



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Everyone's Smart University

Project (Spring 2021)

Student Name	Talal Ali Alshamrani	اسم الطالب
Students I.D	2021203567	الرقم الجامعي

Section

Master

Date

Thursday

18 / 03 / 2021.

Course Code

(PMG506)

Advanced project Management

Anti-phishing software

Project Overview:

The project aims to prevent the stealing of information by phishing attacks against the company employees and its subsidiaries.

Objective, Requirement, and Scope:

Objective: to detect and prevent phishing attacks.

Collected Requirements:

- a. The ability to scan links.
- b. The ability to identify phishing links even if they were newly generated.
- c. Add discovered phishing links to a blacklist.
- d. Allows admin to add links to a global white list.
- e. Allows users to add links to their local white list.
- f. Ability to identify a page as a login or not.
- g. Works on phones.

Defined Scope:

- Establishing a database for a local whitelist linked to the user and a global whitelist linked to admin both require a legitimate link and service provider name and a blacklist.
- Using a library (like ion in java) or a method to retrieve HTML code from the website to check if this page is login/update page or not
 - If not, then do nothing.
 - If yes, then proceed to detection step.
- Using a library (like ion in java) or a method to retrieve HTML code from the website to compare both the link and service provider name to the ones in whitelist
 - If nether are matched it means unknown.
 - If service provider name is a match but the link is not this means phishing.
- Implementing a method that put a phishing link that been discovered in blacklist to ease the process for next detection.

Stakeholders, and Roles:

Stakeholder	Role	Power(H/L) ¹	Interest(H/L)
CTO	Sponsor	H	L
IT managers of 5 subsidiaries	-	H	L
Employees	Users	L	H
IT department Employees	Documentation/Installment	L	H
4 Developers	Development	L	H
Expert Analysist	Domain analysis	L	L

Work Breakdown Structure (WBS):

1. Documentation phase:
 - a. Domain analysis.
 - b. Functional & non-functional requirement.
 - c. Architecture design.
 - d. Delivering documentation.
2. Implementation phase:
 - a. Database.
 - b. Core functions/methods.
 - c. UI.
 - d. Delivering anti-phishing software.
3. Testing phase:
 - a. Unit test.
 - b. Performance test.
 - c. User test.
 - d. Delivering test result.
4. Installation phase:
 - a. Installation on computers/laptops.
 - b. Installation on phones.
 - c. Finishing installation.

¹ H: high, L: low

Milestone List:

Milestone	Description
Delivering documentation	Domain analysis plus all requirement and architecture design must be finished to start implementing the software
Delivering anti-phishing software	The final software must be ready for testing
Delivering test results	All test results (unit, performance, and user tests) must be finalized to determine whether to send the software back or start installing it
Finishing installation	Software must be installed on all devices

Scope Management Plan:

Scope management for the anti-phishing Project will be the sole responsibility of the Project Manager. The scope for this project is defined by the Scope Statement, Work Breakdown Structure (WBS) and WBS Dictionary. The Project Manager, Sponsor, and Stakeholders will establish and approve documentation for measuring project scope which includes deliverable quality checklists and work performance measurements.

Proposed scope changes may be initiated by the Project Manager, Stakeholders or any member of the project team. All change requests will be submitted to the Project Manager who will then evaluate the requested scope change. Upon acceptance of the scope change request the Project Manager will submit the scope change request to the Change Control Board and Project Sponsor for acceptance. Upon approval of scope changes by the Change Control Board and Project Sponsor the Project Manager will update all project documents and communicate the scope change to all stakeholders. Based on feedback and input from the Project Manager and Stakeholders, the Project Sponsor is responsible for the acceptance of the final project deliverables and project scope.

The Project Sponsor is responsible for formally accepting the project's final deliverable. This acceptance will be based on a review of all project documentation, testing results, beta trial results, and completion of all tasks/work packages and product functionality.

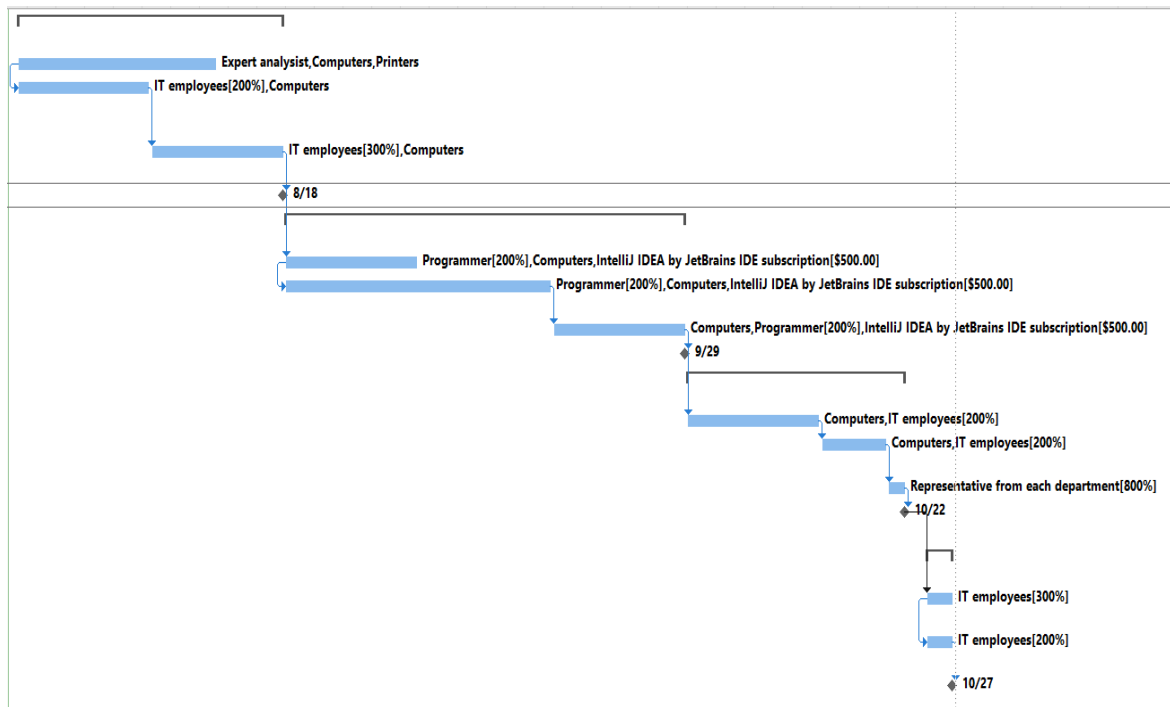
Schedule Management Plan:

Project schedules for the anti-phishing Project will be created using MS Project 2016 starting with the deliverables identified in the project's Work Breakdown Structure (WBS). Activity definition will identify the specific work packages which must be performed to complete each deliverable. Activity sequencing will be used to determine the order of work packages and assign relationships between project activities. Activity duration estimating will be used to calculate the number of work periods required to complete work packages. Resource estimating will be used to assign resources to work packages in order to complete schedule development.

Once a preliminary schedule has been developed, it will be reviewed by the project team and any resources tentatively assigned to project tasks. The project team and resources must agree to the proposed work package assignments, durations, and schedule. Once this is achieved the project sponsor will review and approve the schedule and it will then be base lined.

Activities and Durations:

Activity	Duration
Domain Analysis.	15 days.
Functional & non-Functional requirement.	10 days.
Architecture design.	10 days.
Database.	10 days.
Core functions/methods.	20 days.
UI.	10 days.
Unit test.	10 days.
Performance test.	5 days.
User test.	2 days.
Installation on computer.	3 days.
Installation on phones.	3 days.



Cost Management Plan:

The Project Manager and CTO will be responsible for managing project's cost while The Project Manager will be responsible for reporting on the project's cost throughout the duration of the project. The Project Manager will present and review the project's cost performance during the monthly project status meeting. Using earned value calculations, the Project Manager is responsible for accounting for cost deviations and presenting the Project Sponsor with options for getting the project back on budget. All budget authority and decisions, to include budget changes, reside with the anti-phishing Project Sponsor.

Resources and Estimate costs:

Resource	Cost	Authority to spend/use
1 Expert analyst.	15,000 SAR ² (Assumption)	Project Manager
5 IT employees.	Utilized from existing IT members (Assumption)	CTO
4 Programmers	10,000 SAR ³ (Assumption)	Project Manager
1 Representative from each department.	Utilized from existing company members (Assumption)	CTO
Computers	Utilized from existing resource	CTO
Network	Utilized from existing resource	CTO
Printers	Utilized from existing resource	CTO

Procurement Management Plan:

The Project Manager will provide oversight and management for all procurement activities under this project. The Project Manager is authorized to approve all procurement actions up to \$50,000. Any procurement actions exceeding this amount must be approved by the Project Sponsor.

Procurements:

Product	Price	Authority to spend
IntelliJ IDEA by JetBrains IDE Subscription	1,875 SAR/Month	Project Manager
Ink	1596 SAR	Project Manager

Determine Budget:

² Price is set per activity

³ Freelancers salary per month per programmer

It had been determent that the project will have 70,000 SAR (\$18,667), and the expected cost of this project based on this plan is 62,230.5 SAR (\$16,594.8).

COST OVERVIEW

WED 7/22/20 - TUE 10/27/20

COST

\$16,594.80

REMAINING COST

\$16,594.80

% COMPLETE

0%

COST STATUS

Cost status for top level tasks.

Name	Actual Cost	Remaining Cost	Baseline Cost	Cost	Cost Variance
Documentation Phase	\$0.00	\$4,426.00	\$0.00	\$4,426.00	\$4,426.00
Implementation phase	\$0.00	\$12,168.80	\$0.00	\$12,168.80	\$12,168.80
Testing phase	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
Installation phase	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00

PROGRESS VERSUS COST

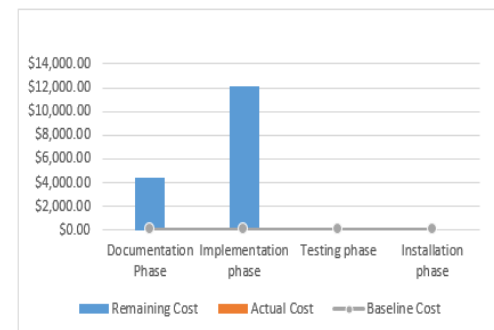
Progress made versus the cost spent over time. If % Complete line below the cumulative cost line, your project may be over budget.



COST STATUS

Cost status for all top-level tasks. Is your baseline zero?

[Try setting as baseline](#)



Quality Management Plan:

All members of the anti-phishing project team will play a role in quality management. It is imperative that the team ensures that work is completed at an adequate level of quality from individual work packages to the final project deliverable. The following are the quality roles and responsibilities for the anti-phishing Project:

The Project Sponsor is responsible for approving all quality standards for the anti-phishing Project. The Project Sponsor will review all project tasks and deliverables to ensure compliance with established and approved quality standards. Additionally, the Project Sponsor will sign off on the final acceptance of the project deliverable.

The Project Manager is responsible for quality management throughout the duration of the project. The Project Manager is responsible for implementing the Quality Management Plan and ensuring all tasks, processes, and documentation are compliant with the plan. The Project Manager will work with the project's quality specialists to establish acceptable quality standards. The Project Manager is also responsible for communicating and tracking all quality standards to the project team and stakeholders.

Quality management:

Project Quality Measurement:

Key measurement	Acceptable level	Comments
Product issues	<2% active users report bugs.	Bug collection done via email reports.
Performance	Response time to an URL in 2sec maximum.	Test via CPU Profiler plugin tool in IntelliJ IDEA.
Availability	At least one backup database exists.	
Alert	Alerting user by a pop-up message with distinct color represent danger.	
User Interaction	User able to view expanded details about detected phishing attack.	
Old attacks	User get to view old attacks and know how many they got in selected course of time.	
Whitelist	Users must be able to view both local and global whitelist.	
Phishing links	Must all phishing links, detected not by blacklist but by other means, be added automatically to blacklist.	Generate a new phishing link and monitor database to verify.
User experience	System should be easy to understand within 2 minutes, and pleasant to interact with.	Use surveys and/or feedback via email to check with the users.

Communication Management plan:

This Communications Management Plan sets the communications framework for this project. It will serve as a guide for communications throughout the life of the project and will be updated as communication requirements change. This plan identifies and defines the roles of anti-phishing project team members as they pertain to communications. It also includes a communications matrix which maps the communication requirements of this project, and communication conduct for meetings and other forms of communication. A project team directory is also included to provide contact information for all stakeholders directly involved in the project.

The Project Manager will take the lead role in ensuring effective communications on this project. The communications requirements are documented in the Communications Matrix below. The Communications Matrix will be used as the guide for what information to communicate, who is to do the communicating, when to communicate it, and to whom to communicate.

Stakeholders and Team Members engagement:

Description	Frequency	Method	Audience	Owner
Project Team Members				
Status report	Weekly	In-person	Team members	Project manager
Task progress updates	Daily	Email	Project manager	Team members
Project review	At milestones	In-person	Team members	Project manager
Post-mortem meeting	At end of project	In-person	Team members	Project manager
Project Stakeholders				
Project status report	Weekly	Email	Stakeholders	Project manager
Project review	At milestones	meeting	Stakeholders	Project manager

Communications Conduct:

Meetings:

The Project Manager will distribute a meeting agenda at least 2 days prior to any scheduled meeting and all participants are expected to review the agenda prior to the meeting. During all project meetings the timekeeper will ensure that the group adheres to the times stated in the agenda and the recorder will take all notes for distribution to the team upon completion of the meeting. It is imperative that all participants arrive to each meeting on time and all cell phones and blackberries should be turned off or set to vibrate mode to minimize distractions. Meeting minutes will be distributed no later than 24 hours after each meeting is completed.

Email:

All email pertaining to the anti-phishing Project should be professional, free of errors, and provide brief communication. Email should be distributed to the correct project participants in accordance with the communication matrix above based on its content. All attachments should be in one of the organization's standard software suite programs and adhere to established company formats. If the email is to bring an issue forward then it should discuss what the issue is, provide a brief background on the issue, and provide a recommendation to correct the issue. The Project Manager should be included on any email pertaining to the anti-phishing Project.

In-person Communications:

While In-person communication is a part of every project and is necessary for successful project completion, any issues, concerns, or updates that arise from informal In-person between team members must be communicated to the Project Manager so the appropriate action may be taken.

Risk Management Plan:

The risks are identified by Project Manager and Project Manager is responsible for providing the proper response to that risk.

Risk	Type	Response
Server reaches over 500 concurrent users	Quantitative	A ready up-to-date server on standby is connected
Database is down	Qualitative	A backup database is connected
Troubles with Ion library	Qualitative	Jsoup library is implemented as well to pick up if Ion is down

Change Management Plan:

he following steps comprise this organization change control process for all projects and will be utilized on the anti-phishing project:

Step #1: Identify the need for a change (Any Stakeholder)

Requestor will submit a completed this change request form to the project manager

Step #2: Log change in the change request register (Project Manager)

The project manager will maintain a log of all change requests for the duration of the project

Step #3: Conduct an evaluation of the change (Project Manager, Project Team, Requestor) The project manager will conduct an evaluation of the impact of the change to cost, risk, schedule, and scope

Step #4: Submit change request to Change Control Board (CCB) (Project Manager)

The project manager will submit the change request and analysis to the CCB for review

Step #5: Change Control Board decision (CCB)

The CCB will discuss the proposed change and decide whether it will be approved based on all submitted information

Step #6: Implement change (Project Manager)

If a change is approved by the CCB, the project manager will update and re-baseline project documentation as necessary as well as ensure any changes are communicated to the team and stakeholders

Any team member or stakeholder may submit a change request for the anti-phishing Project. The anti-phishing Project Sponsor will chair the CCB and any changes to project scope, cost, or schedule must meet his approval. All change requests will be logged in the change control register by the Project Manager and tracked through to completion whether approved or not.

❖ References

- 1) Project Management Professional - Nasser Al-Muhaimid.
- 2) Sandra F. Rowe · 2020
- 3) Lectures and notes PMG506 MPM
- 4) Dennis Lock · 2020