PROJECT: CREATING AN EDUCATIONAL TOOL FOR PHISHING AWARENESS

Cardiff University School of Computer Science and Informatics

ABSTRACT

The project will aim to deliver a software tool that will be used for phishing and spam awareness training. This initial report layout the aim, objectives and the initial plan for the successful completion of the project

PROJECT DETAILS

Author: Emma Hall

Supervisor: Amir Javed

Moderator: Federico Liberatore

Module code: CM3202

Credits: 40

Contents

Project Purpose

Phishing attacks are prevalent within todays society. Whilst technological advancements attempt to support the prevention of phishing emails from even entering our mailboxes, these aren't always "air-tight" solutions. In conjunction with this, and whilst security solutions that work to prevent these attacks increase, the sophistication of phishing emails increases equally. No longer are we faced with the emails that simply read, "click here to win 10,000 million pounds!" but are beginning to encounter more complex means of attackers asserting our information such as imitation emails like Netflix password reset emails, an email from HR department, emails from friends etc[1].

As such, many people can fall victim to these attacks, and it can often be a result of not understanding the traits of these emails or even their existence. The 2020 statistics posted by security boulevard on December 7th determine that 97% of users are unable to recognise a sophisticated phishing email[2]. The detrimental impact falling victim to these attacks is exponentially heightened in companies who work with or store sensitive data including customer credit card details. As majority of businesses have moved online due to the Covid-19 pandemic, it is more important now than ever to educate people, especially the aforementioned companies, on what to be aware of when receiving emails. Statistics dictate that during the pandemic there has been an influx of cybercrimes with phishing and scams being a major player[3] and hence there is a substantial need for educational phishing resources.

Project Description

The main deliverable of this project is to create an interactive educational tool using JavaScript and HTML that can be deployed online to companies. This tool will aid people in recognising phishing emails and ultimately, improve their overall phishing awareness. This project will focus on multi-disciplinary company usage where employees range from ages 25-65 and therefore will need to meet significant usability criteria; this means that the tool will need to have features that can be understood and used by a range of ages and subject matter experts. The tool will act like a question and answer game in which users would be able to view a phishing email example, click on various parts of the email that they deem suspicious, and then receive feedback on how well they recognised each aspect. For this project I will not be focusing on evaluating through participants at this stage where I evaluate how effective the tool is in teaching a user, but rather the applicability of the tool against a list of defined required features. Subsequently, the tools validity will rely on the comprehensiveness of the tool itself and as such, there will be a lot of time and focus dedicated on its design and implementation.

I will be conducting research prior to any development of the tool in order to ascertain key factors that surround phishing emails, and to determine the dataset that I will work with; this dataset will contain examples of relevant, common, and sophisticated phishing emails. Additionally, I will be researching into any existent educational tools that are publicly available, both surrounding phishing and generic, to get a perspective on the most effective learning methods for specific age ranges. Ultimately, this research will be applied to the design of the tool which will ,to some extent, align with traditional and trusted learning methodologies for online resources. While I will not only use the research to complete a concept design of the tool, I will also outline a list of criteria of functionality and non-functionality requirements including its core and desirable features. The criteria will then be utilized in the evaluation stage of the project where I will assess the tools applicability and functionality against it.

Aims and Objectives

The goals for this project is separated into core and desirable traits below. These determine which objectives are mandatory to complete and those which will be beneficial to achieve if time permits it.

Main Aim: Create an interactive educational tool using JavaScript and HTML that can be deployed online to companies.

1. The tool will be a phishing awareness quiz which will display phishing emails to a user, take in their responses and generate on screen feedback after each question(email).
2. At the end of the awareness quiz, the tool should present the user with a final (on screen) report which identifies which emails the user is most likely to be susceptible to, and additional information against it. This information should be regarding each particular email they are more likely to be susceptible to explaining any prevention techniques or awareness techniques they can use.

Core Objectives	How?
Establish an understanding of phishing and the types of phishing emails existing today	Complete research into phishing including what common emails are occurring and gather resources to ascertain a dataset (I will access publicly available dataset).
Establish factors pertaining to phishing susceptibility	Complete research into how and why people are more likely to be suspectable to phishing. This should include any differences in age ranges, industry or security solutions in place.
Understand educational tools and learning styles	Complete research into existent design and usability traits of various phishing tools which could be useful in the project tool design. Determine what educational tools are being used by companies currently and research reviews of these tools.
Create a list of functional and non-functional requirements	From the research regarding existing tools, phishing susceptibility factors and an email dataset, define a list of non-functional and functional requirements of the tool. Make sure to list the purpose and how each requirement meets usability, applicability and functionality traits.
Create user/test cases	Create cases that depicts users' actions and the expected outcomes from it. These will be used to test the code later on and determine its validity/applicability .
Create a concept design for the tool	Create a user interface(UI) design for the tool which should include transitions like navigational screen transitions, colour and overall aesthetic of the tool.
Code the tool	Using JavaScript and HTML, code the tool which should meet the functional requirements established prior. The quiz should have a feedback report which shows what type of emails the user is likely to be susceptible to.
Evaluate the tool against defined criteria and user/test cases	Using the criteria defined, I will evaluate how the tool meets each of the criteria and record how well it met the user/test cases.

Desirable Objectives	How?

Graphical representations of users results	Create a graph out of the user's responses that is displayed at the end of the session showing how well they did in relation to others.
Level variations depending on company requirements	Depending on the company using the tool, create levels which each user should pass in order to meet the companies determined required level of phishing awareness.
Statistical analysis based on the emotional response of the user to be used by the manager/ security team to determine the success of a phishing email.	Store all users' responses in a database and generate analysis report that determines statistics based on certain emotive factors of the email i.e. emails that try to be shock a user like "URGENT" or "Respond now". Could also be emails that attempt to invoke a sad/happy response.

Work Plan

The work plan below documents the project timeline and defines main objectives for each week.

Supervisor meetings: Weekly - Full project review meeting dates have been documented below

Milestone dates are highlighted in red

Week 1 01/02/2021 - 07/02/2021 -Deadline for Initial plan

Main objective: Create initial plan for project

Method

1. Create document establishing aims and objectives, project purpose, project timeline, challenges and considerations, and work plan.

Week 2 08/02/2021 - 14/02/2021

Main objective: Conduct research into phishing types and susceptibility to attacks

Method

1. Research and document phishing statistics within 2020/2021. Determine what and how environmental and social factors play apart in susceptibility of the types of attacks
2. Document types of phishing attacks and define common and sophisticated attacks. Establish attributes of each attack type.

Week 3 15/02/2021 - 21/02/2021

Main objective: Research existent educational tools and define a dataset.

Method

1. Research existent educational tools used within companies
2. Compare tool methods/techniques, establish best practices, proven learning methods and common design themes
3. Define a dataset that is publicly available for phishing attack types

Week 4 22/02/2021 - 28/02/2021

Main objective: Create a list of criteria for tool, user/test cases, and concept design

Method

1. Define a list of non-functional and functional criteria
2. Determine must, should and could features
3. Establish minimum viable product (MVP)
4. Create user and test cases
5. Create concept UI design for tool alongside user cases.

Week 5 & 6 01/03/2021 - 14/03/2021

Main objective: Begin construction of tools backend

Method

1. Finish concept design for UI
2. Begin creating tool by getting familiar with JavaScript tools and techniques for tool design
3. Start building backend utility for the tool
4. Document any challenges or changes made to MVP

Week 7 15/03/2021 - 21/03/2021

Main objective: Continue work on building backend and front end of tool + Supervisor Review Meeting

Method

1. Continue build and documentation of backend and front end work on tool
2. Have review meeting with supervisor to check project is meeting deadlines and discuss any barriers or alterations that need to be made to the overall project.

Week 8 22/03/2021 - 28/03/2021 - Interim testing and review of tool

Main objective: Continue work on building backend and front end utility and conduct Interim testing of tool + Supervisor Review Meeting

Method

1. Continue work on backend and front end of tool adding any changes determined from meeting in previous week
2. Have a final meeting before Easter break to ensure project remains on track
3. Test tool against predefined criteria and user/test cases
4. Write up short interim testing report including challenges faced and changes made to tool

Week 9 & 10 - Easter Holiday

Week 11 & 12 12/04/2021 -25/04/2021

Main objective: Continue work on building backend and front end utility

Method

1. Continue work on backend and front end of tool adding any changes determined from meeting before holidays

Week 13 26/04/2021 - 02/05/2021 - Complete Final Implementation and evaluation of Tool

Main objective: Finish implementation and conduct final testing of tool

Method

1. Continue work on tool implementation
2. Test tool against predefined criteria and user/test cases
3. Write up final evaluation testing report including challenges faced and changes made to tool

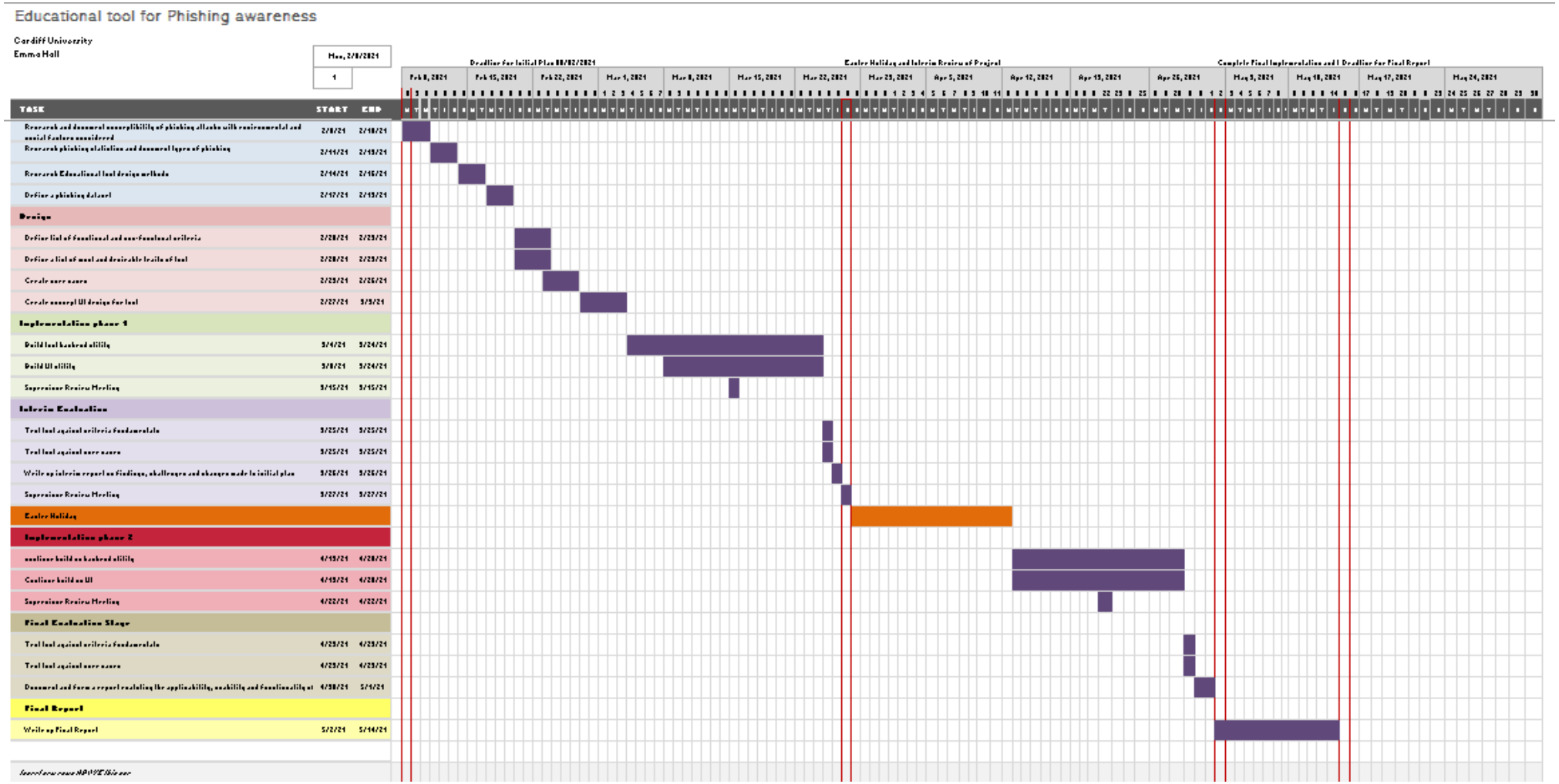
Week 14 & 15 03/05/2021 - 15/05/2021 - Deadline for Final Dissertation Report

Main objective: Create and finalise final dissertation

Method

1. Create final dissertation detailing project thoroughly
2. Send drafts for feedback on any areas which are unclear with the dissertation criteria

Gantt Chart


Educational tool for Phishing awareness
Cardiff University
Emma Hall
Mon, 2/8/2021
1
Deadline for Initial Plan 08/02/2021
Easter Holiday and Interim Review of Project
Complete Final Implementation and Deadline for Final Report
Feb 8, 2021
Feb 15, 2021
Feb 22, 2021
Mar 1, 2021
Mar 8, 2021
Mar 15, 2021
Mar 22, 2021
Mar 29, 2021
Apr 5, 2021
Apr 12, 2021
Apr 19, 2021
Apr 26, 2021
May 3, 2021
May 10, 2021
May 17, 2021
May 24, 2021
TASK
START
END
Research and document susceptibility of phishing attacks with environmental and social factors considered 2/8/21 2/10/21
Research phishing statistics and document types of phishing 2/11/21 2/12/21
Research Educational tool design methods 2/14/21 2/16/21
Define a phishing dataset 2/17/21 2/19/21
Design
Define list of functional and non-functional criteria 2/20/21 2/23/21
Define a list of must and desirable traits of tool 2/20/21 2/23/21
Create user cases 2/23/21 2/26/21
Create concept UI design for tool 2/27/21 3/5/21
Implementation phase 1
Build tool backend ability 3/4/21 3/24/21
Build UI ability 3/8/21 3/24/21
Supervisor Review Meeting 3/15/21 3/15/21
Interim Evaluation
Test tool against criteria fundamentals 3/25/21 3/25/21
Test tool against user cases 3/25/21 3/25/21
Write up interim report on findings, challenges and changes made to initial plan 3/26/21 3/26/21
Supervisor Review Meeting 3/27/21 3/27/21
Easter Holiday
Implementation phase 2
continue build on backend ability 4/19/21 4/28/21
Continue build on UI 4/19/21 4/28/21
Supervisor Review Meeting 4/22/21 4/22/21
Final Evaluation Stage
Test tool against criteria fundamentals 4/29/21 4/29/21
Test tool against user cases 4/29/21 4/29/21
Document and form a report evaluating the applicability, usability and functionality of 4/30/21 5/1/21
Final Report
Write up Final Report 5/2/21 5/14/21

Risk Analysis and Considerations

Ethical Considerations

The project does not require data from participants and as such does not violate any privacy regulations or laws; all phishing data will be free from personal identifiable information. Any evaluation of the tool will be carried out by me and its assessment will be based upon its functionality and how well it meets the established criteria.

Risk Analysis

Risk	Severity	Likelihood	Mitigation Technique
Illness affecting timeline of tasks and their completion date.	Medium	Low	Appropriate time for each task has been given that allows plenty of time for their completion in cases of any unforeseen illness.
Data loss	High	Low	Data is to be backed up frequently to prevent loss of any files, code evaluation report etc. made within the project. Files will be kept in another location to provide further security.
Changes in scope of project	High	Medium	continuous reviews and documentation scheduled of challenges, changes and risks help to also mitigate delays in scope changes and give time to said alterations wherever necessary.
Illness affecting timeline of tasks and their completion date.	Medium	Low	Appropriate time has been given ensuring plenty of time for tasks to be completed.
Limited background knowledge of using JavaScript to implement an educational tool - causes delays in project implementation phase.	Medium	High	Additional time for the implementation stages has been provided in order to understand tools and techniques used to create educational tools through JavaScript. Obtain familiarity with tools and techniques to begin development as soon as possible,

References

1. Evans, CE (2019). 6 sophisticated phishing email examples [online]. *E-Tech.* [viewed 3 February 2021]. Available from: https://www.etechcomputing.com/6-sophisticated-phishing-email-examples-and-why-theyll-trick-you/

2. Meharchandani, DM (2020). Staggering phishing statistics in 2020 [online]. *Security* Boulevard. [viewed 3 February 2021]. Available from: https://securityboulevard.com/2020/12/staggering-phishing-statistics-in-2020/#:~:text=The%20Shocking%20Phishing%20Statistics%20of%202020&text=Only%203%25%20of%20the%20users,the%20malicious%20link%20or%20attachment.

3. Sheng, ES (2020). Cybercrime ramps up amid coronavirus chaos [online]. *CNBC.* [viewed 3 February 2021]. Available from: https://www.cnbc.com/2020/07/29/cybercrime-ramps-up-amid-coronavirus-chaos-costing-companies-billions.html