12 – Security
Warnings

Lorrie Cranor

February 27, 2017

05-436 / 05-836 / 08-534 / 08-734 / 19-534 / 19-734
Usable Privacy and Security
Today’s class

- Project feedback
- Evaluating security warnings
- NEAT and SPRUCE
- Design your own warning
Project feedback

- All teams should have received feedback
- From here on out, you should plan to check in with Lorrie, Javed, or Abby about once per week (via email or arrange a meeting) to go over study protocols, surveys, IRB submissions, etc.
- IRB protocols need to be submitted by March 6
- We suggest you start working on IRB protocol ASAP and go over it with us by Friday
Evaluating security warnings
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.

[View Certificate] [Cancel] [OK]
Something happened and you need to click OK to get on with doing things.

Certificate mismatch security identification administrator communication intercept liliputian snotweasel foxtrot omegaronce.
Users swat away warning dialogs

How can we get users to pay attention?
2007 Phishing warnings study

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
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/
Success!

• Most participants got phishing
• 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”
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
2008 SSL certificate warning study

- Test SSL certificate warnings
- Design a better warning

How do you know when you are actually at risk?
Some hazards are ALWAYS dangerous
Some hazards are context dependent
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)
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
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
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
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
Animated connector
Slow reveal

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
Obstruct install button until user types publisher name
Do any of these work?

• Do attractors and other techniques prevent suspicious installs without preventing benign installs?

• How much do attractors delay benign installs?
Methodology requirements

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

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

Operating System Framed in Case of Mistaken Identity: Measuring the success of web-based spoofing attacks on OS password-entry (ACM CCS 2012)
Amazon Mechanical Turk

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
Online games evaluation survey

Carnegie Mellon University

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 below and select the game to load.
2. When the game loads, play the game for a few minutes.
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 to load the game on your device?
   - Yes
   - No (you will not be able to complete the survey)

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

Do you like this game?

Mars Buggy
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
   - No

Do you think this game is fun?
   - Yes
   - No
Was there any other aspect of the game you thought could have been improved?
Online games evaluation survey

Instructions to evaluate the game:

1. Click on the link to the game.
2. Wait for the game to load.
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)
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></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
Assigned game #3: Colliderix Level Pack


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 \(\rightarrow\) Take small risk, play the game, finish sooner
  – Not install \(\rightarrow\) 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
But what would happen if users saw these attractors repeatedly?

- Conducted more experiments
- Scenario in which participants had to dismiss a dialog repeatedly for several minutes until the dialog changed
- Measured rate of compliance with changed dialog
- Showed that some attractors performed better than control in presence of habituation
- “Harder to Ignore?” paper: Can attractors actually eliminate or reduce effects of habituation?

Habituation experiment

• Show a dialog repeatedly with irrelevant message
• Ask participants to click “Yes”
• Change salient field to “Click on No”
• Check if participants notice the change and click “No”
Those who perform well may be rewarded with opportunities to finish the study early while still receiving their full payment.
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
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
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
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
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
You finished the task. You will be redirected to the rest of the survey in a few seconds. Please wait...
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
“Harder to ignore” experimental design

• \(\{6 \text{ dialogs}\} \times \{4 \text{ exposure conditions}\} = 24 \text{ conditions}\)
  – Dialogs: Control, Swipe, Type, AC + Delay, Reveal, ANSI
  – Exposure to 'irrelevant message': 1 exposure, 3 exposures, 20 exposures, 150 sec. of exposure

• Two phases:
  – Habituation phase: participants are shown irrelevant message, they could only click on “Yes”
  – Test phase: participants are asked to click “No”

Control and ANSI decline with habituation

![Graph showing the decline of compliance rate with exposures for both ANSI and Control groups.](image-url)
Reveal and AC+Delay start out better, decline with habituation
Swipe and Type are resilient to habituation

Could not predict difference between green and purple lines from previous experiments
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
Analyze with NEAT SPRUCE

Your web browser thinks this is a phishing web site. Do you want to go there anyway?

- Necessary
- Explained
- Actionable
- Tested

- Source
- Process
- Risk
- Unique knowledge
- Choices
- Evidence
Class assignment

• USB flash drives can spread infections in a number of ways. See http://www.cioinsight.com/security/the-dangers-of-unsecured-usb-drives

• Attackers may distribute infected flash drives by leaving them around where employees of a target company are likely to pick them up. In addition, a user who uses a flash drive to exchange files with another user whose machine is already infected, may pick up the infection on the flash drive and bring it to their own machine. Some companies are prohibiting their employees from using flash drives, but others are just asking their employees to be careful.

• Imagine a security tool that runs on a user’s computer and monitors the USB ports, looking for programs that run automatically when a flash drive is plugged in. When an autorun program is detected it prevents it from running and displays a warning. The warning dialog offers users the option of letting the program run.

• Your first task (to be done in class) is to design the warning using the design tool at: http://saucers.cups.cs.cmu.edu/woda/

• You may do this yourself or work with someone else. If you are not in class, do this at home. Use the NEAT and SPRUCE guidelines as you develop your design.
Homework assignment

• Your next task (to be done at home and turned in with your homework) is to critique someone else’s warning. Go to http://saucers.cups.cs.cmu.edu/woda/

• Critique the warning that was submitted immediately before yours. If you submitted the first one then critique the last warning submitted. Please write one bullet point addressing each of the NEAT and SPRUCE messages. Then briefly discuss any additional factors you think might be relevant that are not addressed by NEAT and SPRUCE.