Senior Design Final Report

by

Andrew Miller
Gerald Taylor IV
Nicholas Eyl
Sarah Radcliffe
Taylor Cornett

Submitted to
the Faculty of the School of Information Technology
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology/Cybersecurity

Andrew Miller, Gerald Taylor IV, Nicholas Eyl, Sarah Radcliffe, Taylor Cornet Date 11/28/2021

Tyler Hopperton Date 11/28/2021

University of Cincinnati
College of
Education, Criminal Justice, and Human Services

April 2022

Table of Contents

List of Illustrations

Tables:

Figures:

Abstract

Phishing is a dangerous form of cyber-attack that is frequently used due to the lack of awareness and training the public has. The intention of this project is to help small-to-medium-sized businesses prevent and educate their employees on phishing attacks. PhishBait is a free web solution that contains phishing templates, training videos, quizzes, a phishing campaign guide, and a dashboard to view quiz results targeted at small-to-medium-sized businesses. The results of this project will allow more small-to-medium-sized businesses to send out phishing campaigns, along with training and educating their employees about phishing. Preventing them from being the victim of phishing attacks. Overall, this means less time, money and resources spent by these companies.

Introduction

Project Summary

PhishBait is a modern-day cyber security solution to help organizations with phishing attacks. PhishBait will be a web application that provides phishing templates, training modules, a campaign guide, and a dashboard for small-to-medium-sized businesses that may not have the knowledge, training, personnel, or resources to dedicate to implementing these things on their own.

Problem Statement

Phishing attacks give attackers access to information they should not have. This problem affects everyone but is specifically harmful to businesses. Businesses are losing vast amounts of money, intellectual property theft, and damage to their reputation in cyber-attacks. According to the Verizon Data Breach Investigations Report, phishing remains one of the top methods used by attackers, being present in over one-third of breaches (1, p. 15-16). Therefore, businesses need to take measures to educate their staff on the dangers of phishing attacks. Along with the implementation of phishing tests to identify and train particularly vulnerable individuals.

Solution

Our goal is to assist small-to-medium-sized businesses by helping reduce the risks posed by phishing attacks. As stated by Mike Petock, phishing training has seen the click rate on phishing emails go drastically down from 25% in 2012 to 3% in 2018 (2, para. 6). The research shows that proper phishing training does decrease the click rate on phishing emails. We will create adequate phishing training by creating specialized phishing email templates, along with training modules and quizzes associated with each training video. There will also be a campaign guide to assist with the phishing campaign. Finally, we have a dashboard to display all pertinent information regarding users' interaction with the training modules and videos. All the content will be hosted on a website that will be free to access. Companies know their employees best, so they will be able to choose the best phishing email template to evaluate their employees.

Due to our specialized email templates, companies are going to be able to better identify vulnerable employees. Once they identify their vulnerable employees, they can have them complete our vigorous training modules to hopefully reduce the chance of them falling for another phishing email. After they complete our training modules, the company will keep track of their employees' results using our dashboard feature, which will display this information.

Project Source

The inspiration behind PhishBait came from watching multiple phishing campaigns and realizing that people will usually pass the phishing test whenever it is generic. However, they will fail at a higher rate when it concerns more unique topics such as social media or password resets. Gerald initially conceived the topic, but it was revised by the rest of the members of PhishBait.

All members conducted research and analysis. When looking at the market for current phishing email templates and their respective training modules, we did find multiple products already in existence. However, few to no products seem to target our audience, small or medium-sized companies that are new in their phishing expeditions needing a free solution. There are so many sophisticated solutions out there. A company new to phishing would want an easily digestible source of help; this is where PhishBait comes in. We will have a heavy UX focus that provides a user-friendly experience.

The PhishBait team formed when two groups of two combined. Gerald and Andrew combined with Sarah and Taylor. The team needed a fifth member. That is where Nick was brought on. Every member of PhishBait is on the cybersecurity track; however, that did not discourage the team's formation due to the unique skills each member provides outside of their cybersecurity skills.

Discussion

Project Objectives/Goals

At PhishBait, we hope to reduce the number of people clicking on phishing emails. This should help prevent businesses from losing vast amounts of money, intellectual property, and damage to their reputation in cyber-attacks. Our goal is to assist small-to-medium-sized businesses by helping reduce the risks posed by phishing attacks.

The measurable outcomes will be from the companies themselves using the tools we provide. They can run phishing campaigns and measure the number of people who fall for each phishing email. Our goal is for companies to use our templates and training modules. In doing so, the number of people who fall for phishing campaigns will decrease. Administration users can view their employees' information on a dashboard to help keep track of this.

Major Features include:

Web Page

- Easy to use and find information.

Phishing Email Templates

- Helps the company find vulnerable employees.

Phishing Training Modules

- Help the company train their vulnerable employees, so they reduce the likelihood they get caught in a phishing scheme.
- Each module will have a video and quiz.

Campaign Guide

- Directions on how to run a campaign using our tools.

Dashboard

- Keep track of what employee's complete pieces of training and how they do.

Project Scope

Our team will develop a functional application that assists users in running phishing campaigns with the tools we provide for them. Users will do this by utilizing our free and easy-to-use web application. The web application will include specialized email templates for companies to send out and training modules. Users will download the email templates and put them to use with the help of our campaign guide. Our campaign guide will offer informational assistance to our end users on how to run a phishing campaign. Once they have run the campaign, they will send the users who failed the phishing test to our specialized training modules. In each module, there is a training video and quiz. After users complete the quizzes, admins will view the results and other data in a dashboard view.

Quick Project Timeline

This section shows the timeline that we tried to stick to when creating our project. It shows an accurate representation of how our time was spent.

Table 1: Quick Project Timeline

The Quick Project Timeline shows the timeline our group followed. It has what we did and when we did it from the start of our project to the end of it.

Task #	Task Name	Duration	Start Date	End Date
1	Set up a development environment	2 Weeks	October 4	October 18
2	Phishing research	14 Weeks	October 4	January 10
3	Database Creation	6 Weeks	November 1	December 11
4	UX/UI Design	4 Weeks	October 1	October 29
5	Server-side development	6 Weeks	November 29	January 10
6	Front end development	9 Weeks	January 10	March 14
7	Mid-way presentation	1-day	November 22	November 22
8	Email Template creation	17 Weeks	November 1	February 28

9	Video and Quiz training creation	17 Weeks	November 1	February 28
10	Dashboard Creation	8 Weeks	January 1	February 28
11	Input information onto website	11 Weeks	February 1	April 8
12	Documentation	Whole Time	September 27	April 12
13	Presentation Preparation (poster & ppt)	6 Weeks	March 1	April 12
14	In-Class Presentation	1 Day	April 4	April 4
15	IT Expo	1 Day	April 12	April 12

Table 1: Quick Project Timeline

Technologies Used

For the development of the website, we will use HTML, CSS, PHP, and JavaScript. Development software for writing the code is to be Adobe Dreamweaver and GitHub. For website hosting, we plan to use Namecheap. They have quality hosting services that are affordable for students. For the development of the videos, OBS (Open Broadcaster Software), DaVinci Resolve, Adobe Premiere, and Adobe After Effects are the current selections for recording, editing, and post-production work. For the UX/UI design Adobe XD will be used to make clickable prototypes.

Technical Sequence Diagram

Below is a sequence diagram demonstrating how the different components of the website are working together. The components shown are the user, home page, log-in function, other pages, and actions.

Figure 1: Technical Sequence Diagram

The Technical Sequence Diagram shows how PhishBait functions from an admin and a user's point of view.

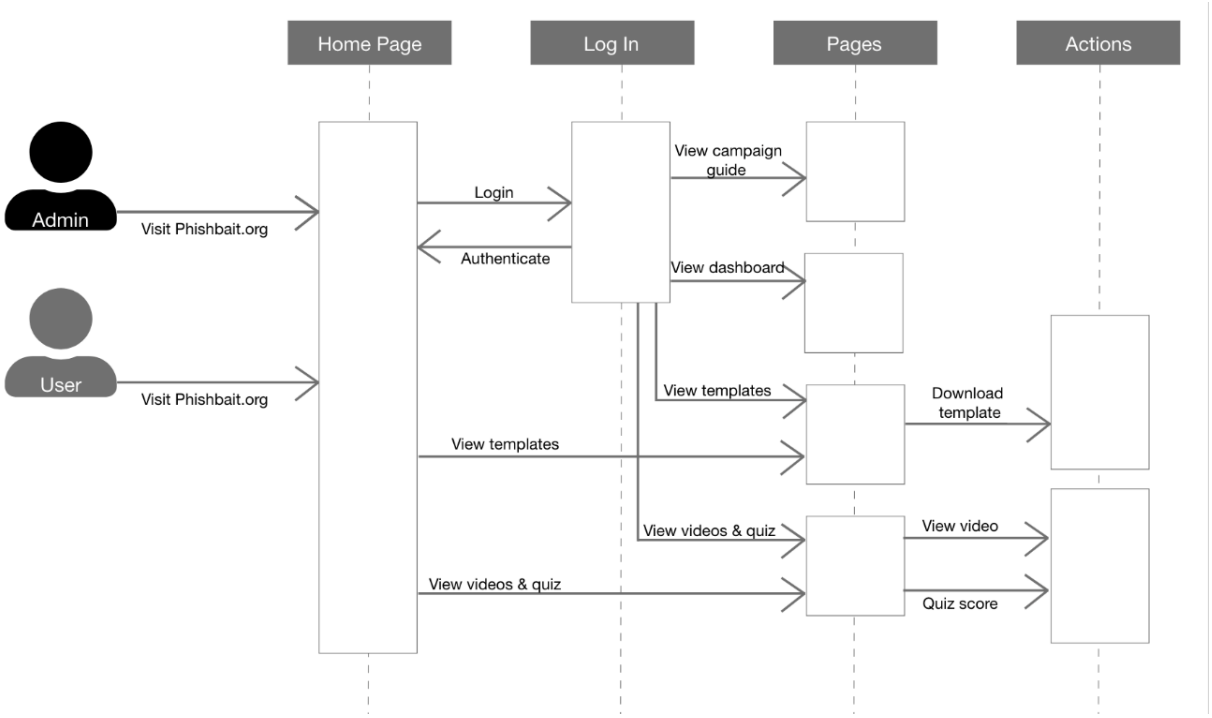

Figure 1: Technical Sequence Diagram

User Personas

Below are the user personas that would utilize our web application PhishBait. Each table is a different user persona. We have a Security Analyst, Security Manager, and Non-IT Sales Associate included in our user personas.

Table 2: User Persona 001

This User Persona chart is to display the Security Analyst and the experience they have in their position as it pertains to PhishBait.

User Persona: 001	
	Title Security Analyst
	Name James Smith
	Age 26
	Gender Male

Behavior	John is a security analyst for a small company. He is one of a few employees working on the company's cybersecurity. He reads that phishing is a vast area of concern to security and preventing attacks. He wants to start a phishing campaign at his company. He has the technology to send phishing emails and store the results, but he does not know what emails would be best to use. He also does not know how to train his employees if they get caught.
Pain	Lack of funding, lack of time to individually teach employees, lack of other security personnel
Needs & Goals	Create a successful phishing campaign, train employees who get caught

Table 2: User Persona 001

Table 3: User Persona 002

This User Persona chart is to display the Sales Associate or a Non-IT staff member and the experience they have in their position as it pertains to PhishBait.

User Persona: 002	
	Title Sales Associate (Non-IT)
	Name Mary Johnson
	Age 48
	Gender Female
Behavior	Mary is a sales associate at a small company that just implemented a phishing test. She has never been good at spotting fake emails and has been caught in a phishing attack in the past. She recently received an email about resetting her Netflix password, and she clicked the link. It was one of the new phishing tests. She now must complete a training module, so she hopefully does not get caught again.
Pain	Lack of knowledge of technology, lack of training in phishing schemes

Needs & Goals	Be able to pass the training module, learn about phishing so she does not get caught again

Table 3: User Persona 002

Table 4: User Persona 003

This User Persona chart is to display the Security Manager and the experience they have in their position as it pertains to PhishBait.

User Persona: 003	
	Title Security Manager
	Name Brian Williams
	Age 52
	Gender Male
Behavior	Brian is a Security Manager for a small company. He overlooks the entire security of the company. He does not have enough time to create phishing emails or videos but wants to see how his employees would respond to them. His budget is very tight; however, he still wants to strengthen security.
Pain	Lack of funding, lack of resources, and lack of experience with phishing campaigns in the company.
Needs & Goals	Provide good, free phishing campaign emails. Get his employees to comply with the training. View employee quiz results.

Table 4: User Persona 003

Use Cases

Below are the Use Cases associated with our web application PhishBait. Each table is a separate use case. The use cases we have are, Security Analyst gets an email template, an employee is sent a training module, and Security personnel sends out a training module.

Table 5: Use Case 001

This Use Case chart is to display the action of the Security Analyst getting an email template from PhishBait.

Use Case ID	001
Use Case Name	Security Analyst gets an email template
End Objective	Use of email template
User/Actor	Security Analyst (IT Staff)
Trigger	Wants to start a phishing campaign
Frequency of Use	As needed
Preconditions	1.Is planning to utilize a phishing campaign
Basic Flow	1. Go to www.PhishBait.org 2. Download the module 3. Send to an employee that failed the test
Postconditions	1.Follow up on employee training 2.Uses more email templates

Table 5: Use Case 001

Table 6: Use Case 002

This Use Case chart is to display the action of the Security Analyst assigning a training module to an employee.

Use Case ID	002
Use Case Name	Security personnel assigning training module completion
End Objective	Have employees complete the training module
User/Actor	Security Analyst (IT Staff)
Trigger	Employees are caught in a phishing campaign
Frequency of Use	Whenever employees get caught in the phishing campaign
Preconditions	1.Employee falls for phishing campaign
Basic Flow	1. Assign modules for completion 2. Send employees to visit www.PhishBait.org and give them the assigned module
Postconditions	1.Employee completes module

Table 6: Use Case 002

Table 7: Use Case 003

This Use Case chart is to display the action of the General Employee getting sent a training module.

Use Case ID	003
Use Case Name	Employees are sent a training module
End Objective	Employees correctly complete the training module
User/Actor	General Employee (Sales Associate)
Trigger	Employees get caught in a phishing campaign
Frequency of Use	When caught in a phishing campaign
Preconditions	1. Employee sent phishing campaign 2. Employee gets caught in a phishing campaign
Basic Flow	1. Go to www.PhishBait.org 2. Choose the training module that needs completion 3. Finish module correctly
Alternate Flow	1. If the employee fails the module restart it until they pass
Postconditions	1. Employee is better educated about phishing dangers

Table 7: Use Case 003

Table 8: Use Case 004

This Use Case chart is to display the action of the Security Analyst viewing the quiz results on a dashboard.

Use Case ID	004
Use Case Name	Admin views quiz results
End Objective	Build report on quiz results
User/Actor	Security Analyst (IT Staff)
Trigger	Needs to report how employees are doing for a phishing campaign that was sent out
Frequency of Use	Monthly
Preconditions	1. Employees take phishing campaign quiz
Basic Flow	1. Go to www.PhishBait.org 2. Log in 3. View the dashboard 3. Use the information
Postconditions	1. Create a report

Table 8: Use Case 004

Use Case Diagram

A use case diagram is a graphical description of a user's interaction with a given system. We show what our users, the IT staff, and general employees have access to on our website, PhishBait.

Figure 2: Use Case Diagram

The Use Case Diagram shows the different use cases that an IT Staff and a General Employee can have while using PhishBait.

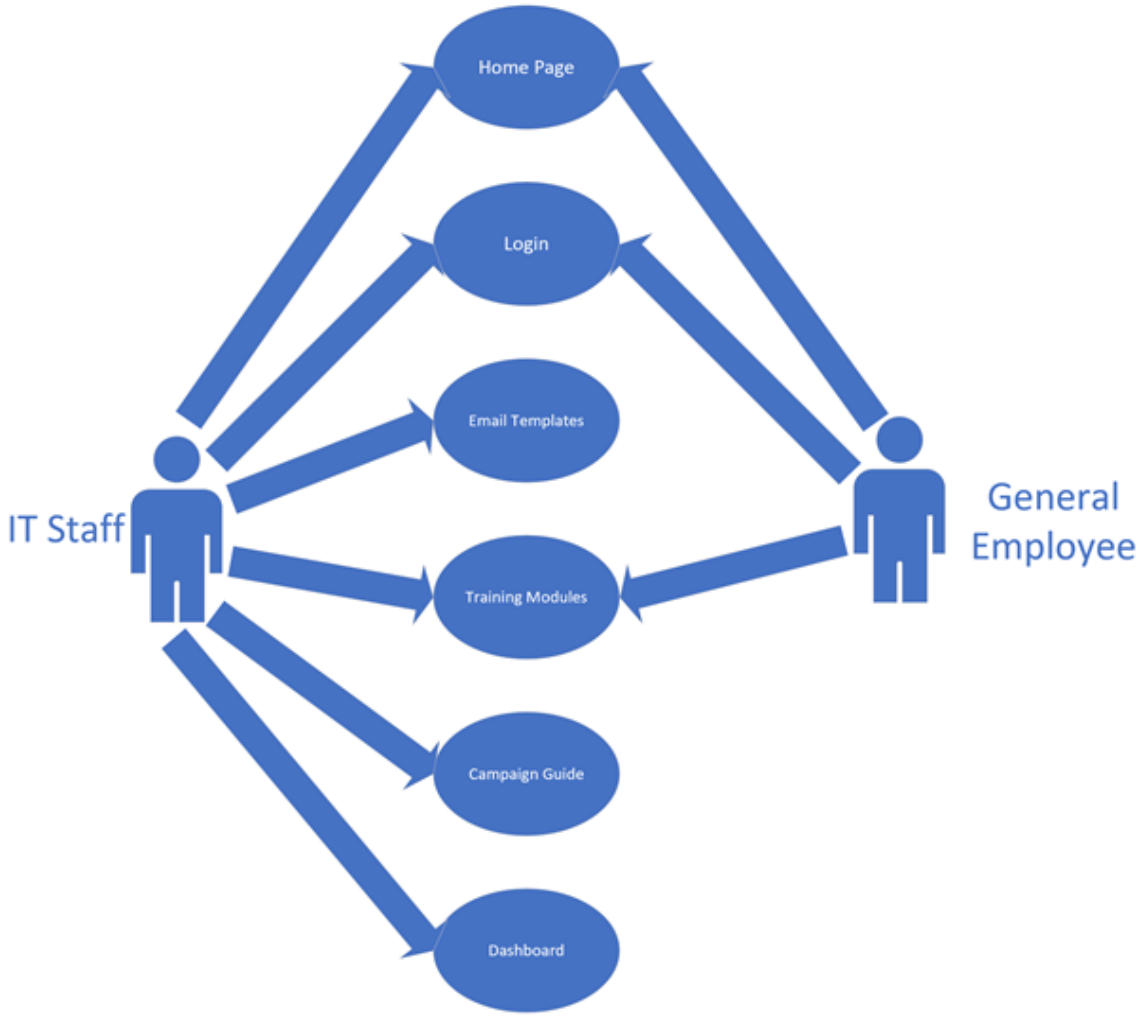

Figure 2: Use Case Diagram

Testing Plan

Overview

This section describes how testing was done on PhishBait. This includes the methodology, scope, objectives, logs, and procedures. There will also be a description of what was learned during the testing phase.

Methodology

The approaches we will be taking throughout the product development cycle are unit testing, user acceptance testing, backup testing, load testing, and penetration testing.

Scope

Features that need testing and why:

- Browser compatibility- make sure the website can be used on many browsers
- Device compatibility- make sure the website can be used on many devices
- Buttons and links on the website- make sure correct information showing
- Website response times- make sure things are not taking forever to load
- Login functionality- make sure things are secure and people can log in
- Use case 001- make sure people can access templates how we want them to
- Use case 002- make sure people can access training modules how we want them to be able to
- Use case 003- make sure people can send out training module links how we want them to be able to
- Use case 004- make sure the dashboard is functioning properly

Objectives

We choose unit testing because it ensures that all our code meets the quality standards set before deploying it into production. We choose user acceptance testing because it gets an

outsider's point of view to verify that the code we wrote as developers does what we intended it to do. We choose backup testing because we want to ensure accurate backups are readily available in case the worst happens to our web hosting service or database. We choose load testing because we want to verify that countless users can access and use our web page to its full potential without crashing or drastically slowing down. We choose penetration testing because we want to ensure the security of our web page and our user's information.

End goal:

a. All major features and use cases need to be accounted for

b. All use cases must account for all the user roles

c. All bugs need to be resolved before IT Expo

d. Make sure it is as user friendly as possible

Test Logs and Procedures

This section shows the complied data from our testing that was conducted using the methodology that was described in the sections above.

Table 9: Test Logs and Procedures

The test results gathered below came from the guidelines we set in the sections above.

Test Case	Date	User Role	Type of Testing	Expected Output	Actual Output	Pass / Fail	Reason for P/F
01	2/21	003	Unit	Login	unsuccessful login attempt	Fail	User was not able to login
02	2/27	003	Unit	Login	Successful login attempt	Pass	User was able to login
03	2/27	003	Unit	View dashboard	Dashboard viewable	Pass	Dashboard was viewable
04	2/27	003	Unit	View campaign guide	Page viewable	Pass	Campaign guide was viewable
05	2/27	003	Unit	View email templates	Viewed templates	Pass	Templates were viewable

05	2/27	002	Unit	View training	Did not view training	Fail	Training was not viewable when clicked on
06	3/3	001	User Acceptance	Login	Successful login attempt	Pass	User was able to login
05	3/3	002	Unit	View training	Viewed training	Pass	Training was viewable when clicked on
07	3/3	001	User Acceptance	View dashboard	Dashboard viewable	Pass	Dashboard was viewable
08	3/4	001	User Acceptance	View campaign guide	Page viewable	Pass	Campaign guide was viewable
09	3/4	001	User Acceptance	View email templates	Viewed templates	Pass	Templates were viewable
10	3/15	N/A	Backup	Successful backup	Successful backup of files	Pass	Our backups were implemented successfully
11	3/18	N/A	Load	Website stays responsive	Website did not slow down	Pass	Website did not slow when used by countless people
12	3/26	N/A	Penetration	SQL injection gets denied	SQL injection is successful	Fail	SQL injections got past our input validation
13	4/3	N/A	Penetration	SQL injection gets denied	SQL injection gets denied	Pass	SQL injection got blocked by our additional security settings
14	4/7	N/A	Penetration	OpenVAS medium to low CVE threats	OpenVAS medium to low CVE threats	Pass	OpenVAS showed threats but they were not anything too bad. We accepted the risks.

Table 9: Test Logs and Procedures

Testing Review

During the testing of PhishBait, we utilized user acceptance testing to ensure the product was working as intended. This testing was done by us preparing scenarios and walking through PhishBait to make sure the website functioned properly. One thing learned during this test was that all our information was out there readily available. However, some pieces of

information were harder to find due to poor placement on our end as developers. We also learned that it is good that we have the users separated where the managers must log in. It takes out the complication of the website for users who are only there to take a test. In the future, user acceptance testing will be put into place every time a new feature is added. This will ensure that each feature is implemented into the website seamlessly.

We also utilized unit testing to make sure that our code did what we intended it to do. We had some failures in our code doing something close to what we wanted but not exactly what we wanted. We eventually fixed all those issues. To end off our unit testing we cleaned up all the code to make it to the standards that we set for ourselves for code cleanliness.

We additionally had backup testing where we restored our backups to make sure they were correct in storage. All backup testing succeeded as planned. We also had load testing to make sure our website could withstand countless users utilizing our entire site. We created scripts to run through automated tasks that simulated web traffic and our reports showed no signs of our website slowing down at all.

Finally, we had penetration testing, we first evaluated against SQL injection and at first, it failed. Once we knew that we went back and added security measures to prevent that attack from occurring such as proper input validation. We retested for SQL injection but after our security additions, we could no longer complete the attack. Next, we used OpenVAS to scan for any potential Common Vulnerabilities and Exposures (CVE). After we completed our scan, we only had medium to low CVEs. We investigated them all and decided that we will accept the risk associated with them because it was not anything harmful to our users or their data. If we had more time, we would investigate resolving these CVEs.

Change Management Plan

A change is an addition, modification, or removal of anything. Anyone on the team can request a change. When a change is suggested, the team will set up a meeting to identify the pros and cons. If three out of the five members agree on the change, we will proceed. The first thing that will happen when a change is decided, is communicating it with our project advisor. If he has no objections to the change, then we will set up additional time to discuss a plan of

action to see the change through. The change will be the main priority of the project. All other tasks will be secondary until the change is complete.

Budget

This budget is to help consumers and stakeholders understand the value behind PhishBait. Below is a table that includes the cost of labor, software, and hardware used in PhishBait.

Project Budget

This section goes over the budget that was required to create PhishBait. It goes over the cost of labor and hardware used. It also goes over the cost of keeping the site up and running after launch.

Table 10: Project Budget

The Project Budget is the total estimated cost of the creation of our cyber security solution, PhishBait.

				Ongoing Annual		
	Rate Per/Hr.	**Work Effort (Hours)**	**1 X Costs**	**Rate Per/Hr.**	**Work Effort (Hours)**	**1 X Support Cost**
Labor - IT	20	2,700	$ 54,000	20	40	$ 800
Labor - External	0	0	$ 0		0	$ 0
Software - External			2,970			40
Hardware - External			4,000			0
Misc.			0			0
TOTAL			$ 60,970			$ 872

Table 10: Project Budget

Problems Encountered and Analysis of Problems Solved

In the initial stages of developing our idea, we chose a solution that was too difficult due to time constraints. We initially wanted to design an application that sent out phishing campaigns, recorded the results, provided training videos, and training quizzes. This would have required too much research and development to complete in our time frame. The proposed solution would have required us to charge for this service; however, products like that already exist in the market. It also went against what we wanted to do, which was to provide free assistance to small-to-medium-sized companies. Instead of being the whole solution for a cost, we can provide the best assistance, while being completely free to the consumer.

Another problem we have encountered was scope creep. As we developed our project, we thought of new things to add. We tried to keep the initial scope of the project, but we still allowed for realistic changes. The biggest change added was our dashboard feature. We had always thought about doing it, but we never had a definitive answer. That was until after our fall semester presentation. The feedback we received was that having a dashboard would improve our site. That feedback pushed us over the edge. We went through our change process and officially added it to our site.

Another massive problem we ran into was personal issues. We had five members working on a tight schedule anything that pushed back development was a detriment to us. Naturally, life happens, and things got delayed; however, we always persisted. We had multiple members get Covid-19, there was a death of a pet, and there was a death of a loved one. We allowed each member to take time until they were ready to get back to work. During those tough times, we relied on each other more, and in doing so we became a better team for it

Conclusion

During the making of PhishBait as a team, we have learned what all a working web application takes to produce. The skills we have developed and enhanced include teamwork, software development, database configuration, UX design, technical thought process, and more. This has been a wonderful experience to understand how all the things we learned in class tie together.

For the spring semester, our team will be focused on many things to round out our project. This includes producing more videos and templates for the website. Implementing a quiz feature with results that go to a dashboard for admins to view. We will be researching to ensure the security of PhishBait. We will also be perfecting the design and testing of the website to make a good user experience.

References

1. Bassett, Gabriel. Hylender, Dylan. Langlois, Phillippe. Pinto, Alexandre. and Suzanne Widup. Data Breach Investigations Report. *Verizon.* Spring, 2021. 15-16.

2. Petock, Mike. “Anti-Phishing Training: Is It Working? Is It Worth It?”. *Carnegie Mellon University.* January 23, 2020.