ArcherPhish

**Senior Design Team Contract**

University of Cincinnati

College of Education, Criminal Justice and Human Services

School of Information Technology

Devon Hughes-Munden

Kyle Doersam

Hanin Baza

Zach Cobb

Table of Contents

[Intent 3](#_Toc139472962)

[Senior Design Contract 4](#_Toc139472963)

[Project Summary 4](#_Toc139472964)

[Problem Statement 4](#_Toc139472965)

[Solution 4](#_Toc139472966)

[Contact Information 4](#_Toc139472967)

[Sponsor Information (if applicable) 4](#_Toc139472968)

[Project Source 4](#_Toc139472969)

[Project Objectives/Goals 4](#_Toc139472970)

[Team Members and Responsibilities 5](#_Toc139472971)

[Project Scope 5](#_Toc139472972)

[Quick Project Timeline 5](#_Toc139472973)

[Technologies Used 5](#_Toc139472974)

[Ethical Considerations 5](#_Toc139472975)

[Team Rules 5](#_Toc139472976)

[Team Signatures: 6](#_Toc139472977)

[References 7](#_Toc139472978)

# Intent

The following contract was written and agreed upon by Devon Hughes-Munden, Kyle Doersam, Hanin Baza, and Zach Cobb. The contract provides expectations, objectives, and results for developing ArcherPhish.

The contract is effective for all team members participating in the Senior Design Capstone class series in the 2025-2026 academic year.

# Senior Design Contract

## Project Summary

The application that we will be creating is designed to provide organizations with an automated and targeted email phishing campaign. This will provide IT and Cybersecurity administrators with real time statistics on ongoing automated phishing exercises resulting in better trained team members on combating adversarial phishing. The application will have a functionality that allows administrators to implement target intelligence to create phishing emails specific to key level targets to showcase how OSINT can be used to fool victims. Emails will be crafted with the aid of artificial intelligence using the latest techniques and allowing unique emails to be generated completely automated.

## Problem Statement

Year after year, the reigning weak point in all of information technology and cybersecurity is the human error factor. Phishing, and specifically email phishing, continues to rise and be a viable attack vector for threat actors looking to victimize companies and institutions around the world. This problem starts at the training level, as there is no simple technical fix to stop this issue. Adversaries are constantly adapting and changing methodology to see better success in their phishing campaigns and better target key individuals that can unwittingly grant access to these attackers.

## Solution

Our solution is an application designed to be implemented and maintained by a security or IT team. This application will generate unique phishing emails using artificial intelligence to be sent to a mail list within your organization. The application will feature the ability to add target specific modifiers that can be used to craft phishing emails crafted to better convince key stakeholders. Data comprising of campaign success will be available to track improvement over time.

## Contact Information

|  |  |  |  |
| --- | --- | --- | --- |
| Team Member | Degree + Track | Email | Phone Number |
| Devon Hughes-Munden | BSCYBER | hughedc@mail.uc.edu | (937)272-4225 |
| Kyle Doersam | BSIT – Software Development | doersakj@mail.uc.edu | (740)851-0944 |
| Hanin Baza | BSCYBER | hbaza@mail.uc.edu | (360)616-8828 |
| Zach Cobb | BSCYBER | cobbzy@mail.uc.edu | (859) 468-6831 |

## Project Source

Phishing and social engineering remain among the largest causes of security incidents in the workplace. As a group, we recognized that many organizations provide the same phishing tests to all employees regardless of whether they are high-value targets. Our phishing service addresses this gap by enabling administrators to craft targeted campaigns against executives, stakeholders, or other high-value individuals. These campaigns can incorporate personally identifiable information (PII) provided by the organization or gathered from open-source intelligence (OSINT), making the simulations more realistic and effective.

## Project Objectives/Goals

* Providing organizations with a way to test and measure employee's awareness of phishing and social engineering attacks by sending real, controlled test emails to employees' actual inboxes.
* Simulate realistic phishing scenarios of varying difficulty to evaluate employee susceptibility.
* Provide administrators with configurable campaign management for high value targets (target lists with more personalized information)
* Maintain user privacy and secure handing of all collected data. Store only necessary data and minimize PII exposure. Document data retention and deletion policy.
* Design the application to be user friendly and accessible for administrators.
* Keep the system simple so phishing templates and campaign types can be updated as attack techniques evolve.

## Team Members and Responsibilities

* *Devon Hughes-Munden: UI Design & Deliverable Design, OSINT implementation*
* *Kyle Doersam: Developer*
* *Hanin Baza: Research, Security*
* *Zach Cobb: Networking, Security*

## Project Scope

Our goal is to create a web-based phishing campaign and training platform that measures, analyzes, and enhances an organization's resistance to phishing and social-engineering attacks by sending actual, controlled test emails to employees' inboxes. All initiatives will adhere to legal and ethical requirements and only be conducted with prior authorization that has been documented.

Main Deliverables:

* Web Application:
  + Administrative dashboard for configuring and running live phishing campaigns, managing targets, and viewing reports.
  + Responsive interface compatible with modern browsers and devices.
* Key features:
  + Send authorized test emails to employee inboxes.
  + Support broad and targeted (spear-phishing) campaigns using organization-provided PII or OSINT derived content when authorized.
  + Campaign controls: target lists, scheduling, template selection, difficulty selection, and variable substitution
  + Individual user data available
* Boundaries:
  + Campaigns will only run with documented authorization from sponsoring organization and/or affected participants.
  + No malware, disruptive payloads, or unauthorized access will be used.
  + OSINT use is limited to publicly available data and organization provided PII. No private or illegally obtained data will be used.
  + No automatic enforcement actions will be taken by the system.
  + The team will comply with applicable laws, institution policies, and documented data retention/deletion policies.

## Quick Project Timeline

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *Task #* | *Task Name* | *Duration* | *Start Date* | *End Date* | *Deliverables/Features expected* |
| *Task 1 (Fall 24’)* | *Finalize Contract* | *2 weeks* | *08/25/2025* | *09/07/2025* | *Signed team contract by advisor.* |
| *Task 2 (Fall 25’)* | *Overall App Planning, Delegation, & Research* | *2 weeks* | *9/22/2025 \** | *10/05/2025\** | *Defined architecture, team roles finalized, research on phishing templates, OSINT, and ethical boundaries.* |
| *Task 3 (Fall 25’)* | *Front End Development* | *10 weeks* | *09/28/2025\** | *12/14/2025\** | *Login/authentication screens, administrative dashboard prototype, responsive layout for campaign management pages.* |
| *Task 4 (Fall 25’)* | *Back End Development* | *10 weeks* | *09/28/2025\** | *12/14/2025\** | *Database schema finalized (SQLite), Web API endpoints for campaign creation, target management, and reporting, email sending functionality integrated.* |
| *Task 5 (Fall 25’)* | *UI Development and Design* | *10 weeks* | *09/28/2025\** | *12/14/2025\** | *Create mock-ups of UI design to be used for front-end HTML dashboard. Create logo and overall design aesthetic for client interface.* |
| *Task 6 (Fall 25’)* | *Milestone Checkpoint. Assess features for finalization.* | *2 weeks* | *12/1/2025\** | *12/14/2025\** | *Assess backlog, roadblocks, and features according to priority.* |
| *Task 7 (Spring 26’)* | *Finalize, Implementation, and Testing* | *4 weeks* | *01/13/2026\** | *02/15/2026\** | *Finalize a working version of the software with finalized features. Test version for issues and remediation.* |
| *Task 8 (Spring 26’)* | *Functionality & Process Documentation* | *2 weeks* | *02/15/2026\** | *02/28/2026\** | *Compile documentation for the project process.* |
| *Task 9 (Spring 26’)* | *Create deliverables for presentation and submission* | *4 weeks* | *03/1/2026\** | *03/31/2026\** | *Create any marketing materials for presentation.* |
| *Task 10 (Spring 26’)* | *Present at UC Expo* |  |  | *04/08/2026\** |  |
| *Task 11 (Spring 26’)* | *Submission* |  |  | *04/26/2026\** | *Submit all required deliverables* |
| *\* Dates subject to slight changes based on future academic calendar.* | | | | |  |

## Technologies Used

* *Figma – UI Design*
* *Development Stack:*
  + *Blazor/Razor – Front End*
  + *ASP.NET Core Web API – Back End*
  + *SQLite – Database (Local Storage)*
  + *Optional APIs*
* *GitHub – Version Control*
* *Microsoft Office Suite – Documentation and Deliverables*

## Ethical Considerations

Campaigns will only be executed after obtaining documented authorization from the sponsoring organization. Participants will be aware (explicitly or via organizational policies) that testing may occur, although specific test content may be undisclosed to maintain realism (Whitman, 2018).

Given that our campaign will store personal information and data, it will be paramount that the information is secured against unwanted access. Proper authentication for access to the campaign will add a level of security on top of the default device security. Any information in transit or stored outside of the end user's device should be encrypted and protected by robust security measures (Patel, 2024).

Only necessary Personally Identifiable Information (PII) will be used, either provided directly by the organization or collected ethically through publicly available sources (OSINT). Data collected during campaigns (clicks, submissions, response times) will be stored securely and minimized to reduce risk exposure. A documented data retention and deletion policy will govern how long user data is kept (NIST, 2021).

With privacy in mind, the campaign should only collect and store information necessary for it to function as intended. Should the application require information storage for functionality, Informed Consent should be provided from the end user. In doing so, the campaign should explain what information is gathered and for what purpose (Patel, 2024).

All campaigns will comply with applicable local and international laws, as well as organizational policies. Unauthorized access, data exfiltration, or unapproved phishing is strictly prohibited (Whitman, 2018)

It will be paramount the campaign operates as intended, however an advisement to the user to have other methods of phishing awareness and prevention. A user should agree to terms that state the campaign, and its developers, cannot be held liable if it does not work as intended or from misuse of the campaign.

## Team Rules

1. Plagiarism will be taken seriously and will not be accepted by members within the group. We will follow all the rules and guidelines set forth by the University of Cincinnati and have a zero-tolerance policy. If a member of the team is found to be plagiarizing the team will handle it internally as much as possible.
2. All individual members of the group will do all their assigned work and have it done according to the scheduled timeline. If a member is unable to complete their assigned work for any reason they must, within a reasonable amount of time, let the other group members know, and a plan will be put in place to correct the issue.
3. All members of the group will be present at all scheduled class times and meetings. If there is an absence or period of extended absence the member must notify the group as soon as possible and inform the instructor of the extended absence.

1. Team members must respond to group communications (email, teams chat, SMS text, call) within 48 hours unless prior notice is given (travel, illness, emergencies, etc).
2. If a member does not respond for 1 week, the team will attempt multiple methods of contact mentioned in rule 4. If a member does not respond for 2 consecutive weeks, the issue will be escalated to the project advisor.
3. If a member is unresponsive or fails to complete assigned tasks, the remaining team members may redistribute the work to ensure project progress. The absent member will not receive credit for redistributed tasks.
4. A member who is unresponsive for 3 weeks without a legitimate reason will be considered to have abandoned the team. The advisor will be notified immediately, and the member will be removed from the team pending advisor guidance.
5. If disputes over fairness of workload or contribution, the team will document the situation and present it to the advisor for mediation.
6. The team will maintain a shared log of task assignments and completions (via Github). Failure to update or complete tasks will be visible to all members and advisor.

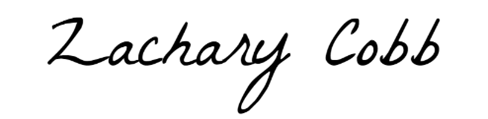
# **Team Signatures:**

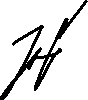


Signature: \_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



Date: \_\_\_\_\_\_09/21/2025 \_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_09/21/2025\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: 



Date: \_\_9/21/2025\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: 9/21/2025

# References

NIST Special Publication 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security (6th Edition). Cengage Learning. [Chapter on Social Engineering]

ENISA. (2020). Guidelines on Security Awareness and Training. European Union Agency for Cybersecurity.