Usable Security: Warnings

Some HCI background

The old computing is about what computers can do; The new computing is about what people can do.

– Ben Shneiderman

Some key HCI questions

- How to DESIGN a computer system?
- How to EVALUATE a computer system?
- What are the PSYCHOLOGICAL THEORIES governing interaction with technology?
- How does emerging technology create SOCIETAL CHANGE?
- How does technology intersect with ECONOMICS and POLICY?

Security & Privacy

+

Human-Computer Interaction

=

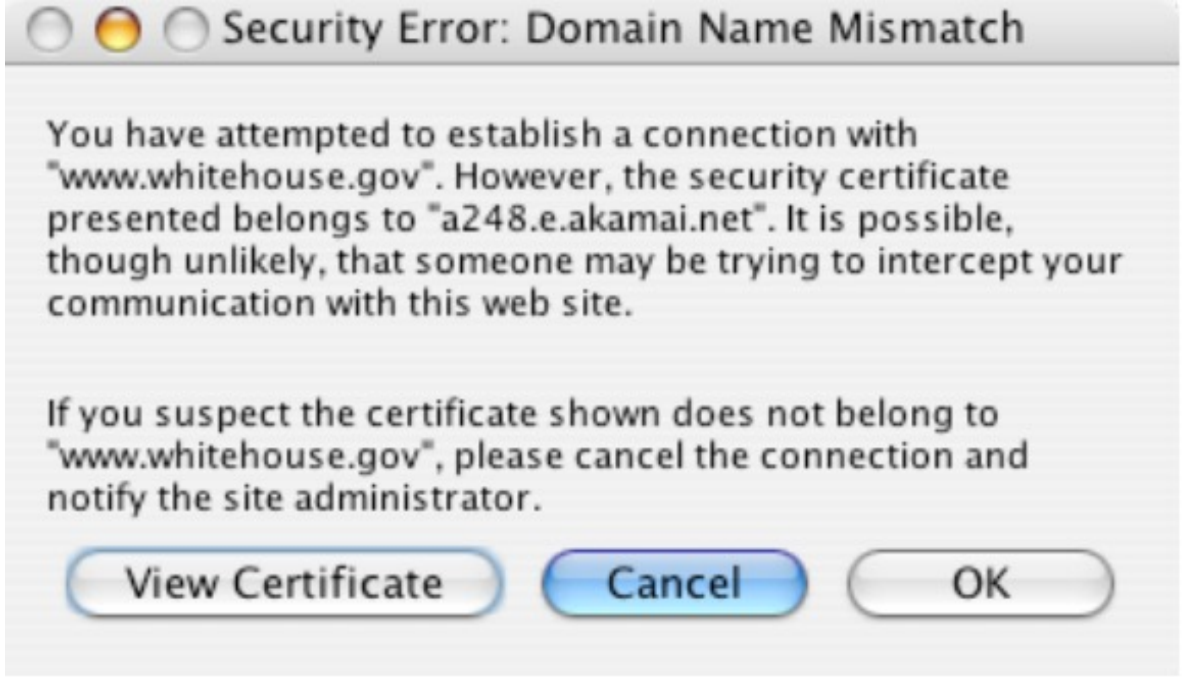
Usable Security and Privacy

Security vs. HCI vs. Usable Security

Security	Usability/HCI	Usable Security
What is the space of possible passwords? How can we make the password space larger to make the password harder to guess? How are the stored passwords secured? Can an **attacker** gain knowledge by observing a user entering her password?	How *difficult* is it for a **user** to create, remember, and enter a password? How long does it take? How hard is it for users to learn the system? Are users *motivated* to put in effort to create good passwords? Is the system *accessible* for users of all abilities?	All the security/privacy and usability HCI questions How do **users** select passwords? How can we help them choose passwords harder for **attackers** to predict? As the password space increases, what are the impacts on usability factors and predictability of human selection?

Security Warnings

Developer’s Perspective

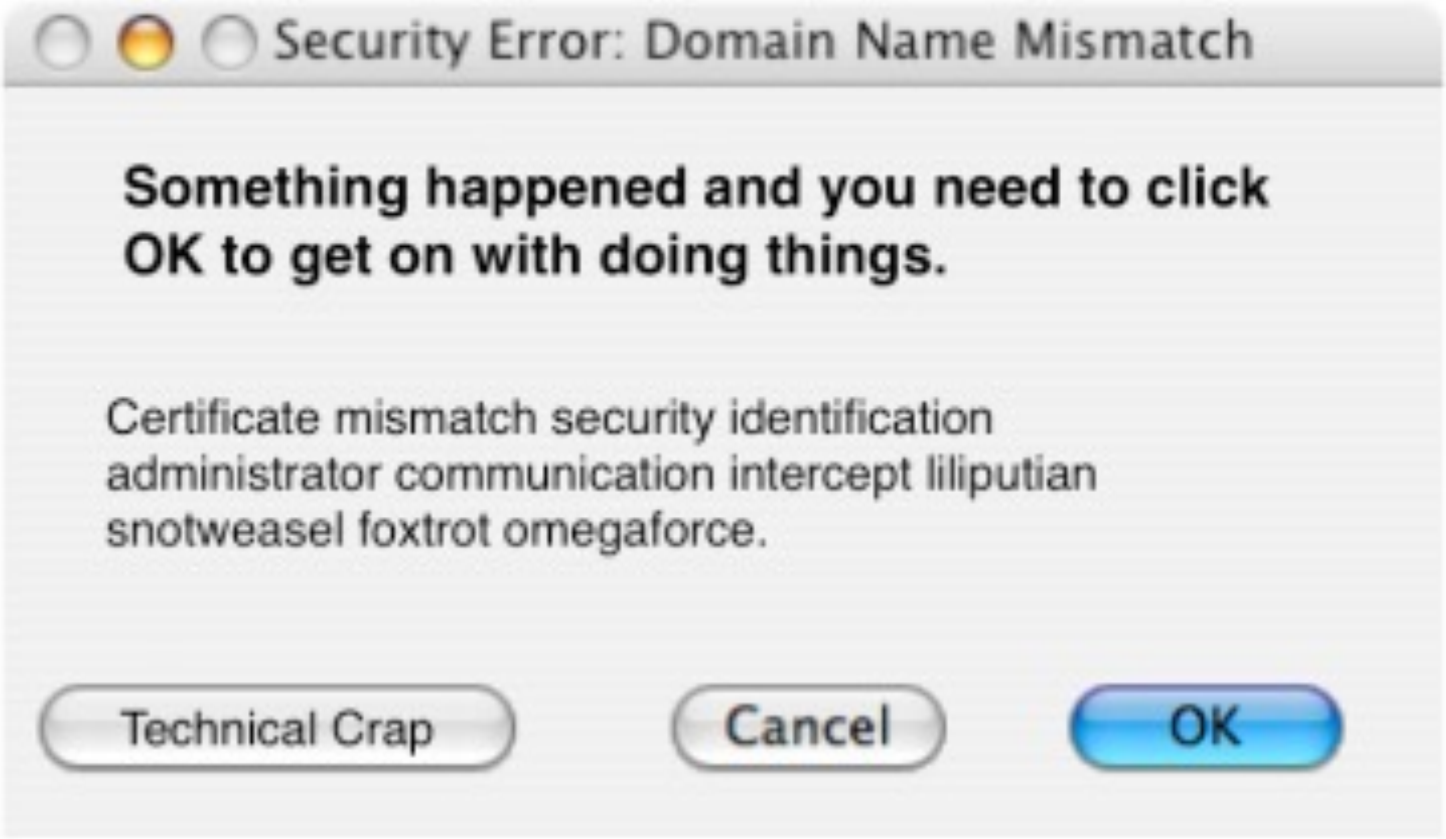


Security Error: Domain Name Mismatch

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.

User’s Perspective



Security Error: Domain Name Mismatch

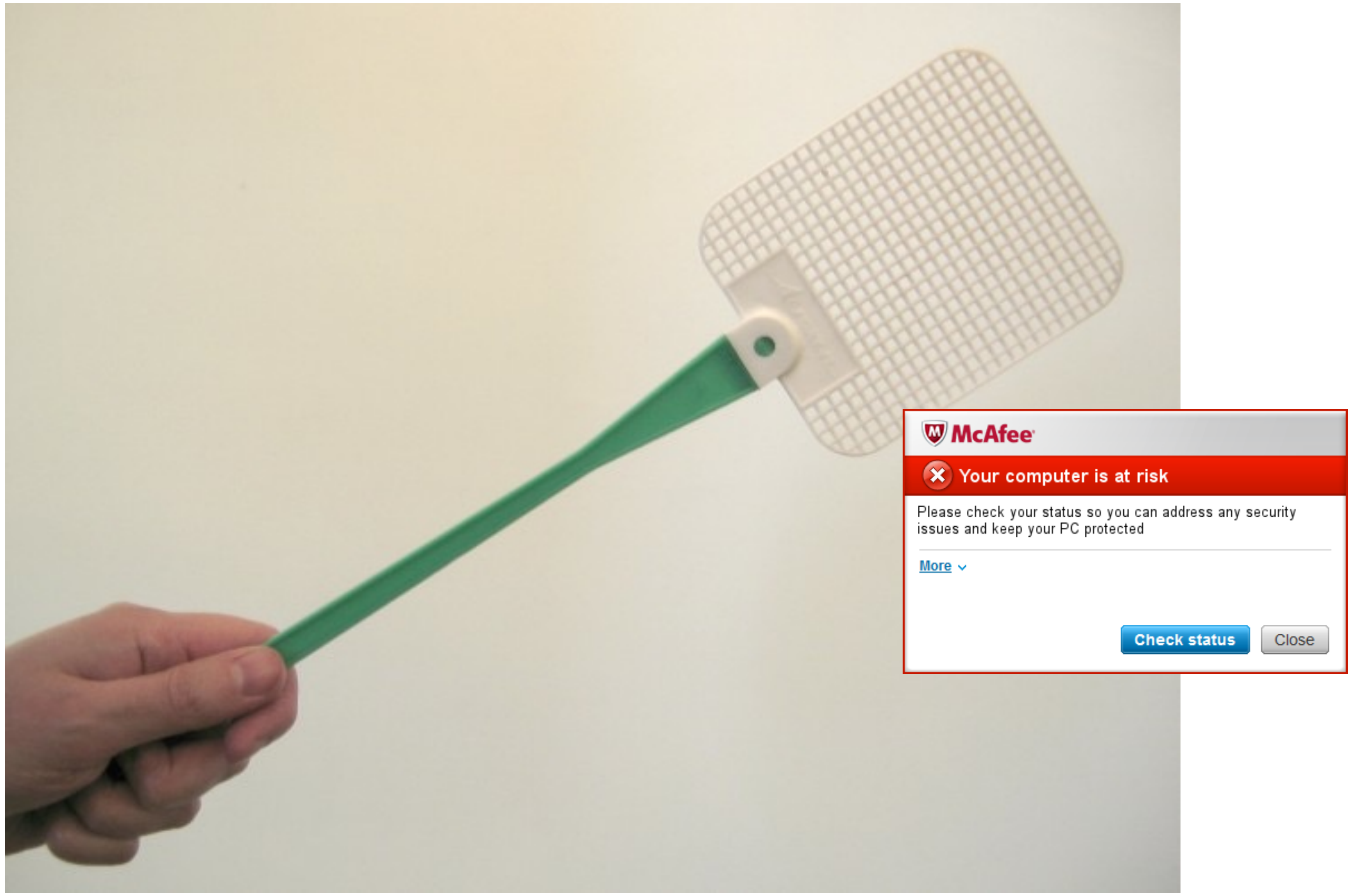
Something happened and you need to click OK to get on with doing things.

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

Users swat away warning dialogs

- RQ: How can we get users to pay attention?
  - *Should we even require them to pay attention?*

- RQ: How do we get users to understand the warning?
  - *Do they even need to understand to do the right thing?*



Your computer is at risk

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

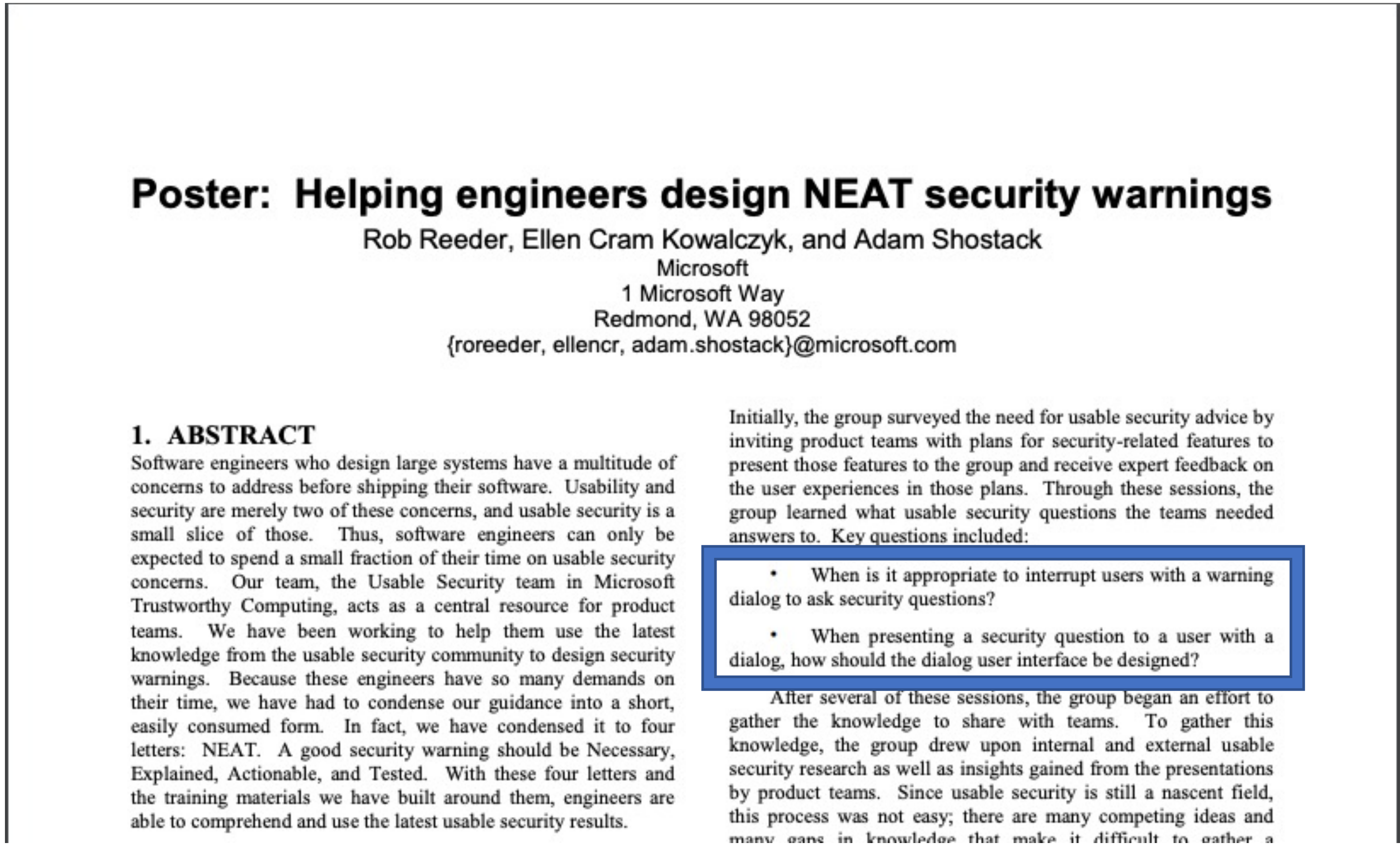
Warnings and the themes of the class

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

Designing NEAT security warnings

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

SOUPS Poster 2011



Poster: Helping engineers design NEAT security warnings

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

1. ABSTRACT

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

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

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

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

Microsoft

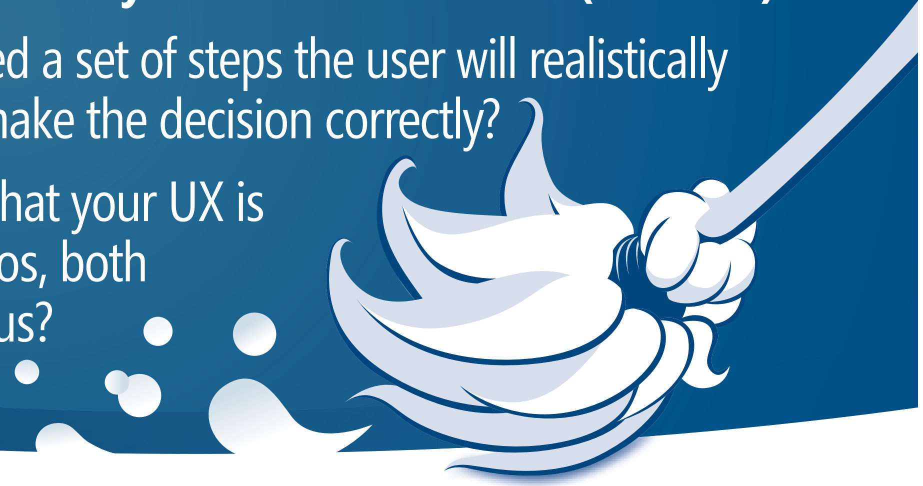
Ask yourself: Is your security or privacy UX:

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

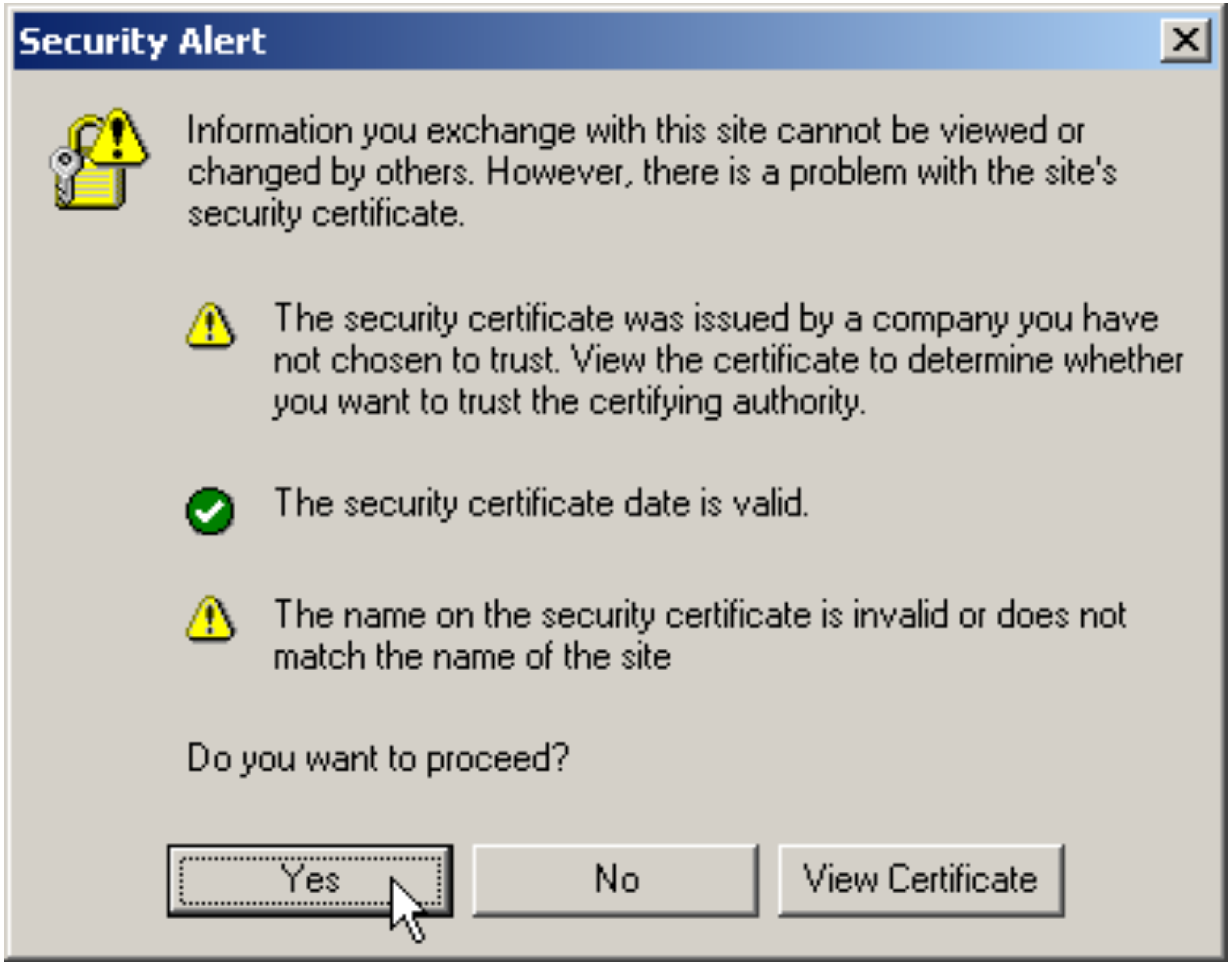
CHOICES: List available options and clearly recommend one

EVIDENCE: Highlight information the user should factor in or exclude in making the decision

SPRUCE

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

What’s wrong?



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

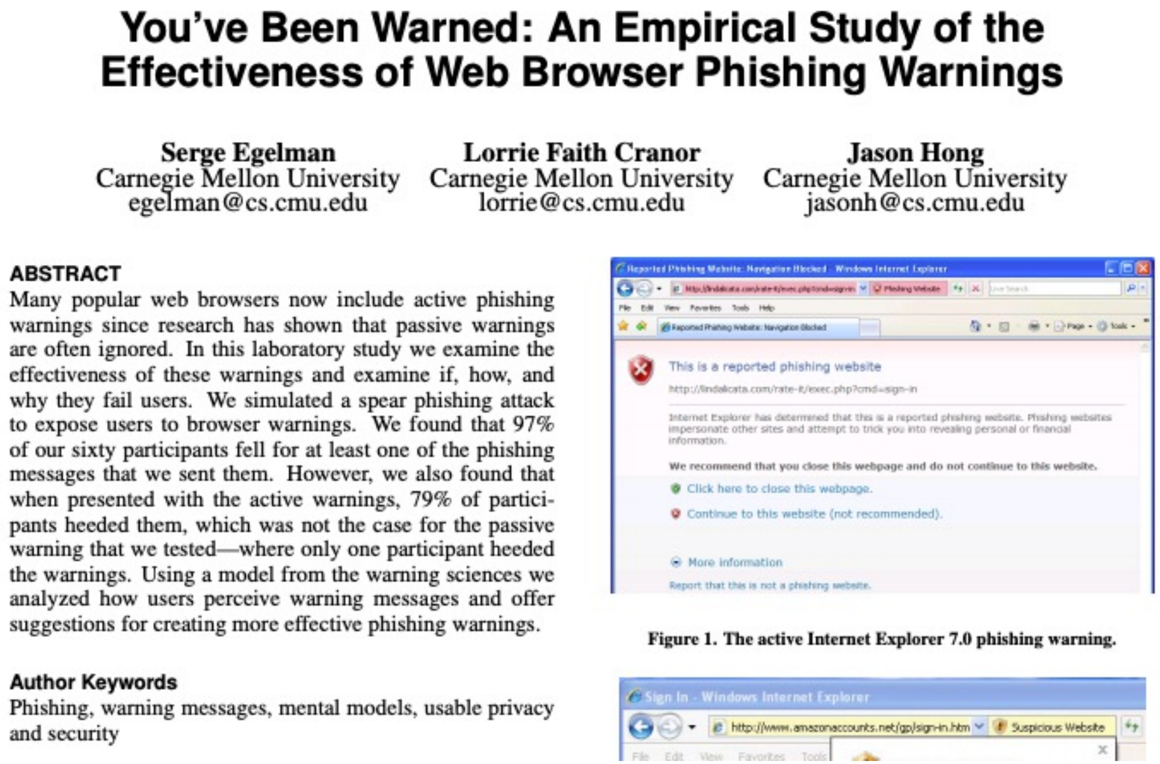
Good Warnings

- Helps users determine whether they are actually at risk
- Stops users from doing something dangerous in risky context
- Doesn’t interfere with non-risky contexts
- **Research CHALLENGE**: *Very difficult to design experiments where there is real risk involved for users.*

Phishing and Warnings

- Study Design Challenges
  - Need to observe users interacting with warnings without them knowing they're being studied
  - Make users feel like they are under attack without actually putting them at risk

CHI 2008



You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings

Serge Egelman
Carnegie Mellon University
egelman@cs.cmu.edu

Lorrie Faith Cranor
Carnegie Mellon University
lorrie@cs.cmu.edu

Jason Hong
Carnegie Mellon University
jasonh@cs.cmu.edu

ABSTRACT
Many popular web browsers now include active phishing warnings since research has shown that passive warnings are often ignored. In this laboratory study we examine the effectiveness of these warnings and examine if, how, and why they fail users. We simulated a spear phishing attack to expose users to browser warnings. We found that 97% of our sixty participants fell for at least one of the phishing messages that we sent them. However, we also found that when presented with the active warnings, 79% of participants heeded them, which was not the case for the passive warning that we tested—where only one participant heeded the warnings. Using a model from the warning sciences we analyzed how users perceive warning messages and offer suggestions for creating more effective phishing warnings.

Author Keywords
Phishing, warning messages, mental models, usable privacy and security

Reported Phishing Website: Navigation Blocked - Windows Internet Explorer
Phishing Website
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 continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

Report that this is not a phishing website.

Figure 1. The active Internet Explorer 7.0 phishing warning.

Sign In - Windows Internet Explorer
http://www.amazonaccounts.net/gp/sign-in.htm
Suspicious Website
File Edit View Favorites Tools

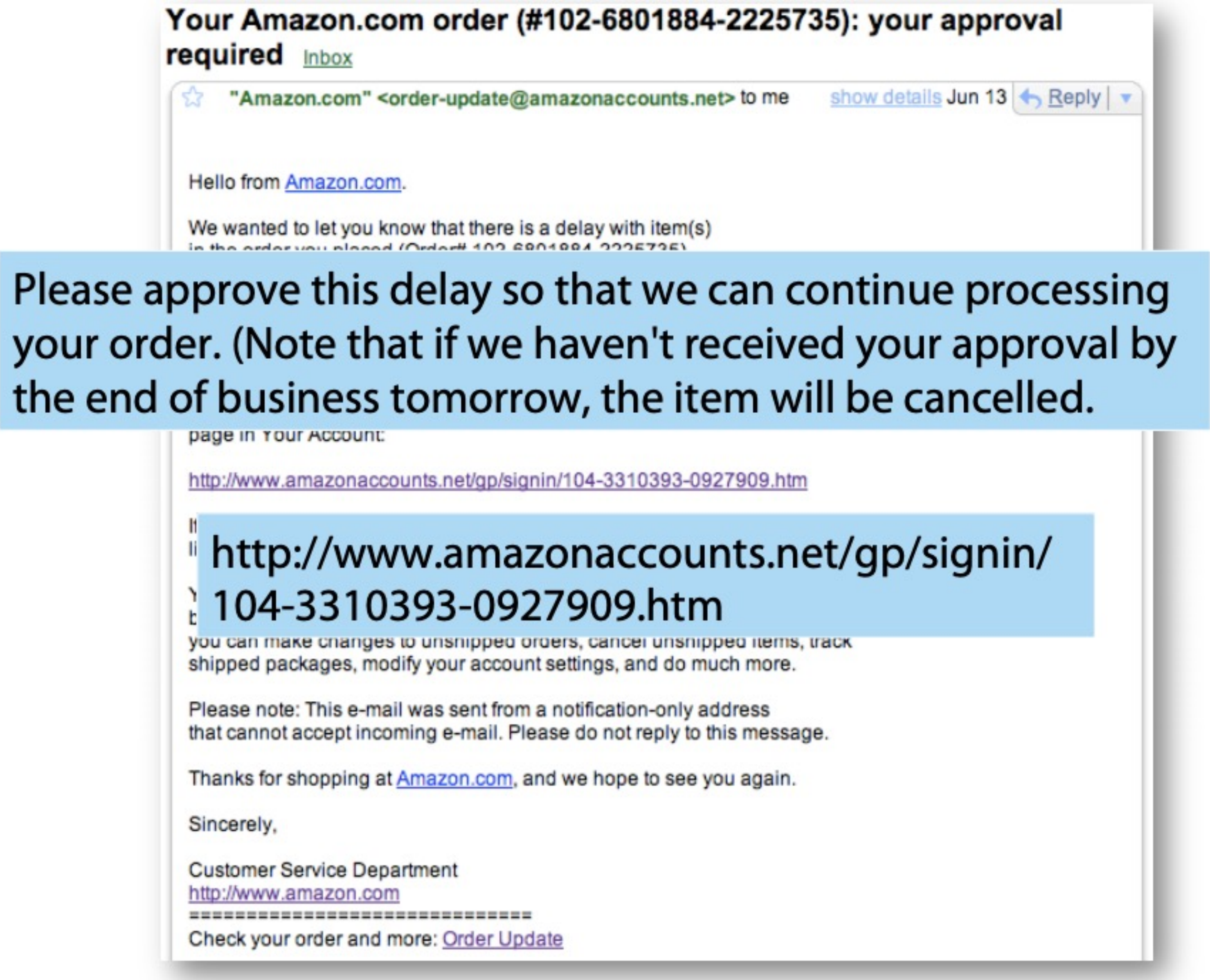
Deception Study

- “Online shopping study”
  - Participants were told the purpose of the study was to measure how they interacted with an online shopping website

- Directed to purchase paperclips on Amazon
  - Answer questions about that experience
  - Also check email for receipt of purchase

- BUT! Researchers sent them a phishing email

- Ensured that the phishing links triggered the warnings in various web browsers being tested



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

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

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.

page in Your Account:

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

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

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.

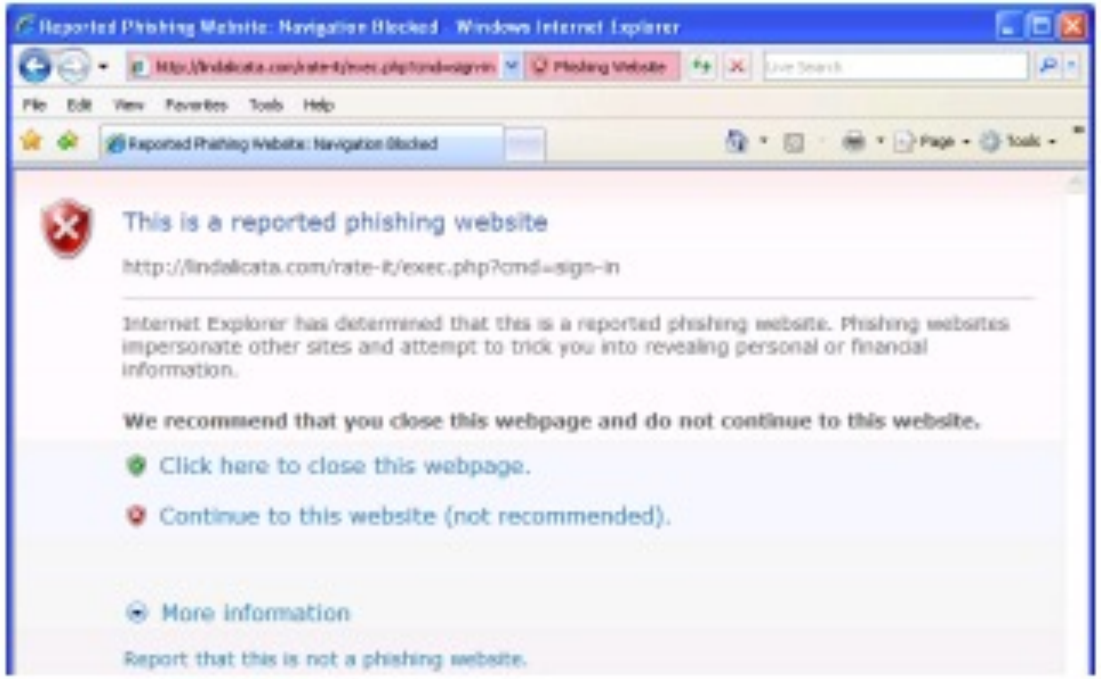
Sincerely,

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

- Emails captures by anti-phishing systems
- Amazon lawyers called CMU

Image from lecture by Lorrie Cranor (https://cups.cs.cmu.edu/courses/ups-sp17/12-warnings.pdf)

Warning Messages (2008)



Reported Phishing Website: Navigation Blocked - Windows Internet Explorer
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 continue to this website.

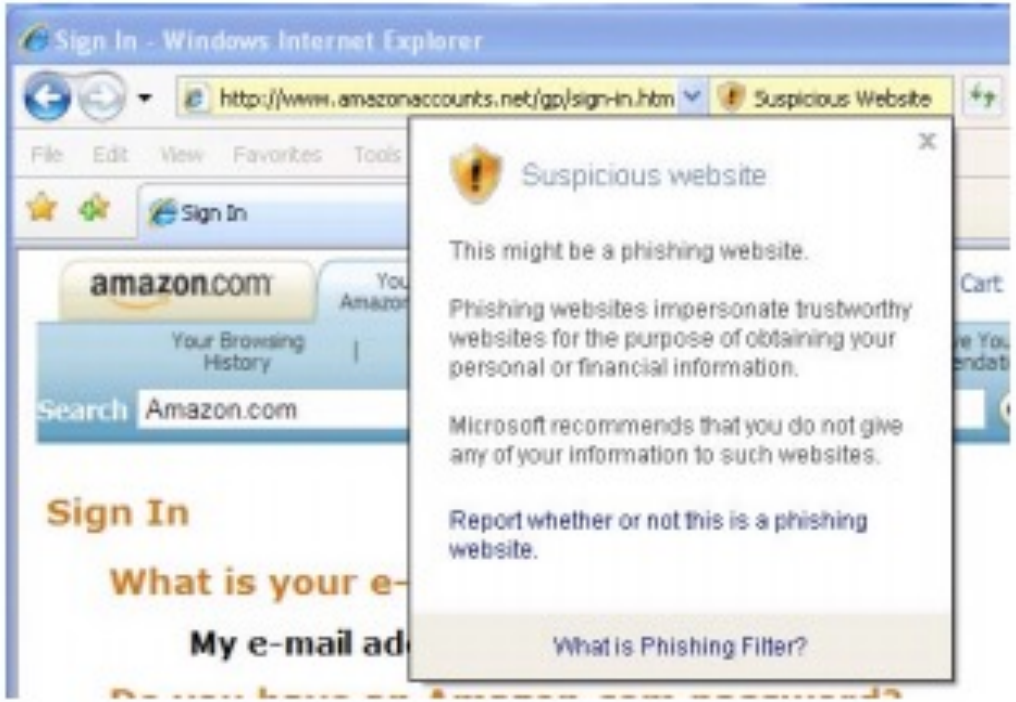
Click here to close this webpage.

Continue to this website (not recommended).

More information

Report that this is not a phishing website.

Figure 1. The active Internet Explorer 7.0 phishing warning.



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?

Figure 2. The passive Internet Explorer 7.0 phishing warning.

Wogalter Model

- Identify reasons that a particular warning is ineffective

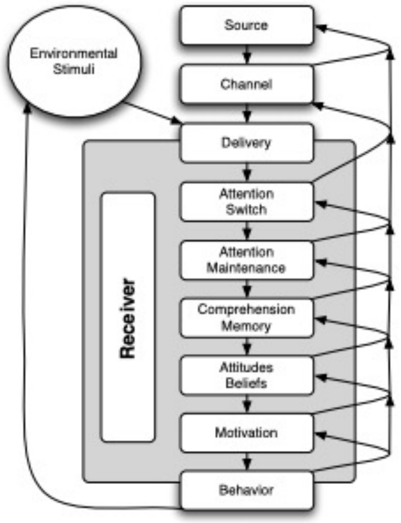
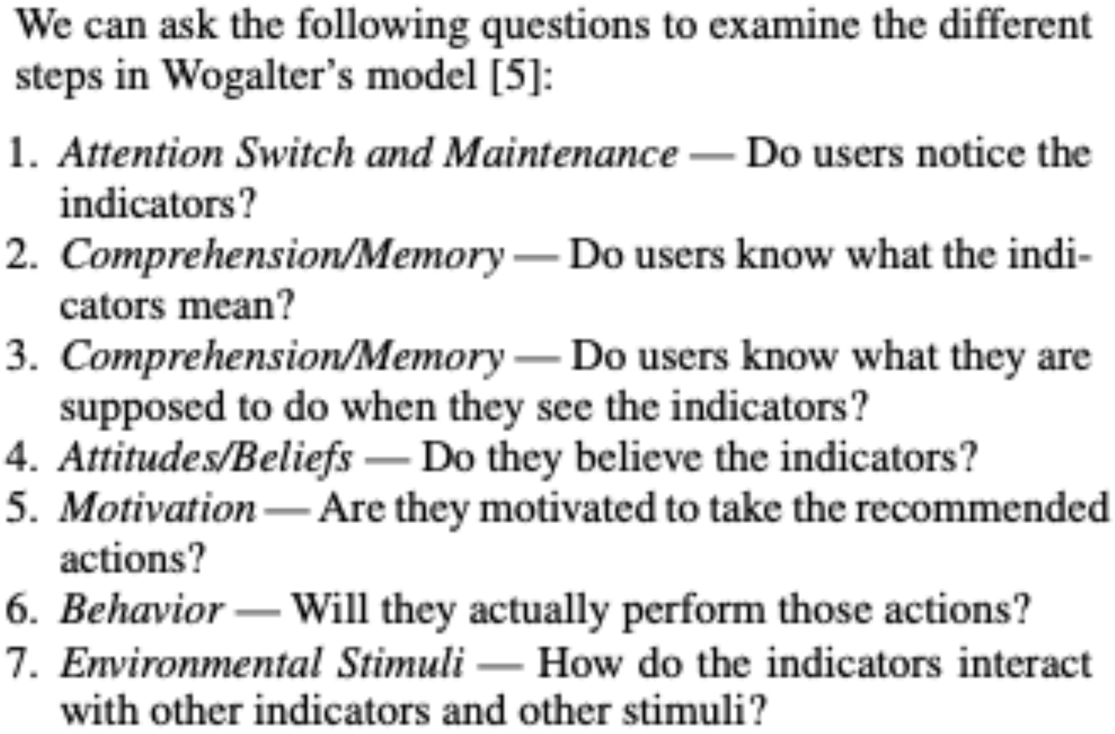


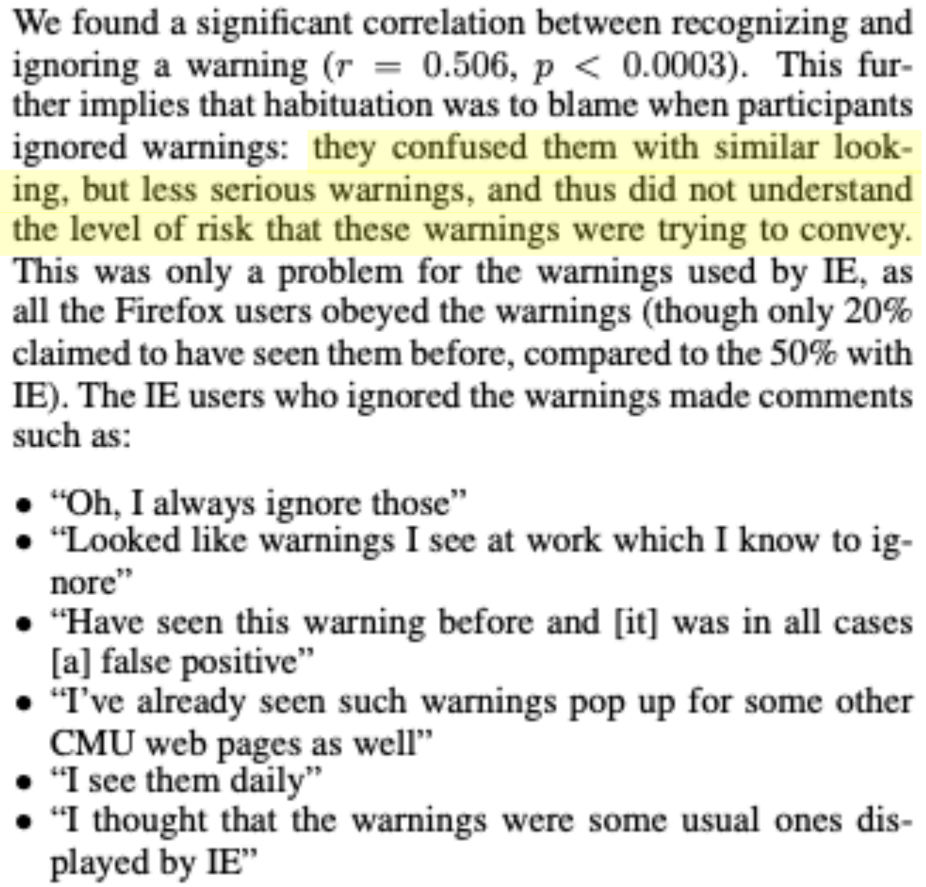
Figure 4. Diagram of the different phases of the C-HIP model [21].



We can ask the following questions to examine the different steps in Wogalter's model [5]:

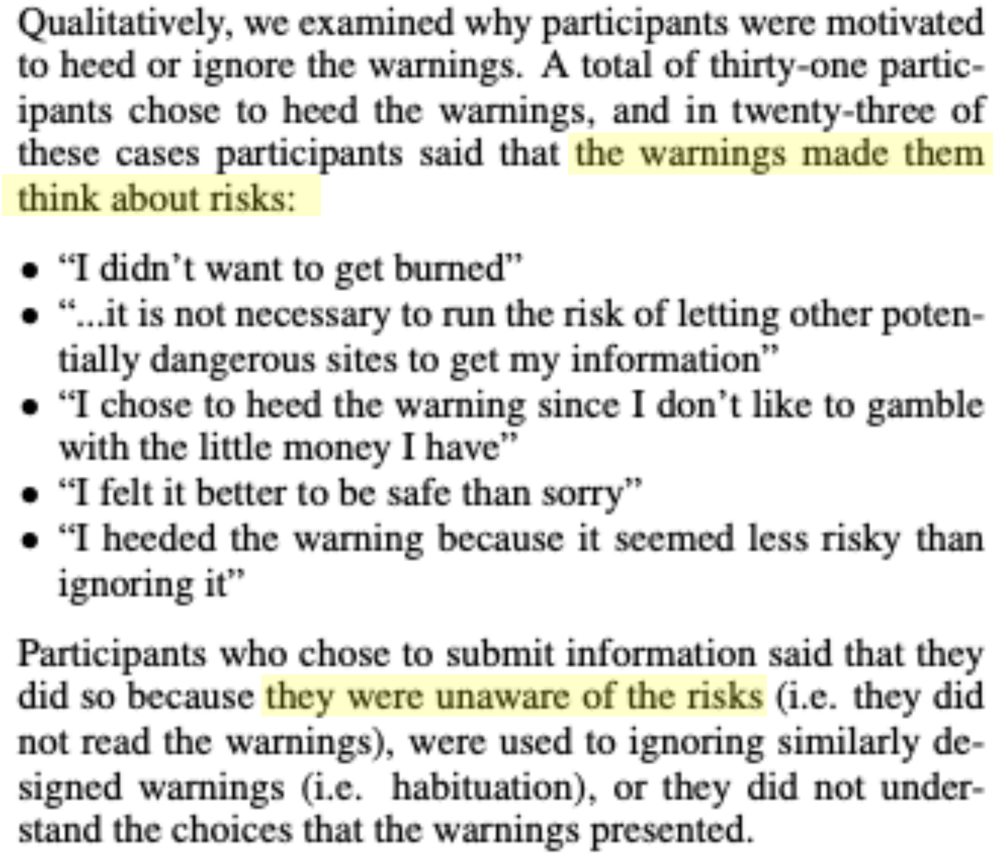
1. *Attention Switch and Maintenance* — Do users notice the indicators?
2. *Comprehension/Memory* — Do users know what the indicators mean?
3. *Comprehension/Memory* — Do users know what they are supposed to do when they see the indicators?
4. *Attitudes/Beliefs* — Do they believe the indicators?
5.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

Habituation and Motivations



We found a significant correlation between recognizing and ignoring a warning ($r = 0.506$, $p < 0.0003$). This further implies that habituation was to blame when participants ignored warnings: they confused them with similar looking, but less serious warnings, and thus did not understand the level of risk that these warnings were trying to convey. This was only a problem for the warnings used by IE, as all the Firefox users obeyed the warnings (though only 20% claimed to have seen them before, compared to the 50% with IE). The IE users who ignored the warnings made comments such as:

- "Oh, I always ignore those"
- "Looked like warnings I see at work which I know to ignore"
- "Have seen this warning before and [it] was in all cases [a] false positive"
- "I've already seen such warnings pop up for some other CMU web pages as well"
- "I see them daily"
- "I thought that the warnings were some usual ones displayed by IE"



Qualitatively, we examined why participants were motivated to heed or ignore the warnings. A total of thirty-one participants chose to heed the warnings, and in twenty-three of these cases participants said that the warnings made them think about risks:

- "I didn't want to get burned"
- "...it is not necessary to run the risk of letting other potentially dangerous sites to get my information"
- "I chose to heed the warning since I don't like to gamble with the little money I have"
- "I felt it better to be safe than sorry"
- "I heeded the warning because it seemed less risky than ignoring it"

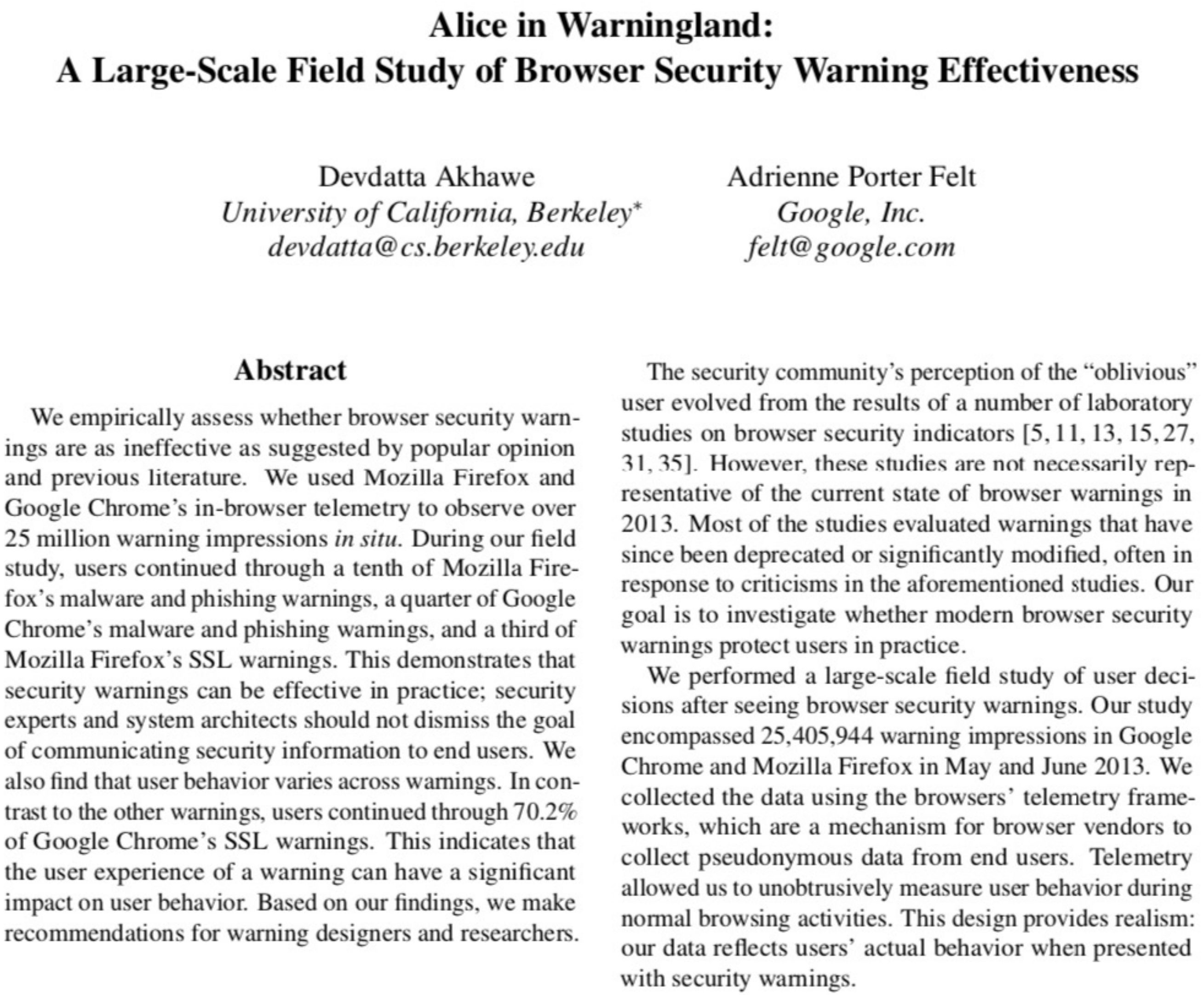
Participants who chose to submit information said that they did so because they were unaware of the risks (i.e. they did not read the warnings), were used to ignoring similarly designed warnings (i.e. habituation), or they did not understand the choices that the warnings presented.

Alice in Warning Land

USENIX Security 2013

- Observe “warning impressions” *in situ* using In-browser telemetry
    - No need for deceptions

- Warning message types
    - Malware/Phishing
    - SSL Warnings



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

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

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

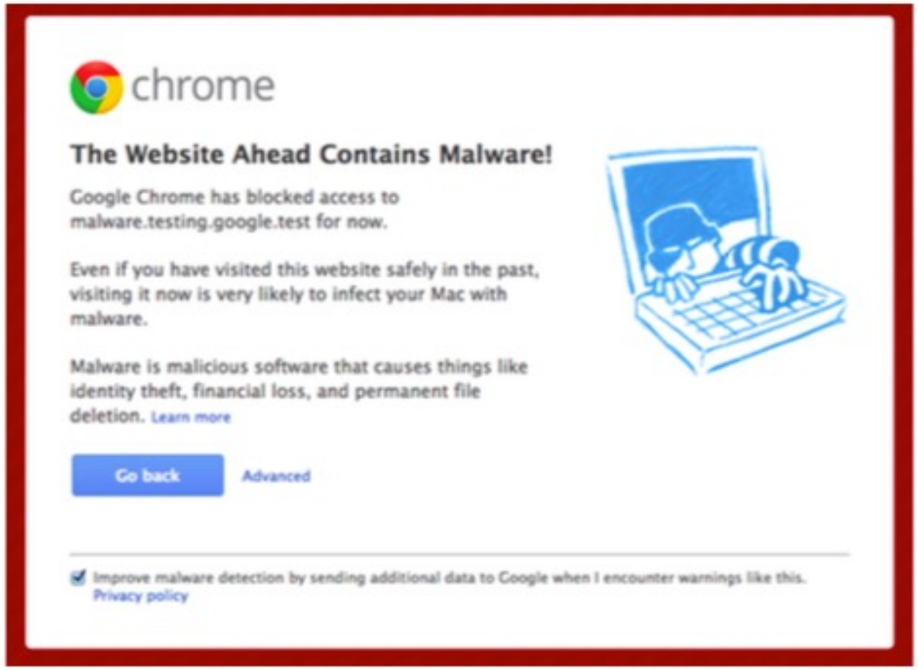
Abstract

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

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

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

Malware Warning Messages (2012/2013)



The Website Ahead Contains Malware!

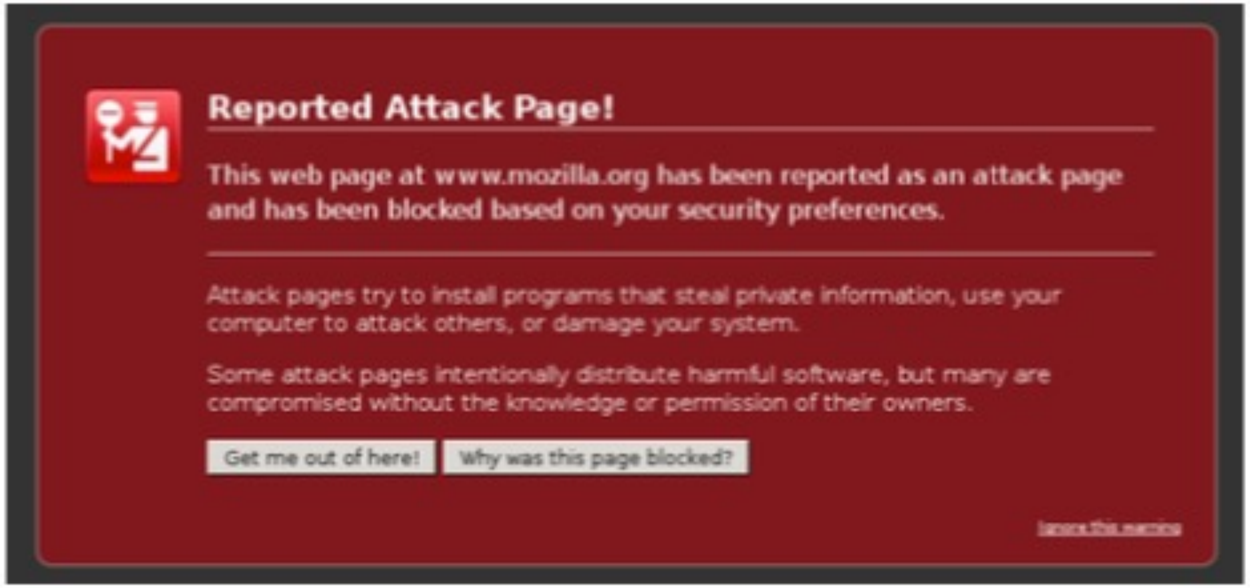
Google Chrome has blocked access to malware.testing.google.test for now.

Even if you have visited this website safely in the past, visiting it now is very likely to infect your Mac with malware.

Malware is malicious software that causes things like identity theft, financial loss, and permanent file deletion. Learn more

☑ Improve malware detection by sending additional data to Google when I encounter warnings like this. Privacy policy

Figure 1: Malware warning for Google Chrome



Reported Attack Page!

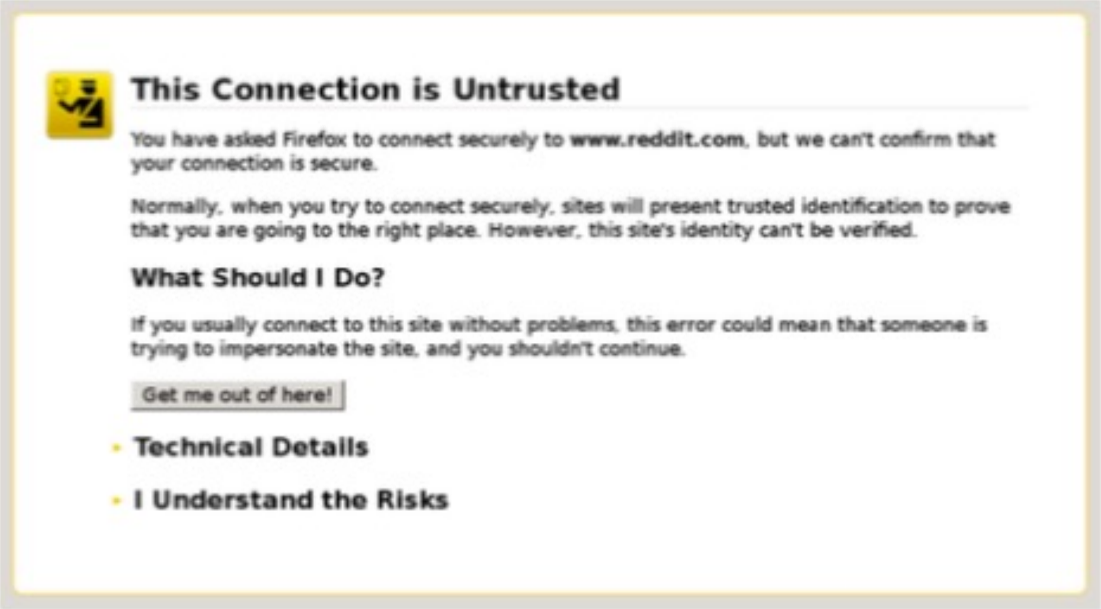
This web page at www.mozilla.org has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Figure 2: Malware warning for Mozilla Firefox

SSL Warning Messages (2012/2013)



This Connection is Untrusted

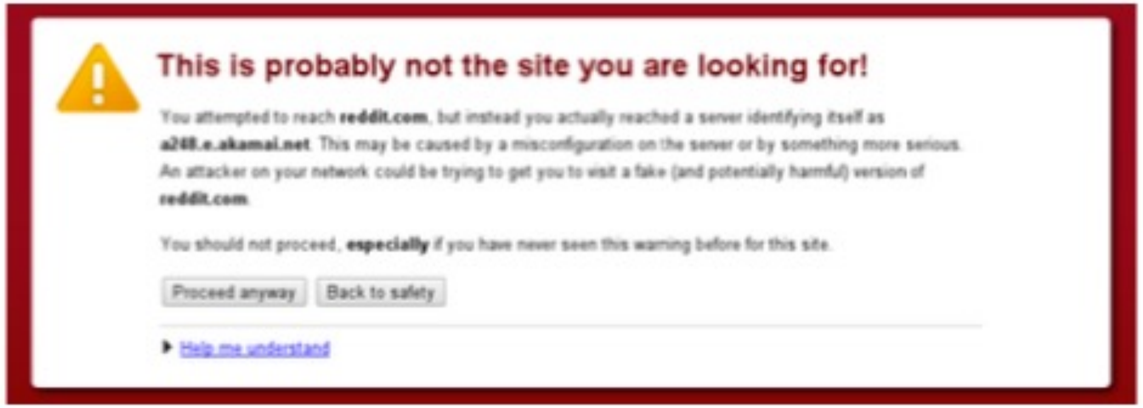
You have asked Firefox to connect securely to **www.reddit.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Figure 4: SSL warning for Mozilla Firefox



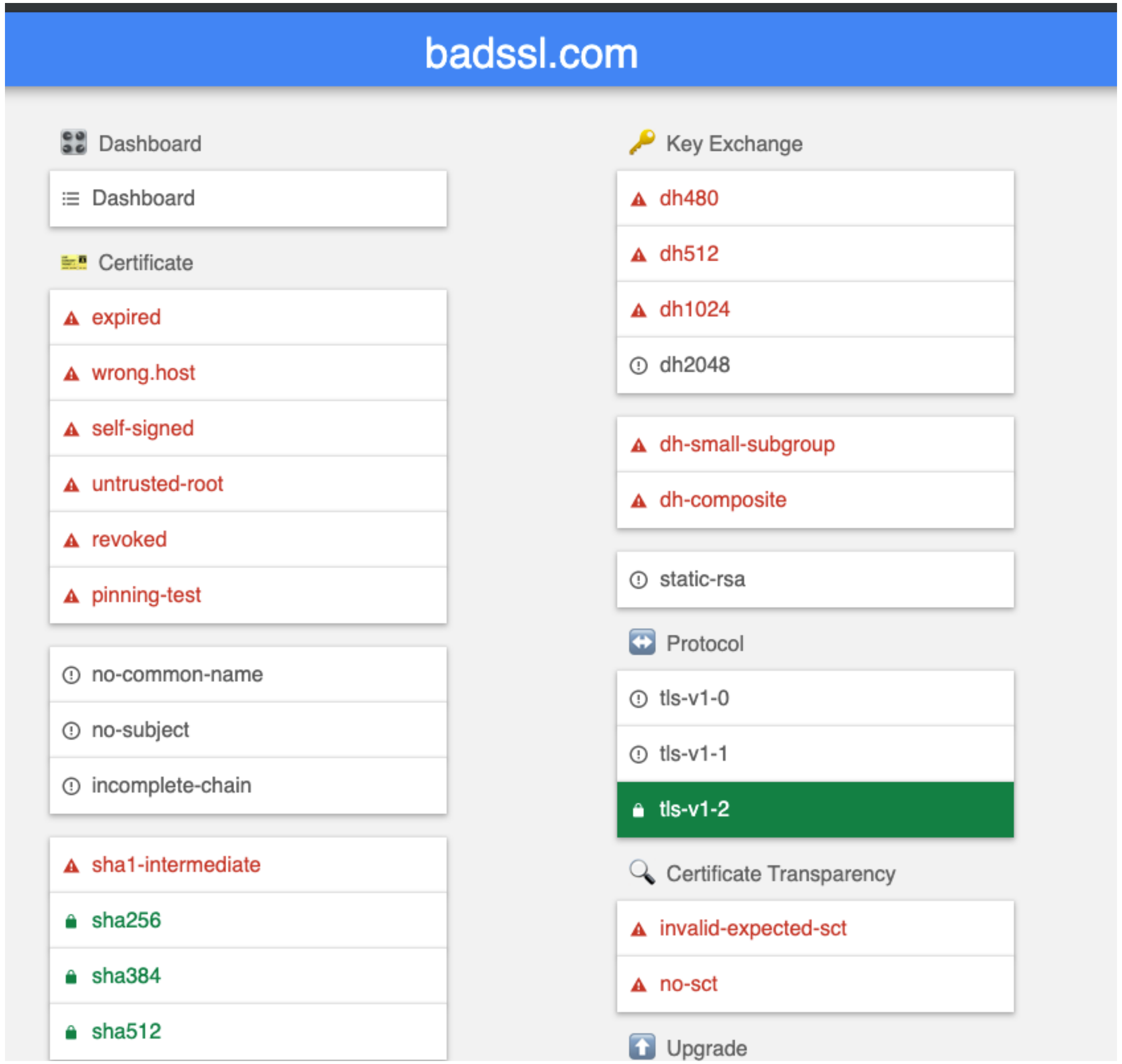
This is probably not the site you are looking for!

You attempted to reach **reddit.com**, but instead you actually reached a server identifying itself as **a248.e.akamai.net**. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of **reddit.com**.

You should not proceed, **especially** if you have never seen this warning before for this site.

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

Viewing SSL Security Warnings Today



badssl.com

Dashboard

- Dashboard

Certificate

- ⚠ expired
- ⚠ wrong.host
- ⚠ self-signed
- ⚠ untrusted-root
- ⚠ revoked
- ⚠ pinning-test

- ⓘ no-common-name
- ⓘ no-subject
- ⓘ incomplete-chain

- ⚠ sha1-intermediate
- 🔒 sha256
- 🔒 sha384
- 🔒 sha512

Key Exchange

- ⚠ dh480
- ⚠ dh512
- ⚠ dh1024
- ⓘ dh2048

- ⚠ dh-small-subgroup
- ⚠ dh-composite

- ⓘ static-rsa

Protocol

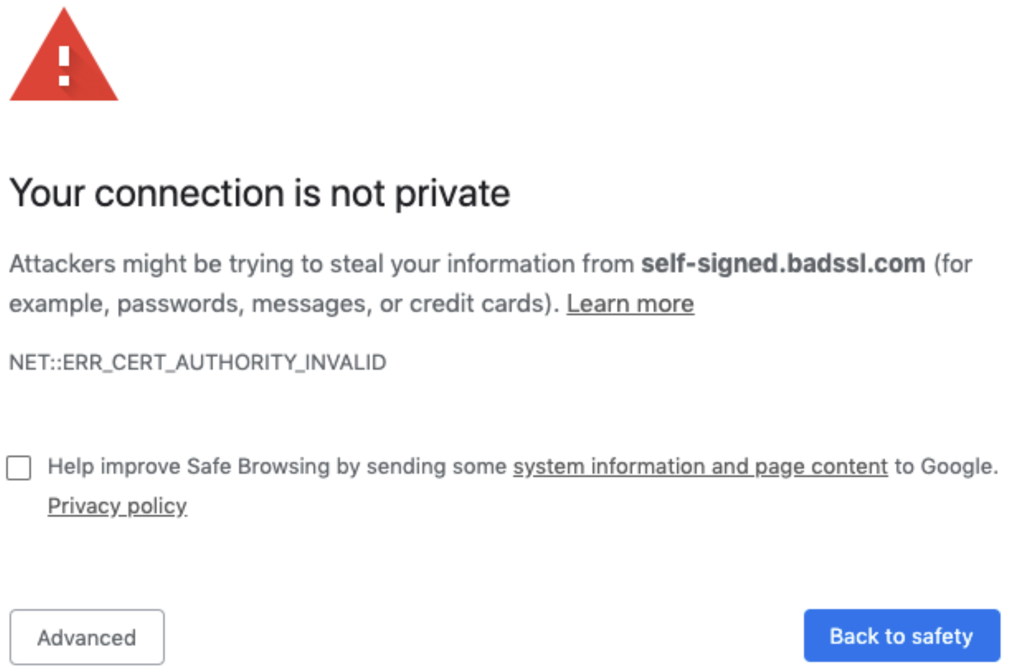
- ⓘ tls-v1-0
- ⓘ tls-v1-1
- 🔒 tls-v1-2

Certificate Transparency

- ⚠ invalid-expected-sct
- ⚠ no-sct

Upgrade

Self Signed/Invalid Authority (2019)



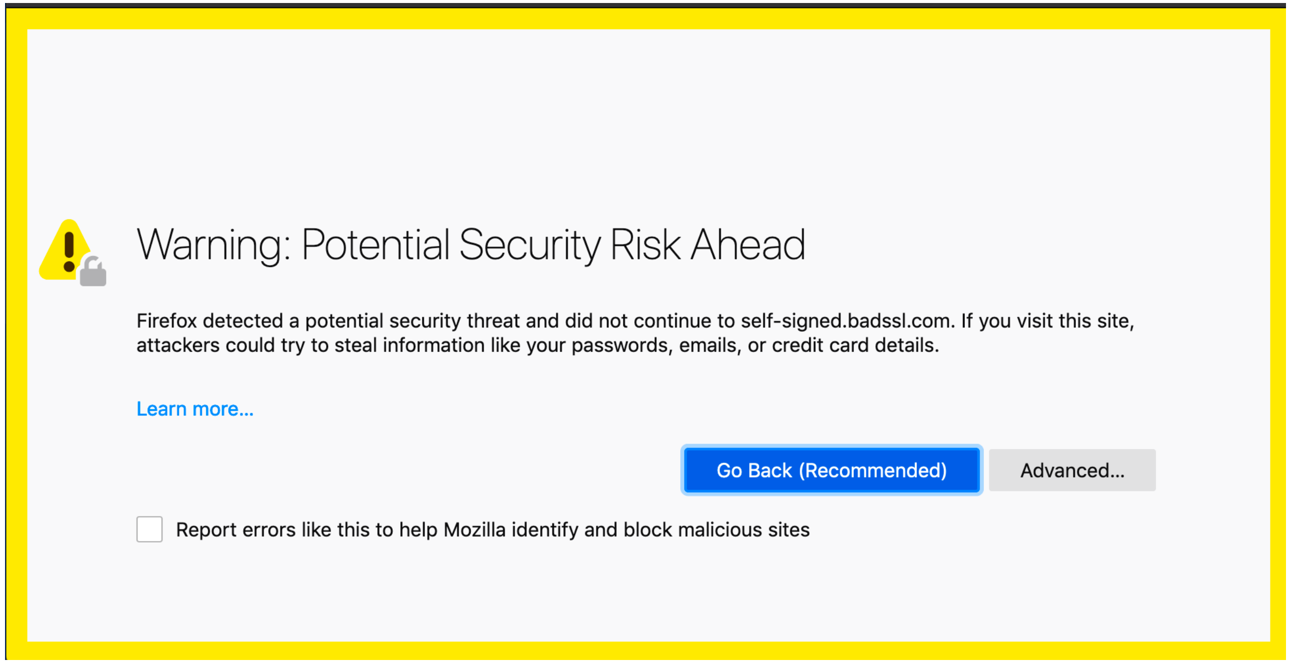
Your connection is not private

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

NET::ERR_CERT_AUTHORITY_INVALID

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

Chrome



Warning: Potential Security Risk Ahead

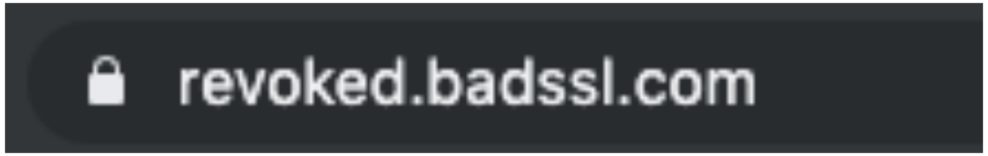
Firefox detected a potential security threat and did not continue to self-signed.badssl.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

Learn more…

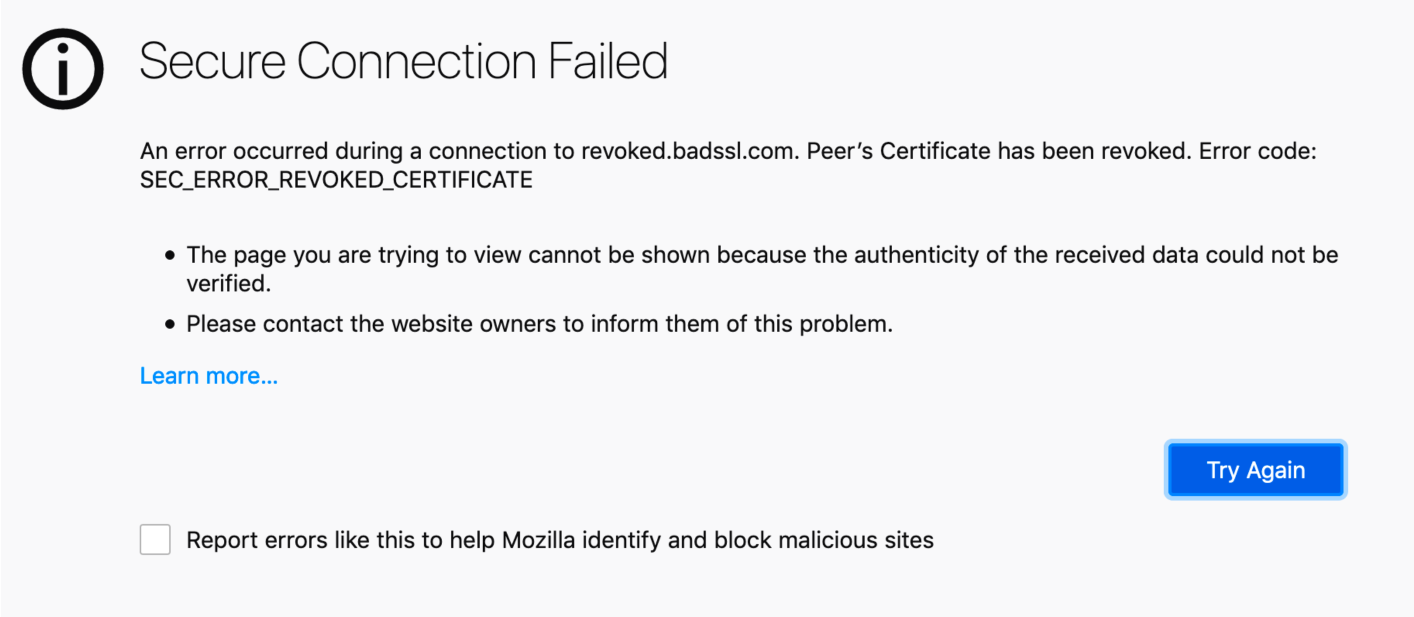
□ Report errors like this to help Mozilla identify and block malicious sites

Firefox

Revoked Certificate (2019)



Chrome



Secure Connection Failed

An error occurred during a connection to revoked.badssl.com. Peer's Certificate has been revoked. Error code: SEC_ERROR_REVOKED_CERTIFICATE

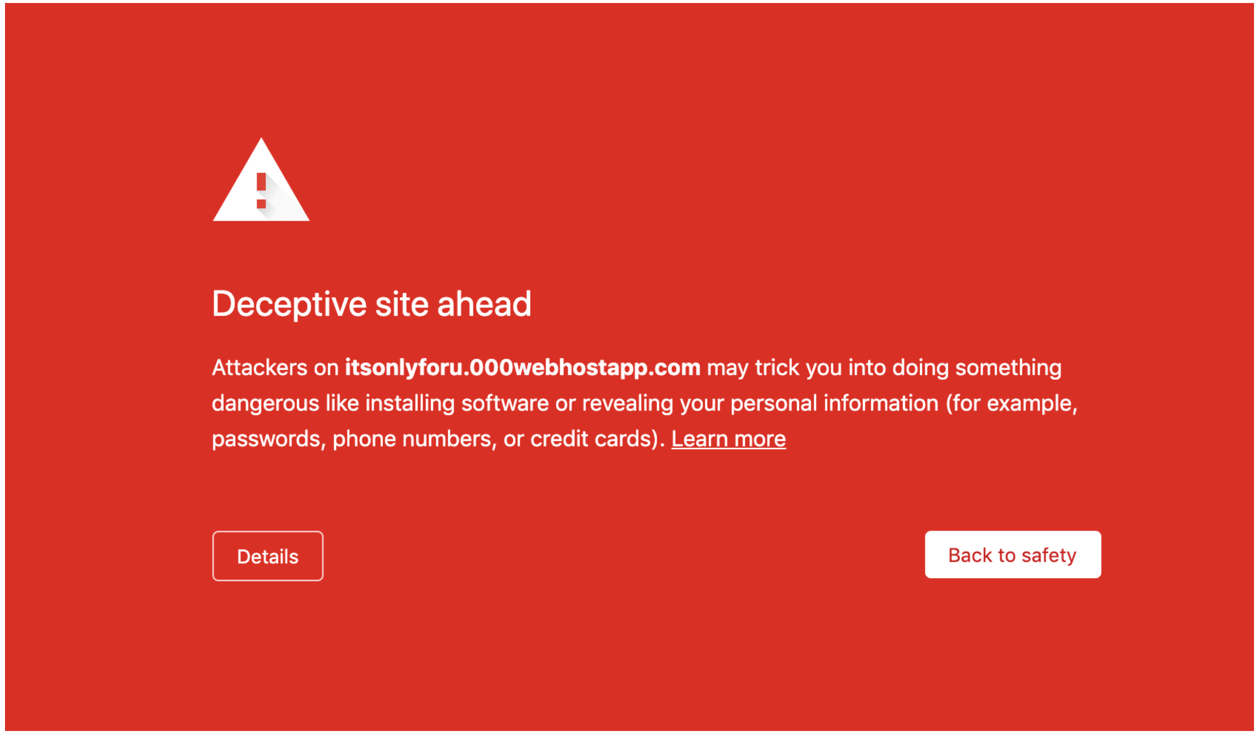
- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Learn more…

□ Report errors like this to help Mozilla identify and block malicious sites

Firefox

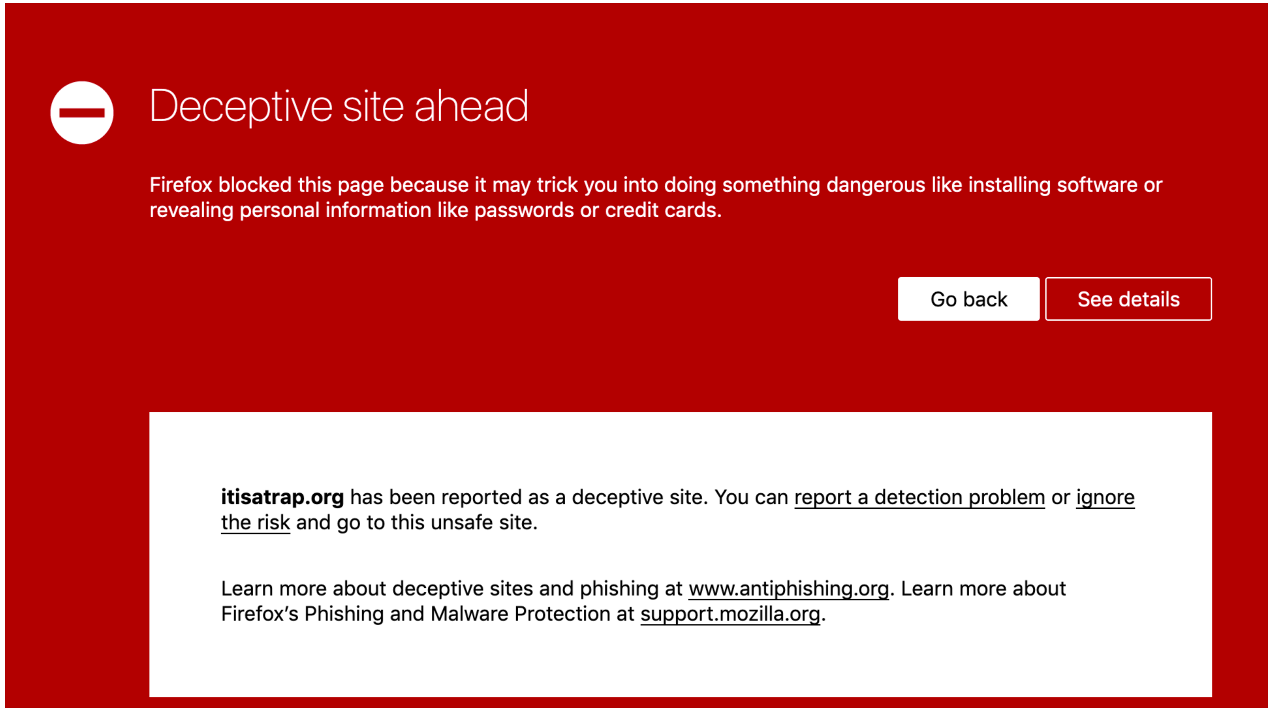
Malware Warnings (2019)



Deceptive site ahead

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

Chrome



Deceptive site ahead

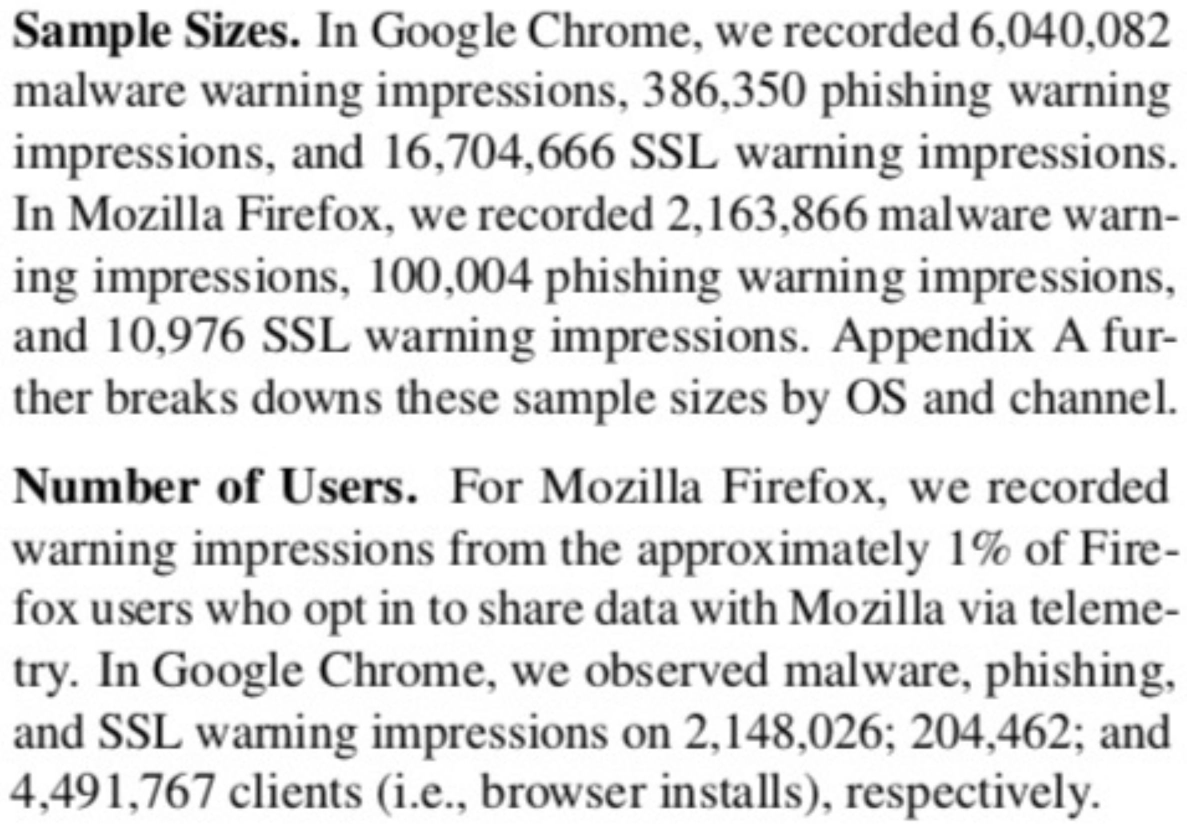
Firefox blocked this page because it may trick you into doing something dangerous like installing software or revealing personal information like passwords or credit cards.

itisatrap.org has been reported as a deceptive site. You can report a detection problem or ignore the risk and go to this unsafe site.

Learn more about deceptive sites and phishing at www.antiphishing.org. Learn more about Firefox's Phishing and Malware Protection at support.mozilla.org.

Firefox

Data Collection --- huge data collection!



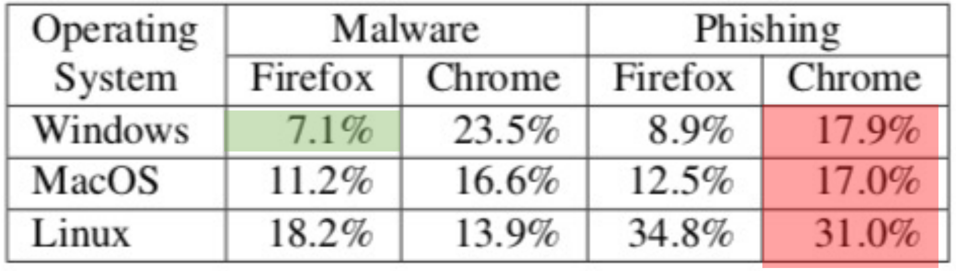
Sample Sizes. In Google Chrome, we recorded 6,040,082 malware warning impressions, 386,350 phishing warning impressions, and 16,704,666 SSL warning impressions. In Mozilla Firefox, we recorded 2,163,866 malware warning impressions, 100,004 phishing warning impressions, and 10,976 SSL warning impressions.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

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

Some Results

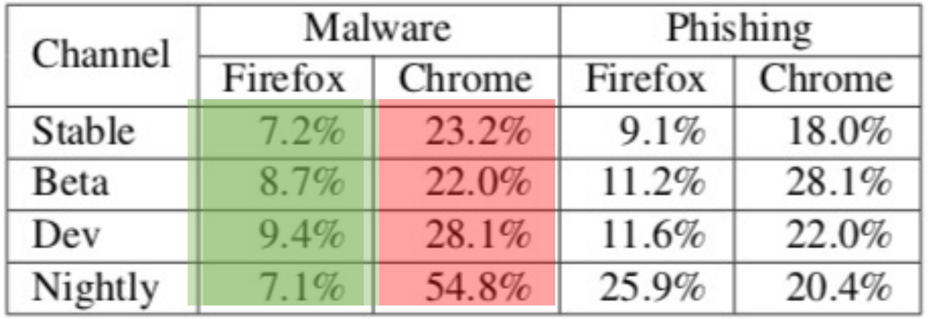
Some warnings seem to work well,
others work very poorly.

What is the difference between Malware and SSL?



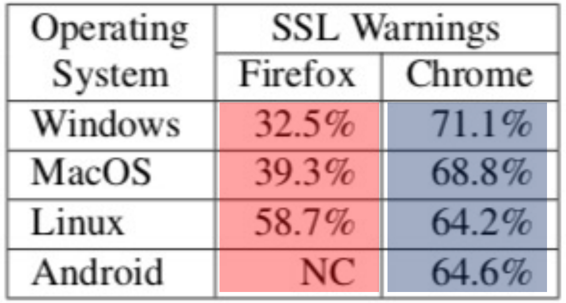
Operating System	Malware		Phishing	
	Firefox	Chrome	Firefox	Chrome
Windows	7.1%	23.5%	8.9%	17.9%
MacOS	11.2%	16.6%	12.5%	17.0%
Linux	18.2%	13.9%	34.8%	31.0%

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



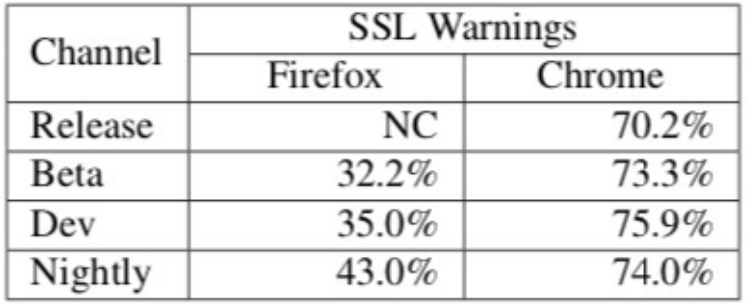
Channel	Malware		Phishing	
	Firefox	Chrome	Firefox	Chrome
Stable	7.2%	23.2%	9.1%	18.0%
Beta	8.7%	22.0%	11.2%	28.1%
Dev	9.4%	28.1%	11.6%	22.0%
Nightly	7.1%	54.8%	25.9%	20.4%

Table 2: Release channel vs. clickthrough rates for malware and phishing warnings, for all operating systems.



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

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

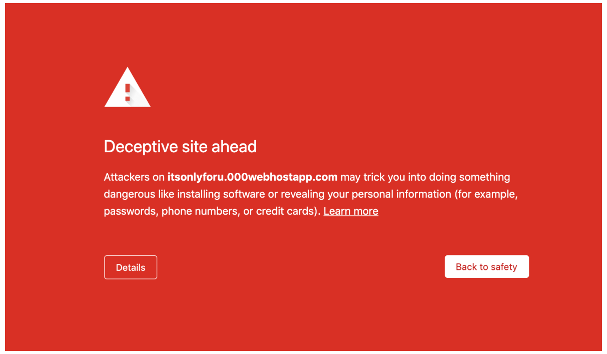


Channel	SSL Warnings	
	Firefox	Chrome
Release	NC	70.2%
Beta	32.2%	73.3%
Dev	35.0%	75.9%
Nightly	43.0%	74.0%

Table 4: Channel vs. clickthrough rates for SSL warnings.

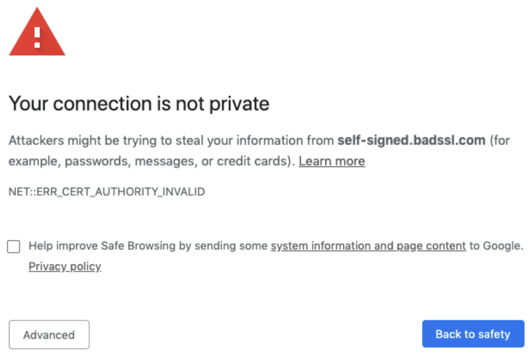
Implications

- Some warnings are effective
  - Some less so (improve those!)
- The kind of error for SSL may have an impact
  - Untrusted vs. Expired
- Technical backgrounds increase clickthrough
  - E.g., users who use Linux
  - Curiousity vs. confidence?
- The number of clicks doesn’t have a large impact
  - Hiding the “proceed” button doesn’t really change behavior
- There’s been real change in Google Chrome since the publication of this study



Deceptive site ahead

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



Your connection is not private

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

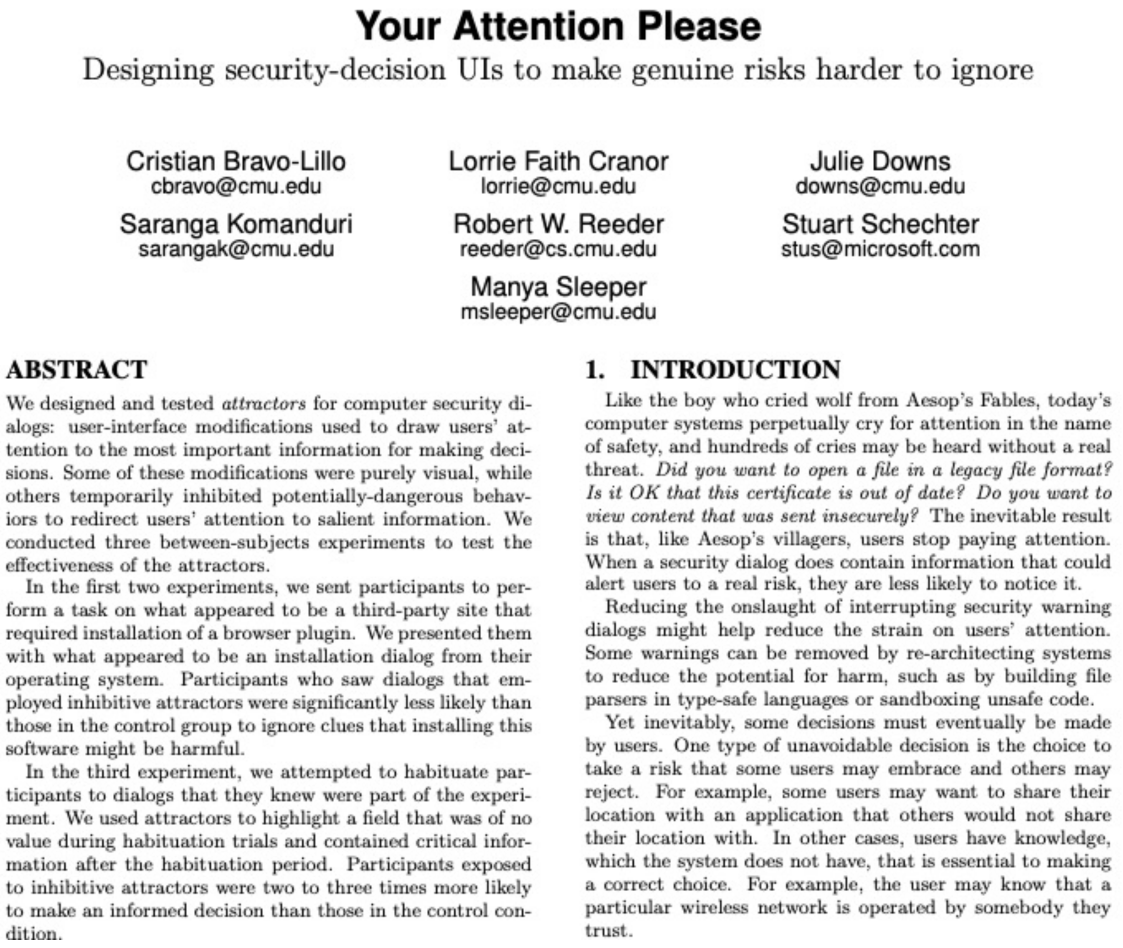
NET::ERR_CERT_AUTHORITY_INVALID

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

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

SOUPS 2013

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



Your Attention Please

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

Cristian Bravo-Lillo
cbravo@cmu.edu

Lorrie Faith Cranor
lorrie@cmu.edu

Julie Downs
downs@cmu.edu

Saranga Komanduri
sarangak@cmu.edu

Robert W. Reeder
reeder@cs.cmu.edu

Stuart Schechter
stus@microsoft.com

Manya Sleeper
msleeper@cmu.edu

ABSTRACT

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

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

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

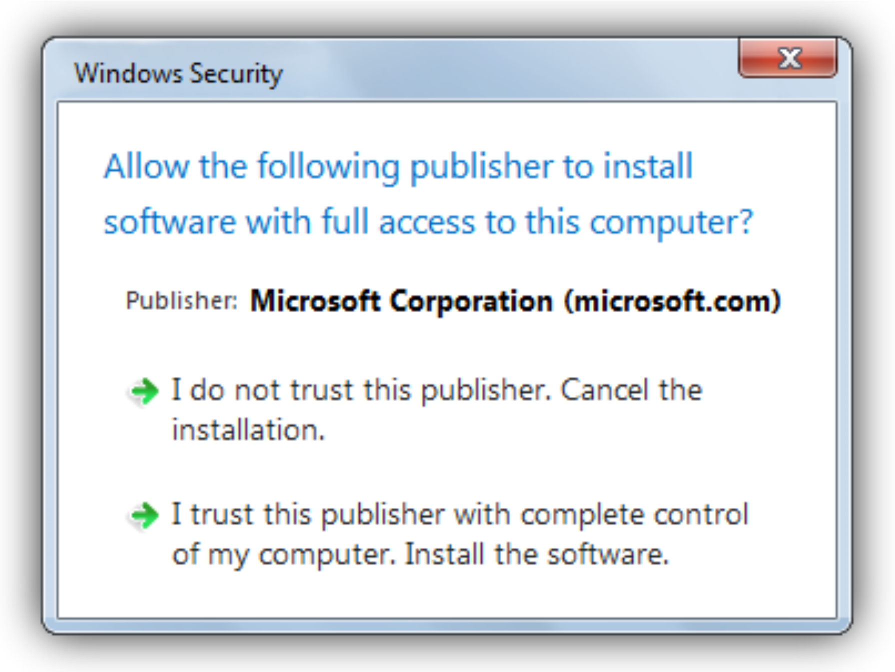
1. INTRODUCTION

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

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

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

The experiment: Can you spot the difference?



Windows Security

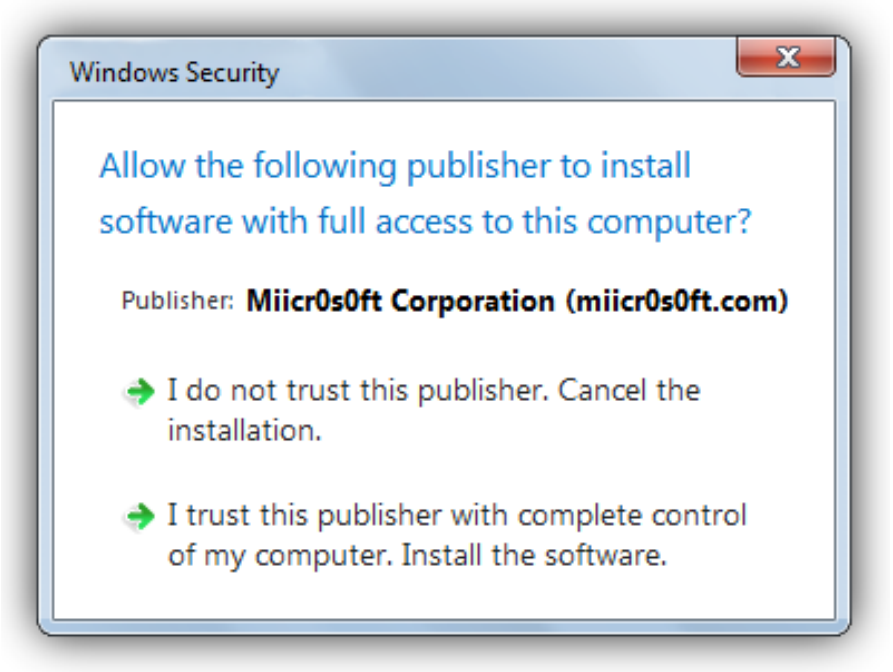
Allow the following publisher to install software with full access to this computer?

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?

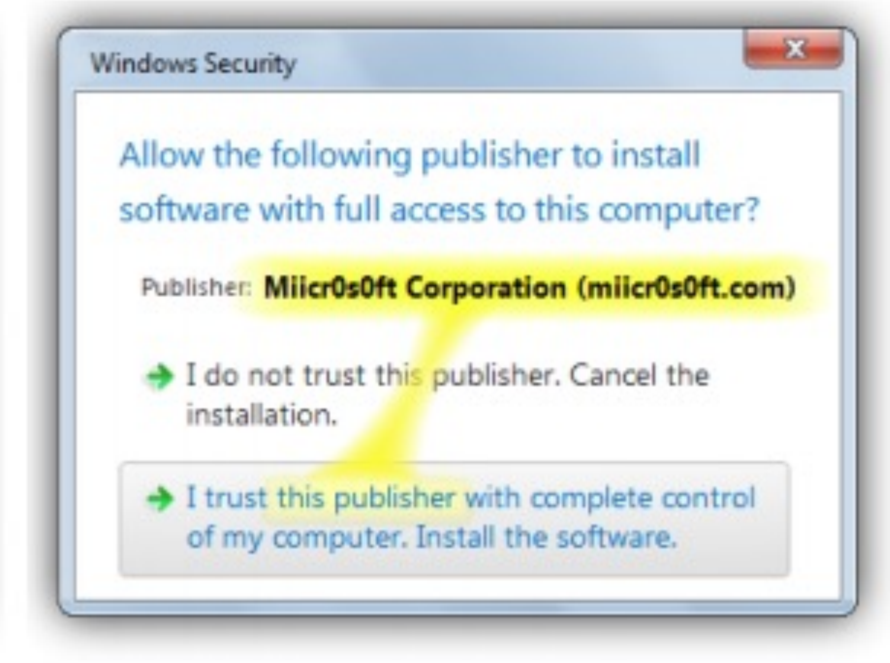
Publisher: **Miicr0s0ft Corporation (miicr0s0ft.com)**

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

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

suspicious

Delay and Focus: Animation and Reveal



Windows Security

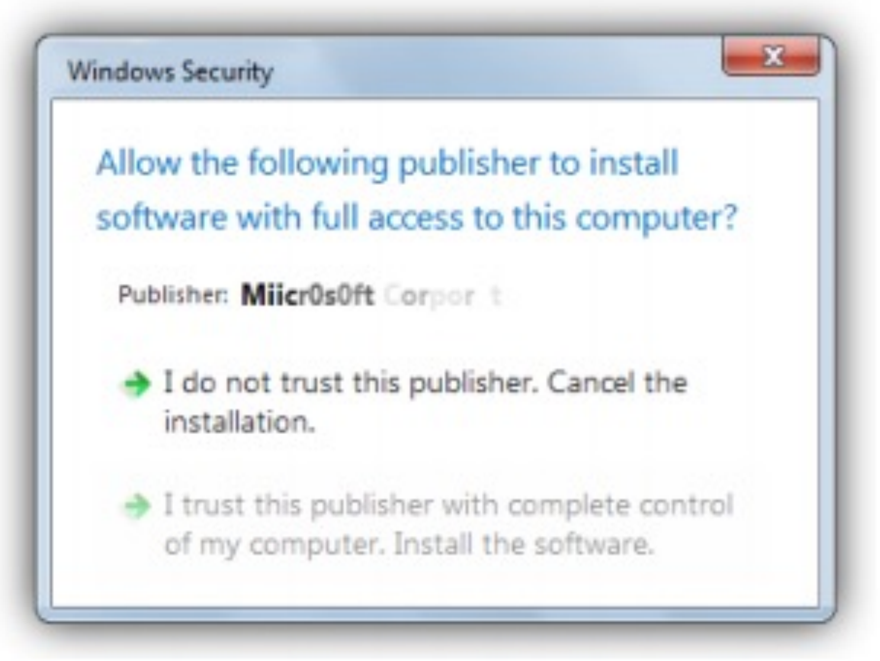
Allow the following publisher to install software with full access to this computer?

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.

(b) *Animated Connector (AC)*



Windows Security

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

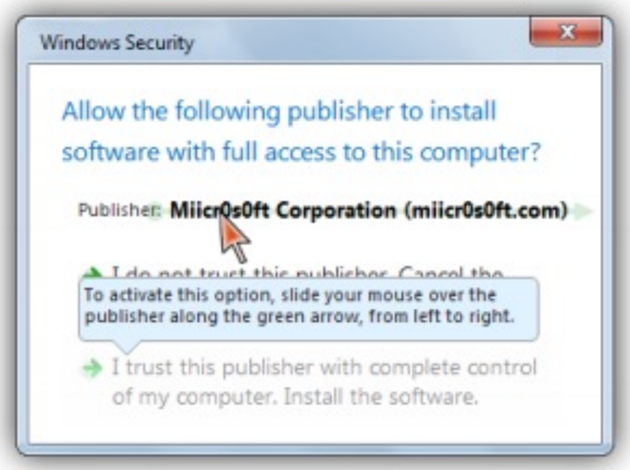
Publisher: **Miicr0s0ft** Corpor t

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

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

(c) *Progressive Reveal*

Force Interaction



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

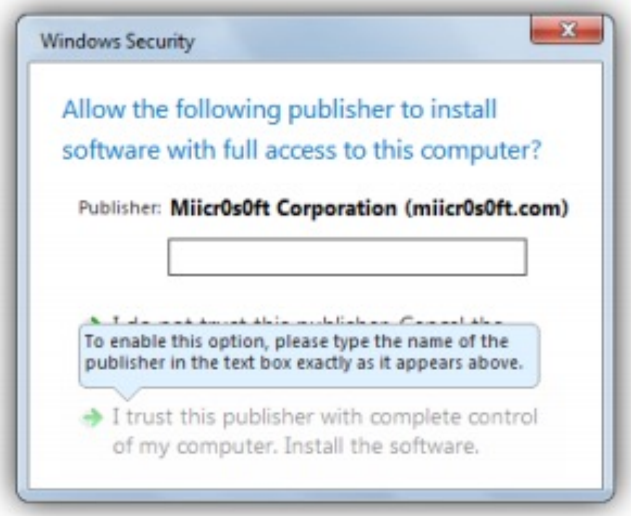
Publisher: Miicr0s0ft Corporation (miicr0s0ft.com)

I do not trust this publisher. Cancel the

To activate this option, slide your mouse over the publisher along the green arrow, from left to right.

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

(d) *Swipe*



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

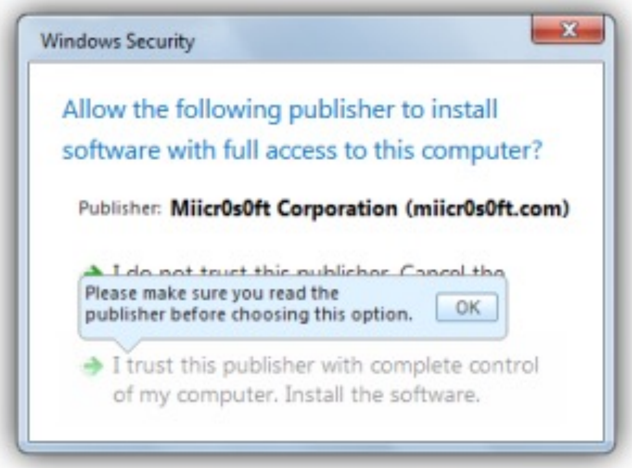
Publisher: Miicr0s0ft Corporation (miicr0s0ft.com)

I do not trust this publisher. Cancel the

To enable this option, please type the name of the publisher in the text box exactly as it appears above.

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

(e) *Type*



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

Publisher: Miicr0s0ft Corporation (miicr0s0ft.com)

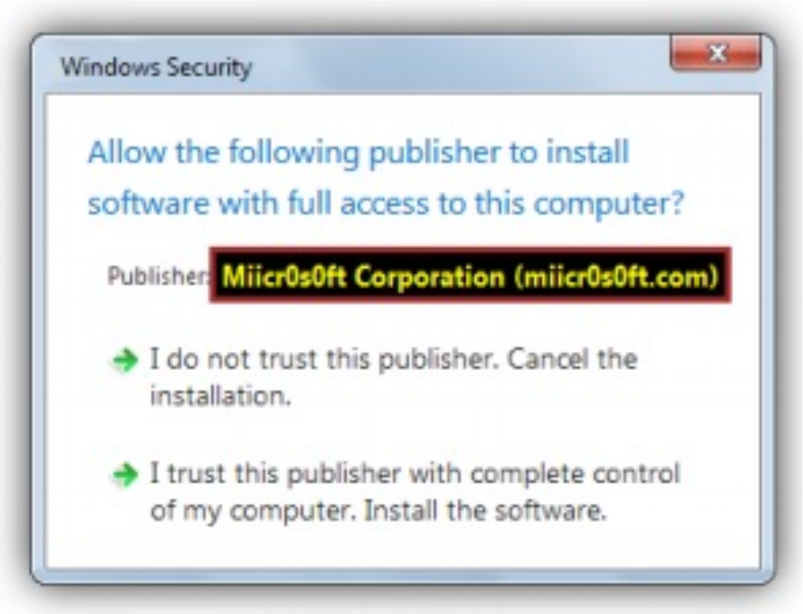
I do not trust this publisher. Cancel the

Please make sure you read the publisher before choosing this option.

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

(f) *Request*

ANSI Standard Warnings



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

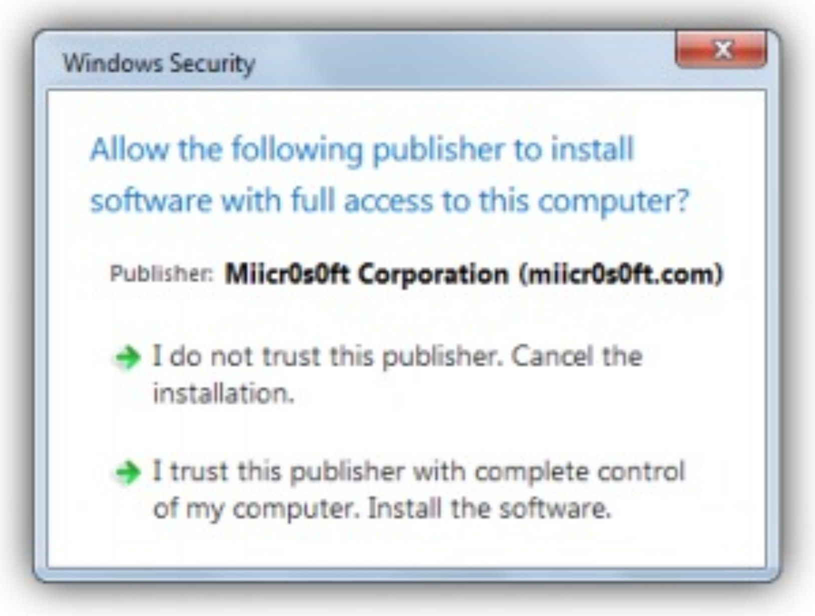
Publisher: Miicr0s0ft Corporation (miicr0s0ft.com)

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

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

(g) *ANSI*

Different Messaging



Windows Security

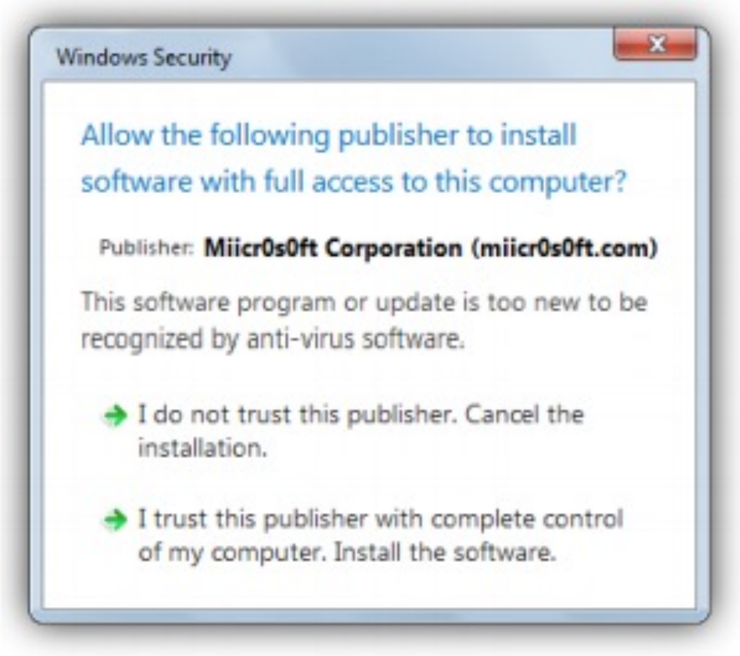
Allow the following publisher to install software with full access to this computer?

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.

(a) *Control*



Windows Security

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

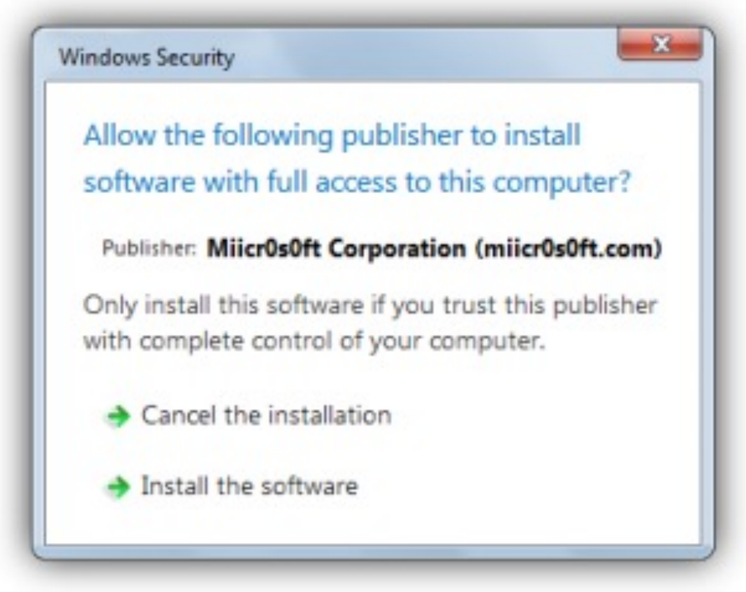
Publisher: **Miicr0s0ft Corporation (miicr0s0ft.com)**

This software program or update is too new to be recognized by anti-virus software.

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

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

(h) *No Antivirus*



Windows Security

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

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

Only install this software if you trust this publisher with complete control of your computer.

→ Cancel the installation

→ Install the software

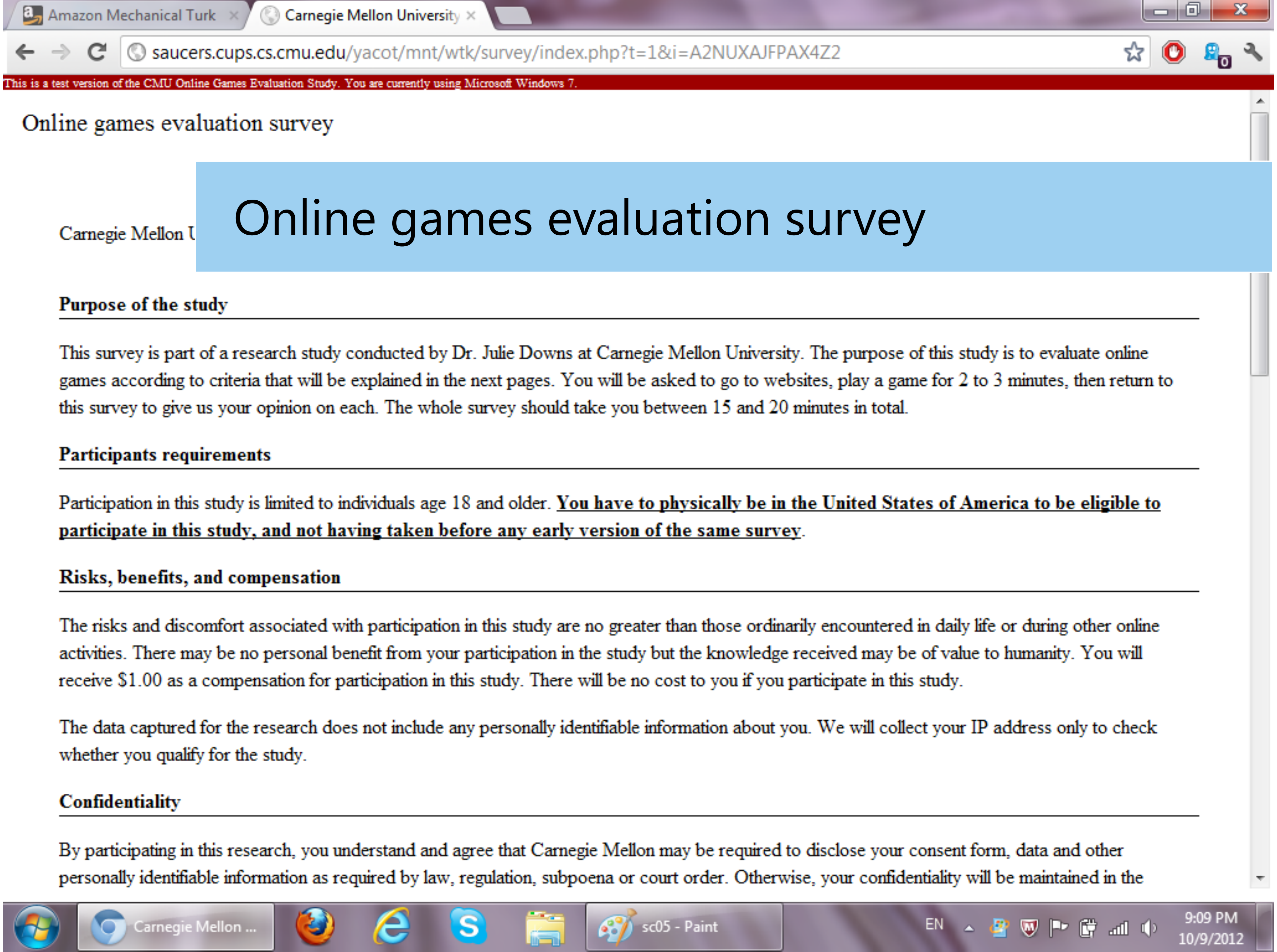
(i) *Short options*

The Task

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

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

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**.

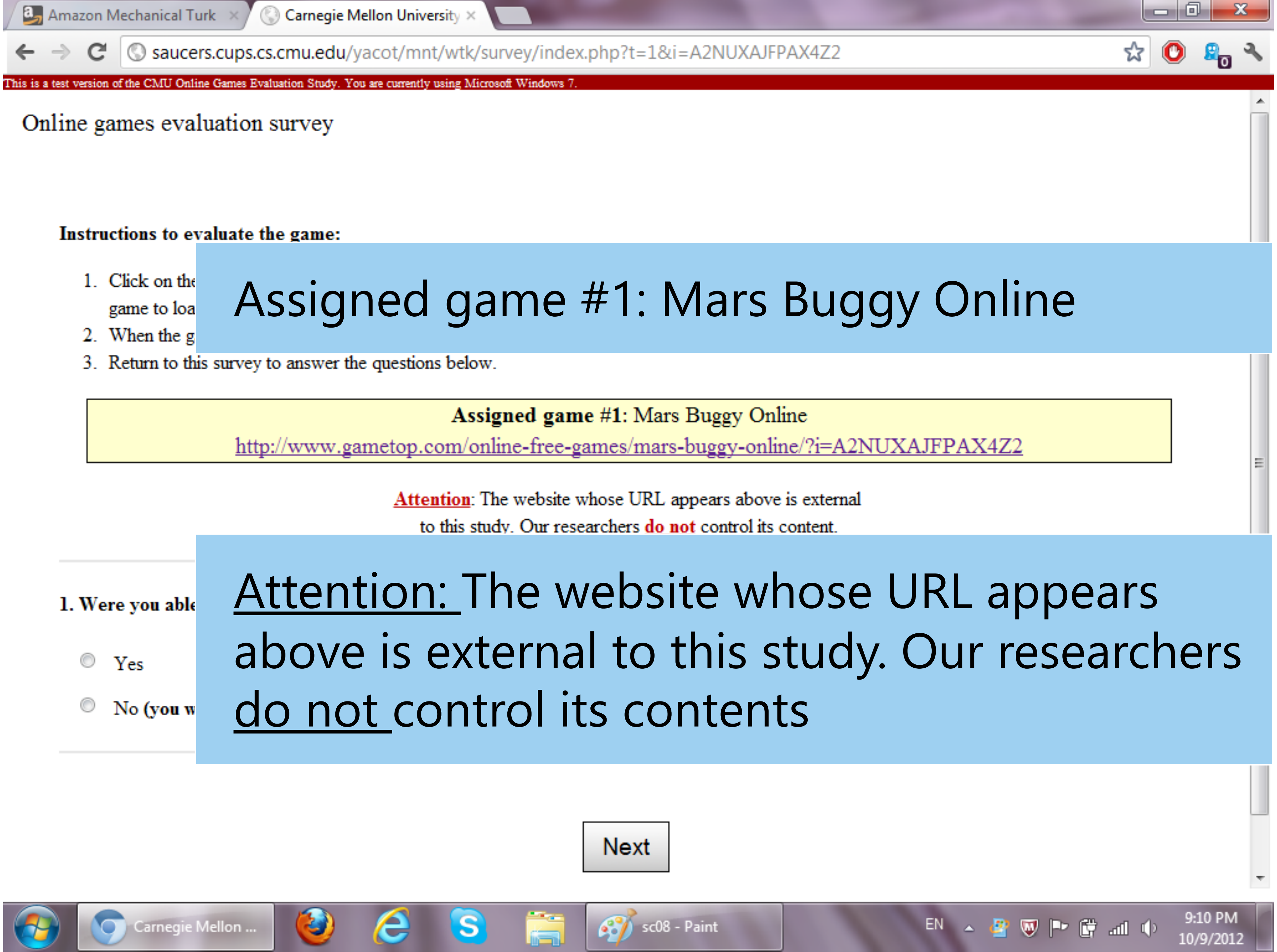
Risks, benefits, and compensation

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

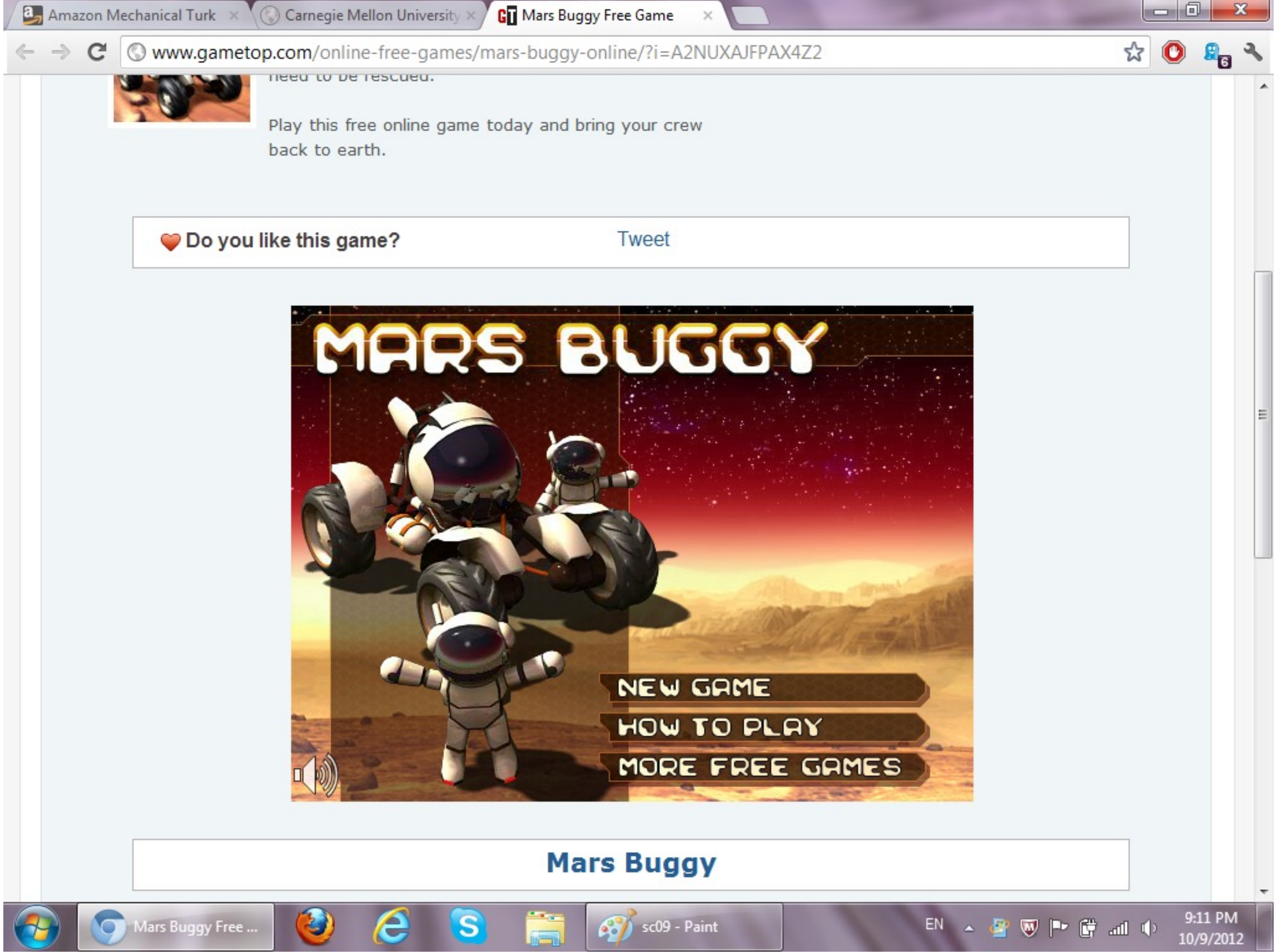
○ Yes

○ No (you w

Next

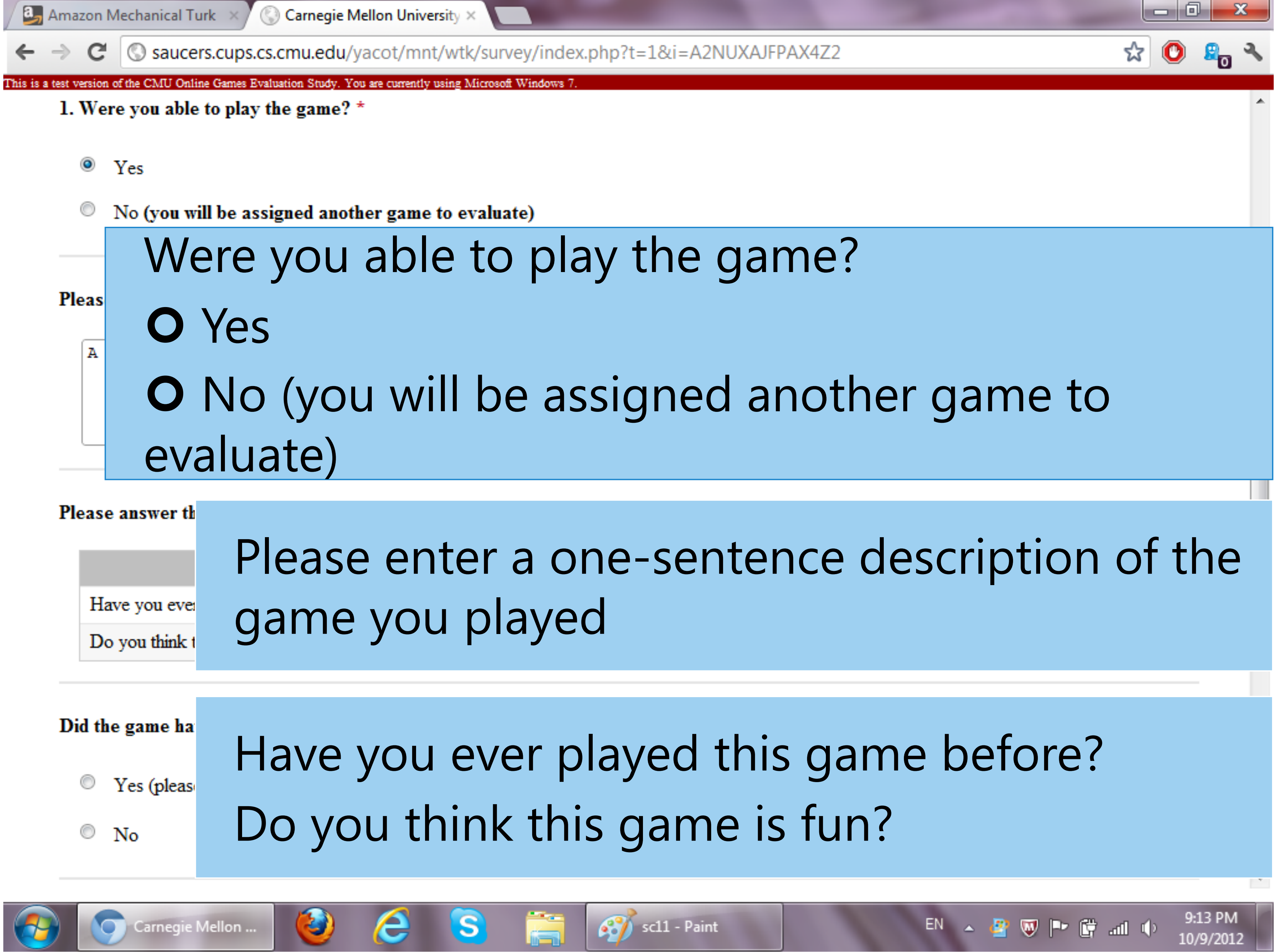
Assigned game #1: Mars Buggy Online

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


Amazon Mechanical Turk
Carnegie Mellon University
Mars Buggy Free Game
www.gametop.com/online-free-games/mars-buggy-online/?i=A2NUXAJFPAX4Z2

need to be rescued.

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


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

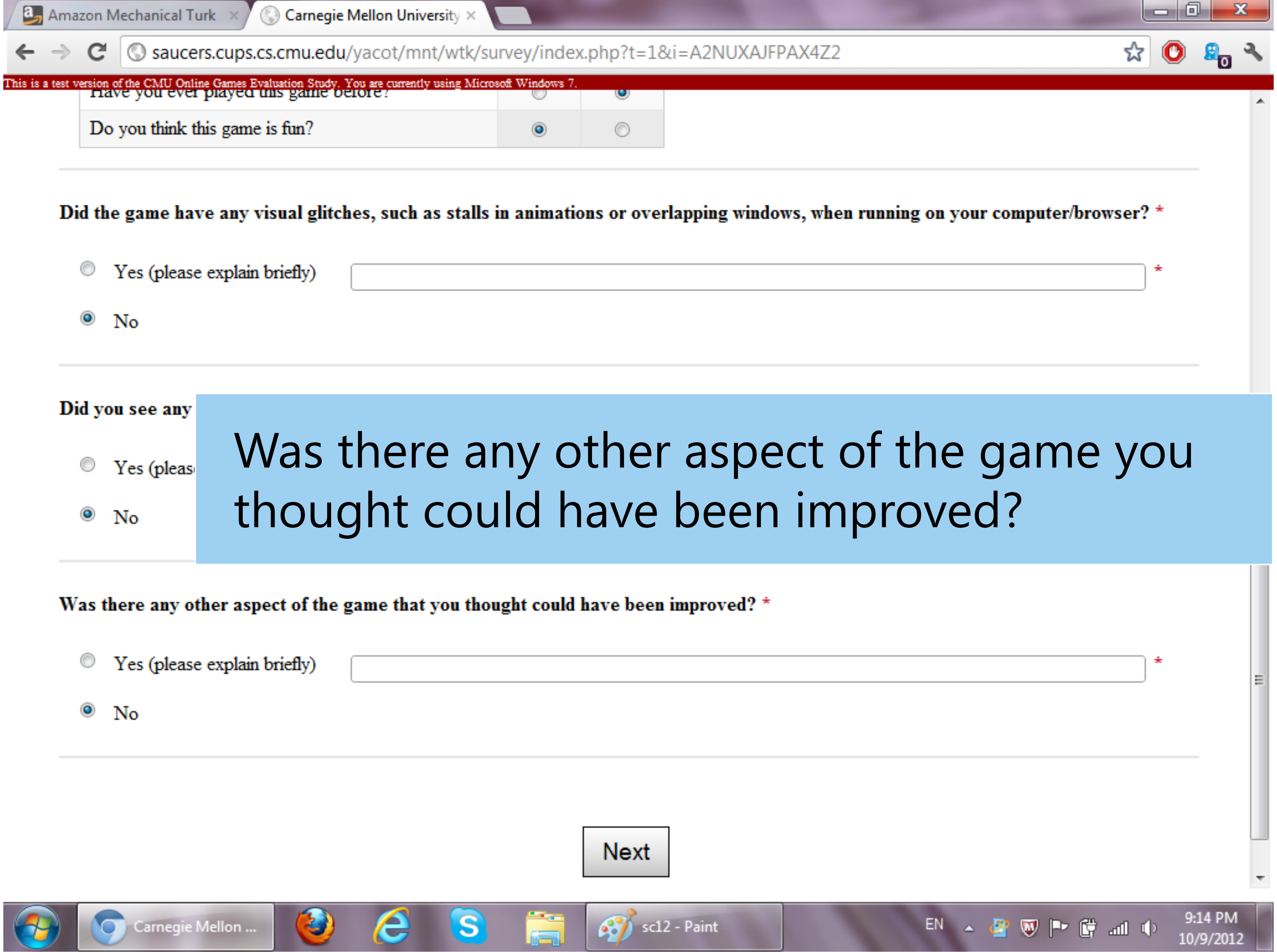
○ No (you will be assigned another game to evaluate)

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?

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



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

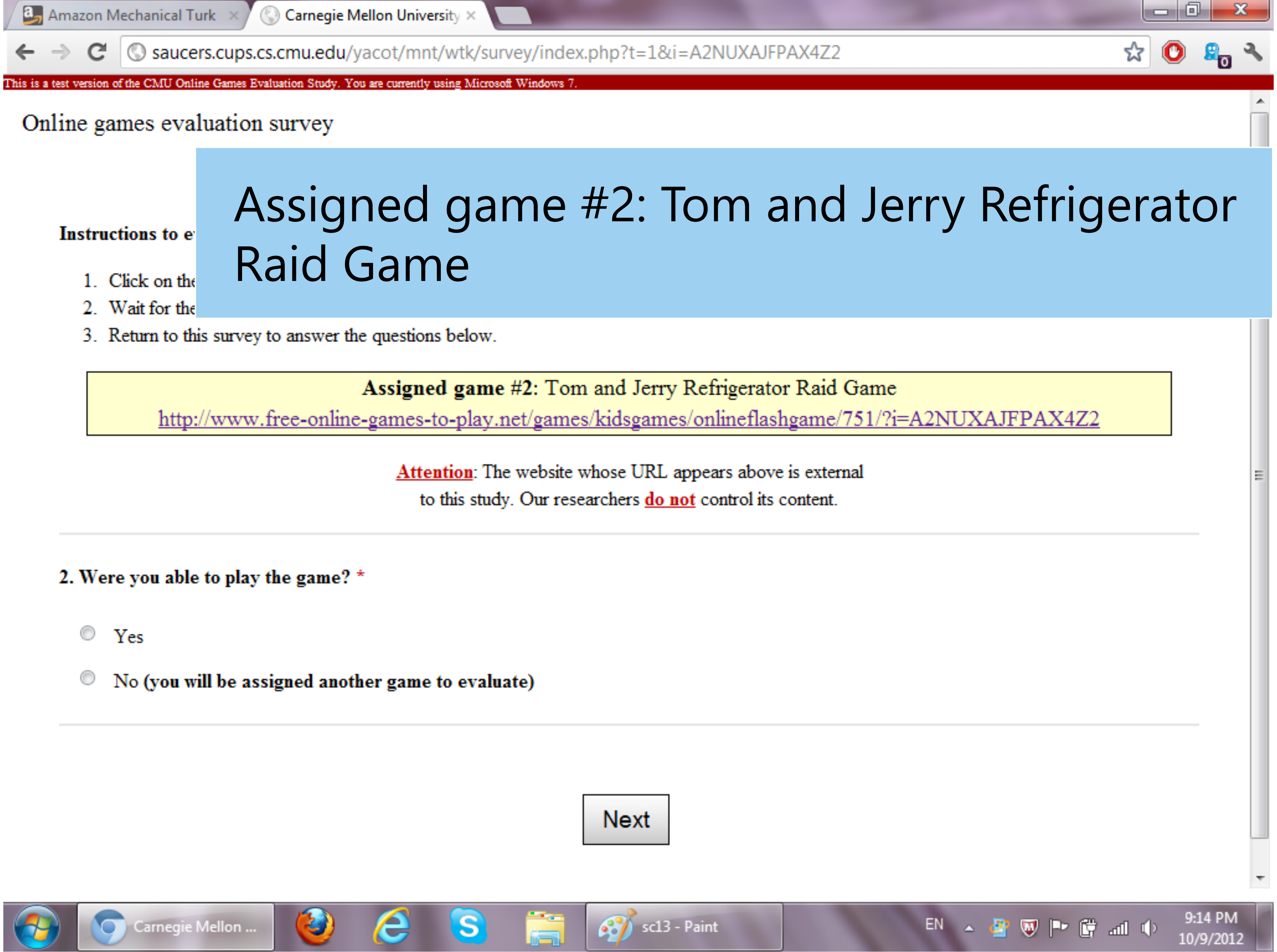
● No

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

○ Yes (please explain briefly) ______________________ *

● No

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.

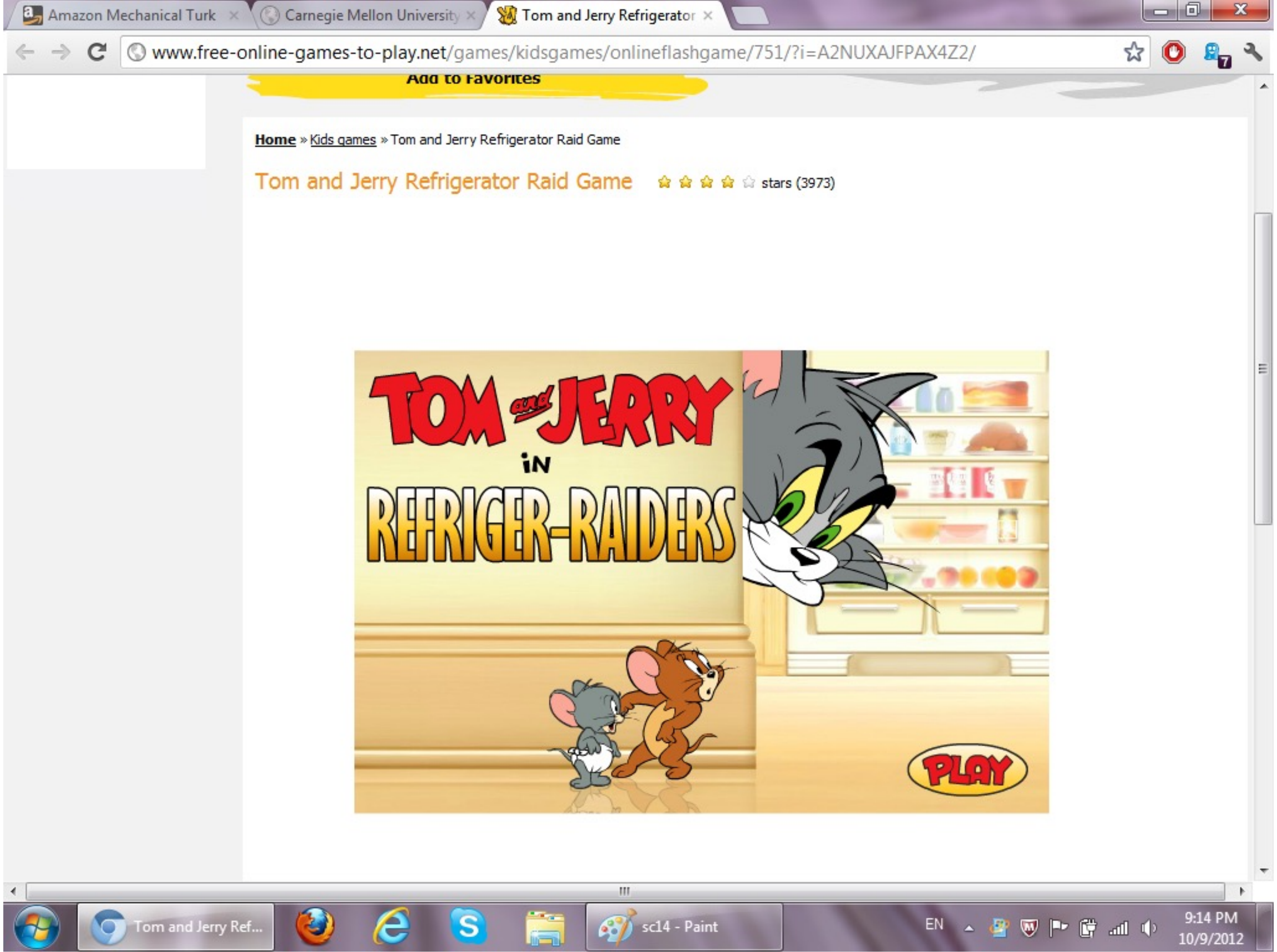
Assigned game #2: Tom and Jerry Refrigerator Raid Game
http://www.free-online-games-to-play.net/games/kidsgames/onlineflashgame/751/?i=A2NUXAJFPAX4Z2

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

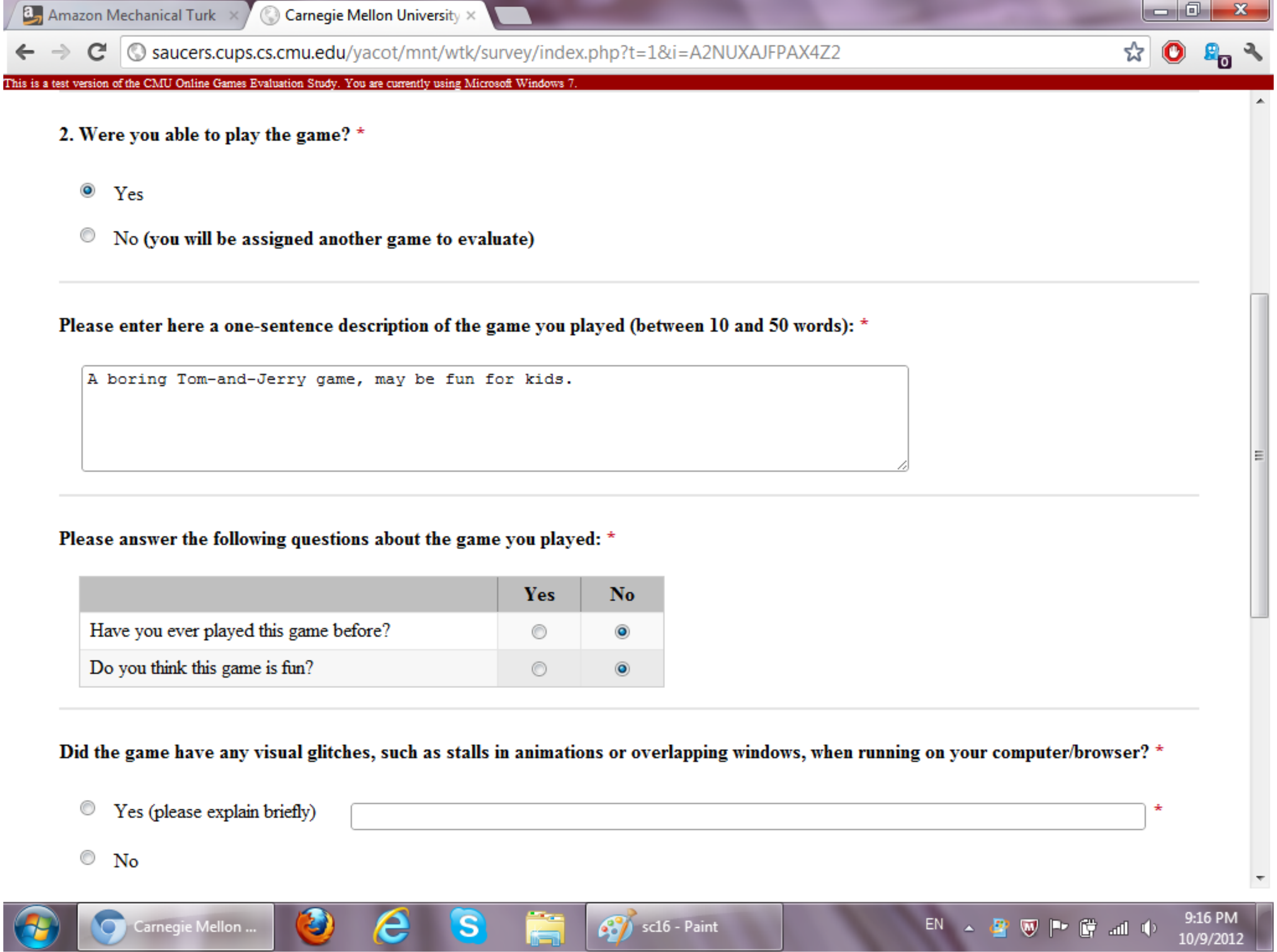
○ No **(you will be assigned another game to evaluate)**



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

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: *

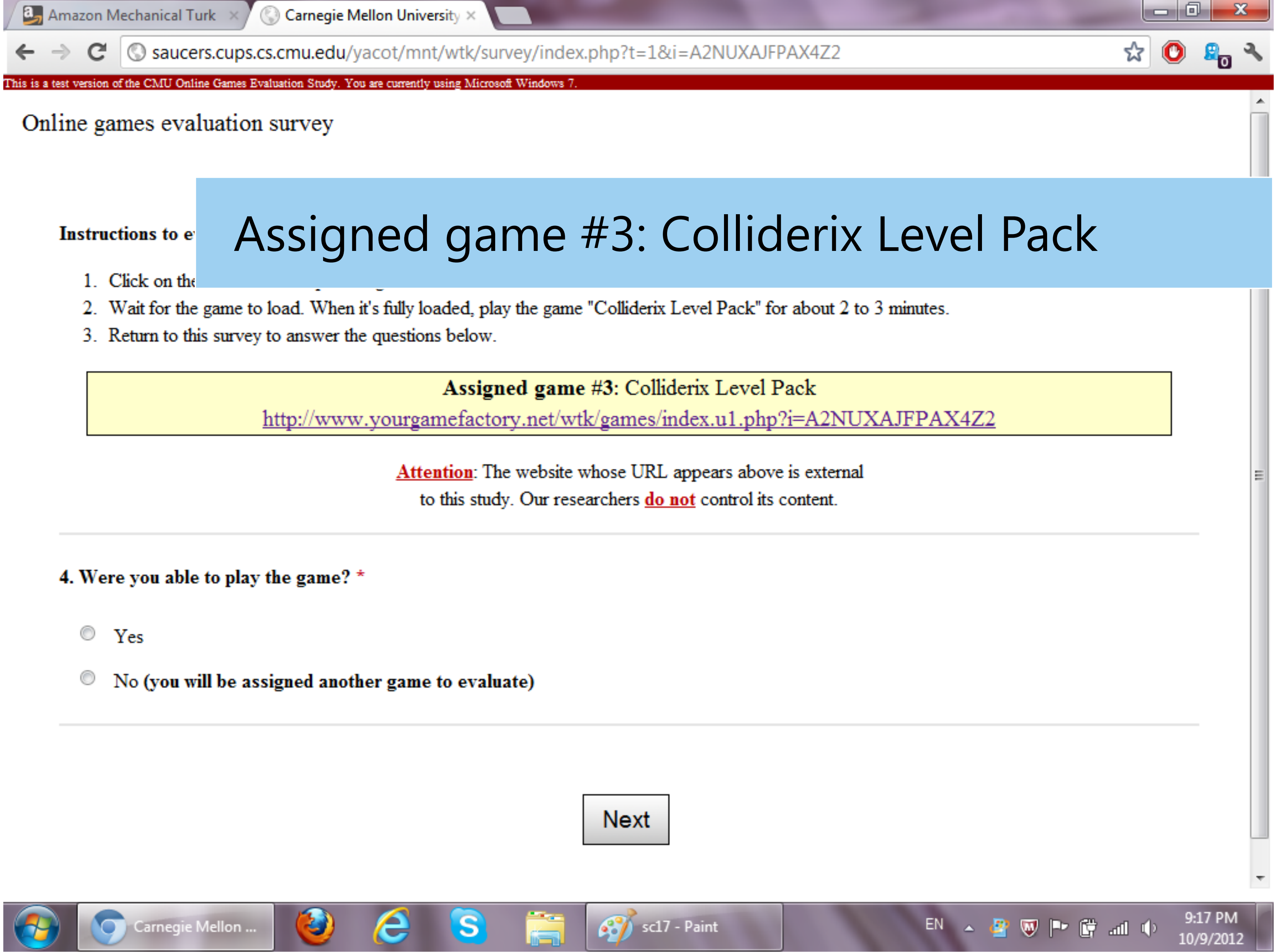
	Yes	No
Have you ever played this game before?	○	●
Do you think this game is fun?	○	●

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


Amazon Mechanical Turk
Carnegie Mellon University
saucers.cups.cs.cmu.edu/yacot/mnt/wtk/survey/index.php?t=1&i=A2NUXAJFPAX4Z2
Carnegie Mellon ...
sc17 - Paint
EN
9:17 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 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

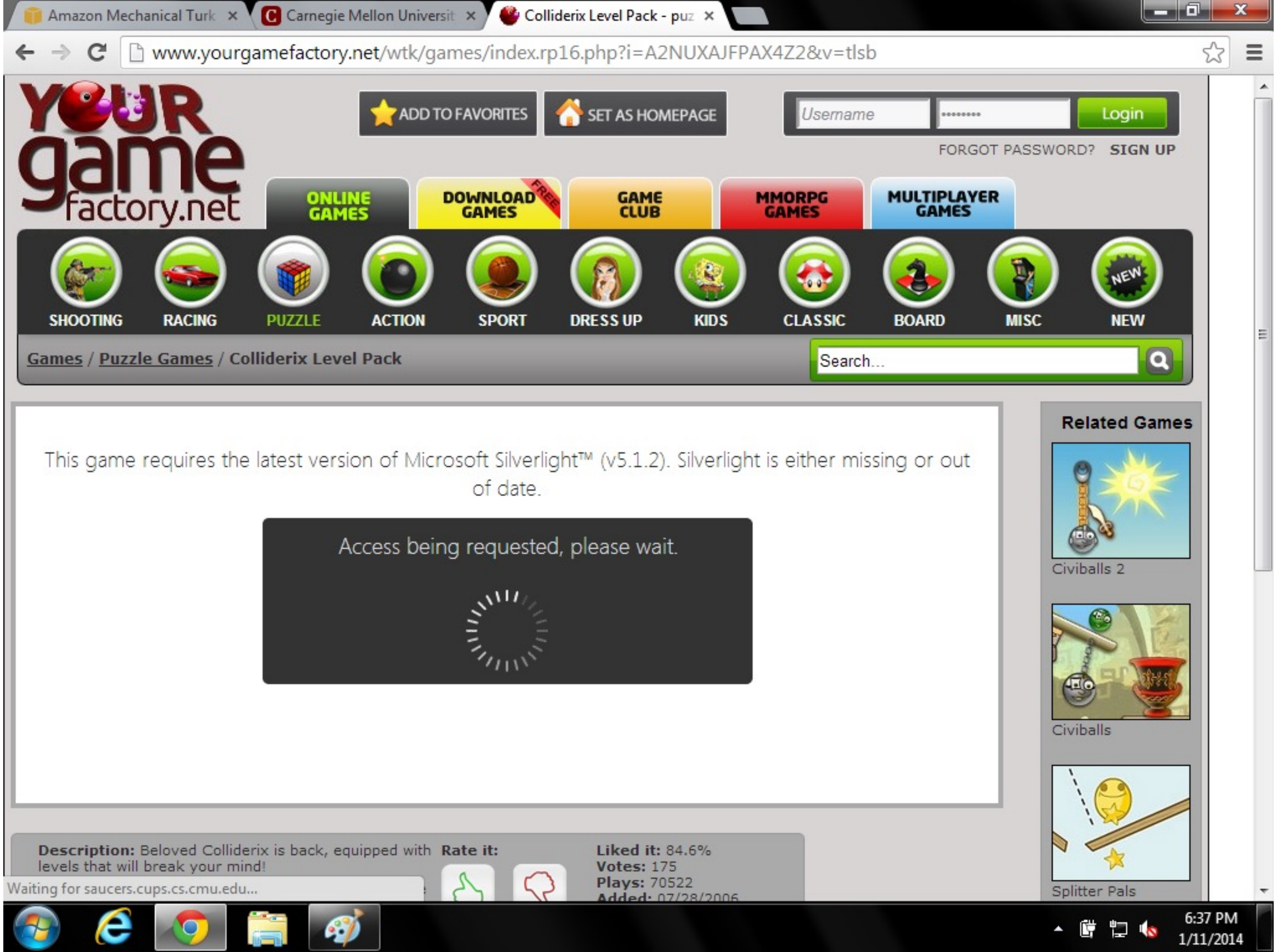
Attention: The website whose URL appears above is external to this study. Our researchers **do not** control its content.

4. Were you able to play the game? *

○ Yes

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

Next



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

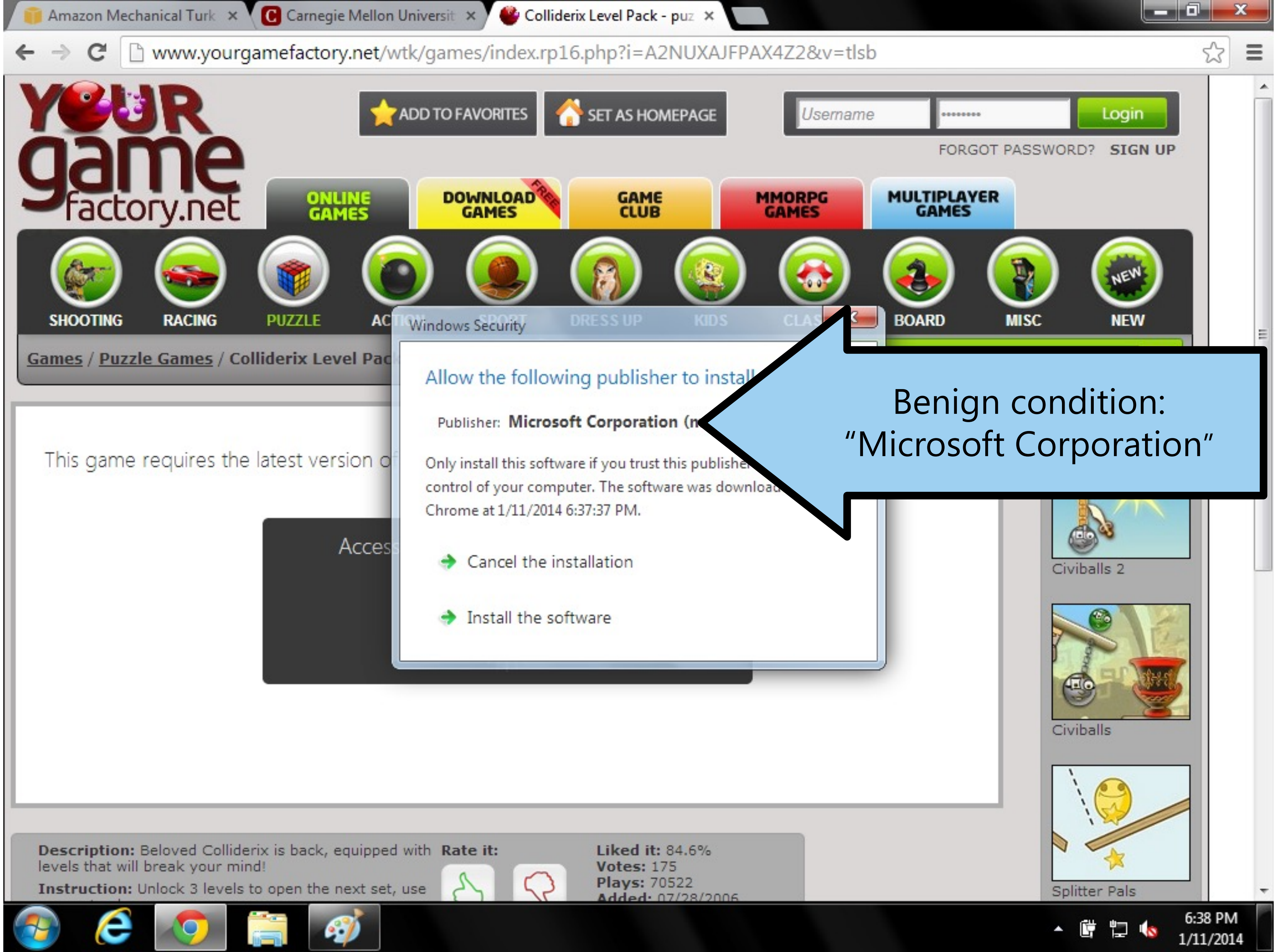
Access being requested, please wait.

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

Acces

Windows Security

Allow the following publisher to install

Publisher: **Microsoft Corporation (n**

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

➔ Cancel the installation

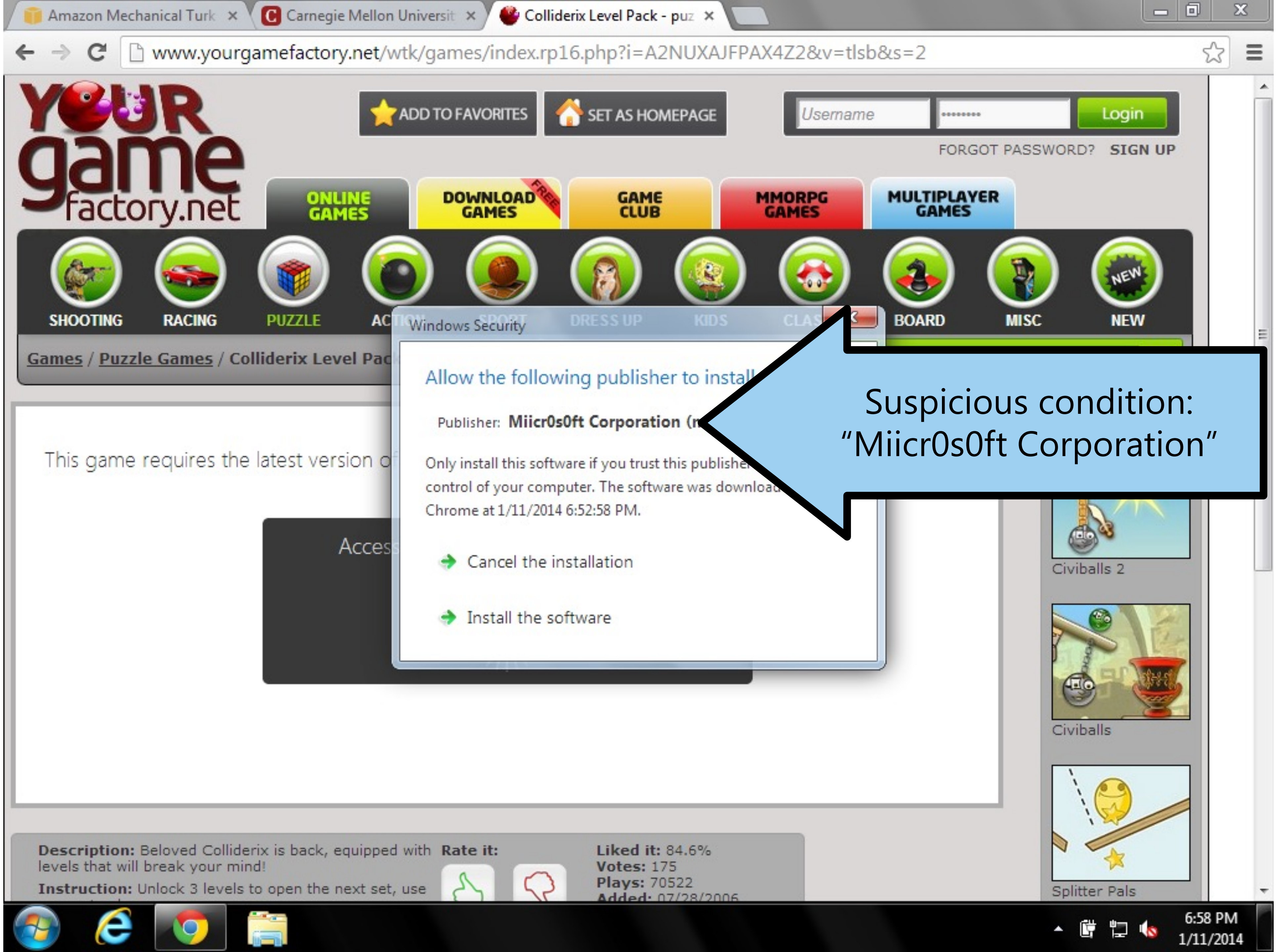
➔ Install the software

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

Instruction: Unlock 3 levels to open the next set, use

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 (**

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

➔ Cancel the installation

➔ Install the software

Suspicious condition:
“Miicr0s0ft Corporation”

Participant Decision Design

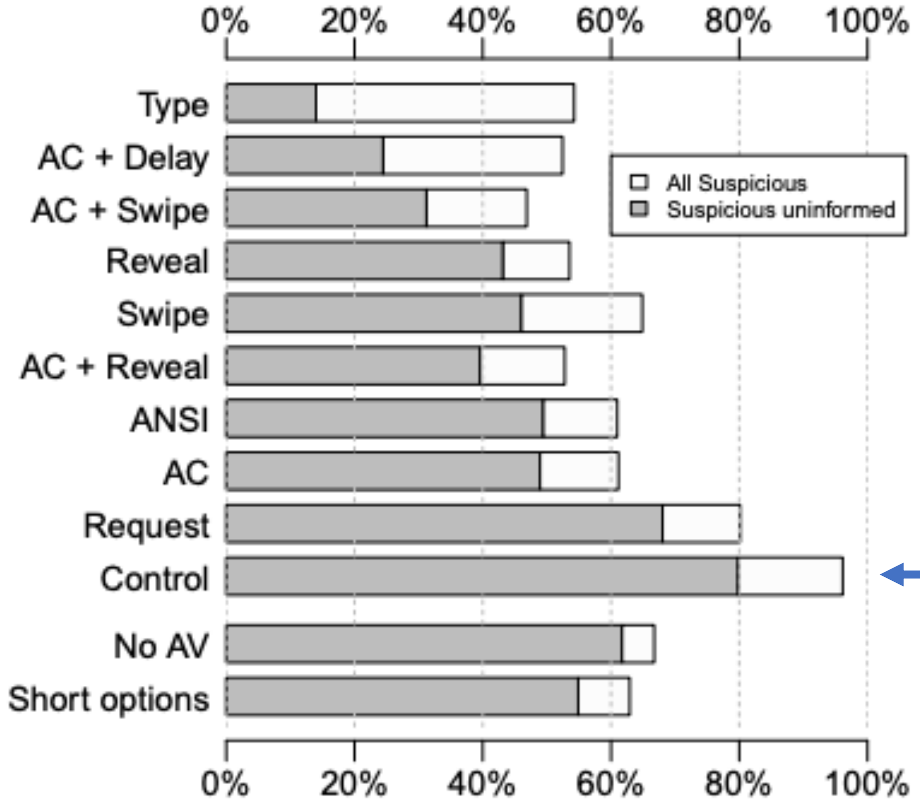
- Amazon Mechanical Turk
  - Must complete the task they accept (otherwise, don’t earn money)
    - Incentivized to finish an accepted task
  - Want to minimize the time and effort on each task
    - Opportunity cost

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

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

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

Some Results



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

All attractors work well

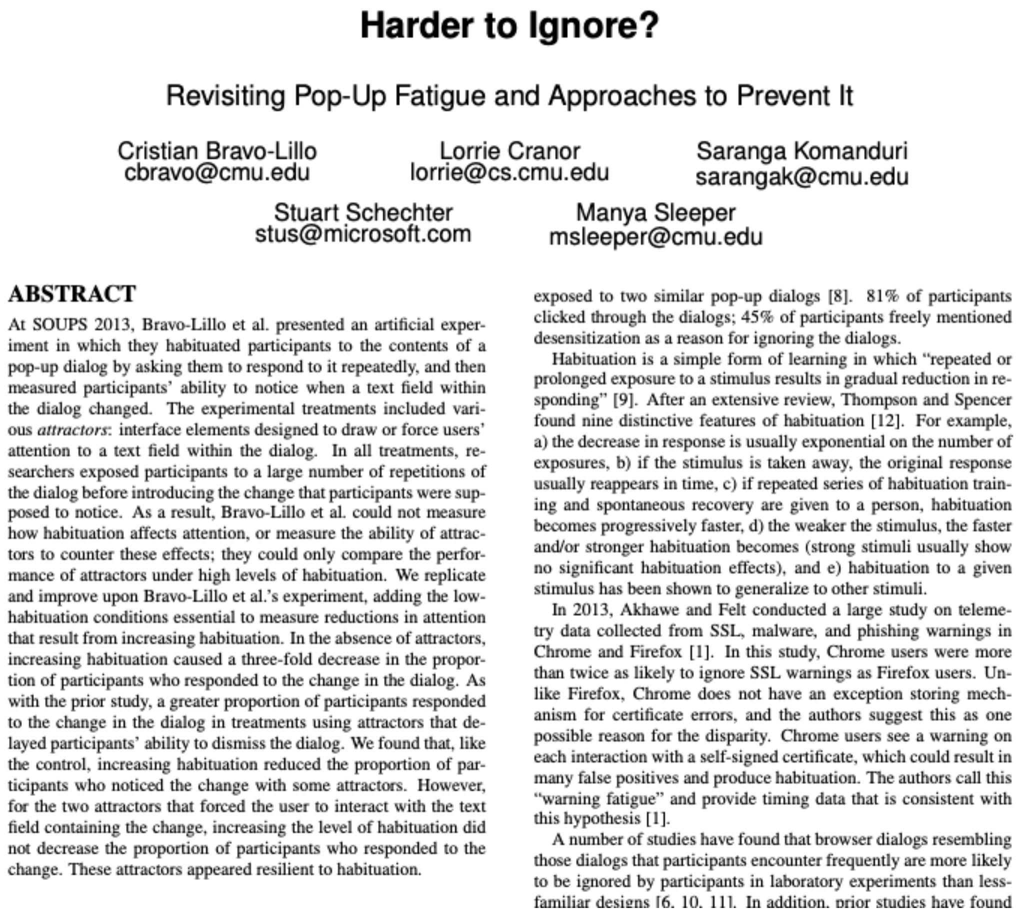
Control

What about habituation/fatigue?

- Test if attractors are still affective after habituation
  - High habituation
  - Low habituation

- Reused Attractors
  - Habituation period
  - Test period

SOUPS 2014



Harder to Ignore?

Revisiting Pop-Up Fatigue and Approaches to Prevent It

Cristian Bravo-Lillo
cbravo@cmu.edu

Lorrie Cranor
lorrie@cs.cmu.edu

Saranga Komanduri
sarangak@cmu.edu

Stuart Schechter
stus@microsoft.com

Manya Sleeper
msleeper@cmu.edu

ABSTRACT

At SOUPS 2013, Bravo-Lillo et al. presented an artificial experiment in which they habituated participants to the contents of a pop-up dialog by asking them to respond to it repeatedly, and then measured participants' ability to notice when a text field within the dialog changed. The experimental treatments included various *attractors*: interface elements designed to draw or force users' attention to a text field within the dialog. In all treatments, researchers exposed participants to a large number of repetitions of the dialog before introducing the change that participants were supposed to notice. As a result, Bravo-Lillo et al. could not measure how habituation affects attention, or measure the ability of attractors to counter these effects; they could only compare the performance of attractors under high levels of habituation. We replicate and improve upon Bravo-Lillo et al.'s experiment, adding the low-habituation conditions essential to measure reductions in attention that result from increasing habituation. In the absence of attractors, increasing habituation caused a three-fold decrease in the proportion of participants who responded to the change in the dialog. As with the prior study, a greater proportion of participants responded to the change in the dialog in treatments using attractors that delayed participants' ability to dismiss the dialog. We found that, like the control, increasing habituation reduced the proportion of participants who noticed the change with some attractors. However, for the two attractors that forced the user to interact with the text field containing the change, increasing the level of habituation did not decrease the proportion of participants who responded to the change. These attractors appeared resilient to habituation.

exposed to two similar pop-up dialogs [8]. 81% of participants clicked through the dialogs; 45% of participants freely mentioned desensitization as a reason for ignoring the dialogs.

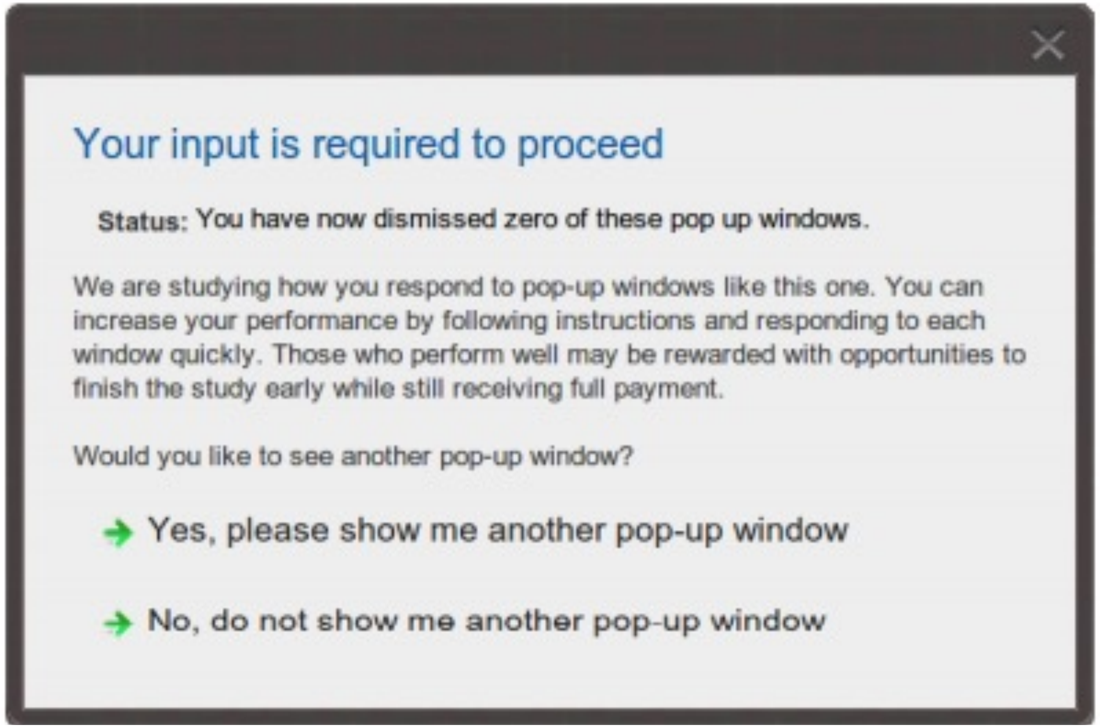
Habituation is a simple form of learning in which "repeated or prolonged exposure to a stimulus results in gradual reduction in responding" [9]. After an extensive review, Thompson and Spencer found nine distinctive features of habituation [12]. For example, a) the decrease in response is usually exponential on the number of exposures, b) if the stimulus is taken away, the original response usually reappears in time, c) if repeated series of habituation training and spontaneous recovery are given to a person, habituation becomes progressively faster, d) the weaker the stimulus, the faster and/or stronger habituation becomes (strong stimuli usually show no significant habituation effects), and e) habituation to a given stimulus has been shown to generalize to other stimuli.

In 2013, Akhawe and Felt conducted a large study on telemetry data collected from SSL, malware, and phishing warnings in Chrome and Firefox [1]. In this study, Chrome users were more than twice as likely to ignore SSL warnings as Firefox users. Unlike Firefox, Chrome does not have an exception storing mechanism for certificate errors, and the authors suggest this as one possible reason for the disparity. Chrome users see a warning on each interaction with a self-signed certificate, which could result in many false positives and produce habituation. The authors call this "warning fatigue" and provide timing data that is consistent with this hypothesis [1].

A number of studies have found that browser dialogs resembling those dialogs that participants encounter frequently are more likely to be ignored by participants in laboratory experiments than less-familiar designs [6, 10, 11]. In addition, prior studies have found

Two dialogs

How long until participants read the status message?



Your input is required to proceed

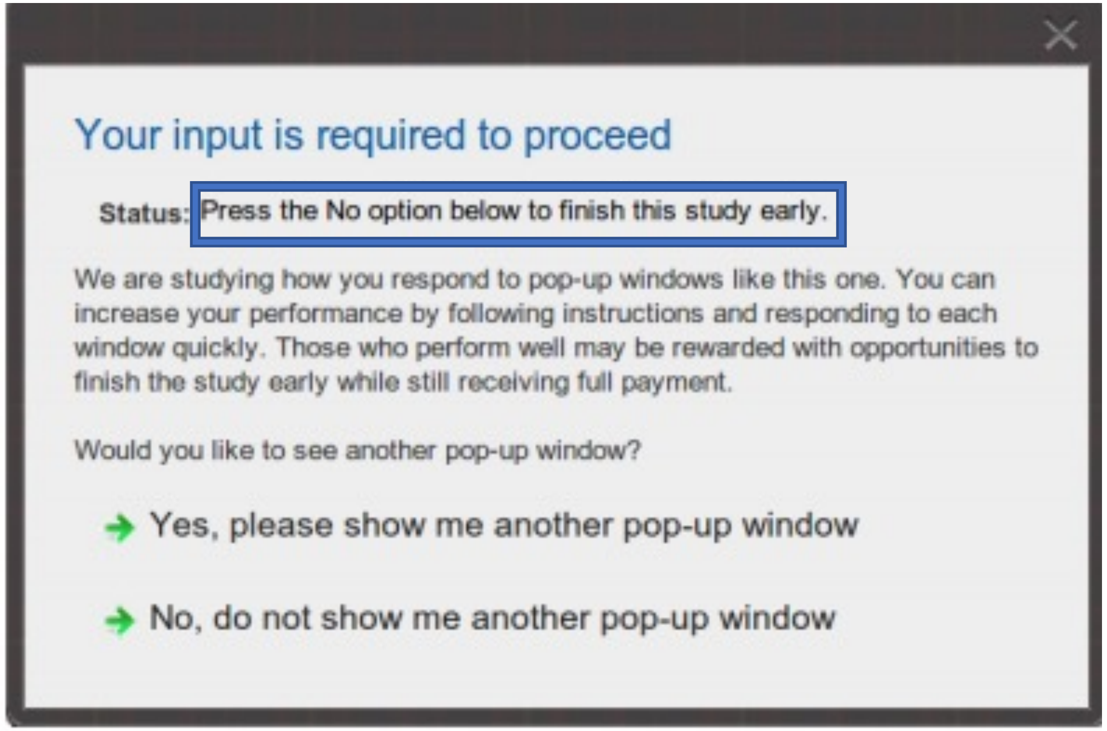
Status: You have now dismissed zero of these pop up windows.

We are studying how you respond to pop-up windows like this one. You can increase your performance by following instructions and responding to each window quickly. Those who perform well may be rewarded with opportunities to finish the study early while still receiving full payment.

Would you like to see another pop-up window?

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

habituation



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.

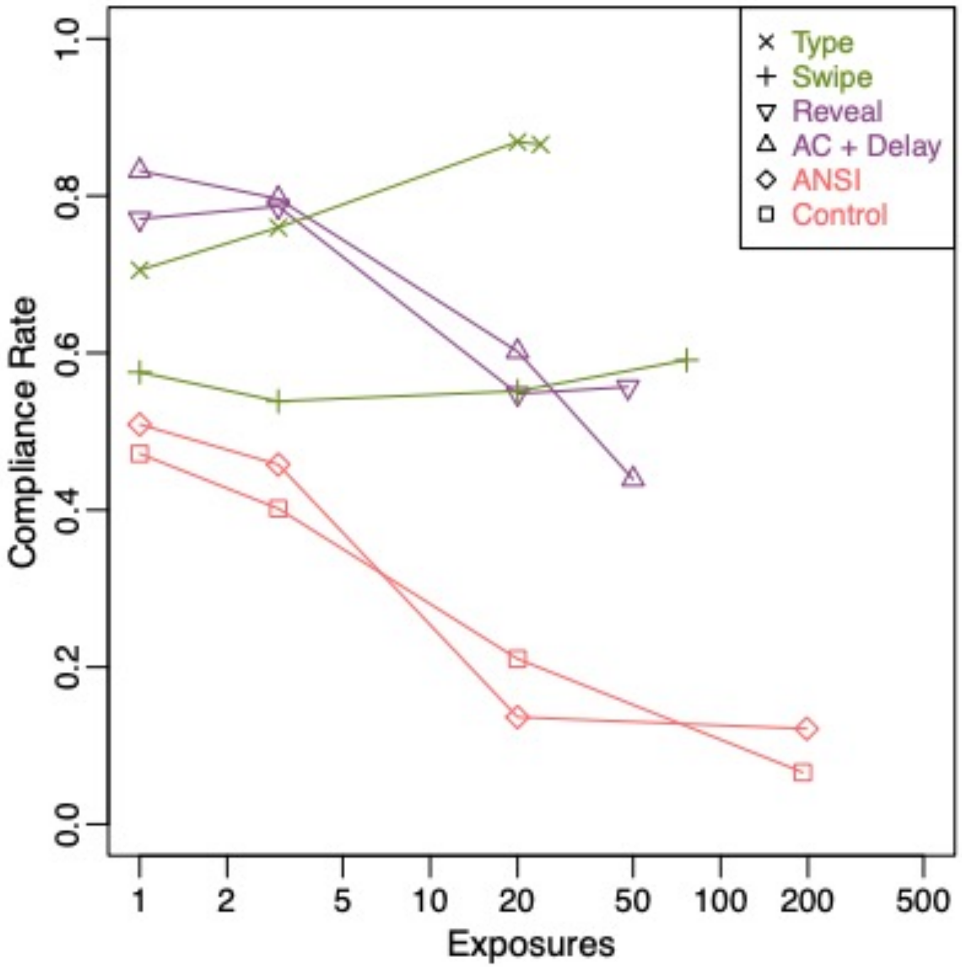
Would you like to see another pop-up window?

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

test

Some Results

Complied with “no” in the first dialog they were asked to do so



Interaction was less habituated with exposure

Delayed also habituated

ANSI Warnings and control showed dramatic habituatoin

The number of habituation exposures