06. Designing and Analyzing Quantitative Studies; Security Warnings

Blase Ur, April 12\textsuperscript{th}, 2017
CMSC 23210 / 33210
Today’s class

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

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

Find an interesting task

Work

Earn money

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

Fund your account

Load your tasks

Get results

Get Started
Security Warnings
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 omegafine.

Technical Crap  Cancel  OK
Users swat away warning dialogs

How can we get users to pay attention?
NEAT and SPRUCE (from Microsoft)

Rob Reeder, Ellen Cram Kowalczyk, and Adam Shostack. Poster: Helping engineers design NEAT security warnings. SOUPS 2011.


• NEAT – 4 questions to ask when you design a security or privacy UX

• SPRUCE – 6 elements to include in a security or privacy UX
  – Good advice, but sometimes it may be better to keep it short and simple rather than include all 6 elements
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?
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

For more info, contact neatux@microsoft.com
Alice in Warningland
Old Warning (IE 6)

Security Alert

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?

Yes  No  View Certificate
Slightly Newer Warning (IE 7)

There is a problem with this website's security certificate.

The security certificate presented by this website was issued for a different website’s address.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

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
Newer Warning (Firefox)

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.

- Get me out of here!
- Technical Details
- I Understand the Risks
Newer Warning (Firefox): Step 2

You are about to override how Firefox identifies this site. Legitimate banks, stores, and other public sites will not ask you to do this.

**Server**
Location: https://reddit.com/

**Certificate Status**
This site attempts to identify itself with invalid information.

**Wrong Site**
Certificate belongs to a different site, which could indicate an identity theft.

- [ ] Permanently store this exception

Confirm Security Exception  
Cancel
Newer Warning (Chrome)

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.

Proceed anyway  Back to safety

Help me understand
Alice in Warningland takeaways

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

• Passive warnings vs. interstitial warnings
• Consent and ethics
• Sampling bias
• Dealing with noisy data
  – Differences between Chrome and Firefox
• Certificate pinning
• HSTS (HTTP Strict Transport Security)
How do you know when you are actually at risk?
Some hazards are ALWAYS dangerous
Some hazards are context dependent
Computer security dialogs are context dependent

- Security warning dialogs more like warnings on wine than warnings on poison
- Software developers place burden of assessing risk on users
A good warning helps users determine whether they are at risk

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

• Encounter self-signed certificate (familiar experience for developers)
Risky context

• Put users in situation where they have something they care about at risk
  – Come to our lab and check bank account balance online

• Make users think they are actually at risk
  – Use web proxy to do man-in-the-middle attack
New plan

• Remove root certificate from browser
• Web site certificates can’t be verified
• Visits to secure sites will trigger warnings
Lab study challenges

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

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

Can you spot the suspicious software?

benign

suspicious
Key question: Do you trust publisher?

Name of publisher is critical information in trust decision
How can we get users to notice suspicious publishers?

• Use **attractors** to draw attention to publisher name
• Force delay before users can install
• Force interaction before users can install
• Force users to read publisher name
ANSI standard warning colors
Obstruct install button until user types publisher name
Do any of these work?

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

• Massive, inexpensive, quick
• Remote observation/recording of behavior
• Participants should feel safety/risk and behave as they would in real life
• But should not actually be at increased risk through participation in experiment
Use Mturk game ruse

- Ruse previously developed for study of whether users would fall for fake OS password dialogs

Operating System Framed in Case of Mistaken Identity: Measuring the success of web-based spoofing attacks on OS password-entry (ACM CCS 2012)
Online games evaluation survey

Purpose of the study

This survey is part of a research study conducted by Dr. Julie Downs at Carnegie Mellon University. The purpose of this study is to evaluate online games according to criteria that will be explained in the next pages. You will be asked to go to websites, play a game for 2 to 3 minutes, then return to this survey to give us your opinion on each. The whole survey should take you between 15 and 20 minutes in total.

Participants requirements

Participation in this study is limited to individuals age 18 and older. You have to physically be in the United States of America to be eligible to participate in this study, and not having taken before any early version of the same survey.

Risks, benefits, and compensation

The risks and discomfort associated with participation in this study are no greater than those ordinarily encountered in daily life or during other online activities. There may be no personal benefit from your participation in the study but the knowledge received may be of value to humanity. You will receive $1.00 as a compensation for participation in this study. There will be no cost to you if you participate in this study.

The data captured for the research does not include any personally identifiable information about you. We will collect your IP address only to check whether you qualify for the study.

Confidentiality

By participating in this research, you understand and agree that Carnegie Mellon may be required to disclose your consent form, data and other personally identifiable information as required by law, regulation, subpoena or court order. Otherwise, your confidentiality will be maintained in the
Online games evaluation survey

Instructions to evaluate the game:

1. Click on the link to load the game.
2. When the game loads, open it and play it.
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 contents.
Play this free online game today and bring your crew back to earth.

Do you like this game?
1. 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? 

- Yes (please enter your description)
- No

Do you think this game is fun?

- Yes
- No
Was there any other aspect of the game you thought could have been improved?
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)
Tom and Jerry Refrigerator Raid Game

Tom and Jerry in Refriger-Raiders

PLAY
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: *

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have you ever played this game before?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you think this game is fun?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

- Yes (please explain briefly)  
- No
Online games evaluation survey

Instructions to evaluate game:

1. Click on the link to open the website.
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?id=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)
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.
Benign condition: “Microsoft Corporation”
Suspicious condition: “Miicr0s0ft Corporation”
Participant decision design

• Workers in Amazon's Mechanical Turk aim to:
  – Complete the tasks they accept (otherwise, don't earn money)
  – Minimize the time and effort in each task (each accepted task has an opportunity cost)

• Our message to participants:
  – “You may skip a game. If you do, we will assign you another”

• The decision was designed to gamble time/money for security:
  – Install → Take small risk, play the game, finish sooner
  – Not install → Not take any risks, not play the game, waste time
Results are encouraging

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

• Explain what the actual purpose of the study was