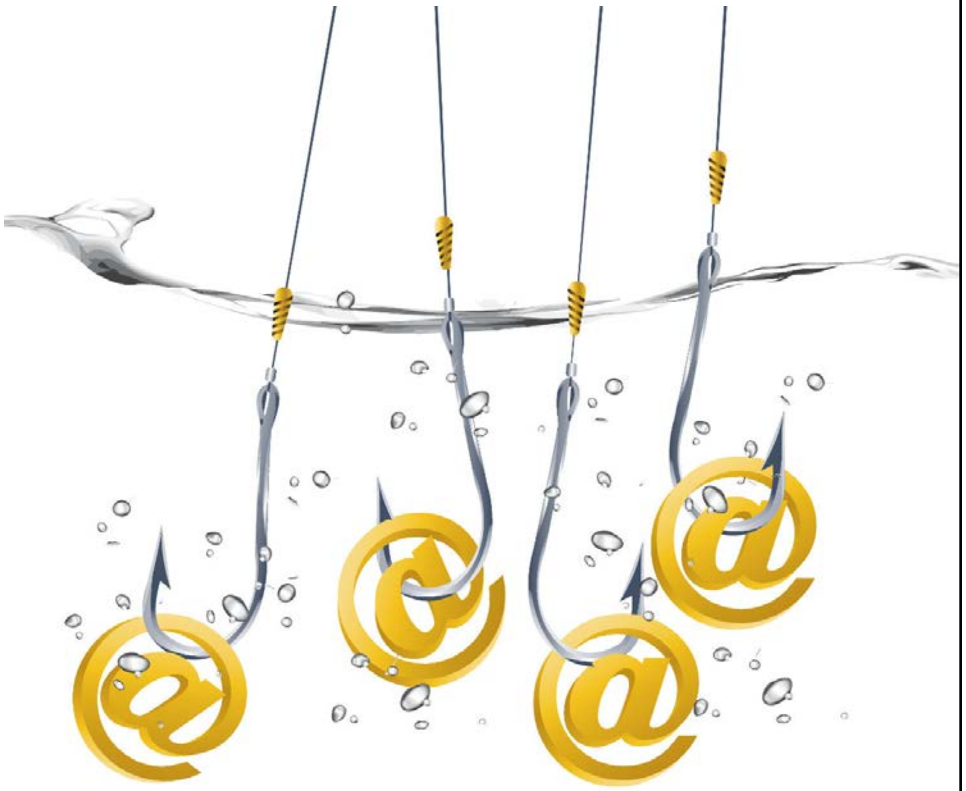


Your computer is at risk

Please check your status so you can address any security issues and keep your PC protected

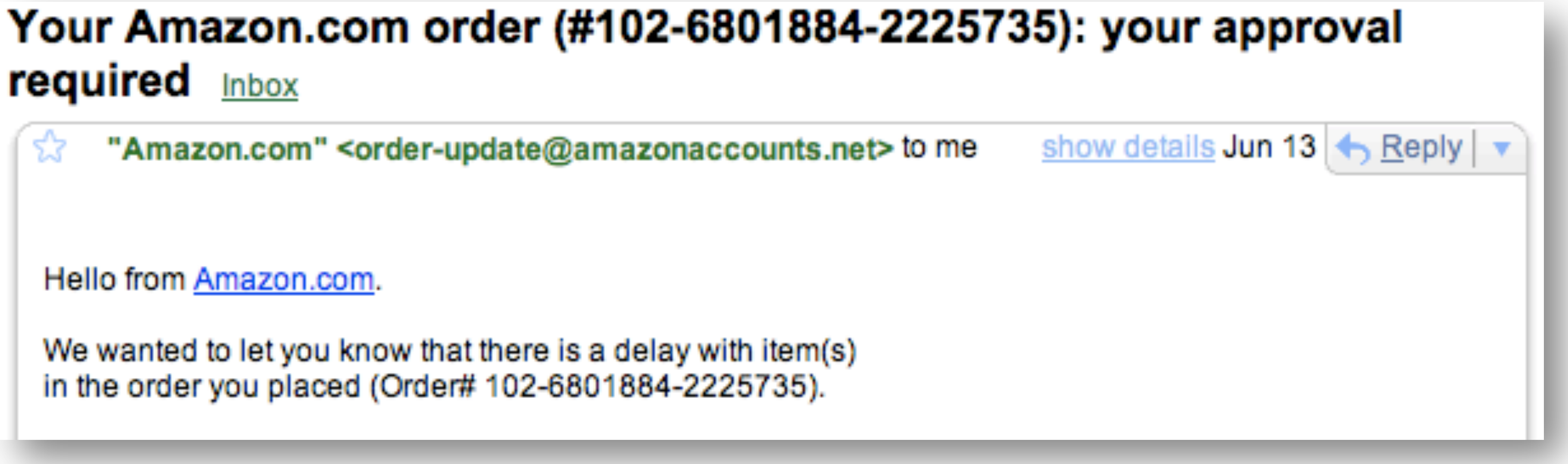
Success!

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



Confused by domain names

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



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

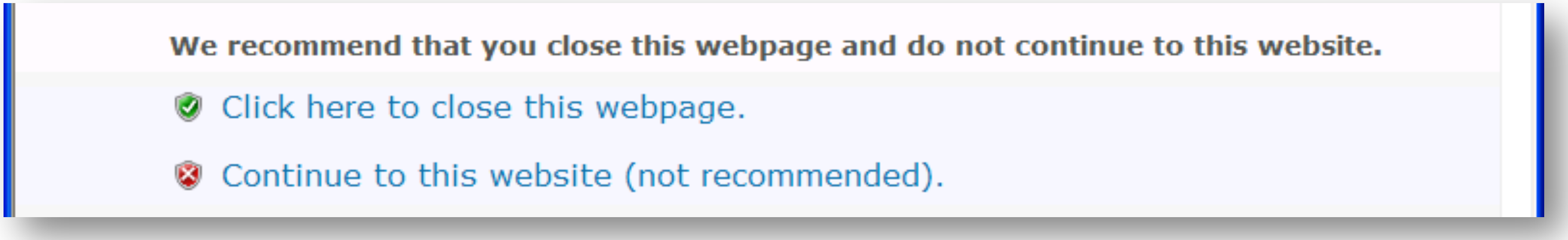
"Amazon.com" <order-update@amazonaccounts.net> to me show details Jun 13

Hello from Amazon.com.

We wanted to let you know that there is a delay with item(s)
in the order you placed (Order# 102-6801884-2225735).

Trusted browser to protect them

"Since it gave me the option of still proceeding to the website, I figured it couldn't be that bad."



We recommend that you close this webpage and do not continue to this website.

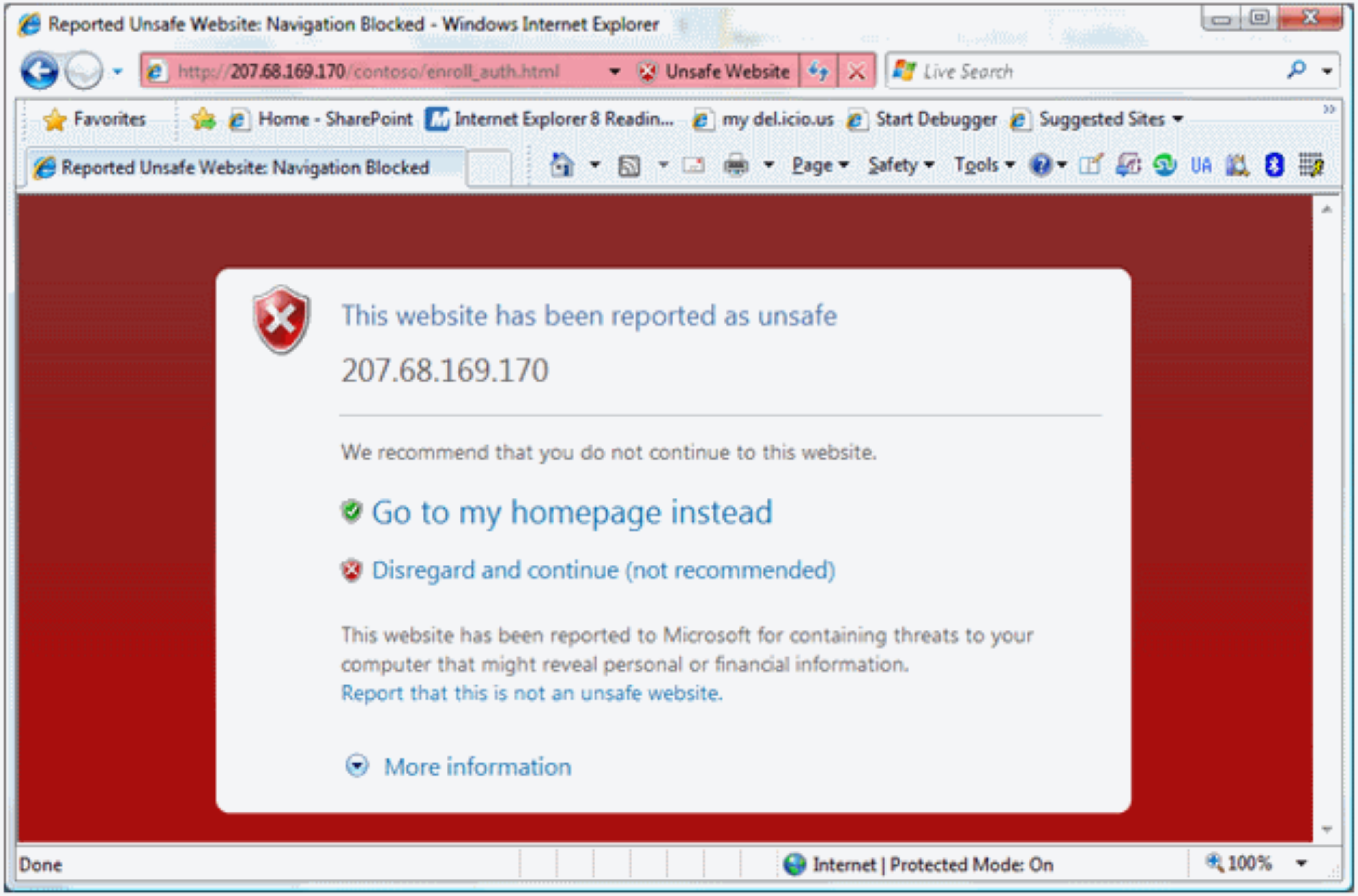
✓ Click here to close this webpage.

✗ Continue to this website (not recommended).

Confused mental models

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

Research led to better phishing warnings



Reported Unsafe Website: Navigation Blocked - Windows Internet Explorer
http://207.68.169.170/contoso/enroll_auth.html
Unsafe Website
Live Search
Favorites
Home - SharePoint
Internet Explorer 8 Readin...
my del.icio.us
Start Debugger
Suggested Sites
Reported Unsafe Website: Navigation Blocked
Page
Safety
Tools
Done
Internet | Protected Mode: On
100%

This website has been reported as unsafe

207.68.169.170

We recommend that you do not continue to this website.

Go to my homepage instead

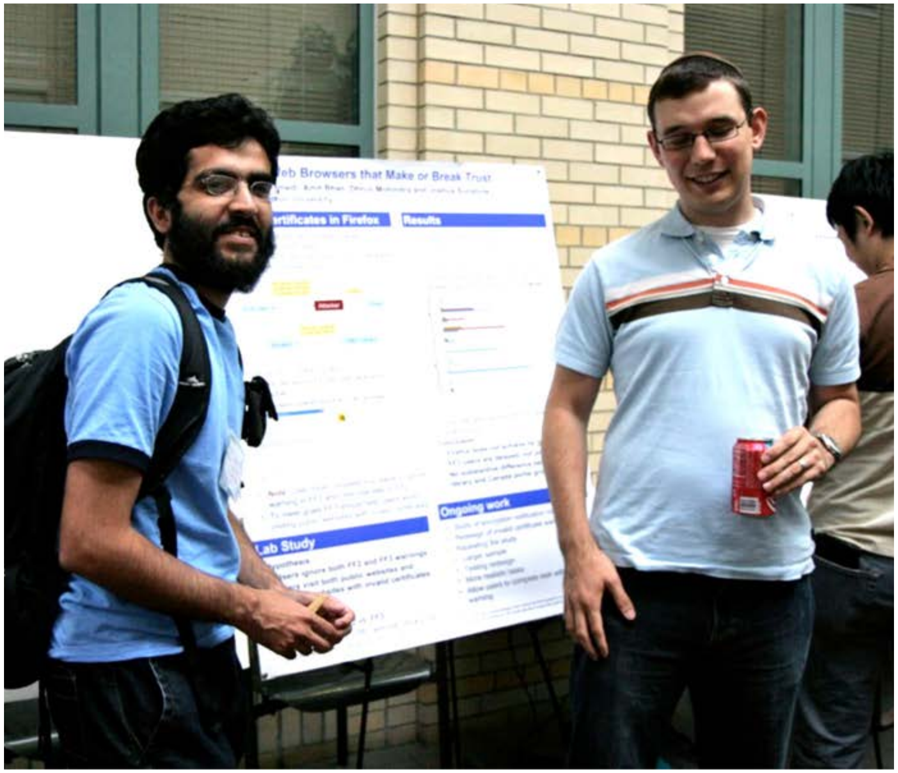
Disregard and continue (not recommended)

This website has been reported to Microsoft for containing threats to your computer that might reveal personal or financial information.
Report that this is not an unsafe website.

More information

2008 SSL certificate warning study

- Test SSL certificate warnings
- Design a better warning

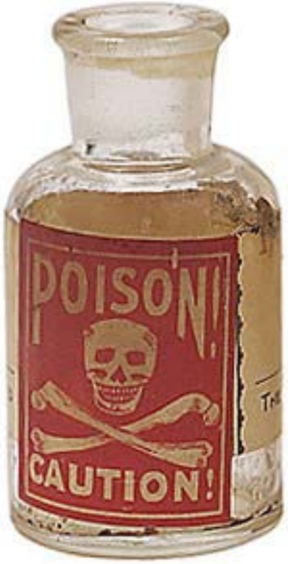


J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, L. Cranor. **Crying Wolf: An Empirical Study of SSL Warning Effectiveness.** USENIX Security 2009.

How do you know when you are actually at risk?

Some hazards are ALWAYS dangerous

B
Titanium
D
250



Some hazards are context dependent

STAY ALIV
DON'T DRINK
AND
DRIVE
PREGNANT?
DON'T DRINK.
ALCOHOL
CAN CAUSE
LIFELONG
BRAIN DAMAGE
TO YOUR CHILD.

"We agree with the CDC:
There is no known amount of alcohol
that is safe to drink while pregnant."
- Dr. Mehmet Oz, M.D.

Join us at NOFAS.org

National Organization on Fetal Alcohol Syndrome

Computer security dialogs context dependent

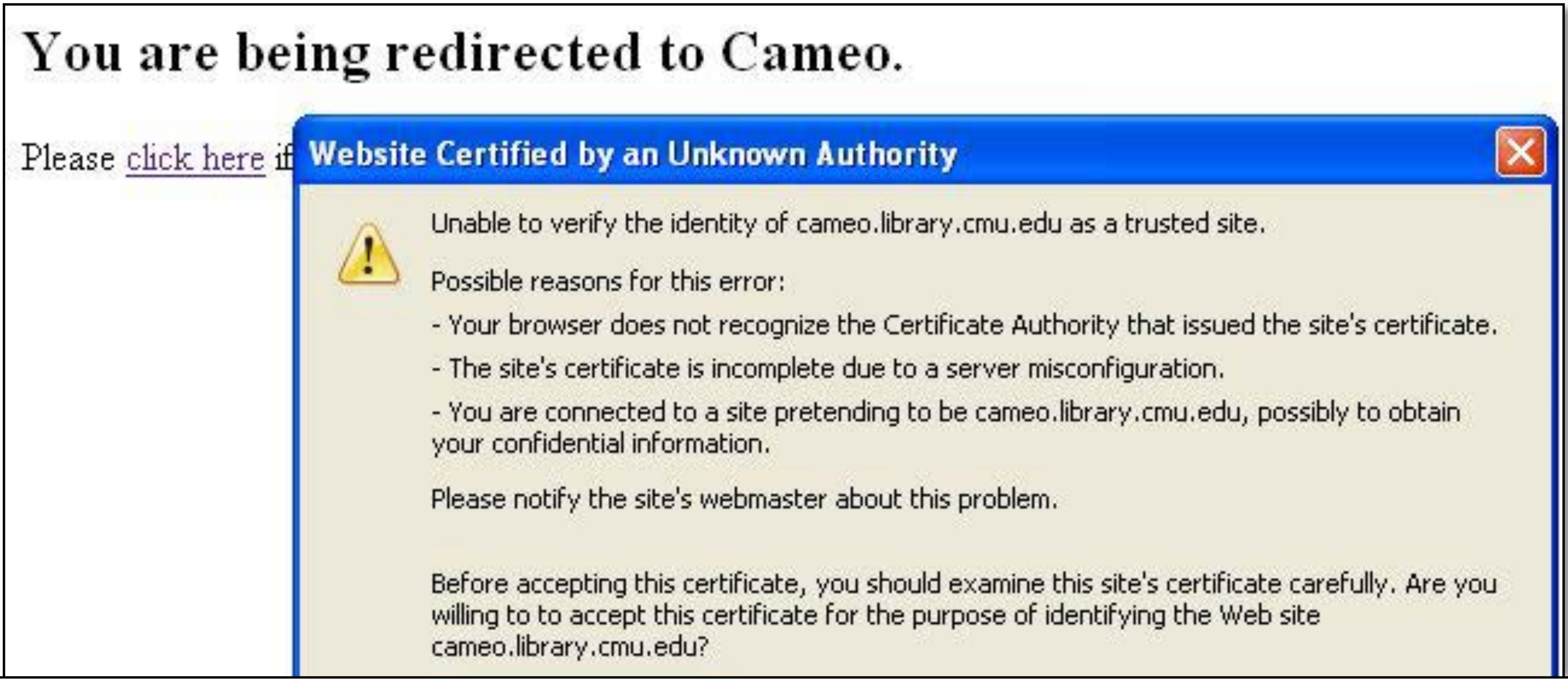
- Security warning dialogs more like warnings on wine than warnings on poison
- Software developers place burden of assessing risk on users

A good warning helps users determine whether they are at risk

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

Non-risky context

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



You are being redirected to Cameo.

Please click here if

Website Certified by an Unknown Authority

Unable to verify the identity of cameo.library.cmu.edu as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.

- The site's certificate is incomplete due to a server misconfiguration.

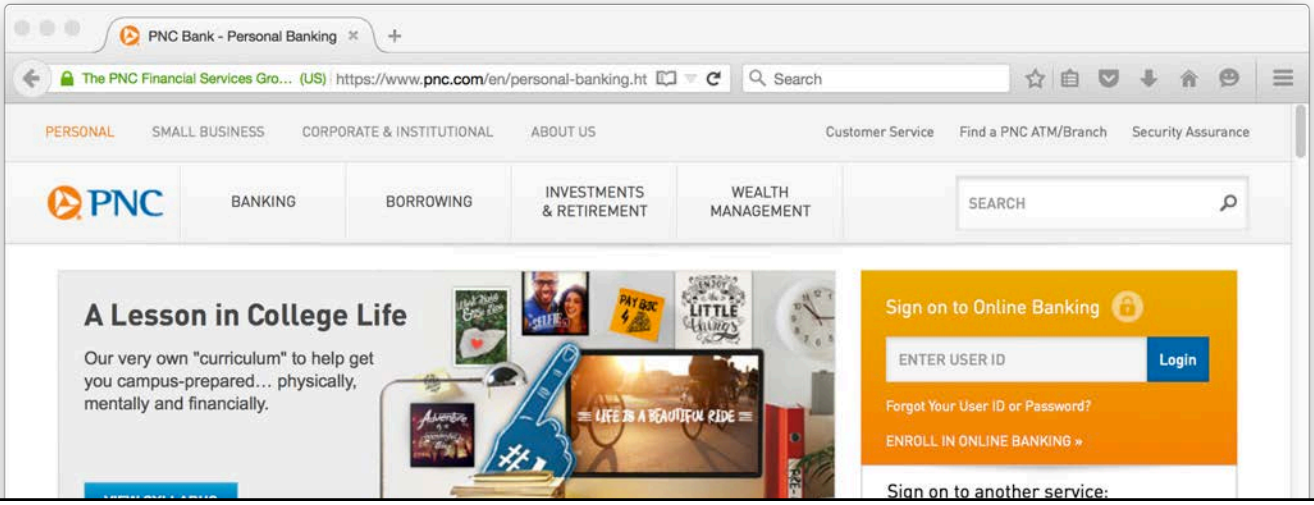
- You are connected to a site pretending to be cameo.library.cmu.edu, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site cameo.library.cmu.edu?

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

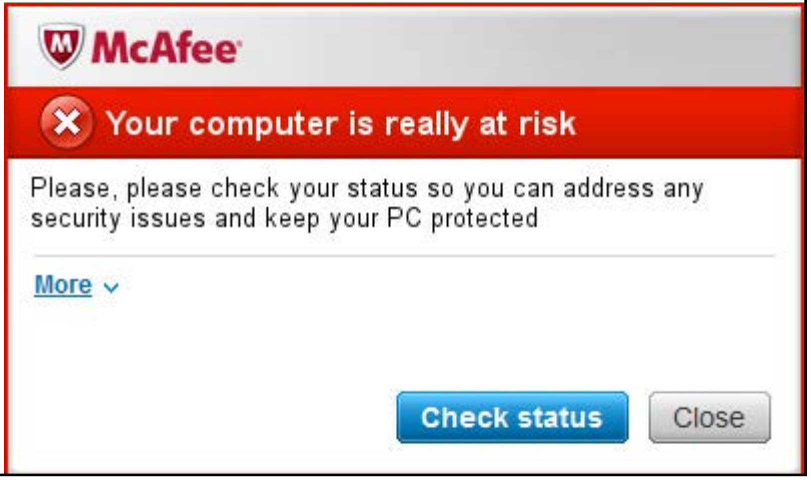

PNC Bank - Personal Banking
The PNC Financial Services Gro... (US) https://www.pnc.com/en/personal-banking.ht
Search
PERSONAL
SMALL BUSINESS
CORPORATE & INSTITUTIONAL
ABOUT US
Customer Service
Find a PNC ATM/Branch
Security Assurance
PNC
BANKING
BORROWING
INVESTMENTS & RETIREMENT
WEALTH MANAGEMENT
SEARCH
A Lesson in College Life
LIFE IS A BEAUTIFUL RIDE
LITTLE things
PAY $
Sign on to Online Banking
ENTER USER ID
Login
Forgot Your User ID or Password?
ENROLL IN ONLINE BANKING »
Sign on to another service:

Our very own "curriculum" to help get you campus-prepared… physically, mentally and financially.

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

New plan

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

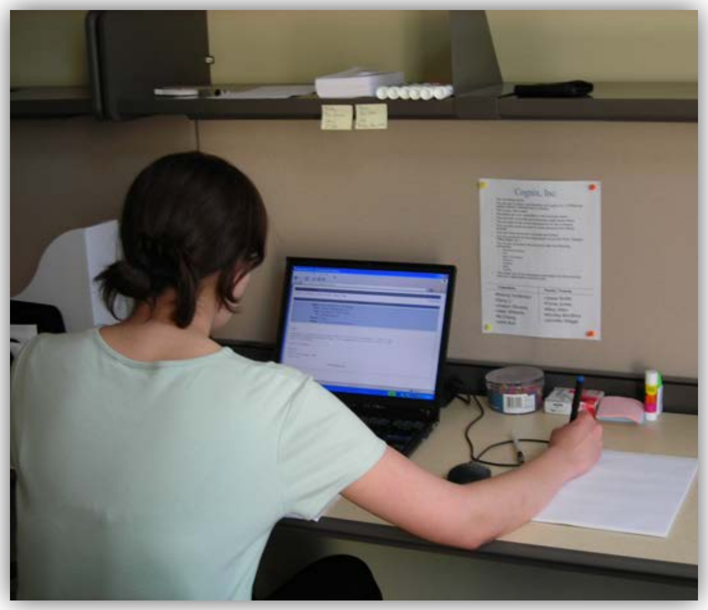


Your computer is really at risk

Please, please check your status so you can address any security issues and keep your PC protected

Lab study challenges

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



Provide easy alternative tasks

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

So what happened?

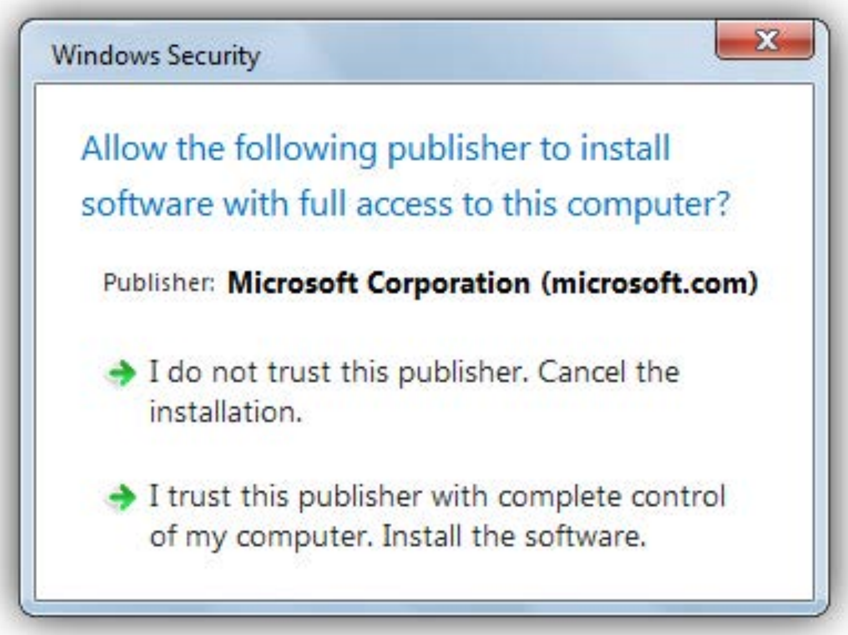
- 100 users tested FF2, FF3, IE7 + 2 new warnings
- **IE7 and FF2:** Most users ignored all warnings
- **FF3:** Most users heeded all warnings, couldn't figure out 4-step override process
- **New warnings:** Most users ignored warnings at library, about half heeded warnings at bank
  - **Big improvement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

More fun with warnings

- 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?



Windows Security

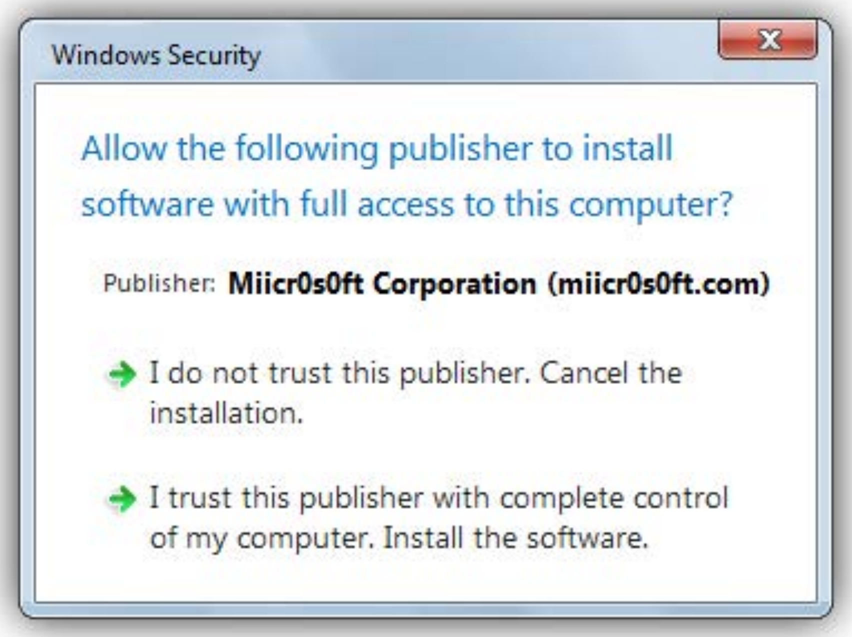
Allow the following publisher to install software with full access to this computer?

Publisher: **Microsoft Corporation (microsoft.com)**

→ I do not trust this publisher. Cancel the installation.

→ I trust this publisher with complete control of my computer. Install the software.

benign



Windows Security

Allow the following publisher to install software with full access to this computer?

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

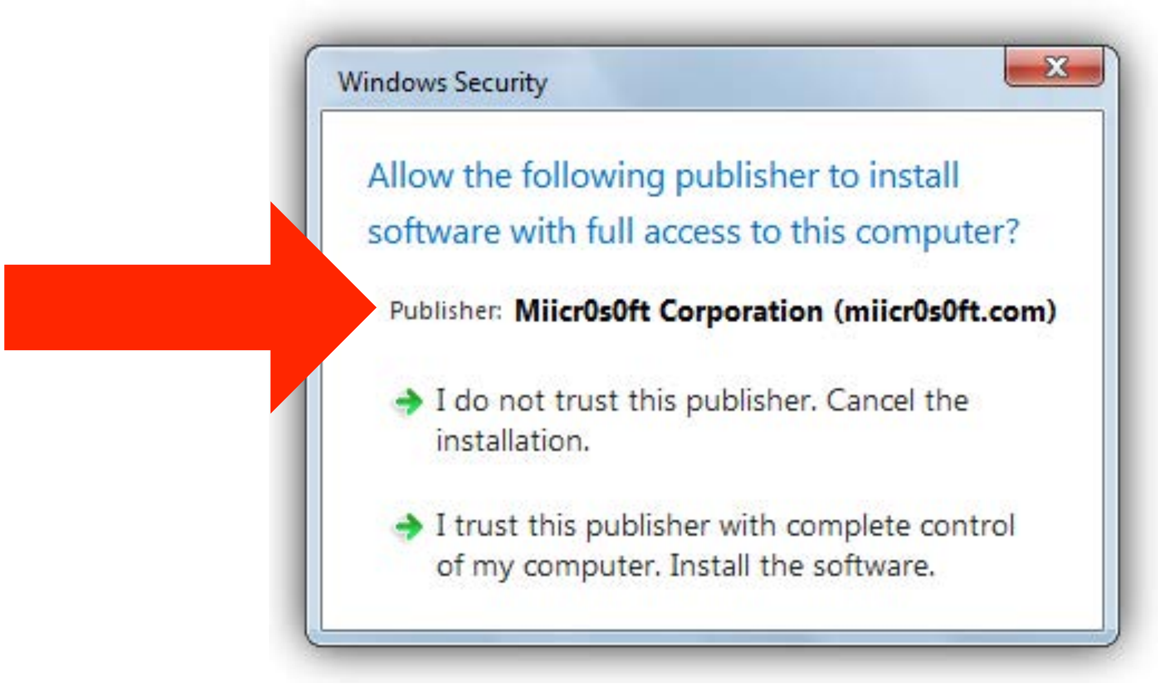
→ I do not trust this publisher. Cancel the installation.

→ I trust this publisher with complete control of my computer. Install the software.

suspicious

Key question: Do you trust publisher?

Name of publisher is critical information in trust decision



Windows Security

Allow the following publisher to install software with full access to this computer?

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

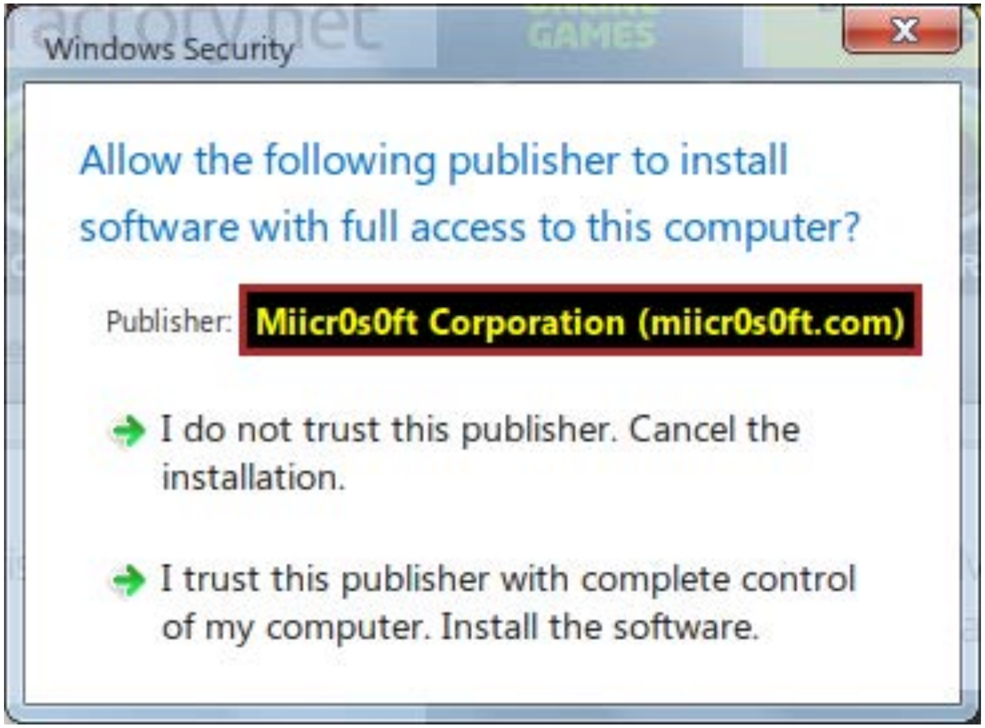
I do not trust this publisher. Cancel the installation.

I trust this publisher with complete control of my computer. Install the software.

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



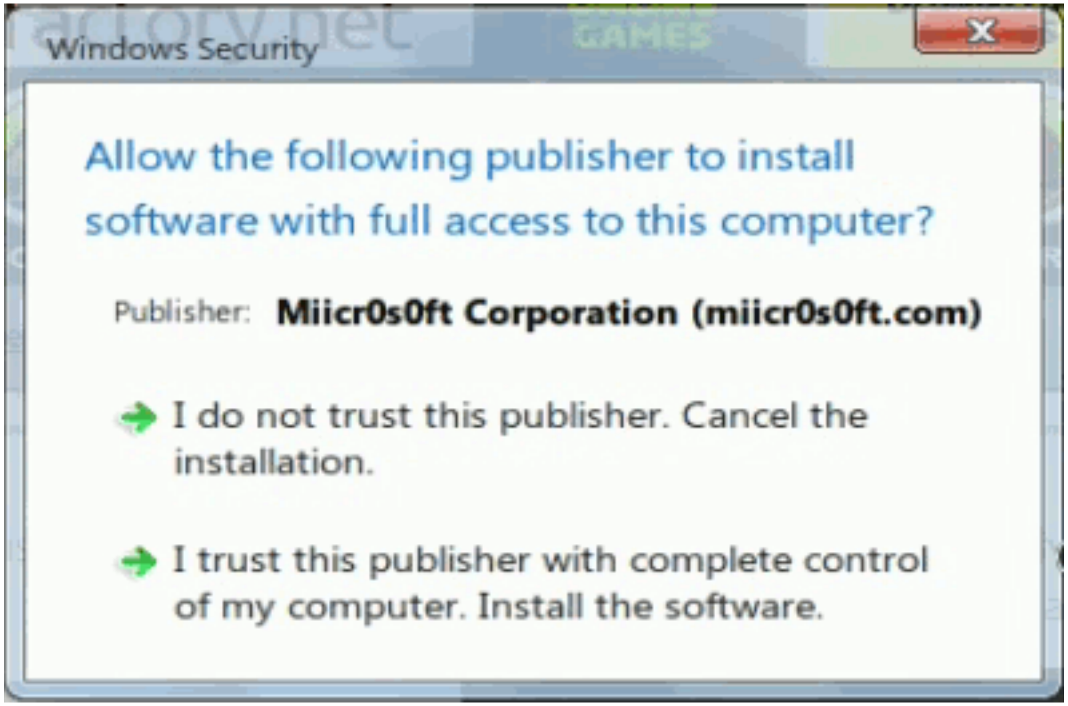
Allow the following publisher to install software with full access to this computer?

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.

Animated connector



Windows Security

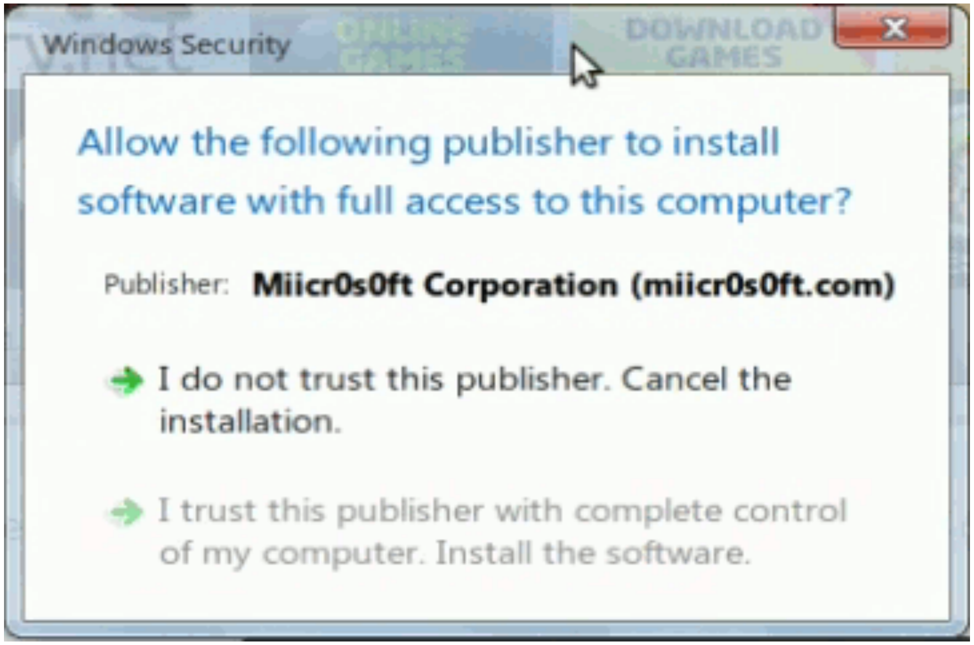
Allow the following publisher to install software with full access to this computer?

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.

Slow reveal



Windows Security

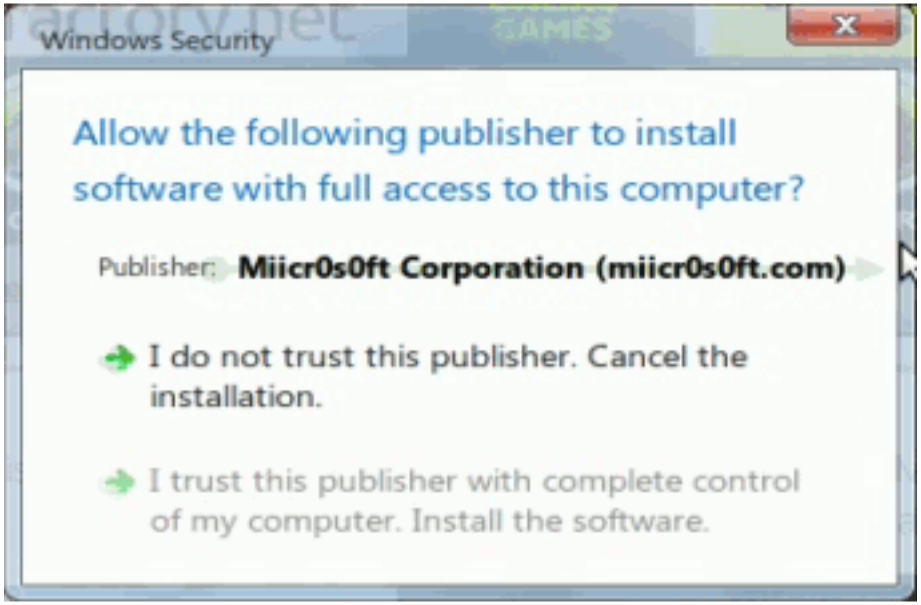
Allow the following publisher to install software with full access to this computer?

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

➔ I do not trust this publisher. Cancel the installation.

➔ I trust this publisher with complete control of my computer. Install the software.

Obstruct install button until user swipes mouse over publisher name



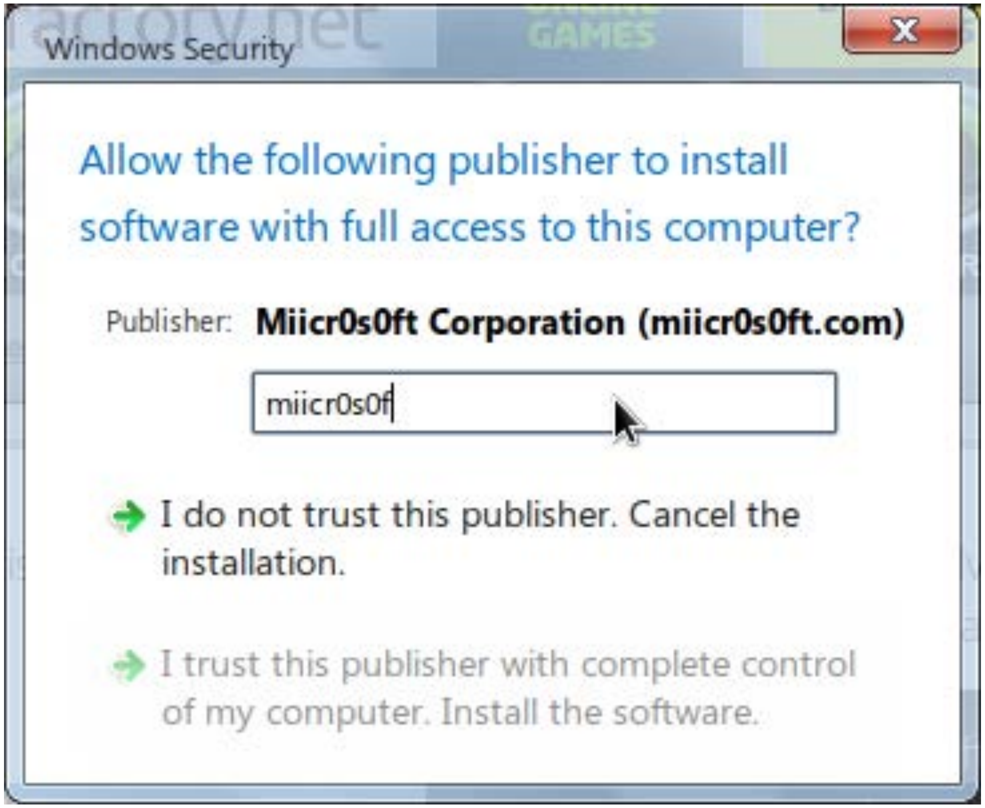
Allow the following publisher to install software with full access to this computer?

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

I do not trust this publisher. Cancel the installation.

I trust this publisher with complete control of my computer. Install the software.

Obstruct install button until user types publisher name



Allow the following publisher to install software with full access to this computer?

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

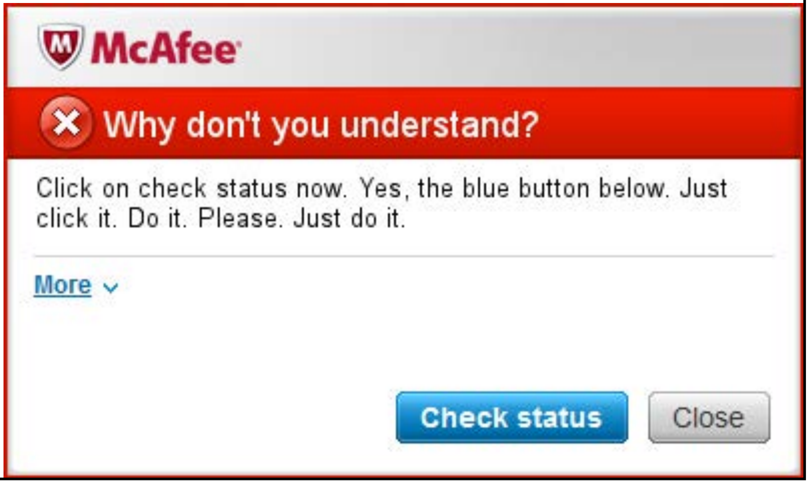
miicr0s0f

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?



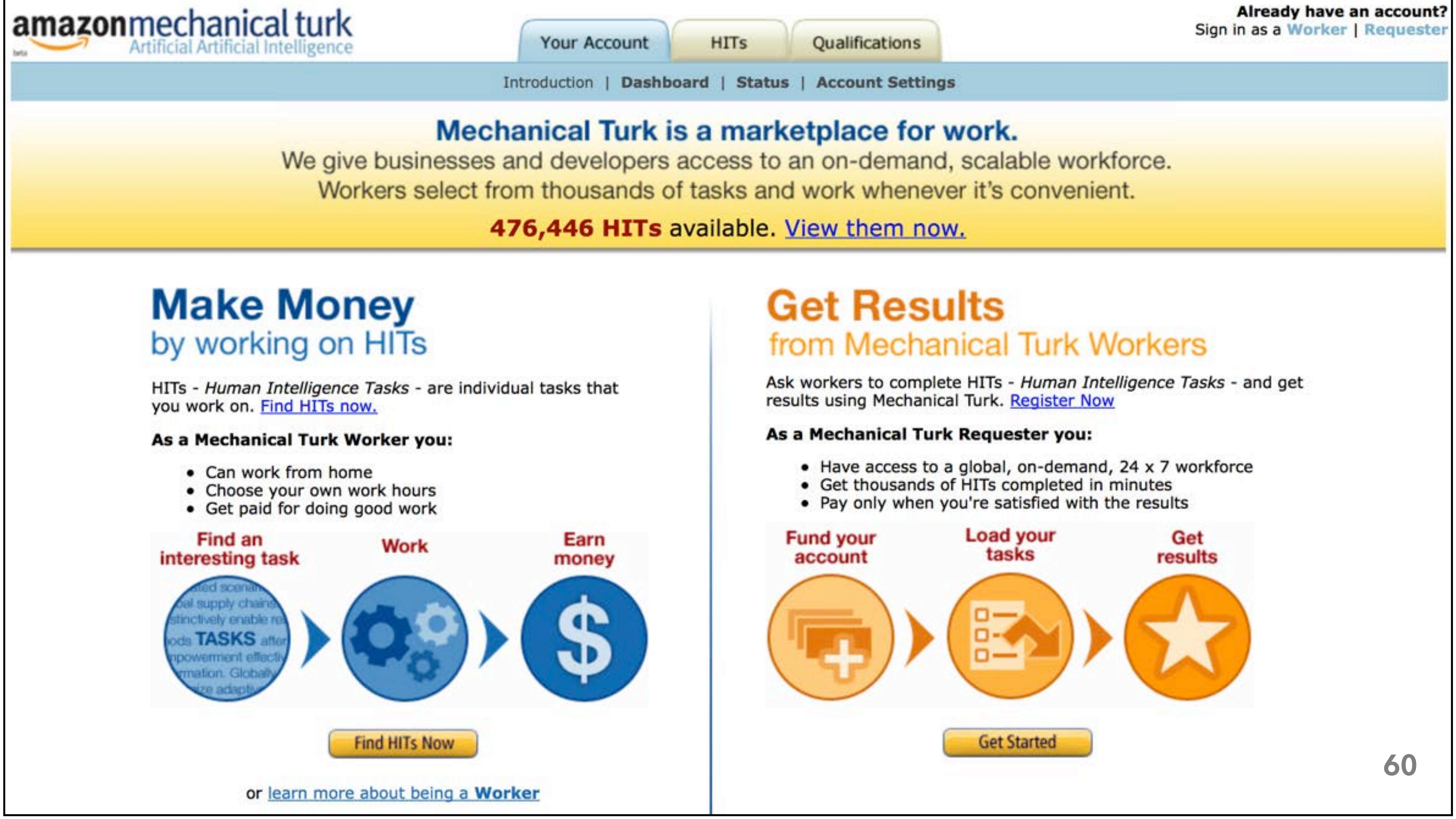
Why don't you understand?

Click on check status now. Yes, the blue button below. Just click it. Do it. Please. Just do it.

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 Amazon Mechanical Turk workers



Mechanical Turk is a marketplace for work.
We give businesses and developers access to an on-demand, scalable workforce.
Workers select from thousands of tasks and work whenever it's convenient.

476,446 HITs available. View them now.

Make Money
by working on HITs

HITs - *Human Intelligence Tasks* - are individual tasks that you work on. Find HITs now.

As a Mechanical Turk Worker you:

- Can work from home
- Choose your own work hours
- Get paid for doing good work

or learn more about being a **Worker**

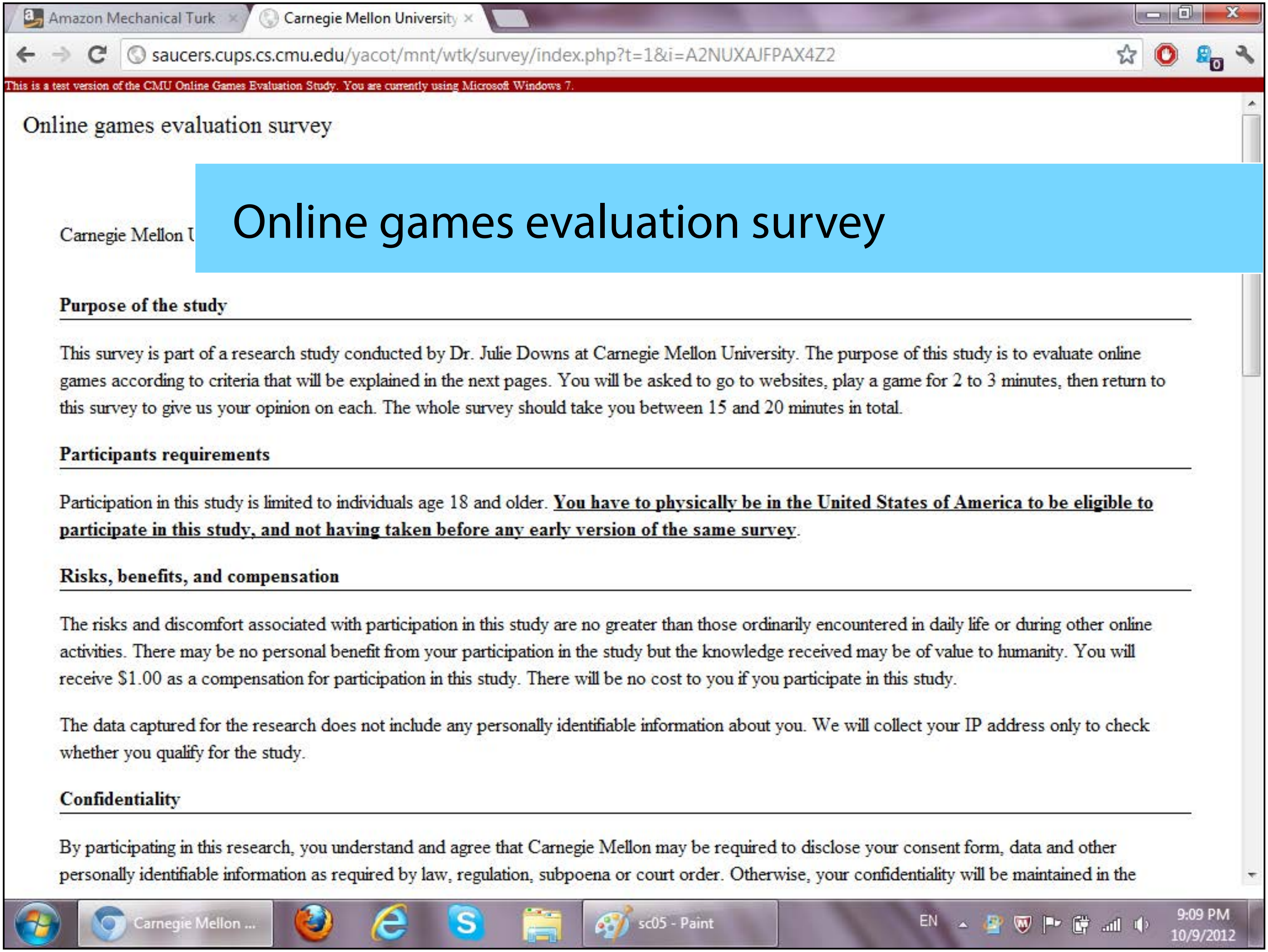
Get Results
from Mechanical Turk Workers

Ask workers to complete HITs - *Human Intelligence Tasks* - and get results using Mechanical Turk. Register Now

As a Mechanical Turk Requester you:

- Have access to a global, on-demand, 24 x 7 workforce
- Get thousands of HITs completed in minutes
- Pay only when you're satisfied with the results

Online games evaluation survey


Amazon Mechanical Turk
Carnegie Mellon University
saucers.cups.cs.cmu.edu/yacot/mnt/wtk/survey/index.php?t=1&i=A2NUXAJFPAX4Z2
Carnegie Mellon ...
sc05 - Paint
EN
9:09 PM
10/9/2012

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

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**.

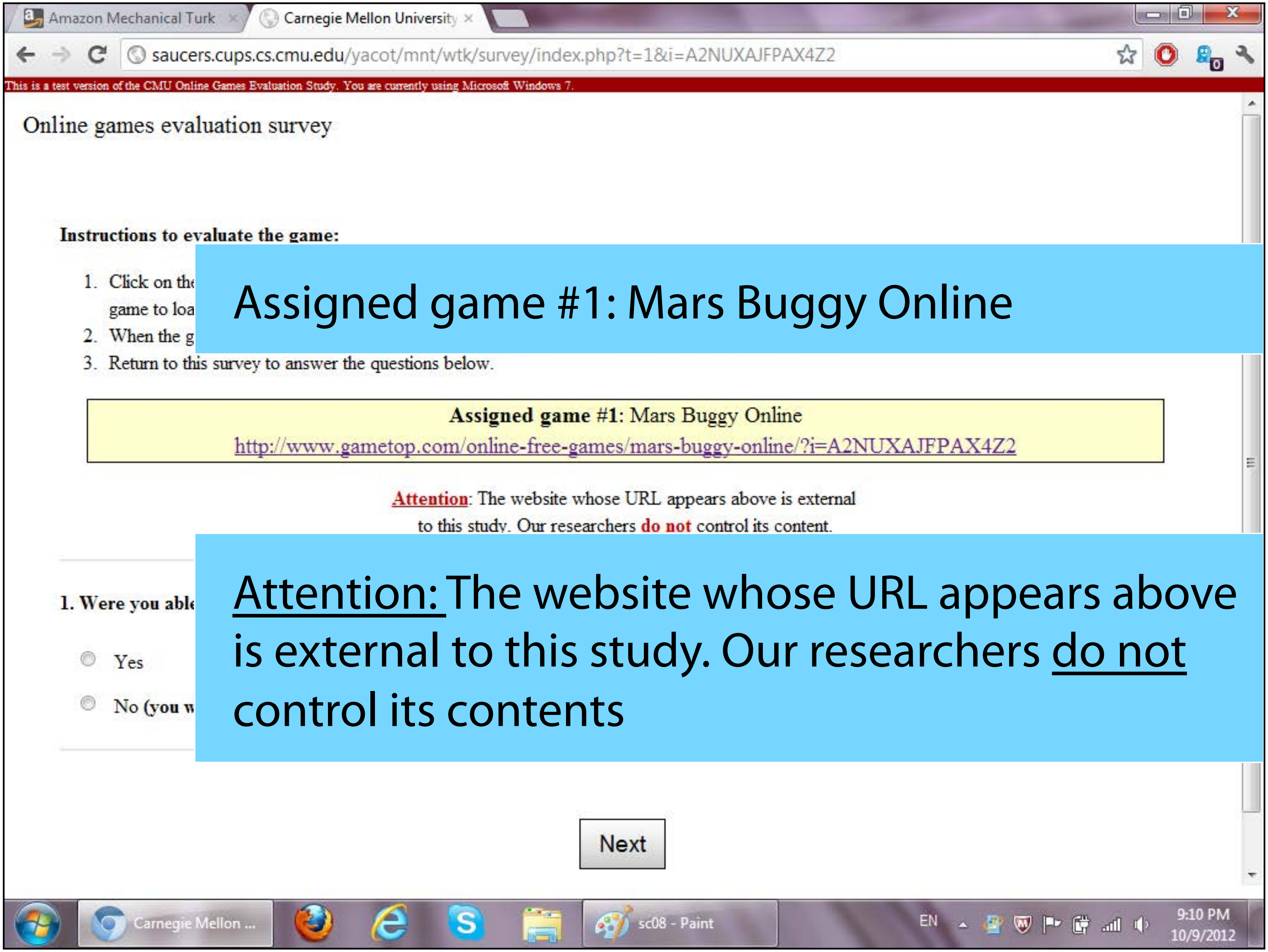
Risks, benefits, and compensation

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
Carnegie Mellon ...
sc08 - Paint
EN
9:10 PM
10/9/2012

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

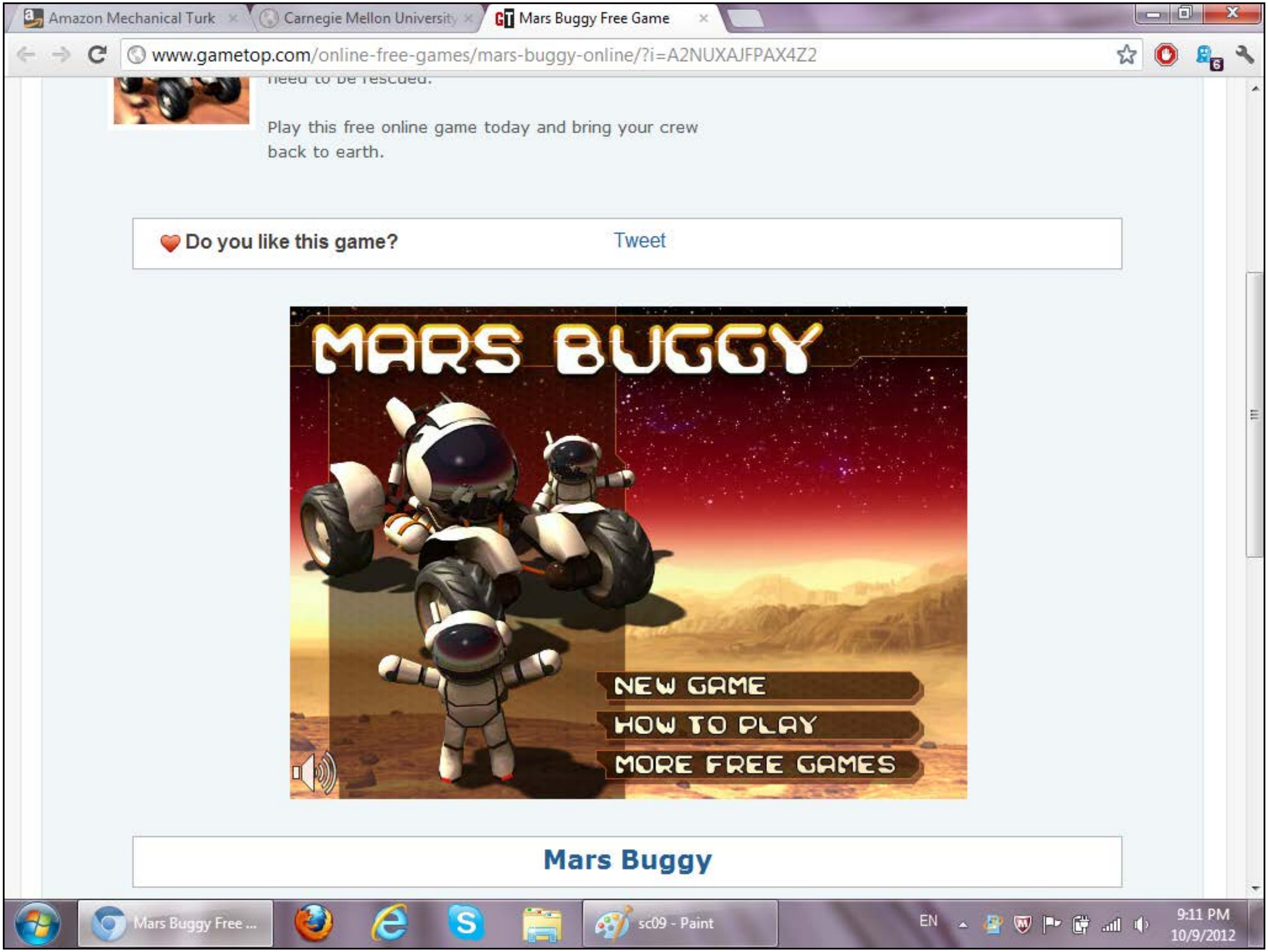
○ Yes

○ 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



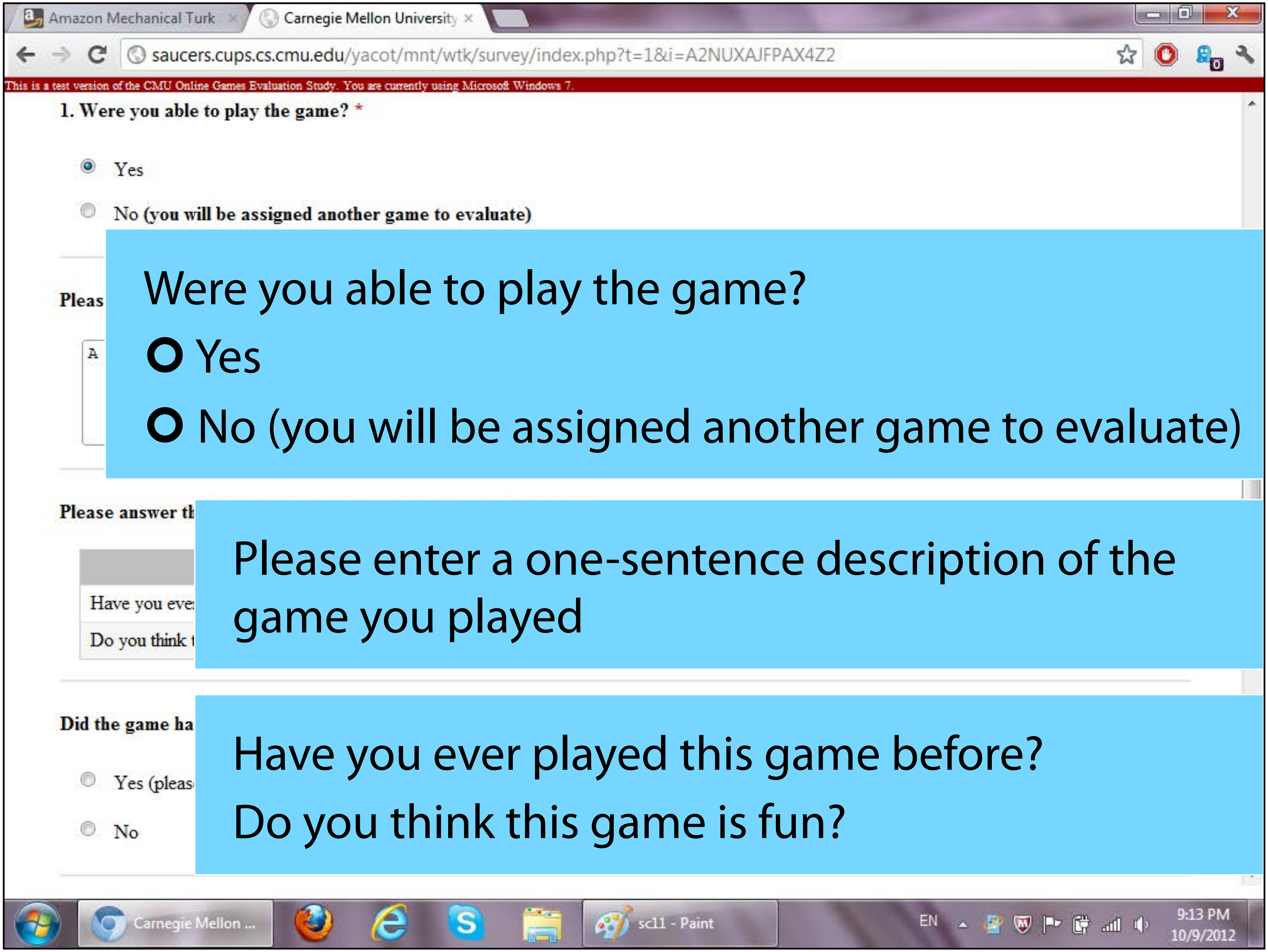
www.gametop.com/online-free-games/mars-buggy-online/?i=A2NUXAJFPAX4Z2

need to be rescued.

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

Do you like this game?

Mars Buggy


Amazon Mechanical Turk
Carnegie Mellon University
saucers.cups.cs.cmu.edu/yacot/mnt/wtk/survey/index.php?t=1&i=A2NUXAJFPAX4Z2
Carnegie Mellon ...
sc11 - Paint
EN
9:13 PM
10/9/2012

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)

Pleas

A

Please answer th

Have you eve

Do you think t

Did the game ha

○ Yes (pleas

○ No

Were you able to play the game?

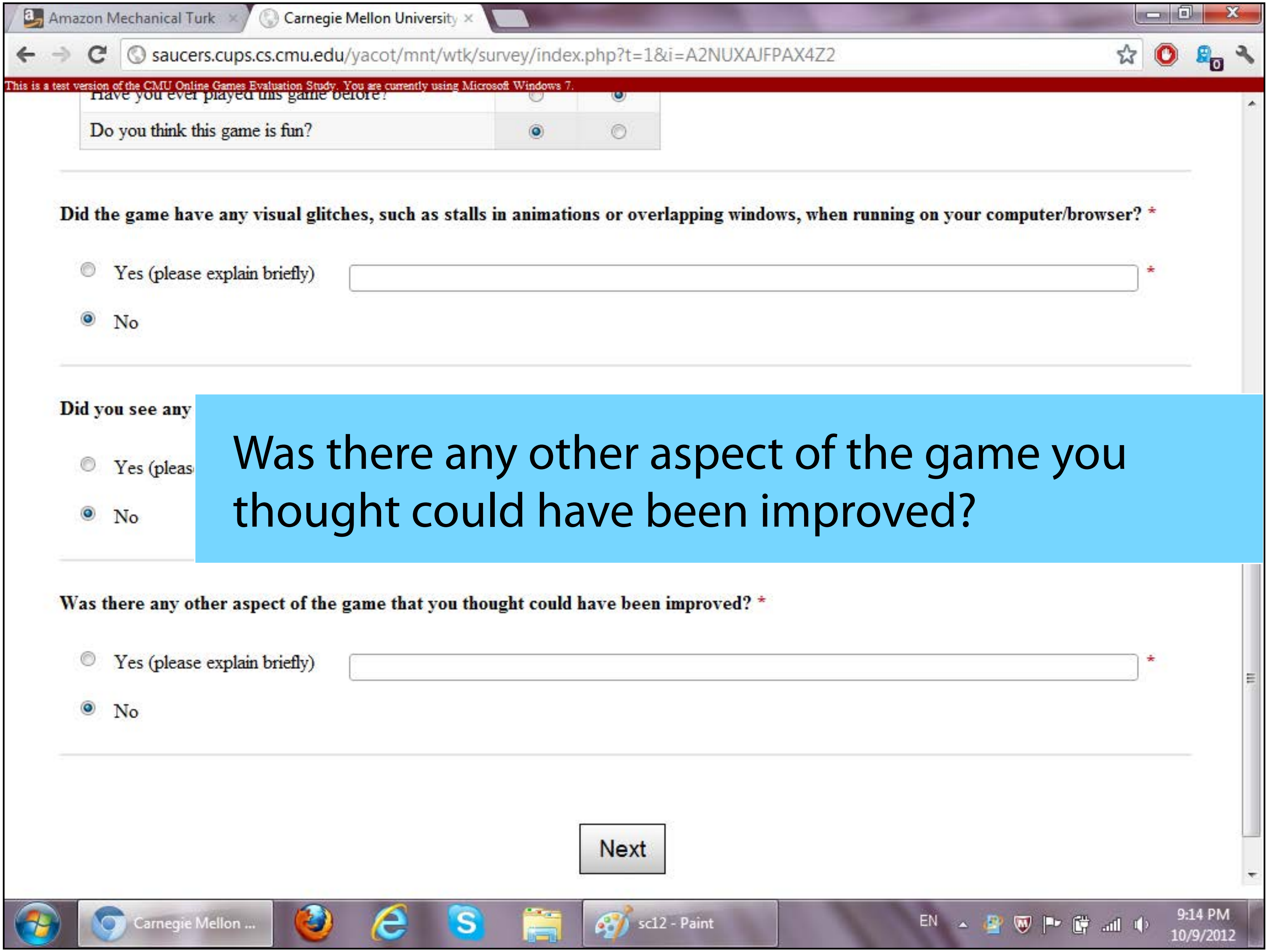
○ Yes

○ 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?


Amazon Mechanical Turk
Carnegie Mellon University
saucers.cups.cs.cmu.edu/yacot/mnt/wtk/survey/index.php?t=1&i=A2NUXAJFPAX4Z2
Carnegie Mellon ...
sc12 - Paint
EN
9:14 PM
10/9/2012

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 that you thought could have been improved? *

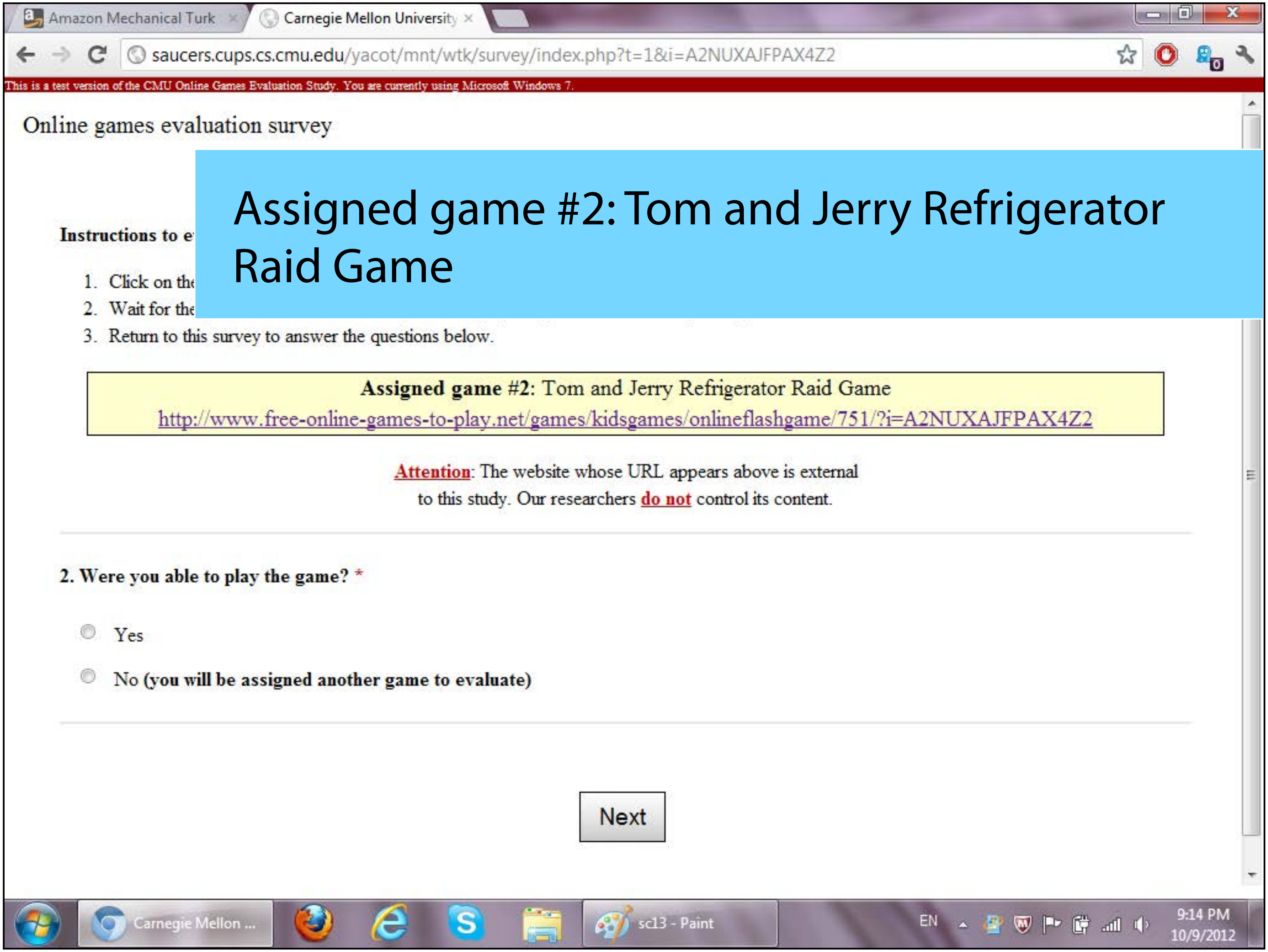
○ Yes (please explain briefly) ______ *

● No

Next

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

Assigned game #2: Tom and Jerry Refrigerator Raid Game


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 e

1. Click on the
2. Wait for the
3. Return to this survey to answer the questions below.

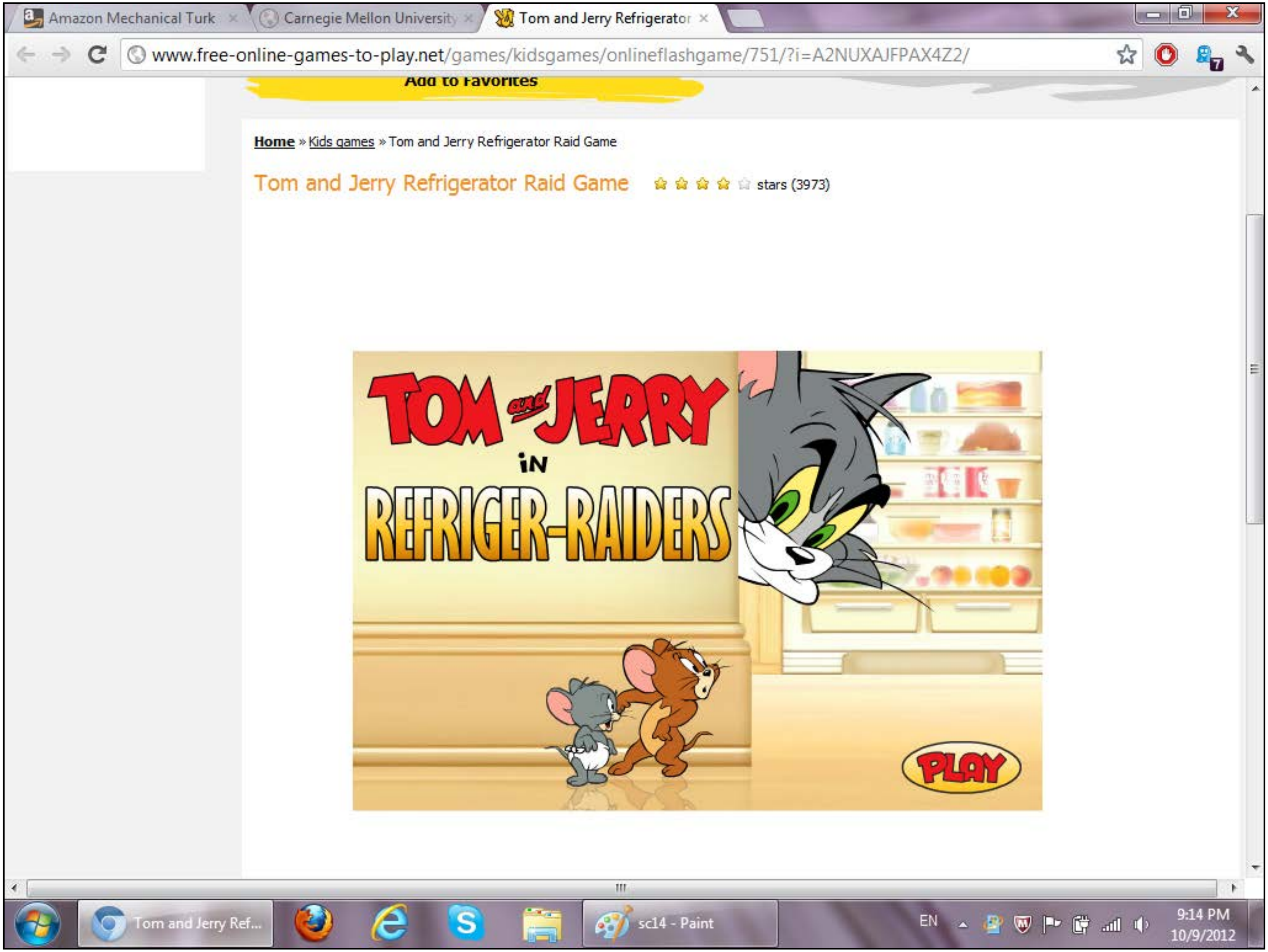
Assigned game #2: Tom and Jerry Refrigerator Raid Game
http://www.free-online-games-to-play.net/games/kidsgames/onlineflashgame/751/?i=A2NUXAJFPAX4Z2

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)**

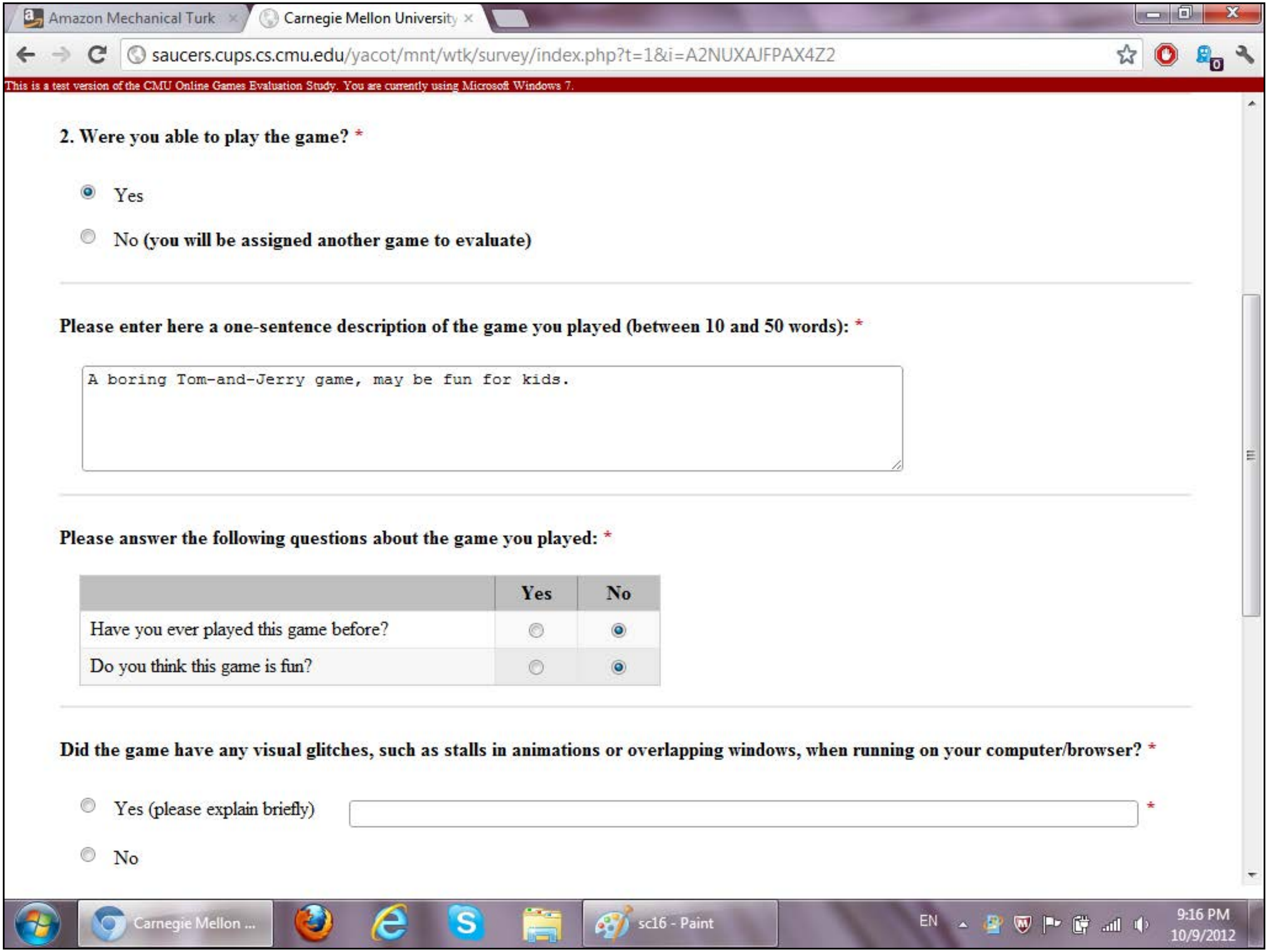


www.free-online-games-to-play.net/games/kidsgames/onlineflashgame/751/?i=A2NUXAJFPAX4Z2/

Add to Favorites

Home » Kids games » Tom and Jerry Refrigerator Raid Game

Tom and Jerry Refrigerator Raid Game ★★★★☆ stars (3973)


Amazon Mechanical Turk
Carnegie Mellon University
saucers.cups.cs.cmu.edu/yacot/mnt/wtk/survey/index.php?t=1&i=A2NUXAJFPAX4Z2
Carnegie Mellon ...
sc16 - Paint
EN
9:16 PM
10/9/2012

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: *

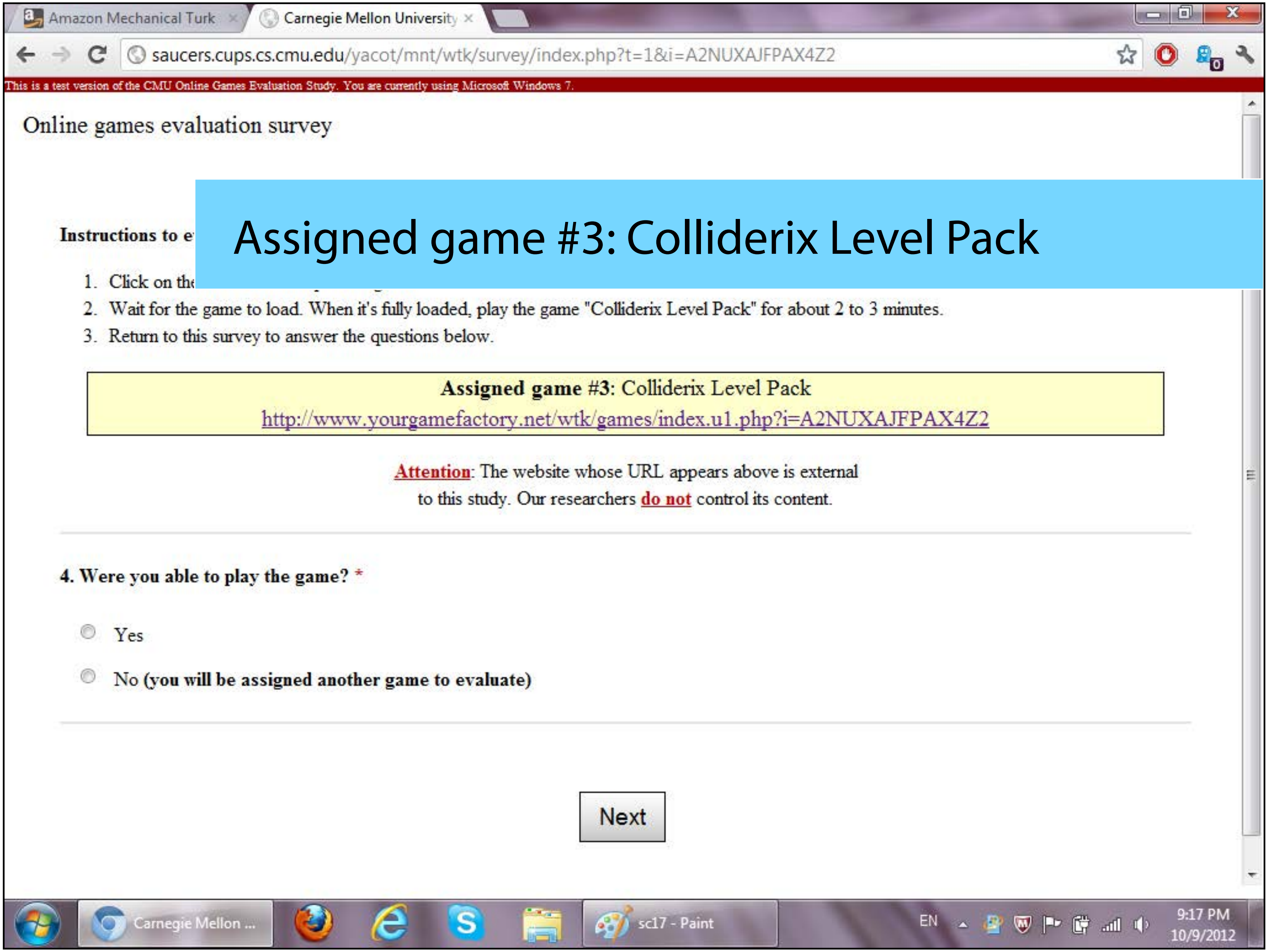
	Yes	No
Have you ever played this game before?	○	●
Do you think this game is fun?	○	●

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

Assigned game #3: Colliderix Level Pack



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 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

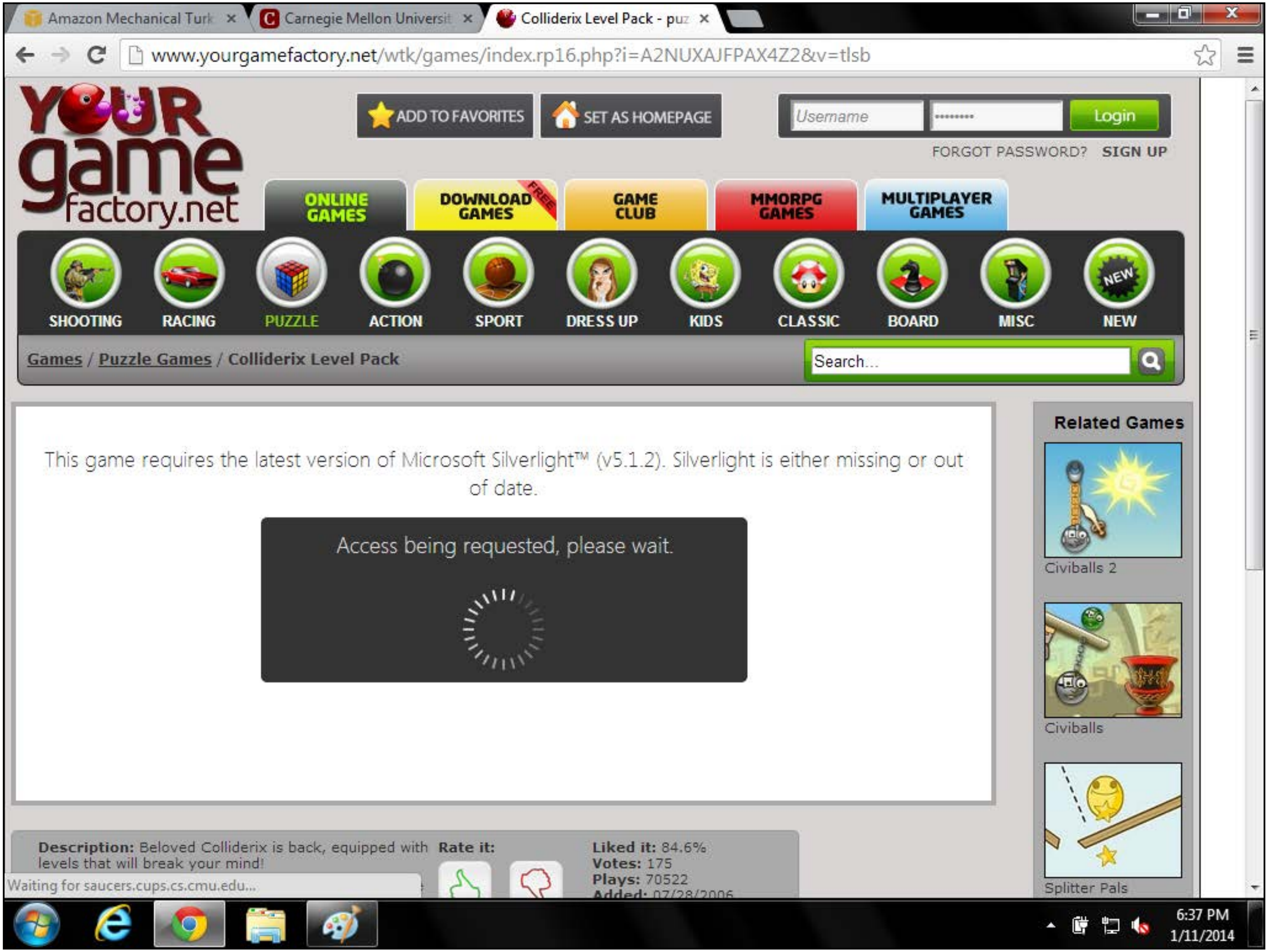
Attention: The website whose URL appears above is external to this study. Our researchers **do not** control its content.

4. Were you able to play the game? *

○ Yes

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

Next



Games / Puzzle Games / Colliderix Level Pack

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

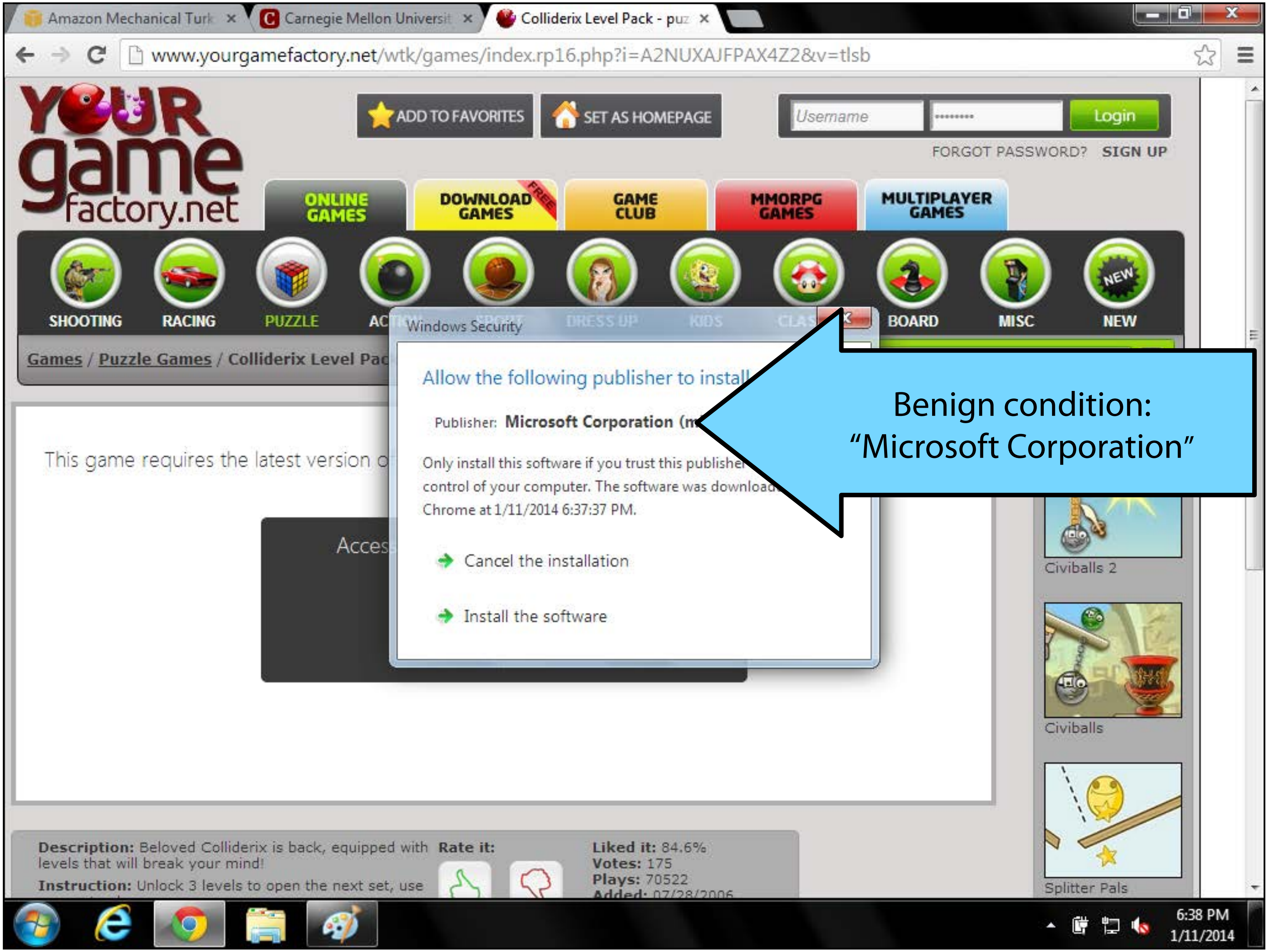
Access being requested, please wait.

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

Rate it:

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

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



This game requires the latest version o

Windows Security

Allow the following publisher to install

Publisher: **Microsoft Corporation (m**

Only install this software if you trust this publisher
control of your computer. The software was download
Chrome at 1/11/2014 6:37:37 PM.

→ Cancel the installation

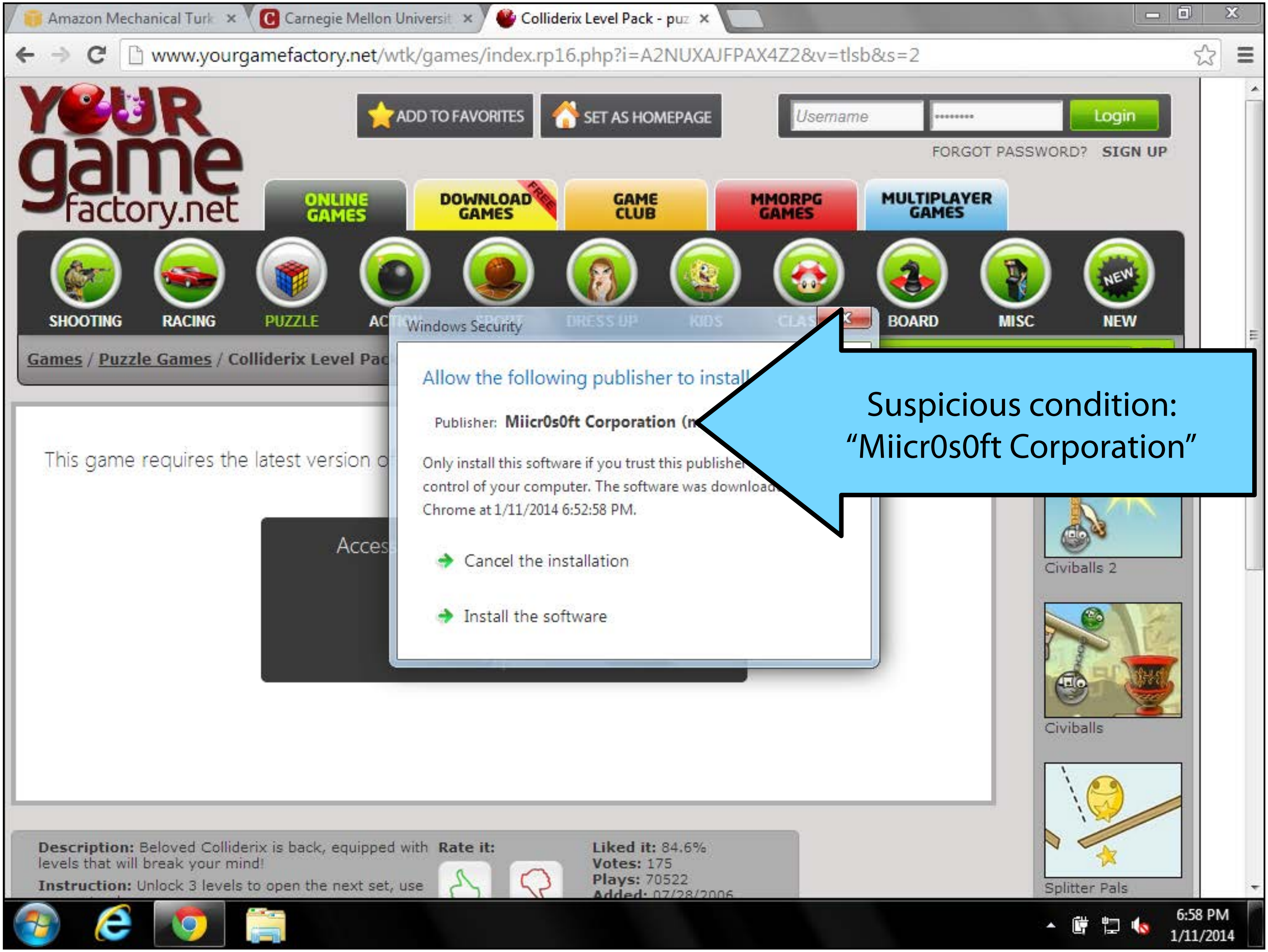
→ Install the software

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

Benign condition:
“Microsoft Corporation”



Windows Security

Allow the following publisher to install

Publisher: **Miicr0s0ft Corporation (m**

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

➔ Cancel the installation

➔ Install the software

This game requires the latest version o

Acces

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

Suspicious condition:
“Miicr0s0ft Corporation”

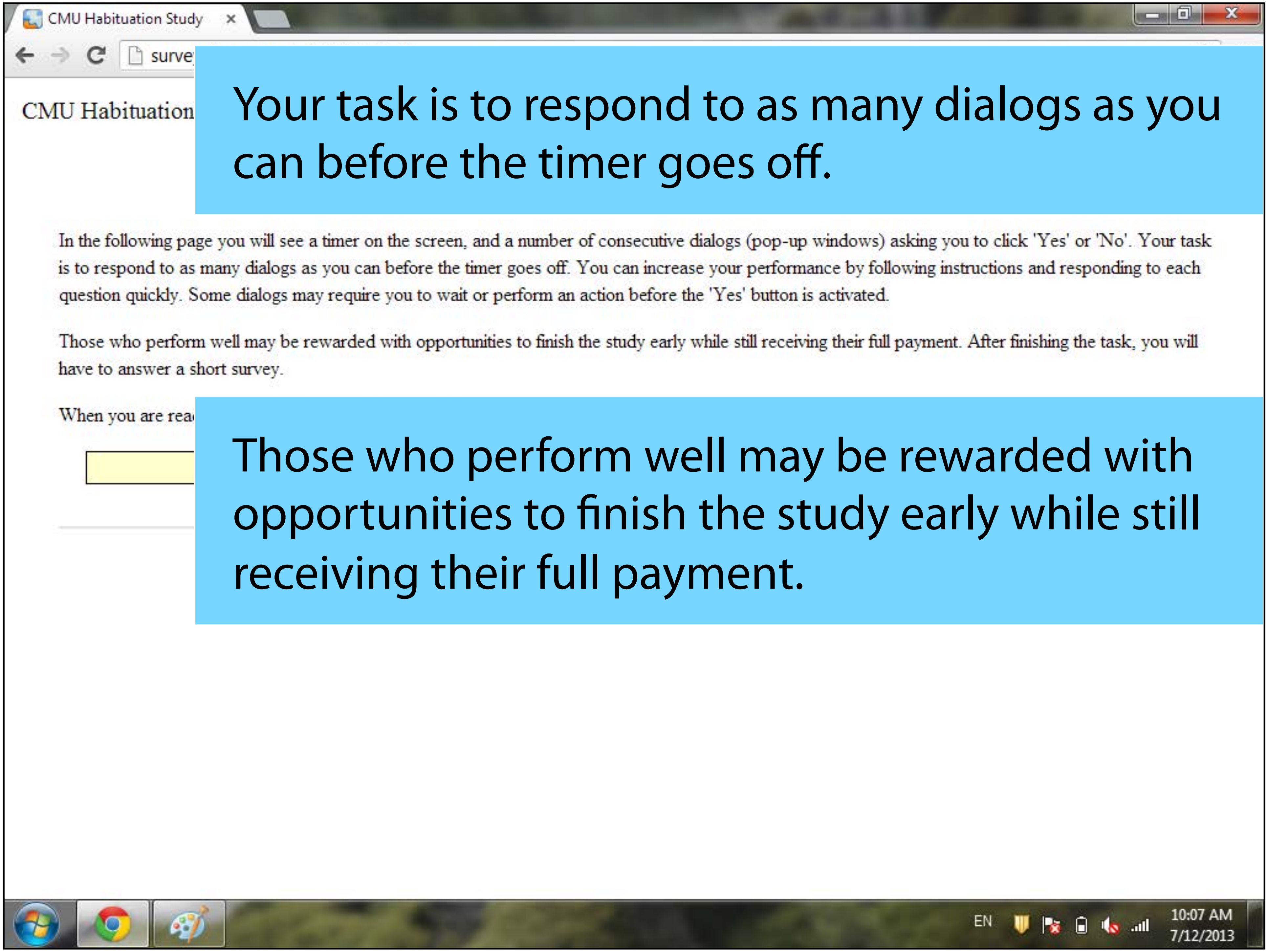
Results are encouraging

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

But what would happen if users saw these attractors repeatedly?

Habituation experiment

- Hard to expose users to same dialog repeatedly in a short period of time and keep it realistic
  - Task in which people had to dismiss a dialog as many times as they could before time ran out
  - Test whether they noticed when the dialog changed
- 9 conditions
- 872 Mturk participants completed task



CMU Habituation

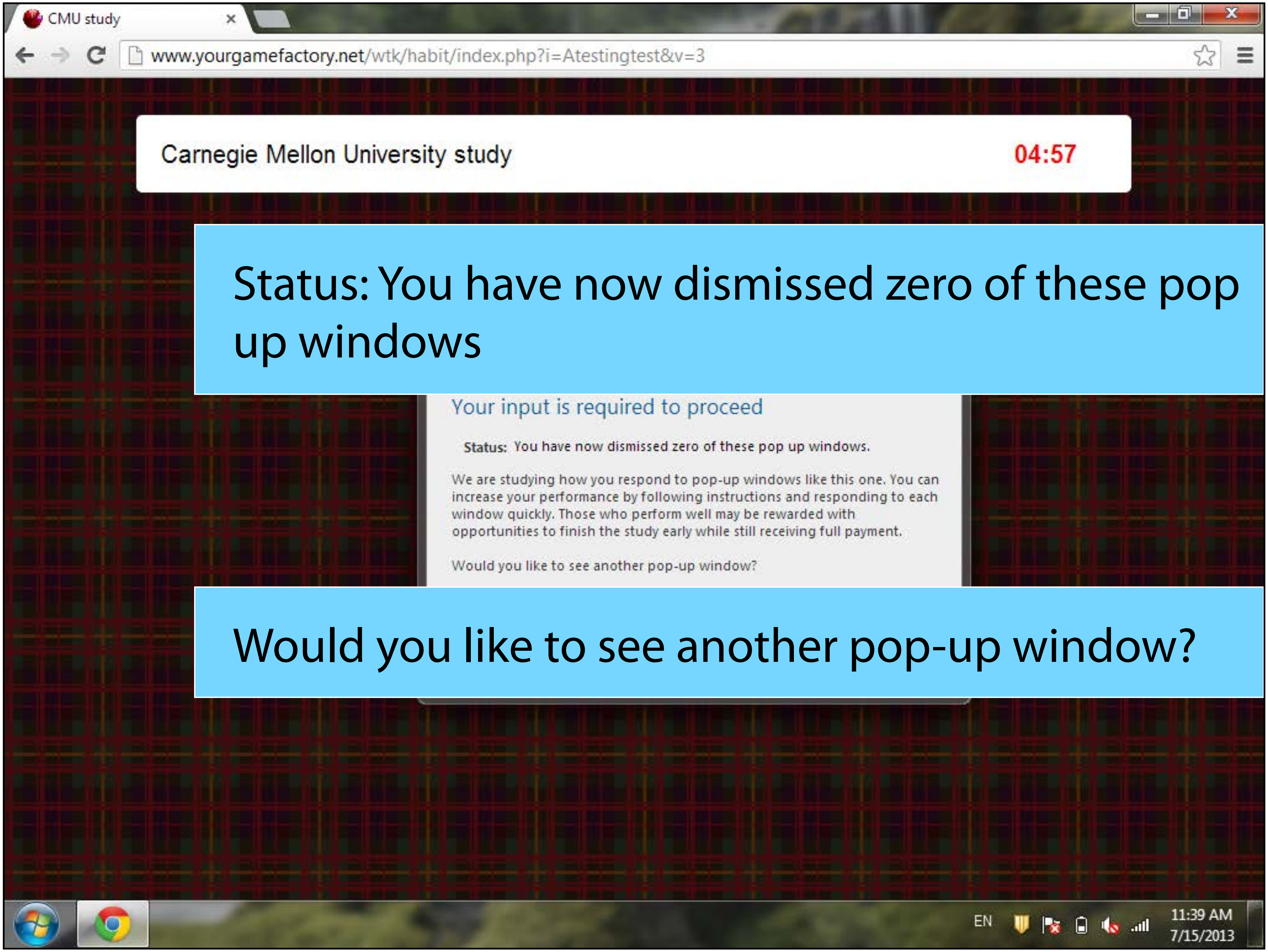
Your task is to respond to as many dialogs as you can before the timer goes off.

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 are rea

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
EN
11:39 AM
7/15/2013

Status: You have now dismissed zero of these pop up windows

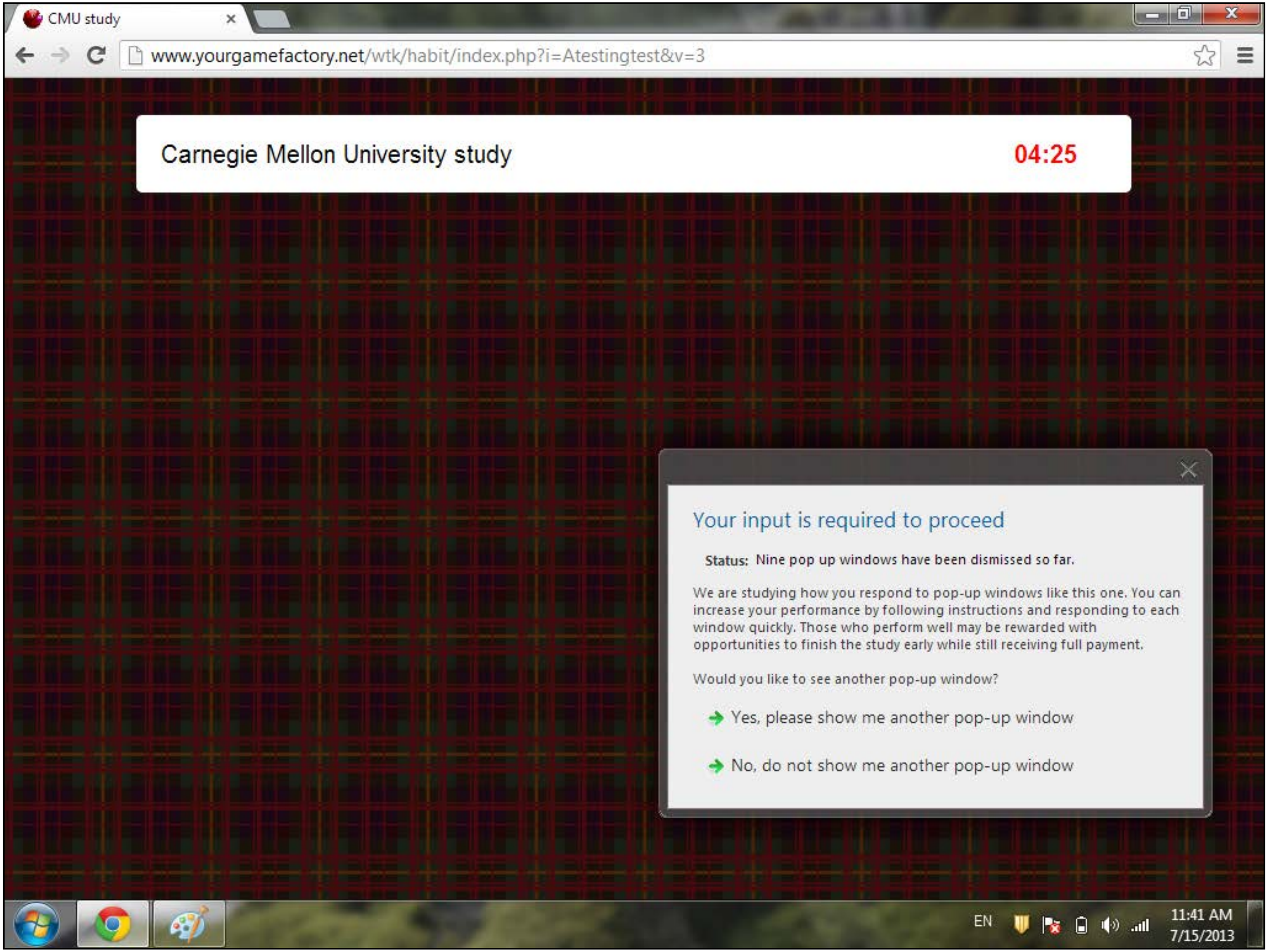
Your input is required to proceed

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?

Would you like to see another pop-up window?


CMU study
www.yourgamefactory.net/wtk/habit/index.php?i=Atestingtest&v=3
EN
11:41 AM
7/15/2013

Carnegie Mellon University study 04:25

Your input is required to proceed

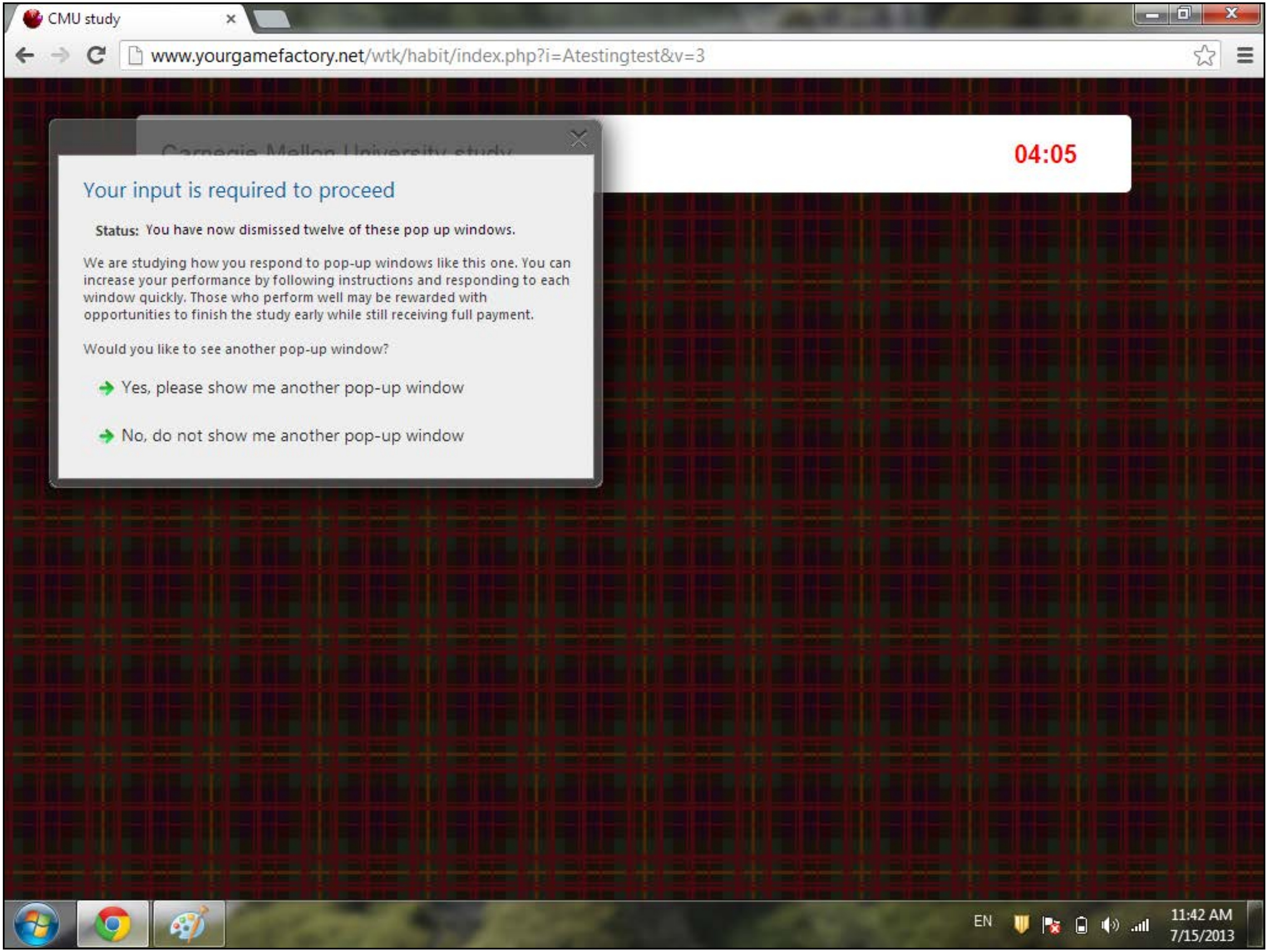
Status: Nine pop up windows have been dismissed so far.

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
Carnegie Mellon University study
04:05
EN
11:42 AM
7/15/2013

Your input is required to proceed

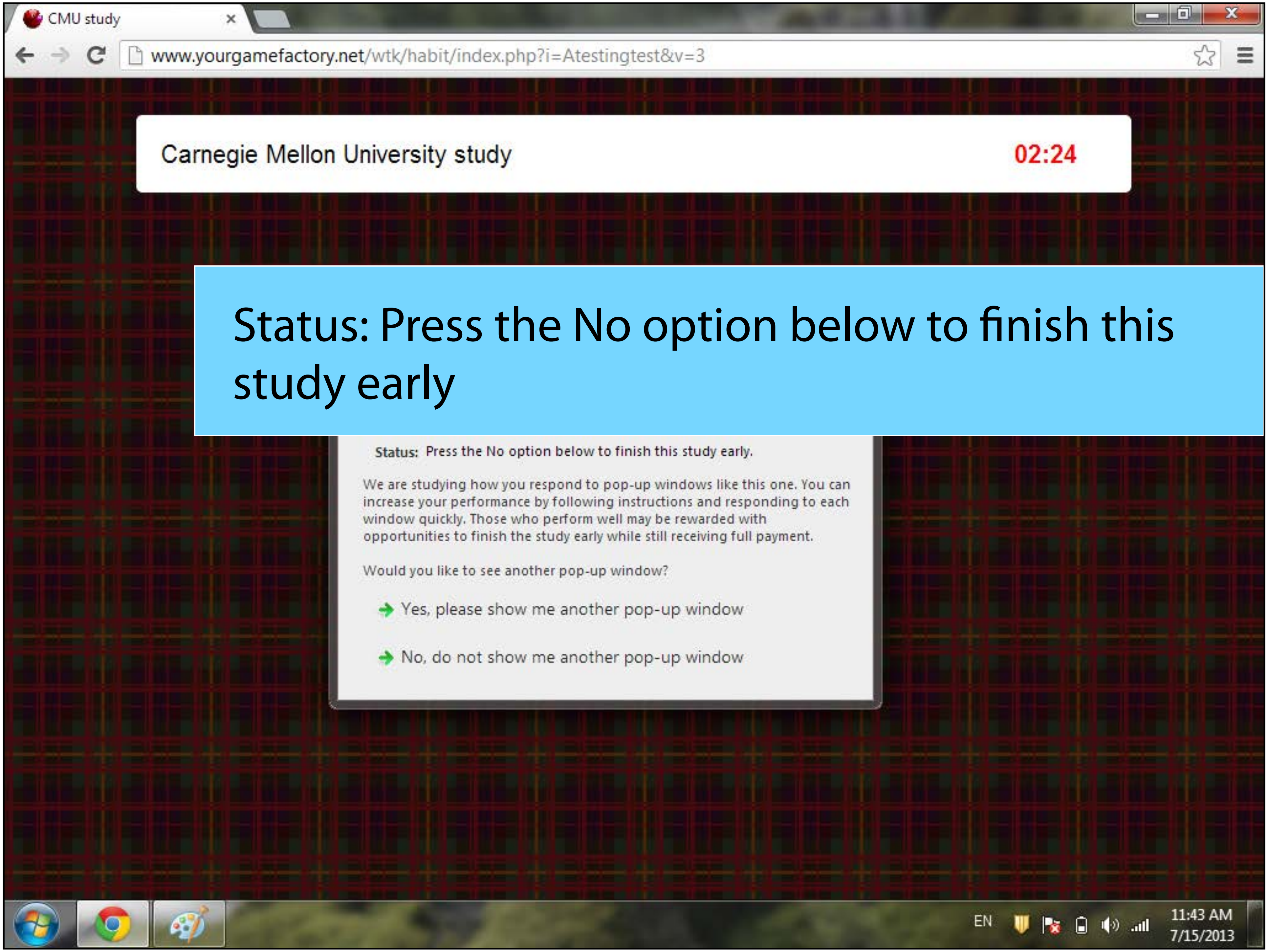
Status: You have now dismissed twelve of these pop up windows.

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



Status: Press the No option below to finish this study early

CMU study
www.yourgamefactory.net/wtk/habit/index.php?i=Atestingtest&v=3

Carnegie Mellon University study

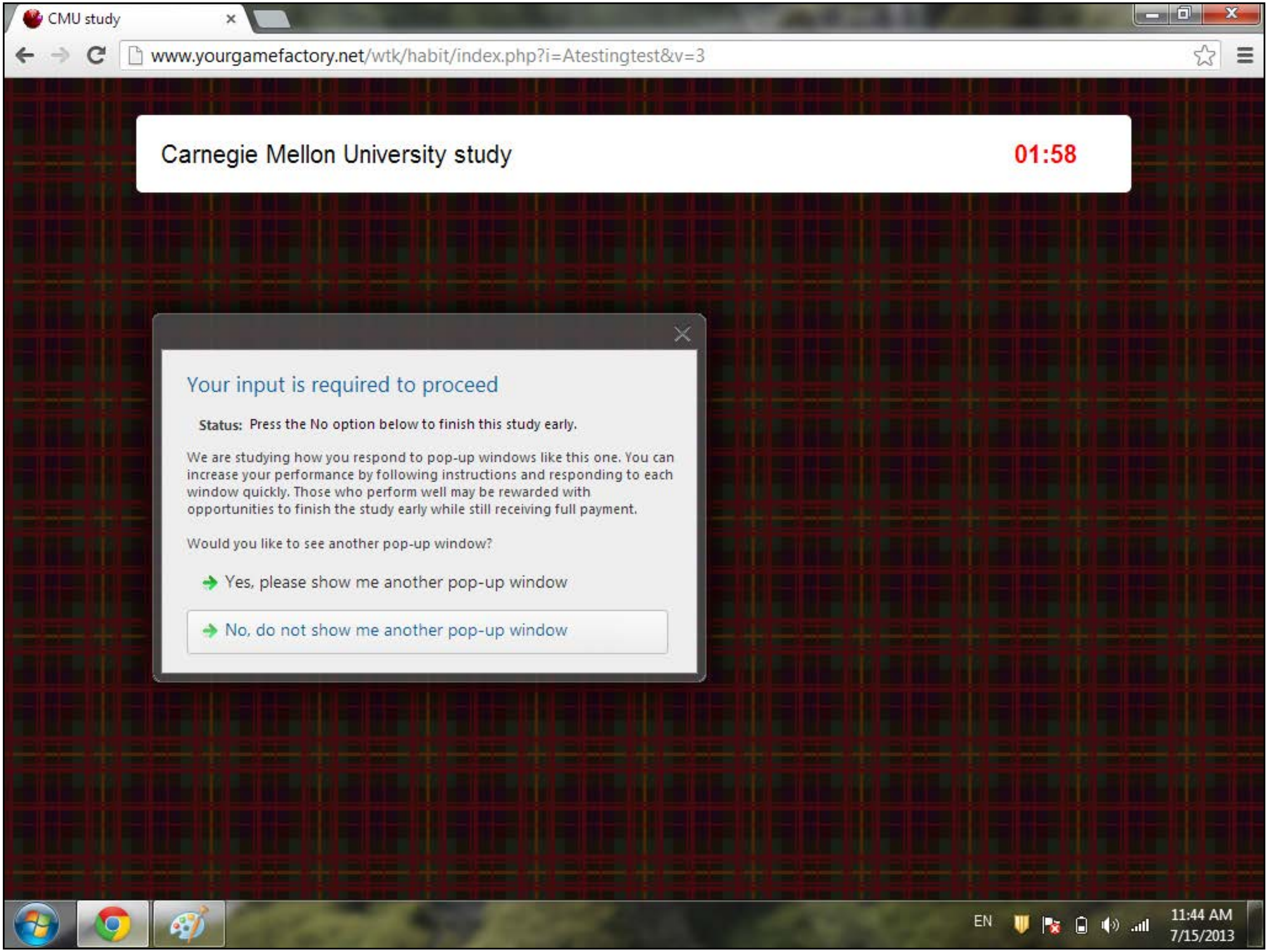
02:24

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

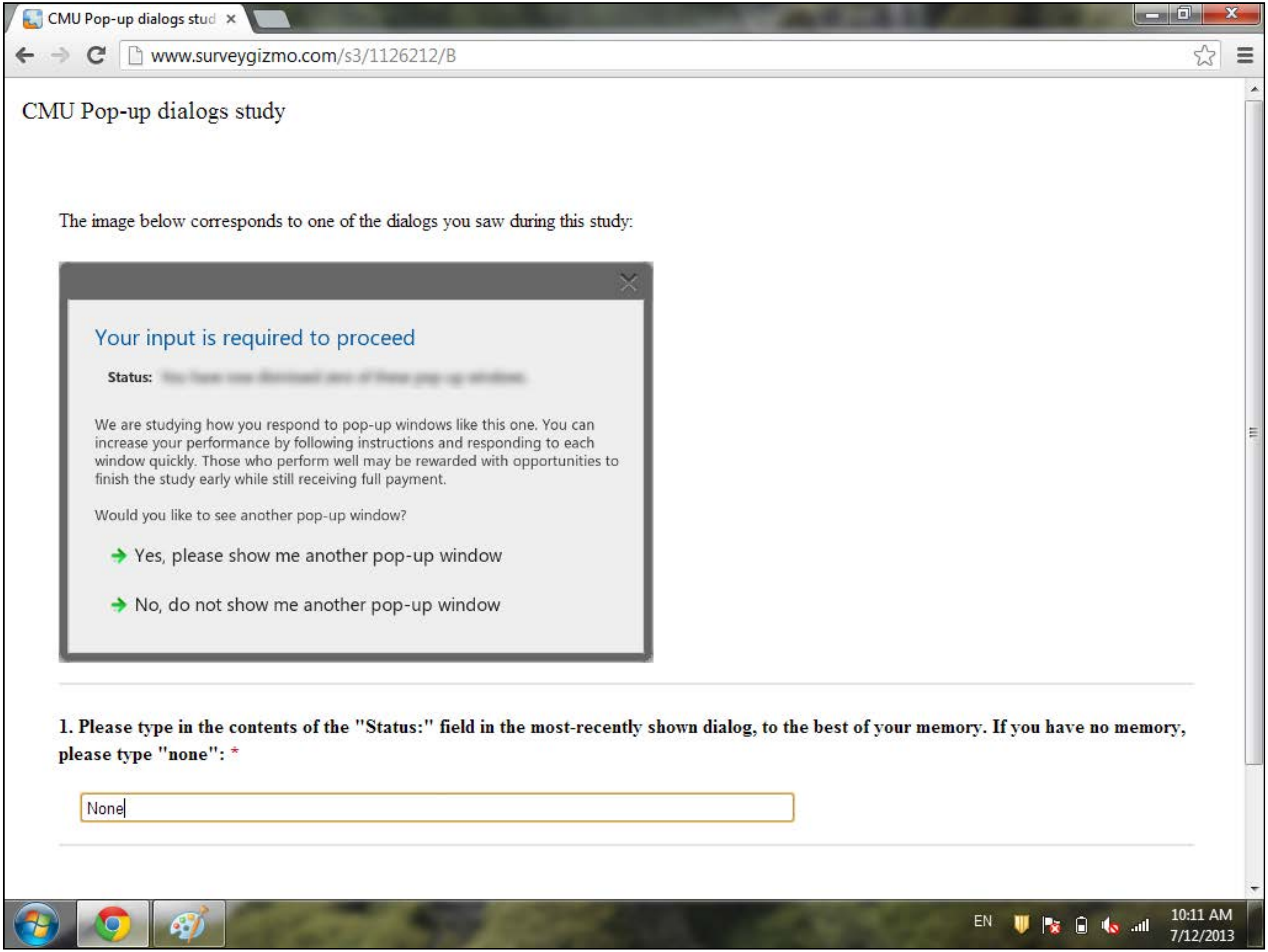
Your input is required to proceed

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
11:44 AM
7/15/2013



CMU Pop-up dialogs study

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

Your input is required to proceed

Status: [redacted]

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

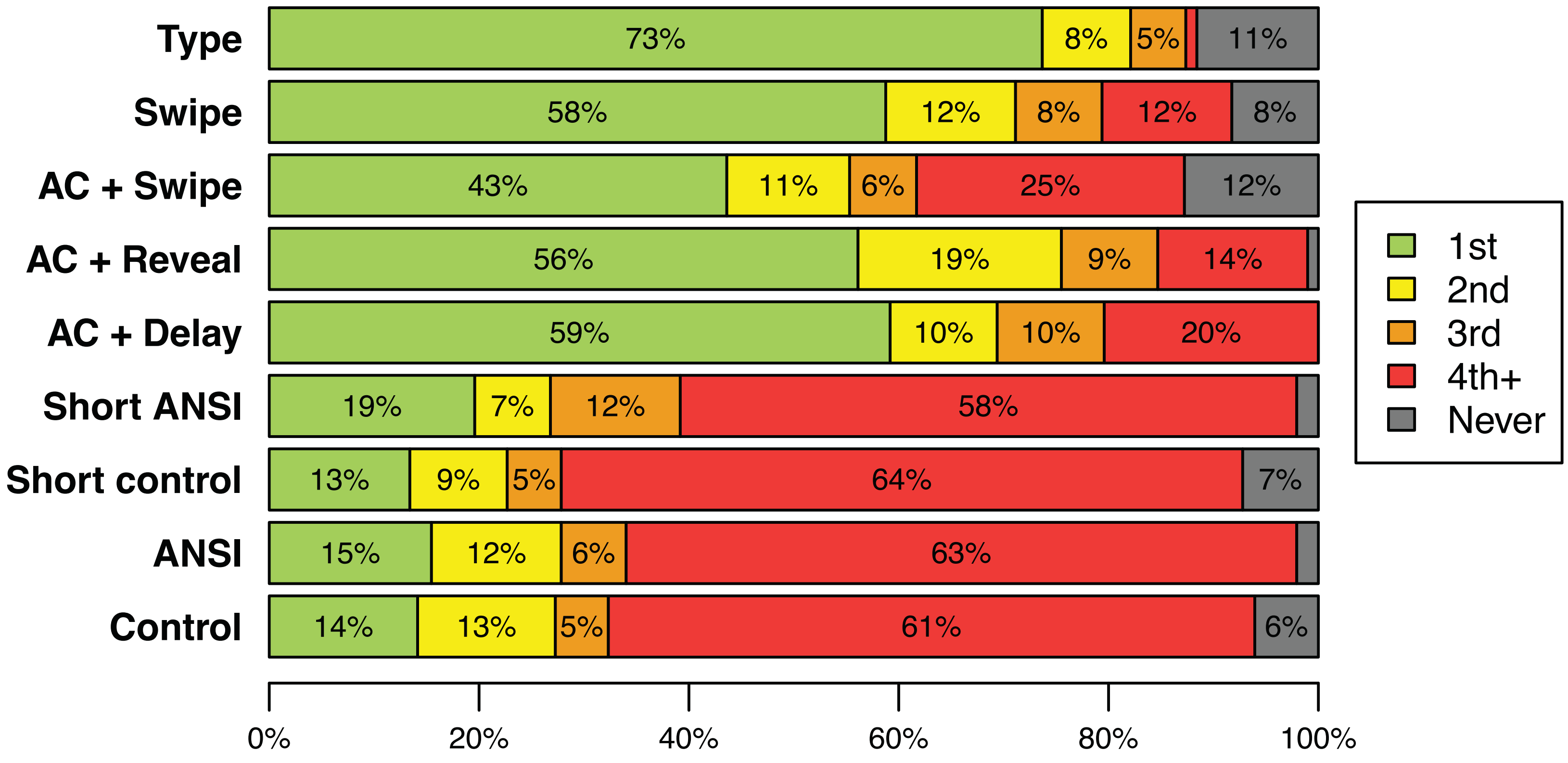
→ No, do not show me another pop-up window

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

Immediate detection rate higher for inhibitive attractors

Other conditions that previously performed well suffered under repeated exposures



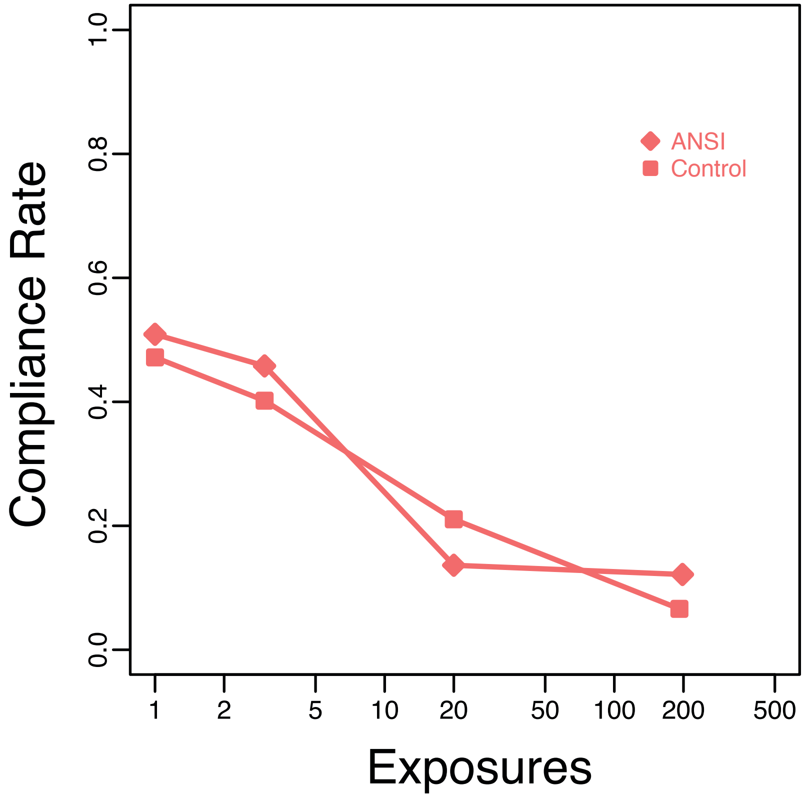
Do inhibitive attractors eliminate or reduce habituation?

- We showed inhibitive attractors perform better than control under habituation
- But we only tested with habituation
- Need another experiment to compare with and without habituation
  - Exposure to irrelevant message: 1 exposure, 3 exposures, 20 exposures, 150 sec. of exposure

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.

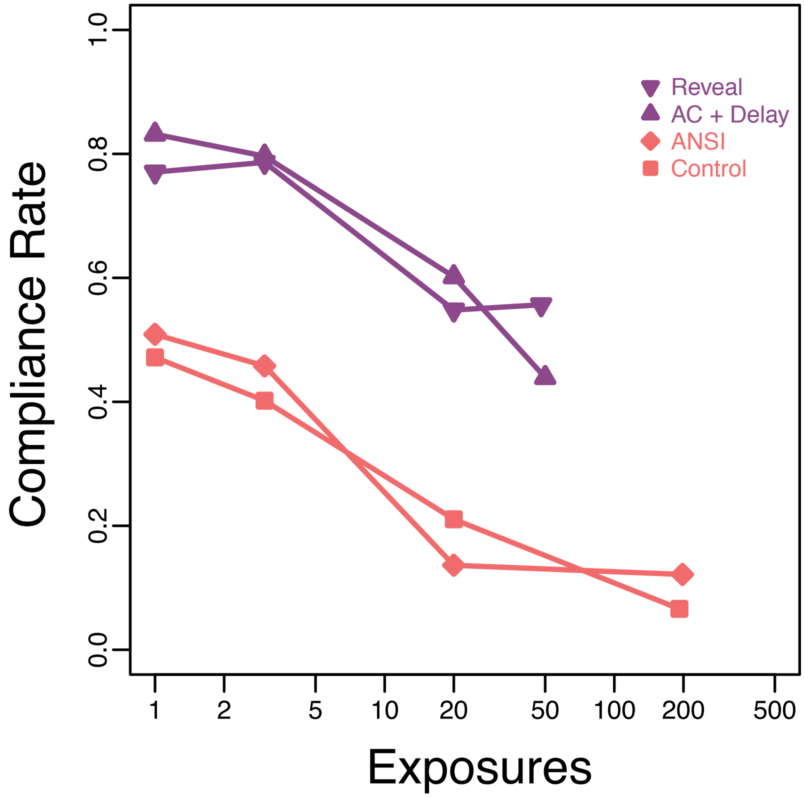
Swipe and Type are resilient to habituation

- Control and ANSI compliance declines with habituation



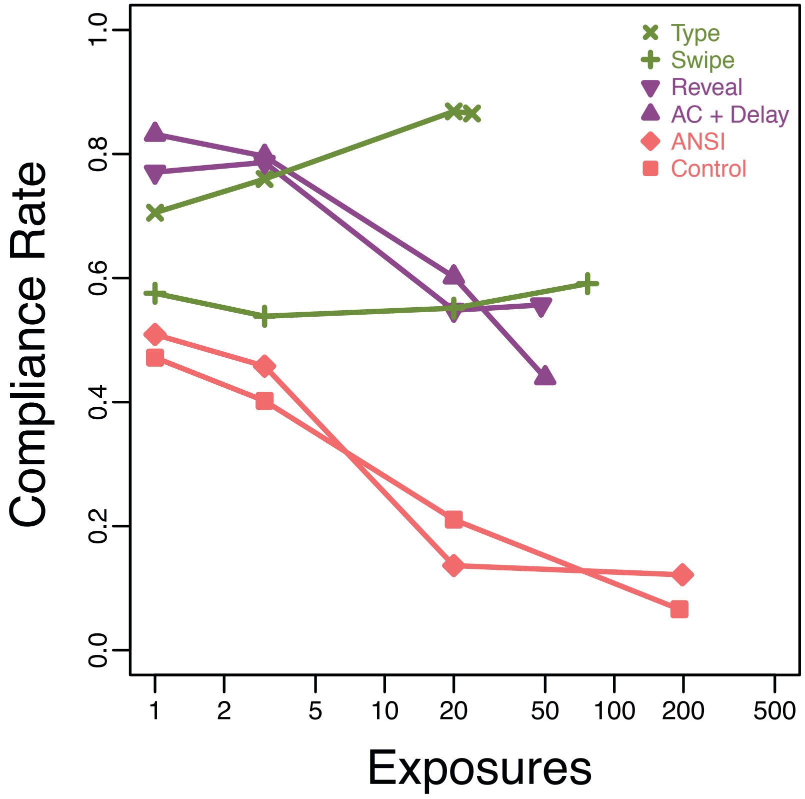
Swipe and Type are resilient to habituation

- Control and ANSI compliance declines with habituation
- Reveal and AC+Delay have higher compliance, decline with habituation



Swipe and Type are resilient to habituation

- Control and ANSI compliance declines with habituation
- Reveal and AC+Delay have higher compliance, decline with habituation
- Swipe and Type show steady or increasing compliance rates

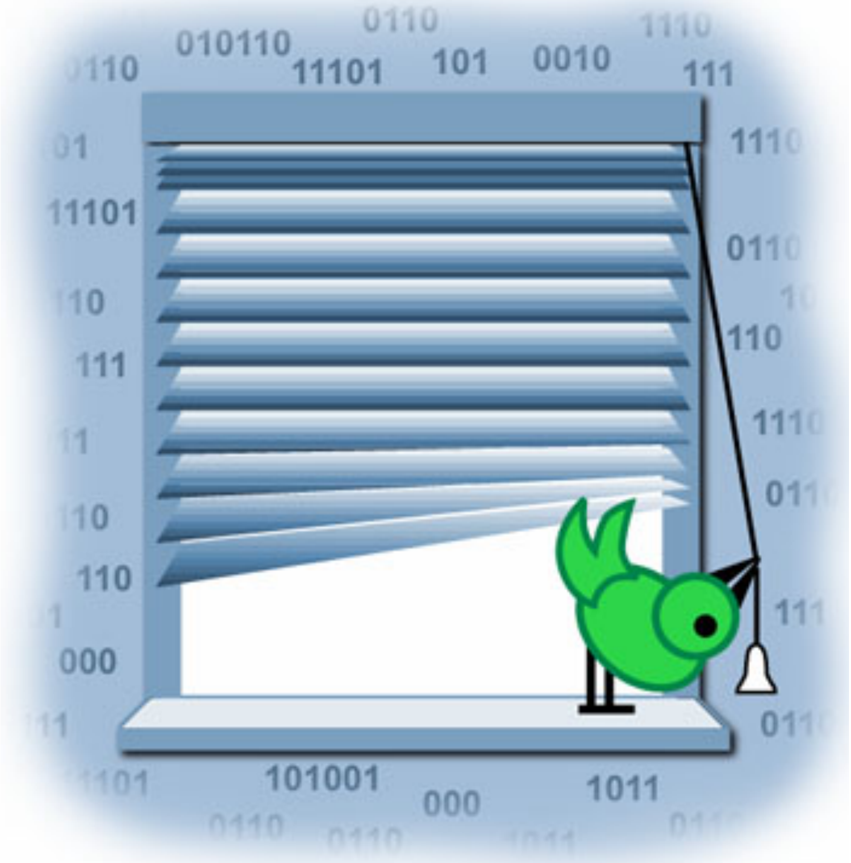


Could not predict difference between green and purple lines from previous experiment

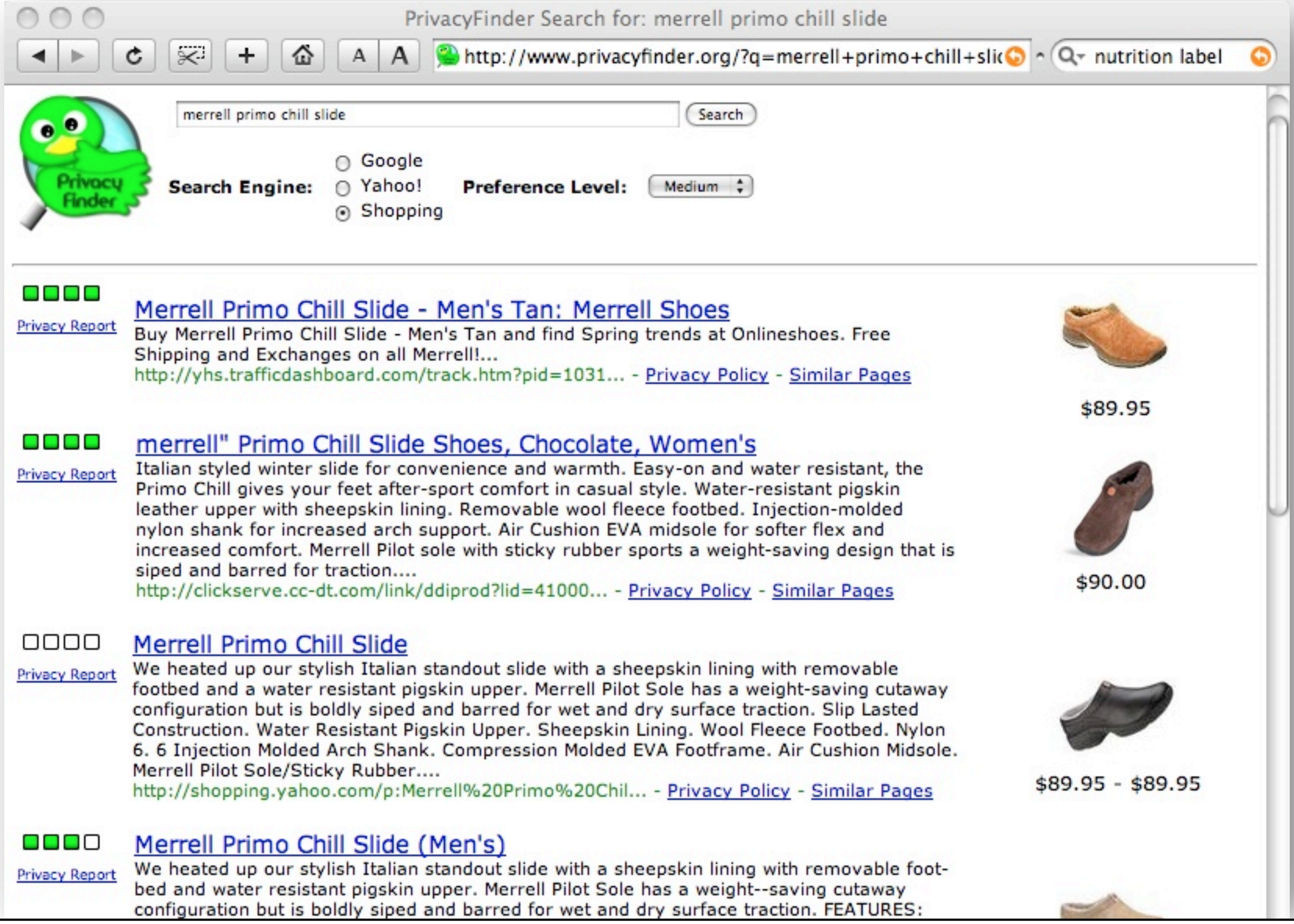
Privacy indicators and willingness to pay for privacy

Will people pay to protect privacy?

- People say they want privacy
- But their behavior suggests otherwise
- What if we make privacy protection easy?



Add privacy meters to search results



PrivacyFinder Search for: merrell primo chill slide

http://www.privacyfinder.org/?q=merrell+primo+chill+slic

nutrition label

merrell primo chill slide [Search]

Search Engine: ○ Google ○ Yahoo! ● Shopping **Preference Level:** Medium

🟩🟩🟩🟩 Privacy Report

Merrell Primo Chill Slide - Men's Tan: Merrell Shoes

Buy Merrell Primo Chill Slide - Men's Tan and find Spring trends at Onlineshoes. Free Shipping and Exchanges on all Merrell!...

http://yhs.trafficdashboard.com/track.htm?pid=1031... - Privacy Policy - Similar Pages

$89.95

🟩🟩🟩🟩 Privacy Report

merrell" Primo Chill Slide Shoes, Chocolate, Women's

Italian styled winter slide for convenience and warmth. Easy-on and water resistant, the Primo Chill gives your feet after-sport comfort in casual style. Water-resistant pigskin leather upper with sheepskin lining. Removable wool fleece footbed. Injection-molded nylon shank for increased arch support. Air Cushion EVA midsole for softer flex and increased comfort. Merrell Pilot sole with sticky rubber sports a weight-saving design that is siped and barred for traction....

http://clickserve.cc-dt.com/link/ddiprod?lid=41000... - Privacy Policy - Similar Pages

$90.00

□□□□ Privacy Report

Merrell Primo Chill Slide

We heated up our stylish Italian standout slide with a sheepskin lining with removable footbed and a water resistant pigskin upper. Merrell Pilot Sole has a weight-saving cutaway configuration but is boldly siped and barred for wet and dry surface traction. Slip Lasted Construction. Water Resistant Pigskin Upper. Sheepskin Lining. Wool Fleece Footbed. Nylon 6. 6 Injection Molded Arch Shank. Compression Molded EVA Footframe. Air Cushion Midsole. Merrell Pilot Sole/Sticky Rubber....

http://shopping.yahoo.com/p:Merrell%20Primo%20Chil... - Privacy Policy - Similar Pages

$89.95 - $89.95

🟩🟩🟩□ Privacy Report

Merrell Primo Chill Slide (Men's)

We heated up our stylish Italian standout slide with a sheepskin lining with removable foot-bed and water resistant pigskin upper. Merrell Pilot Sole has a weight--saving cutaway configuration but is boldly siped and barred for wet and dry surface traction. FEATURES:

How can we test whether privacy meters change behavior?

Hypothetical task

- Search for product
- Which site would you buy from?

Hypothetical

No real privacy tradeoff

Real task

- Search for product
- Make purchase with your credit card

Expensive

Difficult to control

2005 – 2009 Privacy Finder studies

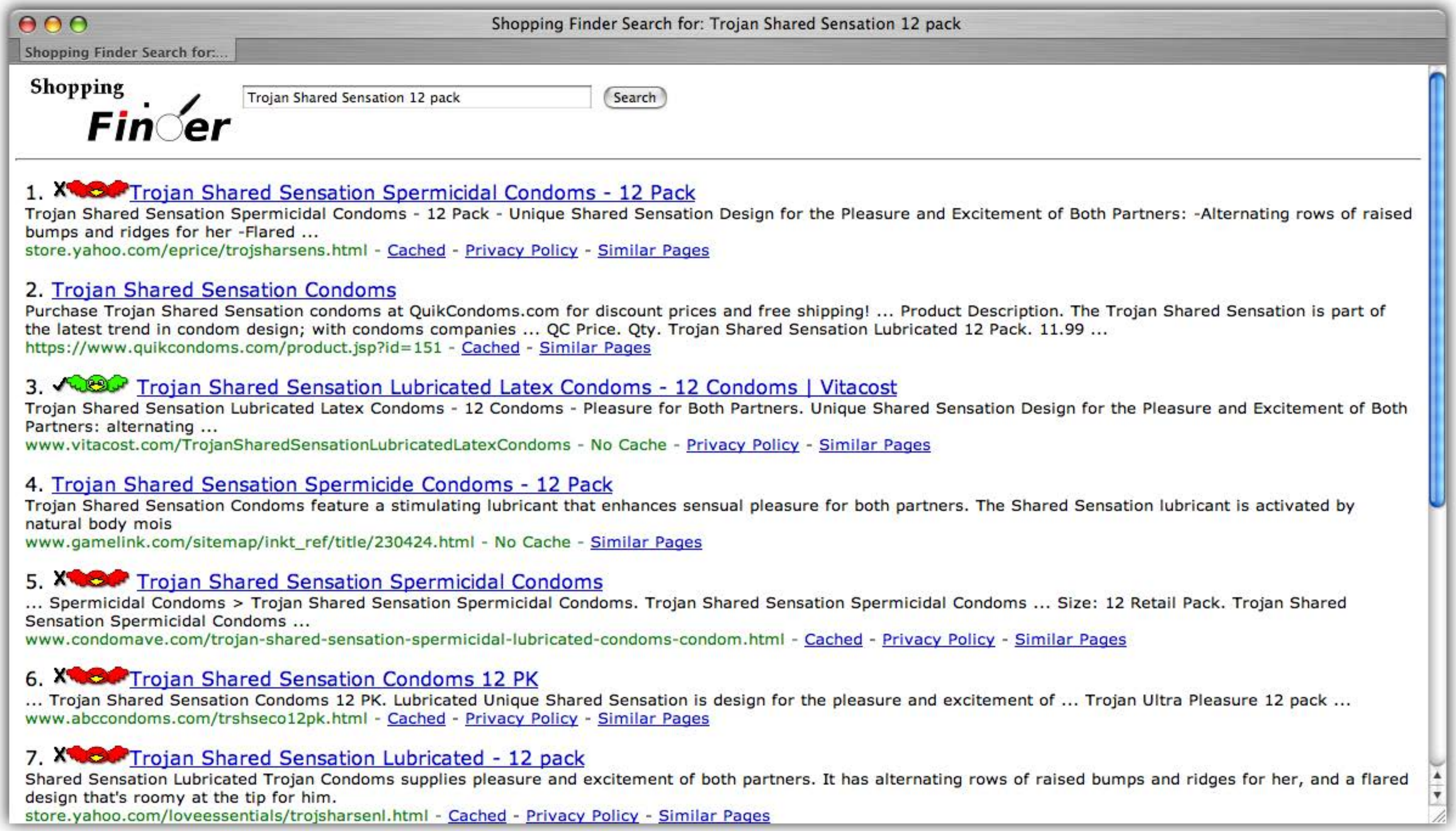
Janice Tsai, Serge Egelman, Rachel Shipman, Kok-Chie Daniel Pu,
Lorrie Cranor, and Alessandro Acquisti
Privacy Symbols
Symbols of privacy and trust
Privacy policies, web seals, trust marks
Convey information and assurance of validity, trustworthiness, and authority
Can be difficult to understand
Privacy Finder Search Icons
Privacy-enhanced search engine displays P3P-based privacy reports with a privacy icon
Based on user tests, the privacy icons were altered to increase usability
Shopping search engine implemented new privacy icons, prices, and pictures
Old Icons
New Icons
Meaning
Privacy Finder Icons
Results
Positive indicators, even ambiguous, influence trust and decision-making
Price was the largest factor when making purchase decisions
Privacy Finder provided useful information to people interested in learning about privacy practices
People who clicked on the Privacy ... were more likely to read the full privacy policy
Future Work
Conduct a field study with AOL to examine the impact of the privacy-enhanced search engine on a larger, more diverse population using it for their normal web activities
AOL will implement our P3P-enabled engine and roll it out to 100,000 ... two weeks
Larger controlled lab studies
Why Johnny Still Can't Encrypt
A pilot usability evaluation of PGP 9.0
Goals
Methodology
Major Findings
Design

Power strips, prophylactics, and privacy, oh my!

- “Online shopping study” in our lab
- 24 students paid $10 plus reimbursement for purchases made with their own credit cards
- Used “Shopping Finder” search engine
  - Control condition: no privacy icons
  - Experimental condition: privacy icons

J. Gideon, S. Egelman, L. Cranor, and A. Acquisti.
Power Strips, Prophylactics, and Privacy, Oh My! SOUPS 2006.

UNIVERSAL
Surge Suppressor
Protectores contra sobretensión
Limiteur de surtension
71644
AMERICA'S #1 CONDOM
TRUSTED FOR OVER 80 YEARS
TROJAN
SHARED SENSATION
SPERMICIDAL LUBRICANT
PLEASURE FOR BOTH PARTNERS
12 PREMIUM LATEX CONDOMS
LUBRICATED



Shopping Finder Search for: Trojan Shared Sensation 12 pack
Shopping Finder Search for:...
Shopping Finder
Trojan Shared Sensation 12 pack
Search

1. ✗ Trojan Shared Sensation Spermicidal Condoms - 12 Pack
Trojan Shared Sensation Spermicidal Condoms - 12 Pack - Unique Shared Sensation Design for the Pleasure and Excitement of Both Partners: -Alternating rows of raised bumps and ridges for her -Flared ...
store.yahoo.com/eprice/trojsharsens.html - Cached - Privacy Policy - Similar Pages

2. Trojan Shared Sensation Condoms
Purchase Trojan Shared Sensation condoms at QuikCondoms.com for discount prices and free shipping! ... Product Description. The Trojan Shared Sensation is part of the latest trend in condom design; with condoms companies ... QC Price. Qty. Trojan Shared Sensation Lubricated 12 Pack. 11.99 ...
https://www.quikcondoms.com/product.jsp?id=151 - Cached - Similar Pages

3. ✓ Trojan Shared Sensation Lubricated Latex Condoms - 12 Condoms | Vitacost
Trojan Shared Sensation Lubricated Latex Condoms - 12 Condoms - Pleasure for Both Partners. Unique Shared Sensation Design for the Pleasure and Excitement of Both Partners: alternating ...
www.vitacost.com/TrojanSharedSensationLubricatedLatexCondoms - No Cache - Privacy Policy - Similar Pages

4. Trojan Shared Sensation Spermicide Condoms - 12 Pack
Trojan Shared Sensation Condoms feature a stimulating lubricant that enhances sensual pleasure for both partners. The Shared Sensation lubricant is activated by natural body mois
www.gamelink.com/sitemap/inkt_ref/title/230424.html - No Cache - Similar Pages

5. ✗ Trojan Shared Sensation Spermicidal Condoms
... Spermicidal Condoms > Trojan Shared Sensation Spermicidal Condoms. Trojan Shared Sensation Spermicidal Condoms ... Size: 12 Retail Pack. Trojan Shared Sensation Spermicidal Condoms ...
www.condomave.com/trojan-shared-sensation-spermicidal-lubricated-condoms-condom.html - Cached - Privacy Policy - Similar Pages

6. ✗ Trojan Shared Sensation Condoms 12 PK
... Trojan Shared Sensation Condoms 12 PK. Lubricated Unique Shared Sensation is design for the pleasure and excitement of ... Trojan Ultra Pleasure 12 pack ...
www.abccondoms.com/trshseco12pk.html - Cached - Privacy Policy - Similar Pages

7. ✗ Trojan Shared Sensation Lubricated - 12 pack
Shared Sensation Lubricated Trojan Condoms supplies pleasure and excitement of both partners. It has alternating rows of raised bumps and ridges for her, and a flared design that's roomy at the tip for him.
store.yahoo.com/loveessentials/trojsharsenl.html - Cached - Privacy Policy - Similar Pages

Privacy icons influenced purchases

- **With privacy info:** more people purchased from sites with better privacy
- Larger effect for privacy-sensitive purchase

But study had significant limitations

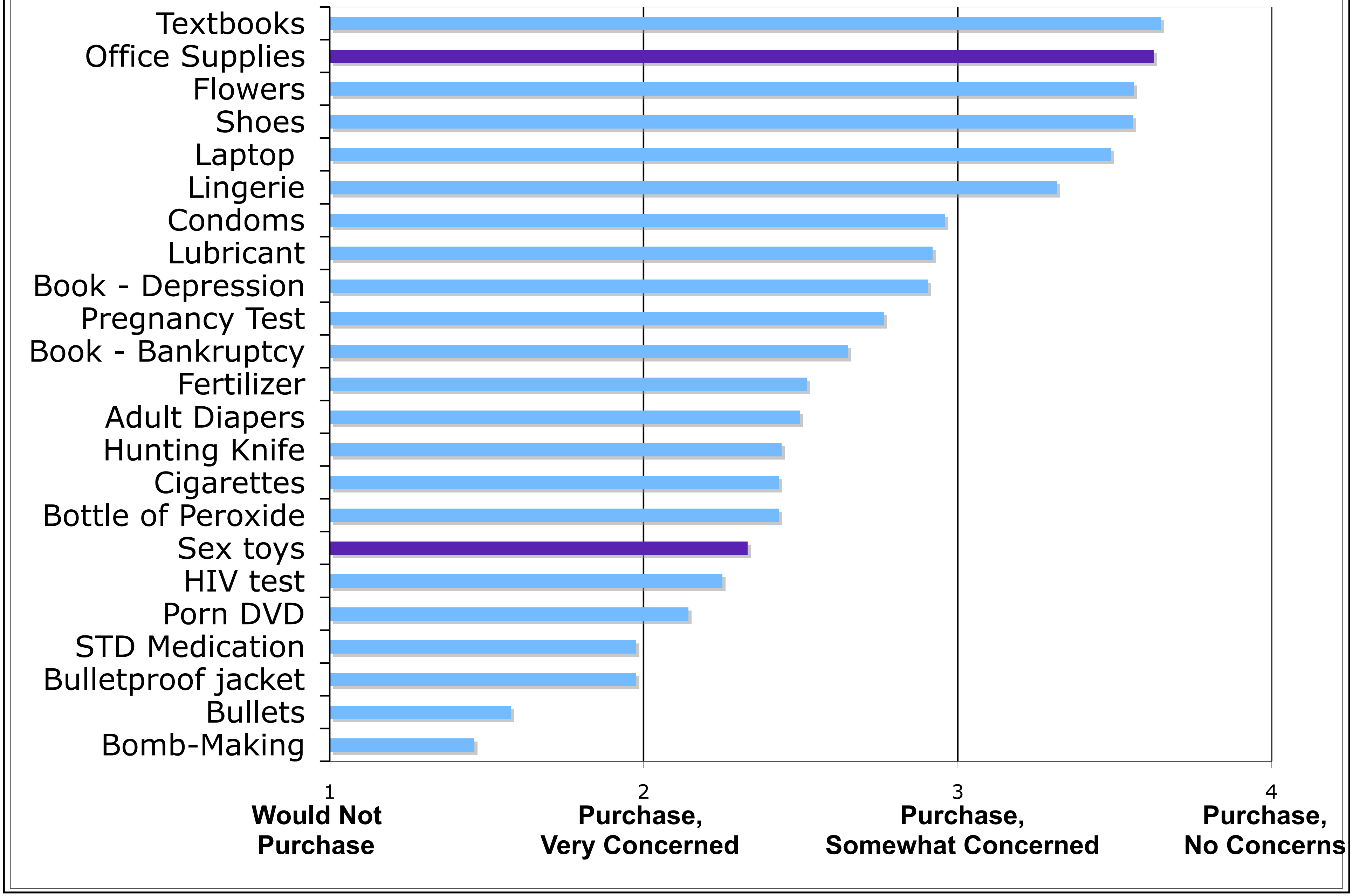
- Participants were all students
- Reimbursement did not incentivize saving
- Price/privacy tradeoff not obvious
- Maybe people just like pretty indicators
- Privacy-sensitive item not sensitive enough

So we tried again

- 72 Pittsburgh residents
- Price/privacy tradeoff
- Fixed payment, keep the change
- New icons, new products, new conditions

J. Tsai, S. Egelman, L. Cranor, A. Acquisti. **The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study.** ISR 2011.

User Study Items



OFFICIAL PARTNER OF NASCAR
DURACELL
COPPERTOP
Pocket Rocket Jr.
Prepare yourself For Blast Off!
AA 8
DURACELL

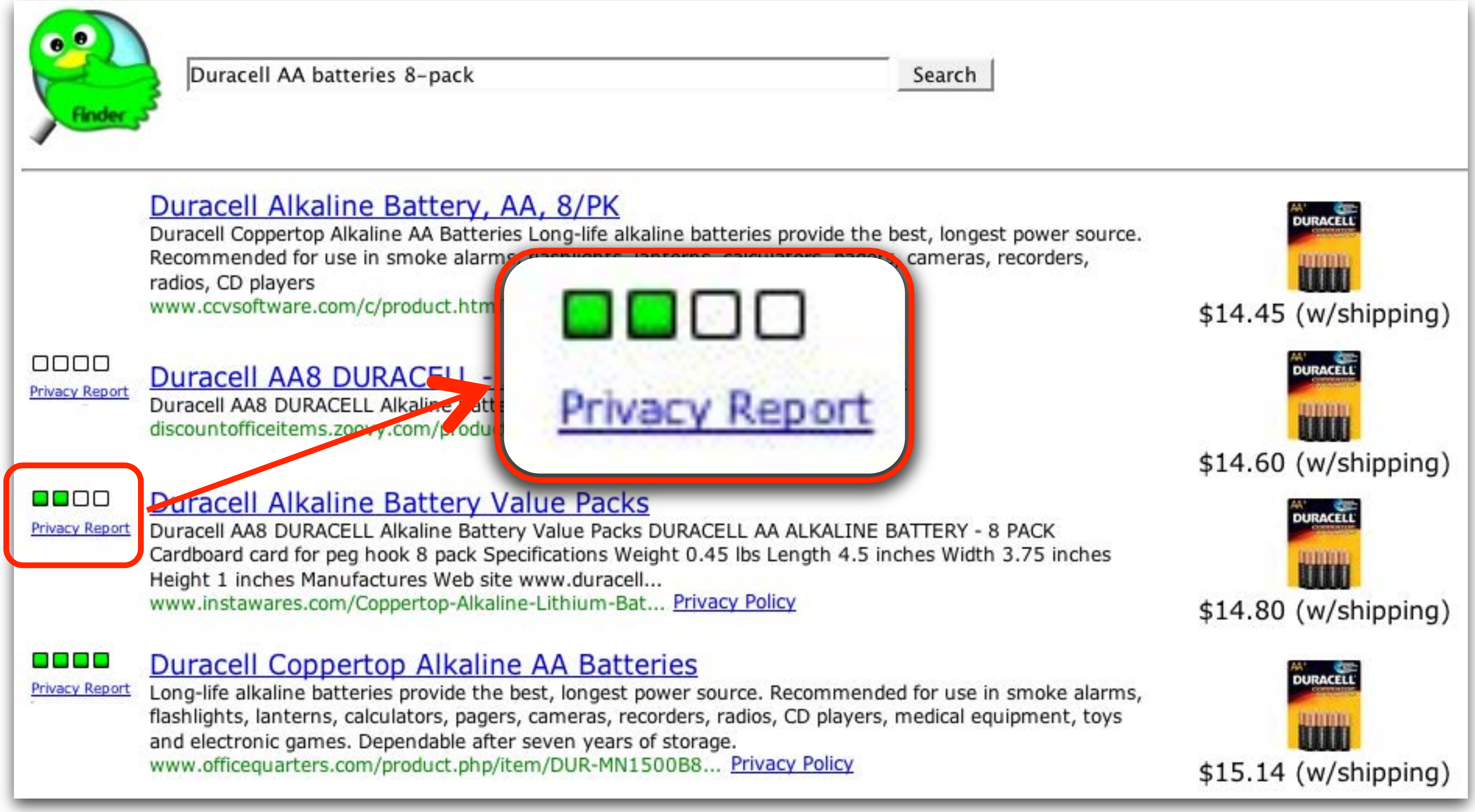
Merchant selection

- Selected 10 merchants for each product
- No well-known merchants
- Controlled first four search results: more expensive → better privacy

Merchant	Privacy score	Price w/ shipping
ccvsoftware.com	?	$14.45
discountofficeitems.zoovy.com	0/4	$14.60
instawares.com	2/4	$14.80
officequarters.com	4/4	$15.14

$.69 privacy premium

Privacy information condition



[Duracell Alkaline Battery, AA, 8/PK]
Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source. Recommended for use in smoke alarms cameras, recorders, radios, CD players
www.ccvsoftware.com/c/product.htm
$14.45 (w/shipping)

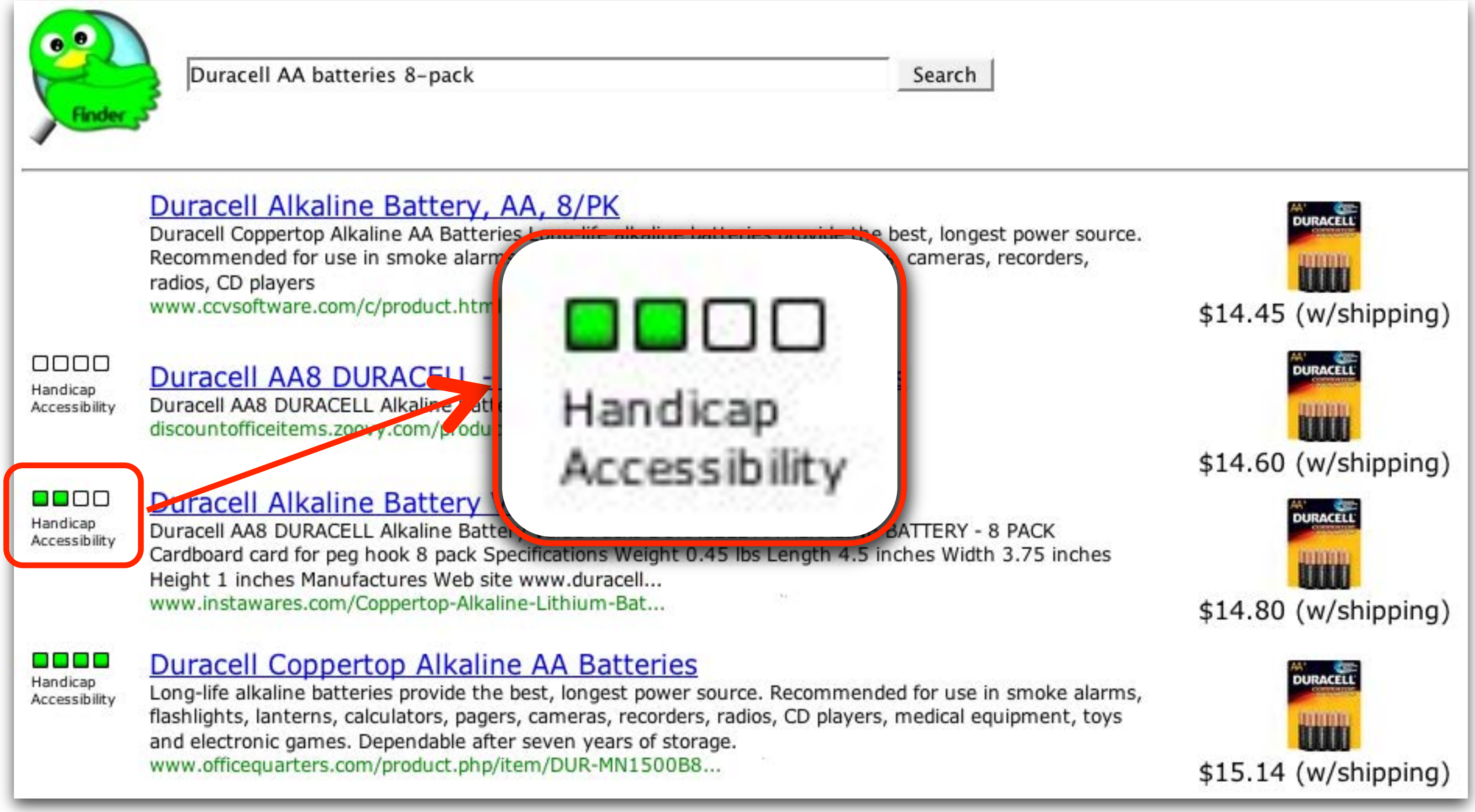
□□□□
Privacy Report
[Duracell AA8 DURACELL -]
Duracell AA8 DURACELL Alkaline
discountofficeitems.zoovy.com/produ
$14.60 (w/shipping)

🟩🟩□□
Privacy Report

🟩🟩□□
Privacy Report
[Duracell Alkaline Battery Value Packs]
Duracell AA8 DURACELL Alkaline Battery Value Packs DURACELL AA ALKALINE BATTERY - 8 PACK Cardboard card for peg hook 8 pack Specifications Weight 0.45 lbs Length 4.5 inches Width 3.75 inches Height 1 inches Manufactures Web site www.duracell...
www.instawares.com/Coppertop-Alkaline-Lithium-Bat... Privacy Policy
$14.80 (w/shipping)

🟩🟩🟩🟩
Privacy Report
[Duracell Coppertop Alkaline AA Batteries]
Long-life alkaline batteries provide the best, longest power source. Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players, medical equipment, toys and electronic games. Dependable after seven years of storage.
www.officequarters.com/product.php/item/DUR-MN1500B8... Privacy Policy
$15.14 (w/shipping)

Irrelevant information condition



Duracell AA batteries 8-pack Search

Duracell Alkaline Battery, AA, 8/PK
Duracell Coppertop Alkaline AA Batteries ... best, longest power source. Recommended for use in smoke alarm... cameras, recorders, radios, CD players
www.ccvsoftware.com/c/product.htm...
$14.45 (w/shipping)

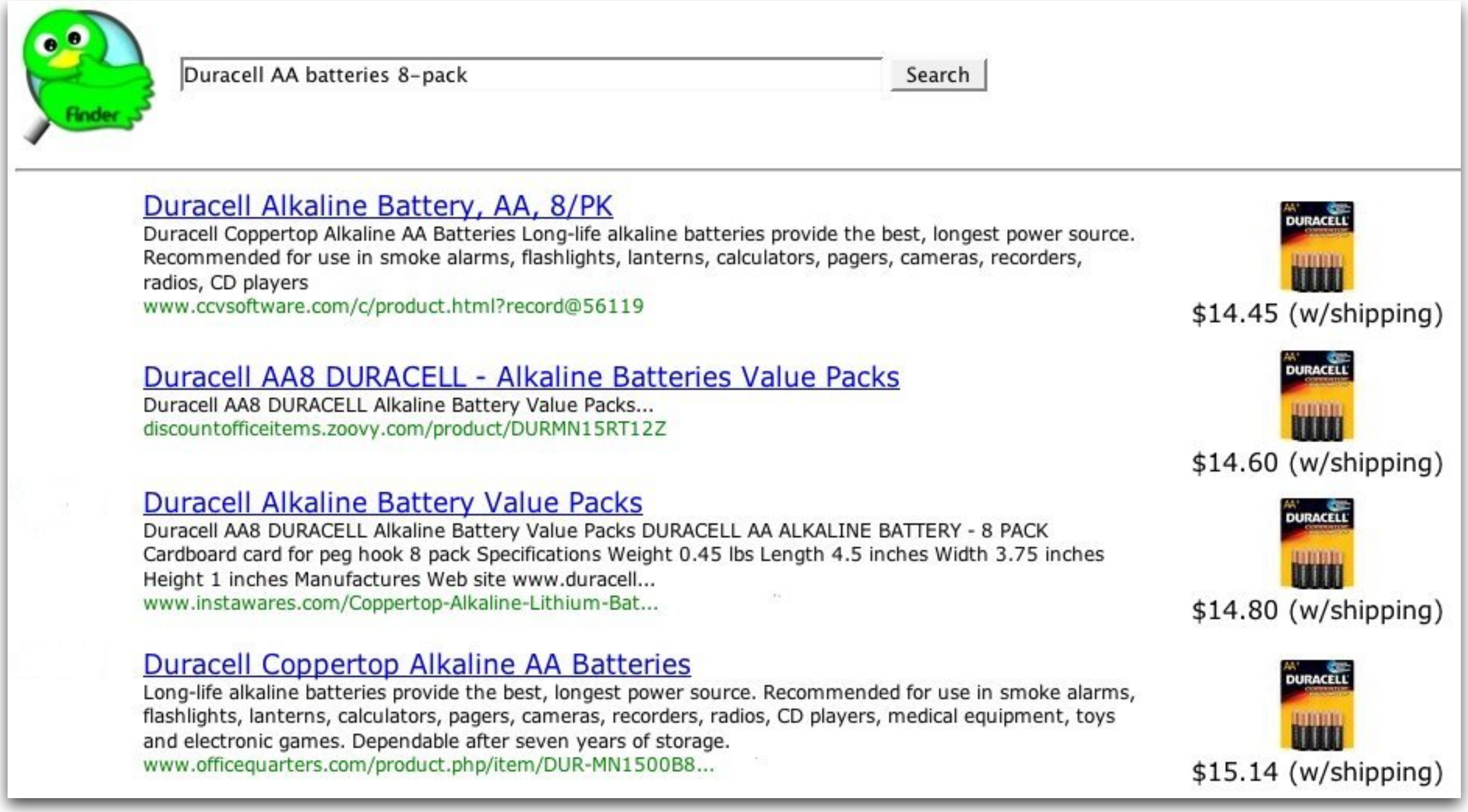
□□□□ Handicap Accessibility
Duracell AA8 DURACELL ...
Duracell AA8 DURACELL Alkaline ...
discountofficeitems.zoovy.com/produ...
$14.60 (w/shipping)

🟩🟩□□ Handicap Accessibility
Duracell Alkaline Battery ...
Duracell AA8 DURACELL Alkaline Batte... BATTERY - 8 PACK Cardboard card for peg hook 8 pack Specifications Weight 0.45 lbs Length 4.5 inches Width 3.75 inches Height 1 inches Manufactures Web site www.duracell...
www.instawares.com/Coppertop-Alkaline-Lithium-Bat...
$14.80 (w/shipping)

🟩🟩🟩🟩 Handicap Accessibility
Duracell Coppertop Alkaline AA Batteries
Long-life alkaline batteries provide the best, longest power source. Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players, medical equipment, toys and electronic games. Dependable after seven years of storage.
www.officequarters.com/product.php/item/DUR-MN1500B8...
$15.14 (w/shipping)

🟩🟩□□ Handicap Accessibility

No information condition



Duracell AA batteries 8-pack

[Duracell Alkaline Battery, AA, 8/PK]

Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source. Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players

www.ccvsoftware.com/c/product.html?record@56119

$14.45 (w/shipping)

[Duracell AA8 DURACELL - Alkaline Batteries Value Packs]

Duracell AA8 DURACELL Alkaline Battery Value Packs...

discountofficeitems.zoovy.com/product/DURMN15RT12Z

$14.60 (w/shipping)

[Duracell Alkaline Battery Value Packs]

Duracell AA8 DURACELL Alkaline Battery Value Packs DURACELL AA ALKALINE BATTERY - 8 PACK Cardboard card for peg hook 8 pack Specifications Weight 0.45 lbs Length 4.5 inches Width 3.75 inches Height 1 inches Manufactures Web site www.duracell...

www.instawares.com/Coppertop-Alkaline-Lithium-Bat...

$14.80 (w/shipping)

[Duracell Coppertop Alkaline AA Batteries]

Long-life alkaline batteries provide the best, longest power source. Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players, medical equipment, toys and electronic games. Dependable after seven years of storage.

www.officequarters.com/product.php/item/DUR-MN1500B8...

$15.14 (w/shipping)

Privacy icons influenced purchases

- **No privacy info:** most people purchased where price was lowest
- **With privacy info:** more people purchased from expensive sites with better privacy
- No clear difference between products
  - Because we didn't control **privacy premium**?

Follow-up study with cooperation of vendors to control privacy premium

- Contacted 46 battery and sex toy vendors
- Convinced 8 to adjust prices for our study
  - Asked one to lower prices and promised to pay the difference
  - Sent $140 check to The Dirty Bunny for "research project assistance"

Sure enough…

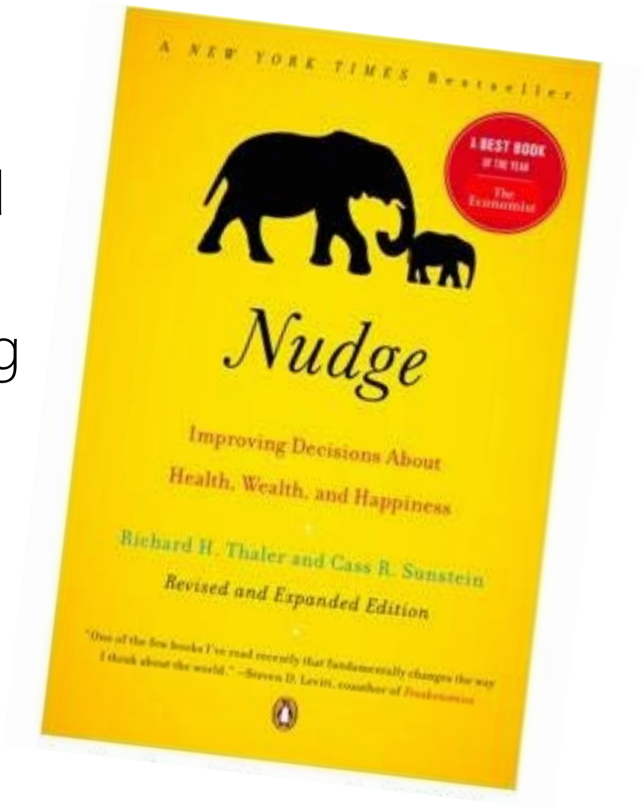
Privacy-sensitive nature of product impacts willingness to pay a premium for privacy

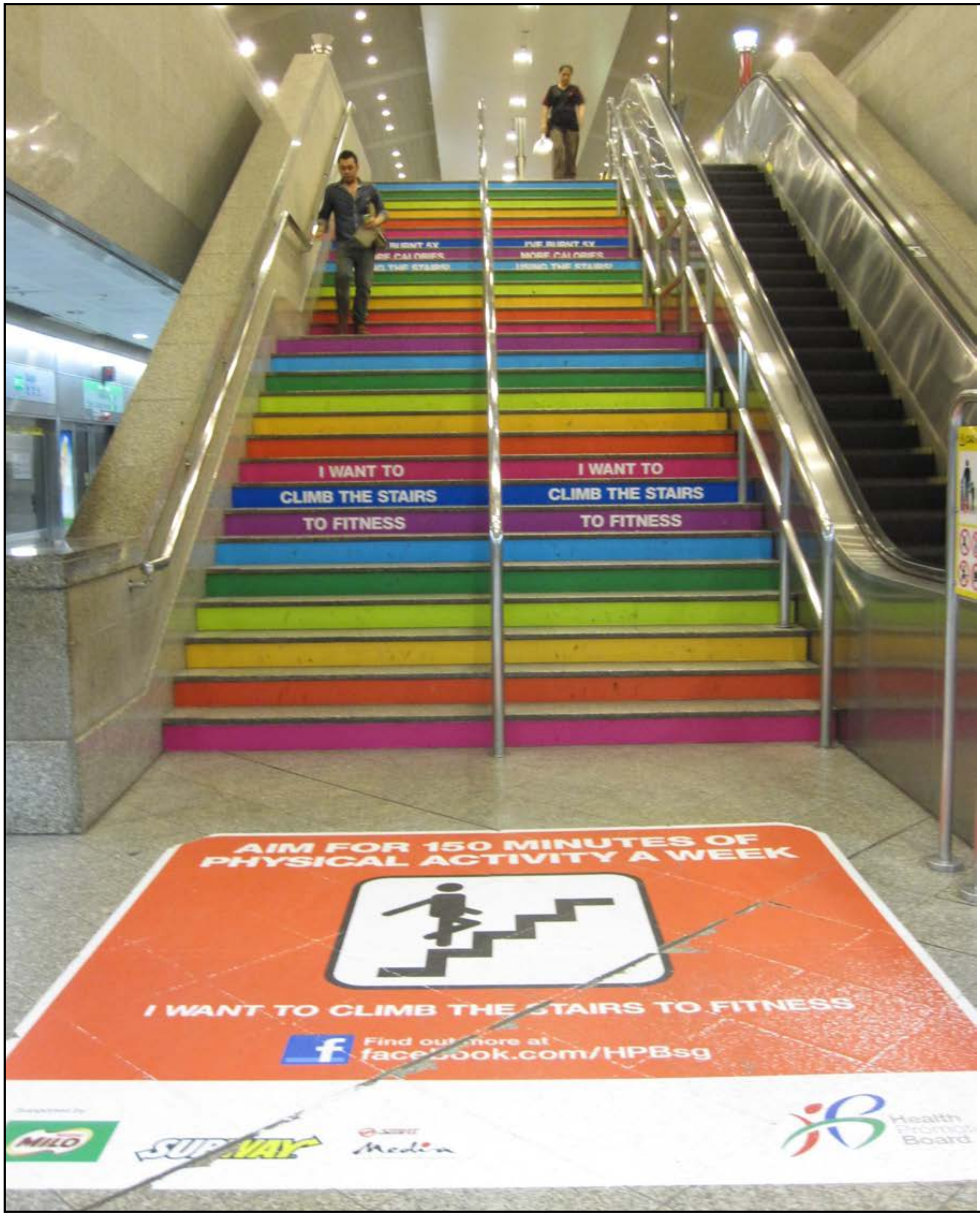
S. Egelman, J. Tsai, L. Cranor, A. Acquisti. **Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators.** CHI 2009.

Designing and evaluating privacy nudges

Nudge project

- Goal
  - Anticipate and exploit cognitive and behavioral biases that hamper privacy and security decision making
  - Don't limit freedom
- Approach
  - Understand biases
  - Understand problems (regrets)
  - Prototype and evaluate nudges


A NEW YORK TIMES Bestseller
1 BEST BOOK OF THE YEAR
The Economist
Nudge
Improving Decisions About
Health, Wealth, and Happiness
Richard H. Thaler and Cass R. Sunstein
Revised and Expanded Edition



Bugis MRT station in Singapore

“I want to climb the stairs to fitness”

http://inudgeyou.com/health-nudge-the-stairs-to-fitness/

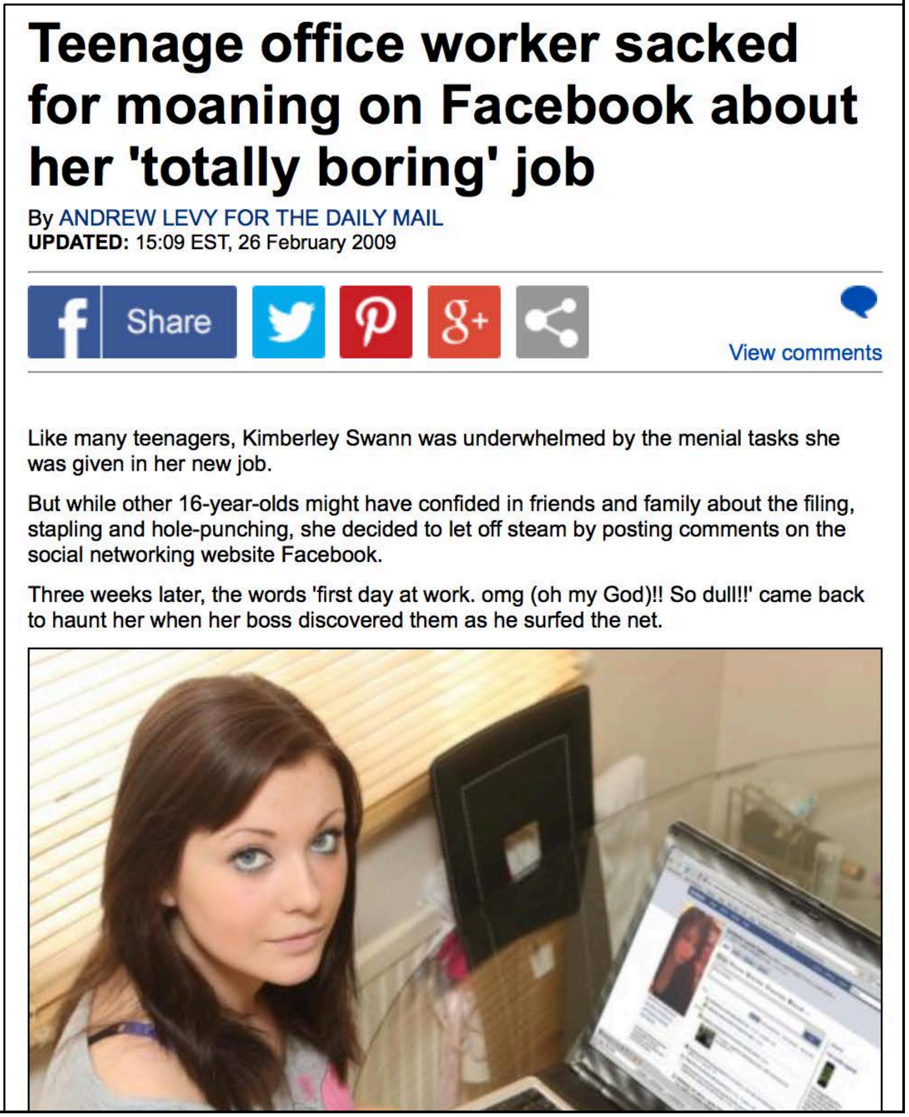
I regretted the minute I pressed share

- Collected hundreds of anecdotes about Facebook regret through interviews, diary studies, surveys
- Aimed to assess needs and understand root causes behind regrets

Y. Wang, S. Komanduri, P.G. Leon, G. Norcie, A. Acquisti, L.F. Cranor. **”I regretted the minute I pressed share”: A Qualitative Study of Regrets on Facebook.** SOUPS 2011.

Underlying cause of regrets

- Not thinking
  - Very excited or angry
- Lack of awareness of how post/tweet will be perceived by others
- Lack of awareness of audience



Teenage office worker sacked for moaning on Facebook about her 'totally boring' job

By ANDREW LEVY FOR THE DAILY MAIL
UPDATED: 15:09 EST, 26 February 2009

Like many teenagers, Kimberley Swann was underwhelmed by the menial tasks she was given in her new job.

But while other 16-year-olds might have confided in friends and family about the filing, stapling and hole-punching, she decided to let off steam by posting comments on the social networking website Facebook.

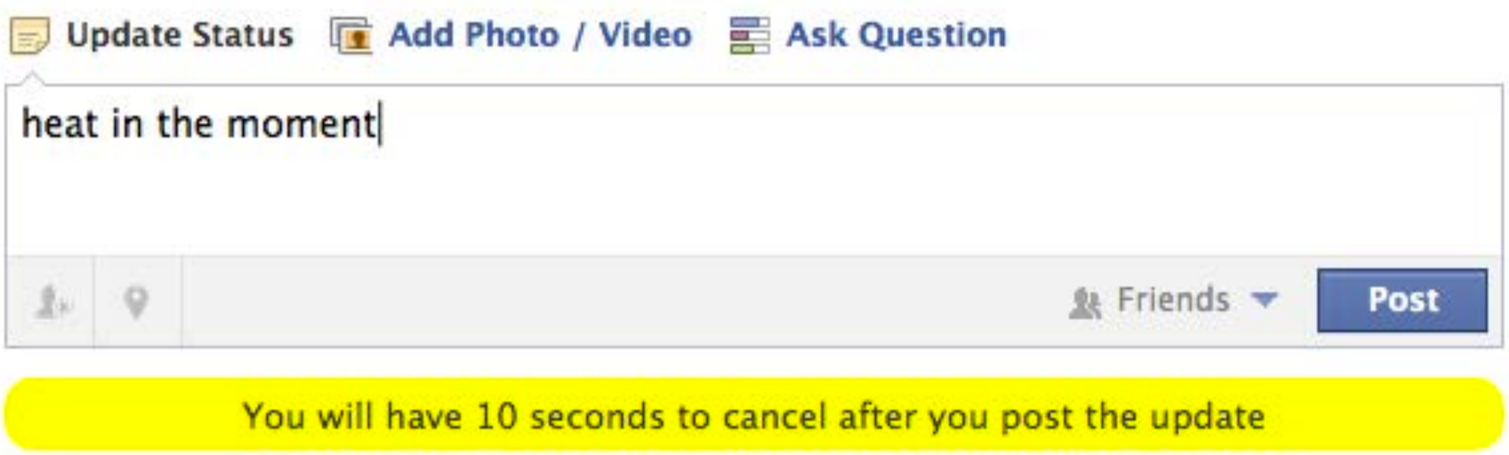
Three weeks later, the words 'first day at work. omg (oh my God)!! So dull!!' came back to haunt her when her boss discovered them as he surfed the net.

Nudge goals based on regrets

- Encourage people to stop and think
- Make people aware of how others might perceive their post
- Remind people of their audience

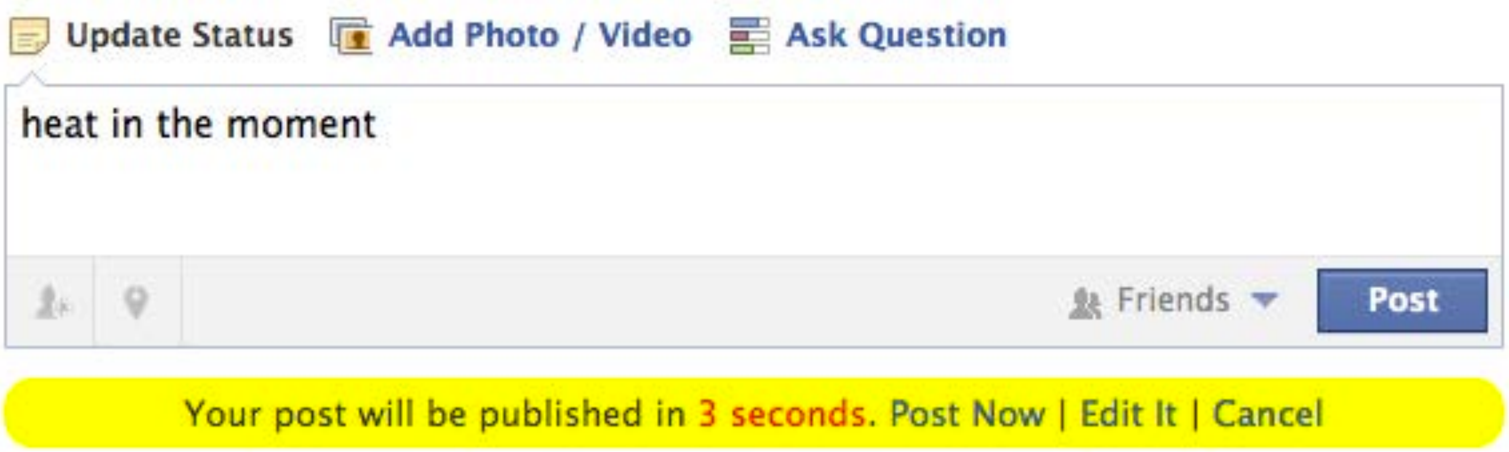
(Former) Representative Anthony Weiner

Stop and think: Timer nudge



heat in the moment

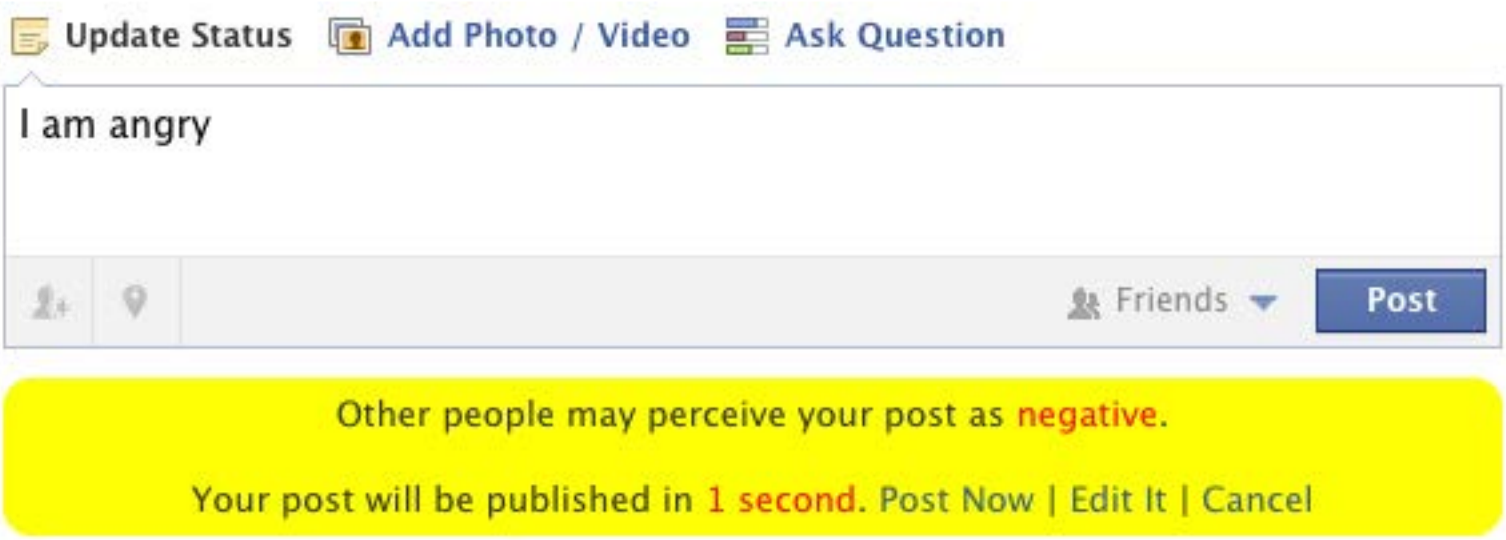
You will have 10 seconds to cancel after you post the update



heat in the moment

Your post will be published in 3 seconds. Post Now | Edit It | Cancel

Post perception: Sentiment nudge

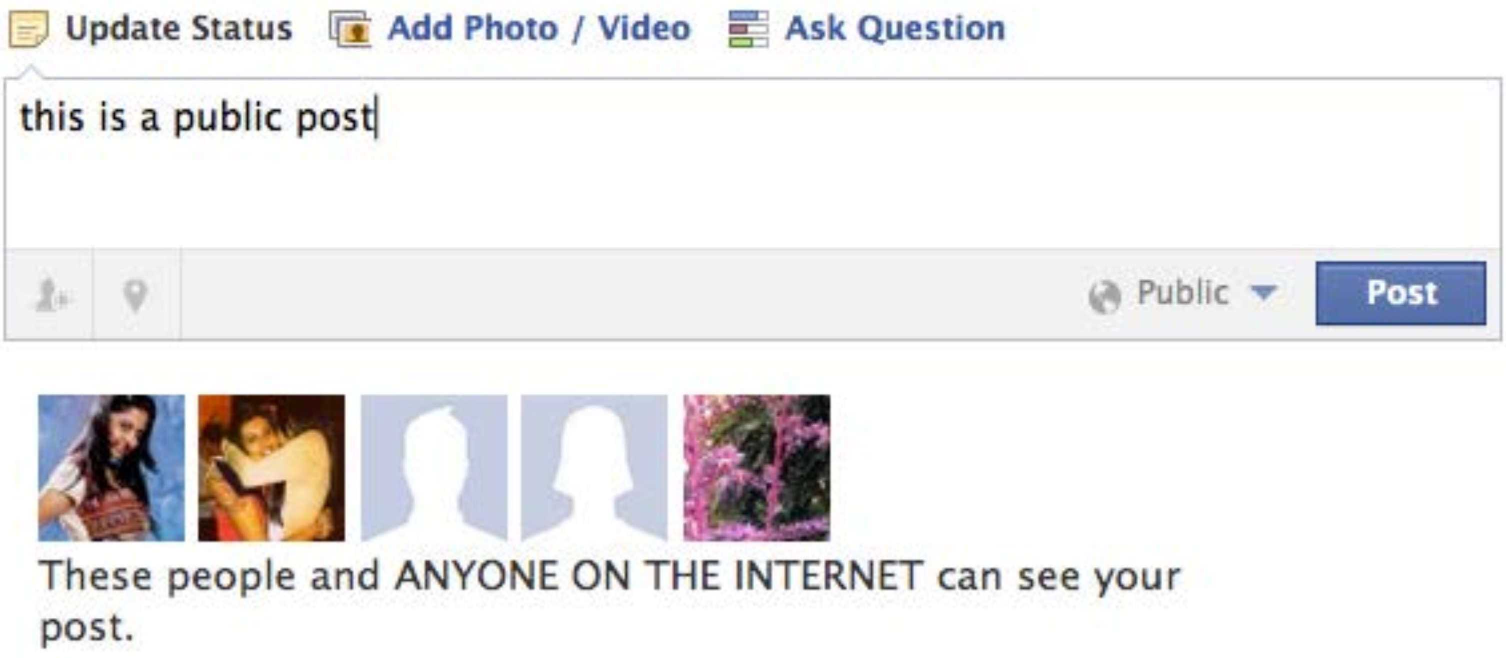


I am angry

Other people may perceive your post as negative.

Your post will be published in 1 second. Post Now | Edit It | Cancel

Audience: Profile picture nudge



this is a public post

These people and ANYONE ON THE INTERNET can see your post.

Are nudges effective?

- 3-week, 21 participant study
- Research questions
  - Do users like nudges and find them useful and usable?
  - How do nudges impact posting behavior and do they prevent regret?
- Post-study survey and interviews

Y. Wang, P. Leon, L. Cranor, A. Acquisti, X. Chen, and K. Scott. **Privacy Nudges for Social Media: An Exploratory Facebook Study.** PSOSM '13.

Studying the effectiveness of nudges was challenging

- Difficult to find participants
- Difficult to determine whether regret was prevented
- Regretful posts are not that frequent
- Facebook changes break nudges and instrumentation

Results

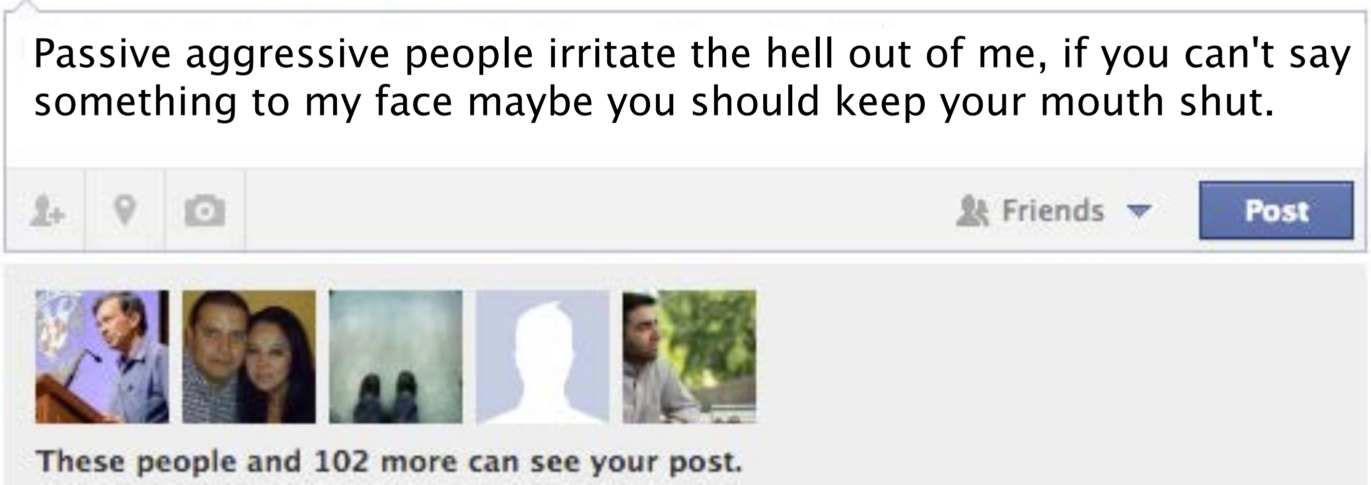
- **Picture nudge** increased awareness of audience
- **Timer nudge** encouraged participants to stop and think, but some annoyed by delay
- **Sentiment nudge** mostly annoyed participants

Another field study

- Developed new audience+timer nudge based on previous study results
- Improved data collection and event logging
- Performed daily tests for Facebook changes
- 6-week study, 28 participants
- Still difficult to make measure significant behavior change with small sample

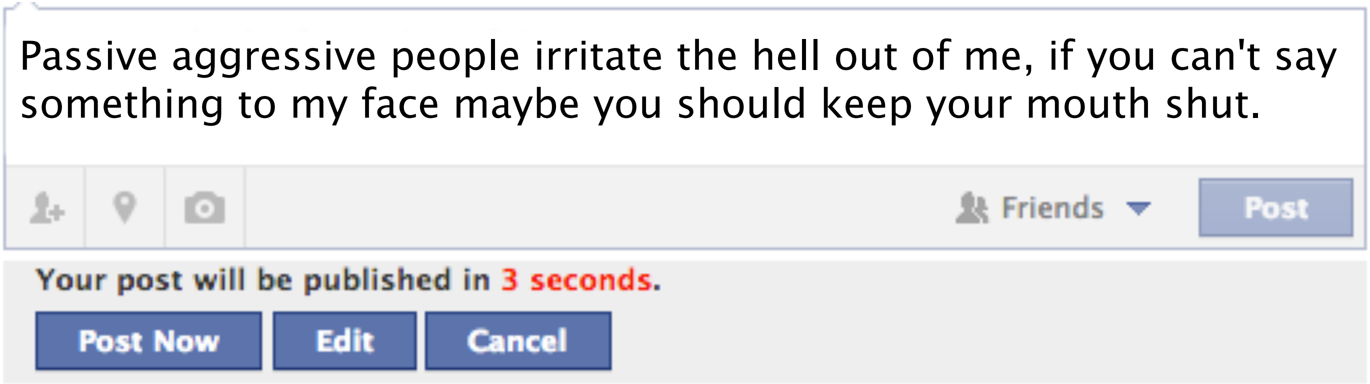
Y. Wang, P. Leon, A. Acquisti, L.F. Cranor, A. Forget, N. Sadeh. **A Field Trial of Privacy Nudges for Facebook.** CHI2014.

Audience+timer nudge



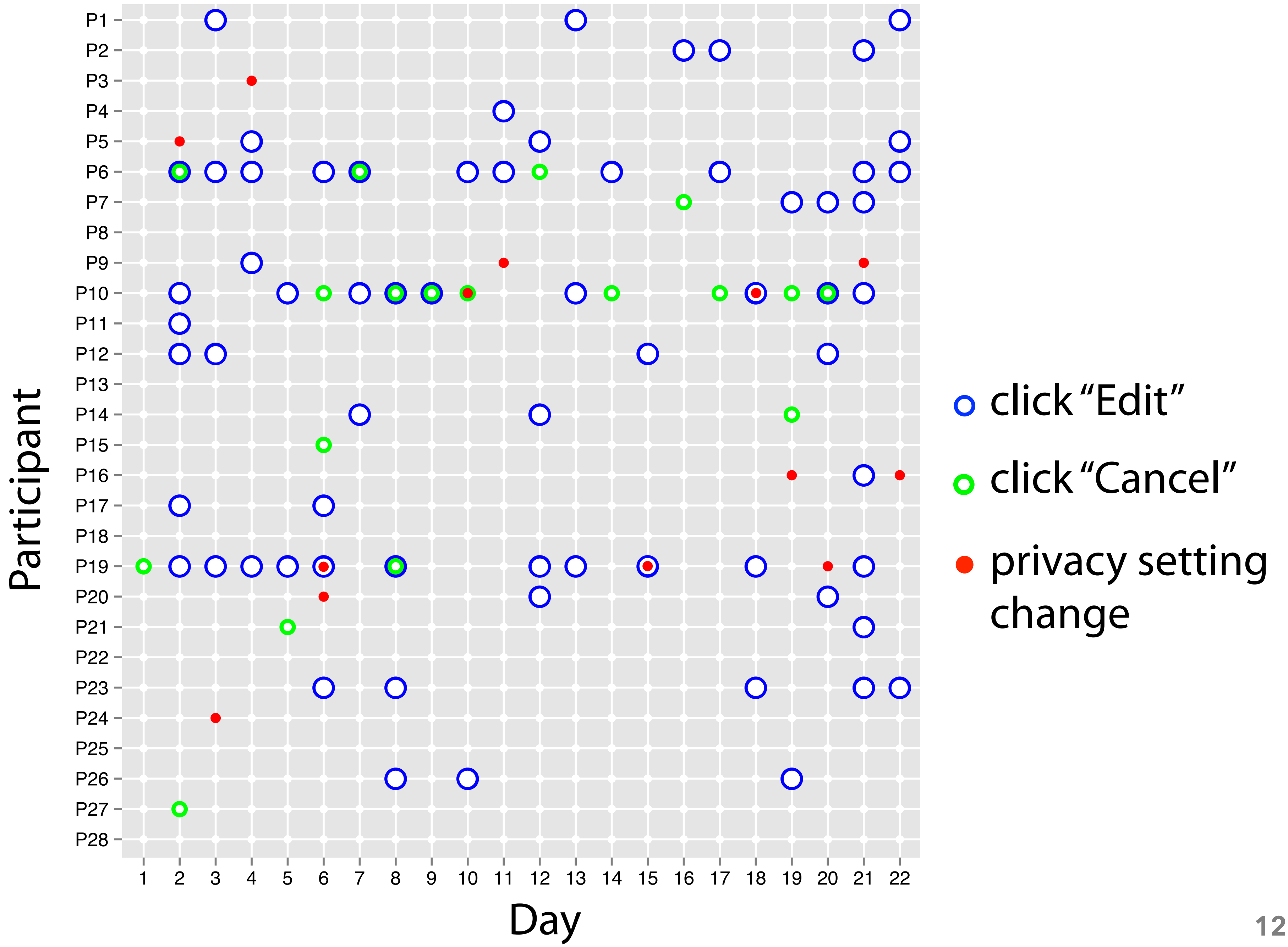
Passive aggressive people irritate the hell out of me, if you can't say something to my face maybe you should keep your mouth shut.

These people and 102 more can see your post.

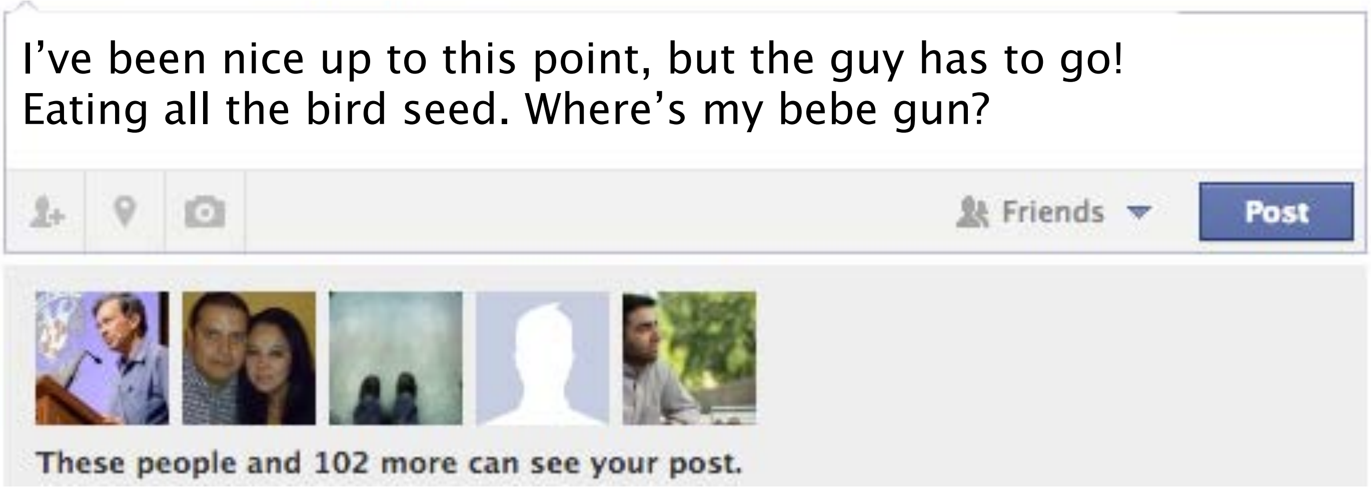


Passive aggressive people irritate the hell out of me, if you can't say something to my face maybe you should keep your mouth shut.

Your post will be published in 3 seconds.


Participant
P1
P2
P3
P4
P5
P6
P7
P8
P9
P10
P11
P12
P13
P14
P15
P16
P17
P18
P19
P20
P21
P22
P23
P24
P25
P26
P27
P28
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
Day
click “Edit”
click “Cancel”
privacy setting change

Improved awareness of audience

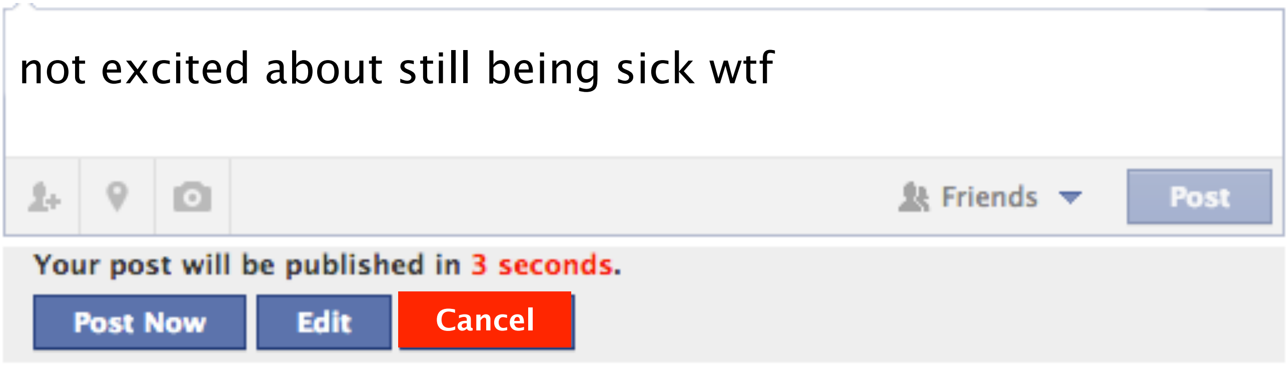


I’ve been nice up to this point, but the guy has to go!
Eating all the bird seed. Where’s my bebe gun?

These people and 102 more can see your post.

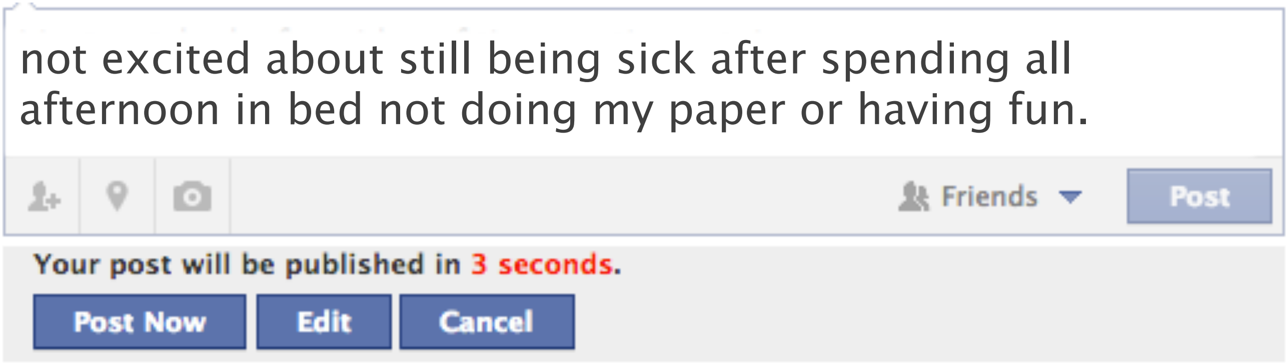
“It was a snide remark and then one of the pictures that popped up was one of the people I work with. It is probably not the best idea”

Encouraged people to stop and think



not excited about still being sick wtf

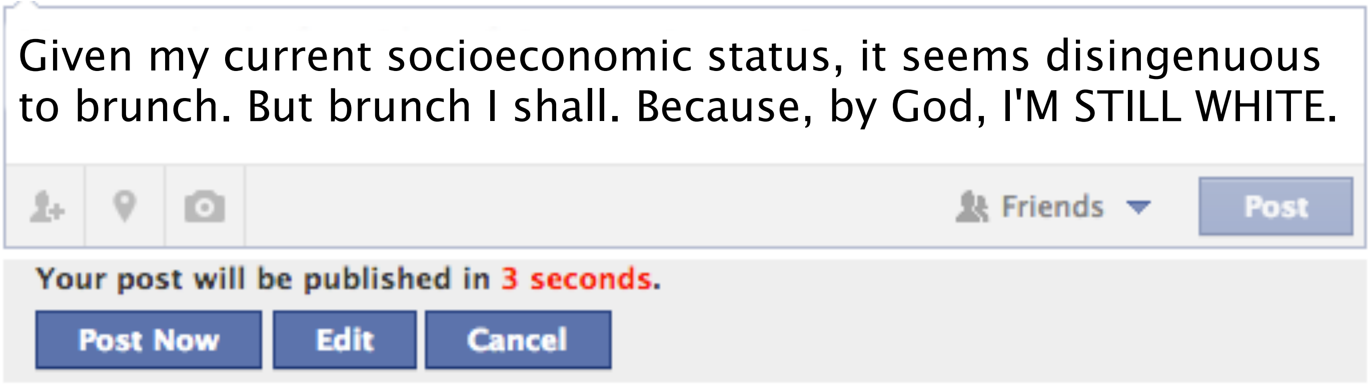
Your post will be published in 3 seconds.



not excited about still being sick after spending all afternoon in bed not doing my paper or having fun.

Your post will be published in 3 seconds.

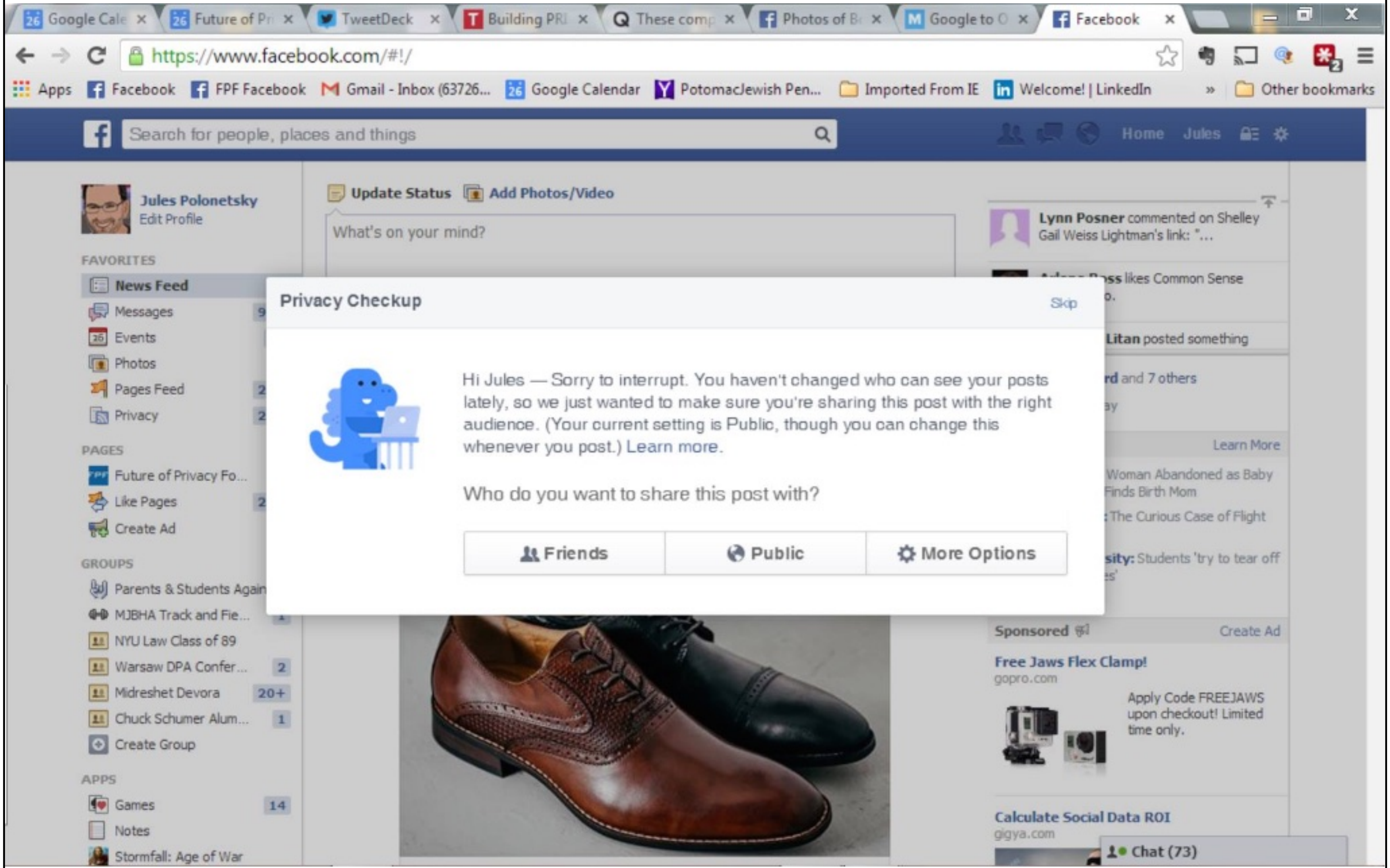
But some people were not fans



Given my current socioeconomic status, it seems disingenuous to brunch. But brunch I shall. Because, by God, I'M STILL WHITE.

Your post will be published in 3 seconds.

“there is no way to protect people from posting embarrassing information online while mad or upset… it’s human nature to be stupid sometimes.”



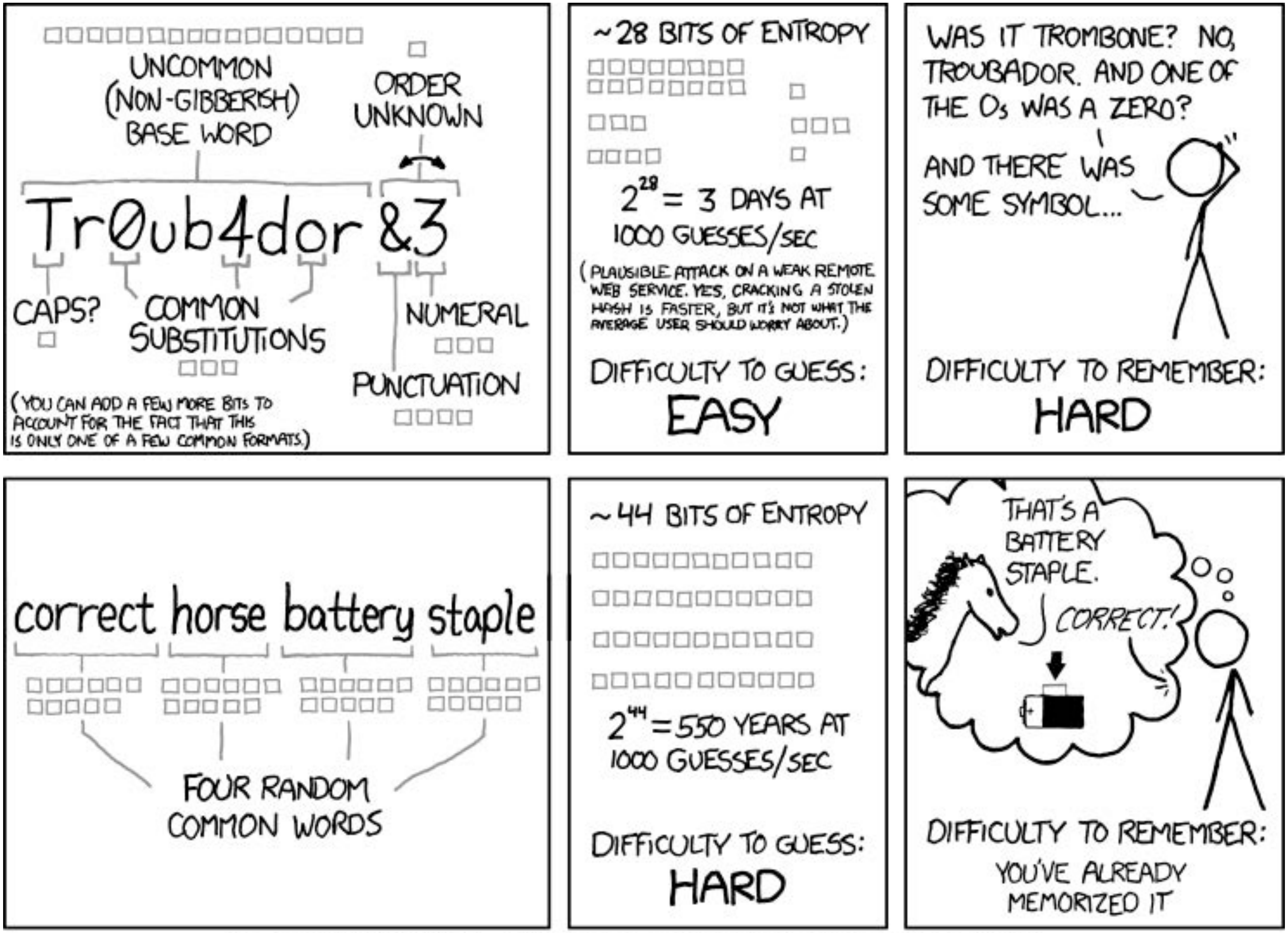
Privacy Checkup

Hi Jules — Sorry to interrupt. You haven't changed who can see your posts lately, so we just wanted to make sure you're sharing this post with the right audience. (Your current setting is Public, though you can change this whenever you post.) Learn more.

Who do you want to share this post with?

Investigating the XKCD passphrase assertion

Should you believe everything you read in XKCD?

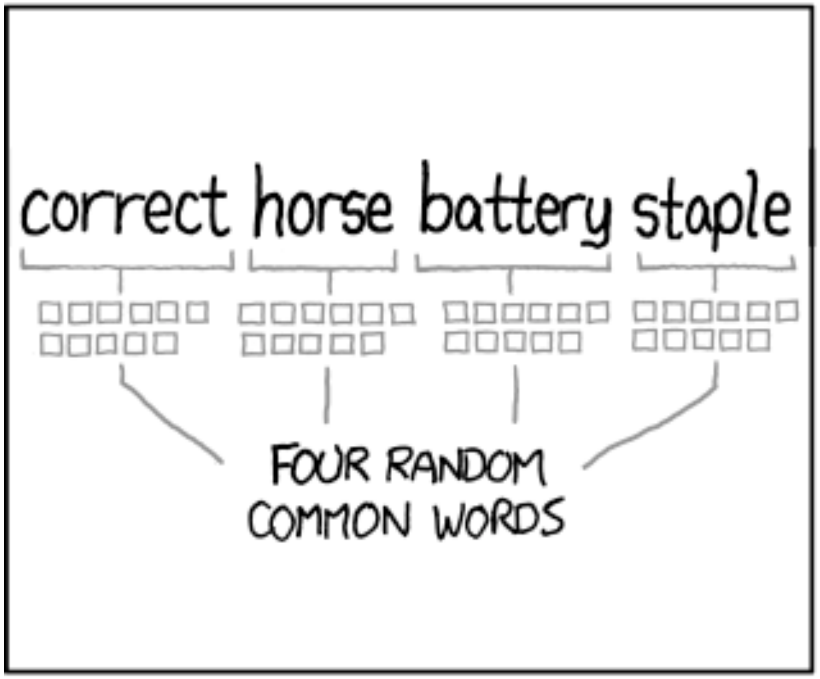

UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

http://xkcd.com/936/

Passphrase study

- Explore usability of system-assigned passphrases
- Compare to system-assigned passwords of similar security
- System-assigned assures random selection



R. Shay, P.G. Kelley, S. Komanduri, M. Mazurek, B. Ur, T. Vidas, L. Bauer, N. Christin, L. Cranor. **Correct horse battery staple: Exploring the usability of system-assigned passphrases.** SOUPS 2012.

Methodology

- 1,476-participant Mturk study
- Participants randomly assigned password or passphrase
- Enter password/phrase, take survey, enter it again
- Emailed to come back two days later
- Enter password/phrase, take another survey

Conditions

- 8 passphrase conditions, 3 password conditions
- Varied factors:
  - Size of dictionary words are selected from
  - Whether order matters
  - Parts of speech
  - Number of words
  - Instructions

4 common words

`try there three come`

`one between high tell`

Noun verb adjective noun

plan builds sure power

end determines red drug

System-assigned passwords

@J#8x

*2LxG

Pronounceable passwords

```
tufritvi

vadasabi
```

Empirical results contradict XKCD

- No clear user favorite
- Passphrases are not easier to remember
- Passphrases slower to enter, more mistakes
- Error correction helps passphrase accuracy
- Pronounceable passwords were faster to enter with fewer mistakes than other passwords or passphrases

Usable security studies FTW

- Complicated
- Challenging
- Interesting
- **Necessary**

Technical program chairs:

- Sunny Consolvo
- Matthew Smith

June 22-24, 2016, Denver

usenix
ASSOCIATION

Conducting Usable Security Studies

IT'S COMPLICATED!

^

necessary

&

CyLab Usable Privacy & Security Laboratory

HTTP://CUPS.CS.CMU.EDU