

INFO2222 Assignment 1 – Helping Sydney University students learn about phishing

Due: 11:59pm, Week 7, Wednesday 25th April, 2018

(This is the Anzac Day public holiday.)

Submit: Report should be submitted as a PDF via Canvas

Assessment:

- This work will be assessed with Turnitin.
- This assessment is worth 10% of your overall grade.
- This is a group assignment
 - The ideal group size is 5 students.
Groups are not to be less than 4, nor greater than 6 students.
 - Groups are formed in Week 4 labs (except the Friday which did this in week 3)

Goals:

- Practice in all the core usability methods studied for determining user needs, design and evaluation
- Written presentation skills
- Group work skills

Description

The situation of concern: The University of Sydney is concerned about phishing.

Transformation: To provide new approaches to phishing education for **students** at the University of Sydney.

The **basic solution to the assignment** requires your group to design a set of webpages to help a University of Sydney student understand:

- the risks of phishing;
- the attributes in mail that should trigger suspicions – where the basic set is:
 - social engineering in at least 2 forms your group selects (e.g. creating a sense of urgency);
 - URL is obviously implausible;
 - URL is plausible but on careful examination it is not quite right;
- Techniques to check mail systematically, to determine if a link is likely to be dangerous.

A basic solution to this assignment could take many different forms, however the self-test website you worked through in Mini-Assignment 2 could form a basic model or starting point.

For the **basic solution to the assignment**, your group must:

- Create a persona for the Sydney University student that your group will focus on (your tutor will allocate different personas to different groups in the class);
- Create a set of email messages designed for teaching people, which matches your persona. Each person in your group is to create a pair of email messages, 1 authentic and 1 phishing for use as part of the teaching;

- Design and build an interface, as a set of webpages, making use of your set of email as well as one for the broader risks of phishing – you may use any tool your group wishes for this e.g. Wix, Google-sites, etc.;
- Conduct at least 3 user evaluations across the complete set of pages created by the group, and write up the results. Students should work in pairs to perform user evaluation as described in lectures and below (pre- and post-test, think-aloud usability).

Grading of the report

- 10% - **Overall structure, quality of writing** including:
 - Cover page with student names and email addresses;
 - Contents page so that the tutor can easily navigate to each part;
 - List of relevant URLs (for your website) – so the tutor can navigate to particular sections easily;
 - High level organisation and structure;
 - Appropriate grammar, spelling, and punctuation;
 - For full marks it should be a delight to read – very clear, concise, complete, easy for the tutor to find each aspect in the order listed in this grading outline.

- 10% - **Persona** - a good solution should fit on 1 page using 12-point font.

Your persona should include:

- Name
- Photo
- Mental model: worldview, detailed goals, current knowledge - relevant to learning about phishing.
- Context and constraints (including the nature of authentic email that this student persona is likely to receive)
- A clear focus on University of Sydney students

Make sure this matches the person agreed with your tutor in Week 4 – if your group wants to revise this after Week 4, that must be done no later than the end of the Week 5 lab and you need to explain to your tutor why you want to alter it. The tutor will grade this against their notes about the persona allocated to our group.

- 10% - A list of **learning goals** your interface aims to teach.
 - Table with columns for
 - ID – an “identifier” you can use through the report to annotate interface screenshots and generally refer to a learning goal. (e.g. link-similar-to-authentic)
 - A brief description of the learning topic (e.g. 1. Link name is similar to the authentic URL for the actual site)
 - Relevance to Sydney University students
 - IDs of mail items used to teach this topic (e.g. phish1-link-sender)
 - IDs of interface pages where this is taught
 - This must include all the learning goals listed above for the “basic assignment” –if you omit any, make clear that you realise this as a shortcoming of your solution
 - Make clear any additional learning objectives your group has incorporated.

- Clear focus on University of Sydney students
- Clear focus on any special aspects of your persona
- 10% - **Set of mail items**
 - Summary table for the mail items, with columns for:
 - ID (e.g. Mail-1-phish, Mail-2-safe);
 - brief description of the relevance of the email for teaching goal(s) (e.g. Link name is similar to authentic URL, Sender name is implausible for purported sender);
 - Brief explanation of how it matches the persona;
 - **Name of the team member who created this mail item*.**
 - Annotation and clarification of each mail item explaining key features of the mail item, in terms of **what it teaches** and how it matches the **persona**.
 - Quality of the design of the mail items – for the lesson that they are used to teach and the match to the persona (this relies on how well you did the annotation PLUS how well the mail items were designed.)
 - Clear focus on University of Sydney students
 - Clear focus on special aspects of your persona
- 10% - **Design of the interface website**
 - Screenshot of each page of the website with
 - annotations to explain key features of the design for **teaching effectiveness**
 - annotations to explain key features of the design for **usability**
 - labels, as needed, so that later parts of the report
 - Clarity of the annotation of each screenshot in the actual interface
 - Quality of the design for teaching
 - Quality of the design for usability
 - Clear focus on University of Sydney students
 - Clear focus on special aspects of your persona
- 10% - **Detailed materials and recordings for think-aloud testing, for each participant.**
This should include:
 - Heading materials
 - Participant ID (e.g. P1) NOTE: Please do not give actual names.
 - Brief statement of how well this participant matches your persona
 - **The name of team members who conducted this user study*;**
 - Actual pre-test and post-test written by participant ** (see below)
 - Table with observations from think-aloud for each participant with columns for:
 - Mail ID;
 - Notes on mail features the user correctly identified as suspicious and why they thought this;
 - Notes on mail features incorrectly identified as suspicious by the user – what these were and why they were identified.
 - Summary of things this user missed – based on checking the notes above against the features in the email
 - Summary of key lessons from this participant:
 - What the participant already knew before the study;

- Observations as the participant worked through the materials;
 - What the participant learnt from the materials, based on both the observations and the post-test, with comments about the discrepancies between these;
 - Timing details: how long it took to complete the pre-test, work through the interface, and complete the post-test.
- 10% - **Summary of key lessons from the user study** from the whole group
 - Table summarising key results gained from at least 3 participants;
 - Comparison with actual evidence;
 - Clear and easy to follow.
- 20% - **Tutor evaluation of the interface** of the teaching website, based on the tutor doing a walkthrough assessing:
 - Essential requirement: is it really well targeted for Sydney University students?
 - Essential requirement: did the actual system match the annotated screenshots?
 - Does it have good usability?
 - Does it match the annotated screenshots in the report?
 - Is it particularly easy for a user to work through efficiently?
 - Is it particularly pleasing (perhaps even fun) to use?
 - For full marks we should be keen to send it to ICT for use in their real teaching at the university.
- 10% - for going **beyond the basic solution**.
 - **Only applies if the total mark for parts above > 70 out of 90;**
 - For additional aspects in your interface, e.g. additional interactivity in the teaching at the website, going beyond the basic in the teaching to go into topics like mail headers.
 - Makes a clear statement of how the solution goes beyond the basics.
 - Rationale for these additions – for usability, for teaching effectiveness or for deeper evaluation

Notes:

1. The format for each part will be presented and explained in the lectures and the labs.
2. **Items marked * are for the individual contributions to the project.**
 - *Each student must complete all of these to be eligible for the group mark.*
 - *Failure to contribute to the group will result in a mark of zero.*

**** Pre- and post-test for basic solution** (as in Week 3 slides):

- Please write a brief description of what phishing means.
- Please explain the risks that phishing can pose for you.
- Please state the attributes in mail that would make you suspect that it may be phishing.
- Please state how would check mail before clicking on a link.