

MICHIGAN STATE
UNIVERSITY

Project Plan Phish Phinder

The Capstone Experience

Team Auto-Owners

Gabrielle Singher – Client Liaison & Back-End Developer

Madison Bowden – Data Science Lead

Jacob Loukota – Project Manager & Front-End Developer

Hunter Hysni – Back-End Lead

Alex Larson – Front-End Lead

Department of Computer Science and Engineering

Michigan State University

Spring 2020



*From Students...
...to Professionals*

Functional Specifications

- Improve current methods for dealing with phishing emails in the workplace.
- Outlook Add-in
 - Allows users to send emails to an algorithm that will scan them.
- Phishing Detection Algorithm
 - Determines whether an email is Innocuous, Suspected Phish, Confirmed Phish, or Spam with an associated confidence score.
 - The algorithm will also pull key features known to phishing attempts from the email to present back to the user in Outlook an educational manner.
- Administrator and Executive Webpages
 - Two webpages will be available for admin users and executives to view aggregated reports and logistics relating to the Outlook Add-in.

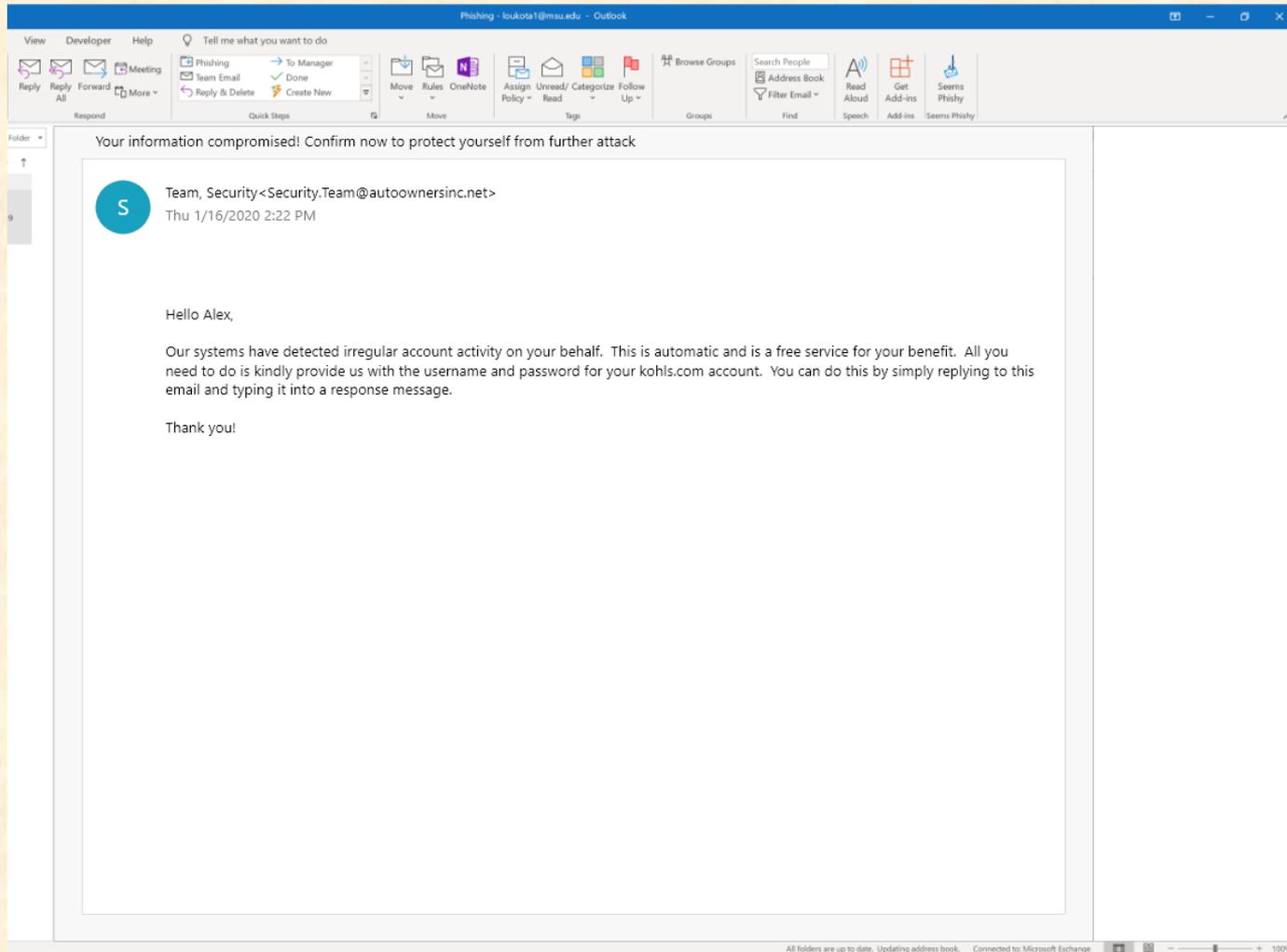


Design Specifications

- Outlook Add-in
 - Associate-facing feature
 - Needs to have a button in a convenient and noticeable place.
 - Provide quick feedback times and be convenient for the associates so they will actually read and understand the contents of the tutorial to be presented to them in a sidebar on Outlook.
- Analytics Dashboard Webpage
 - Simplistic using graphs and visuals to get the most important aggregated statistics across so that the logistics can be understood and used by executives to monitor the effectiveness of the Phish Phinder and any current threats to the company.
- Email Review Webpage
 - Allow filtering and categorization so that the admins and security team feel less overwhelmed by allowing the team to deal with potential threats in a more streamlined manner.



Screen Mockup: Outlook Add-in



Screen Mockup: Outlook Add-in (Phishing Email)

The screenshot displays the Outlook interface with a phishing email and a security notification. The email is from 'Team, Security' with a suspicious sender address. The 'Phish Finder' add-in provides a confidence rating of 95% and identifies two suspicious elements: a suspicious address and an offering of free service.

Your information compromised! Confirm now to protect yourself from further attack

S Team, Security <Security.Team@autoownersinc.net>
Thu 1/16/2020 2:22 PM

Hello Alex,

Our systems have detected irregular account activity on your behalf. This is automatic and is a **free** service for your benefit. All you need to do is kindly provide us with the **username** and **password** for your **kohls.com** account. You can do this by simply replying to this email and typing it into a response message.

Thank you!

Thanks for alerting us!

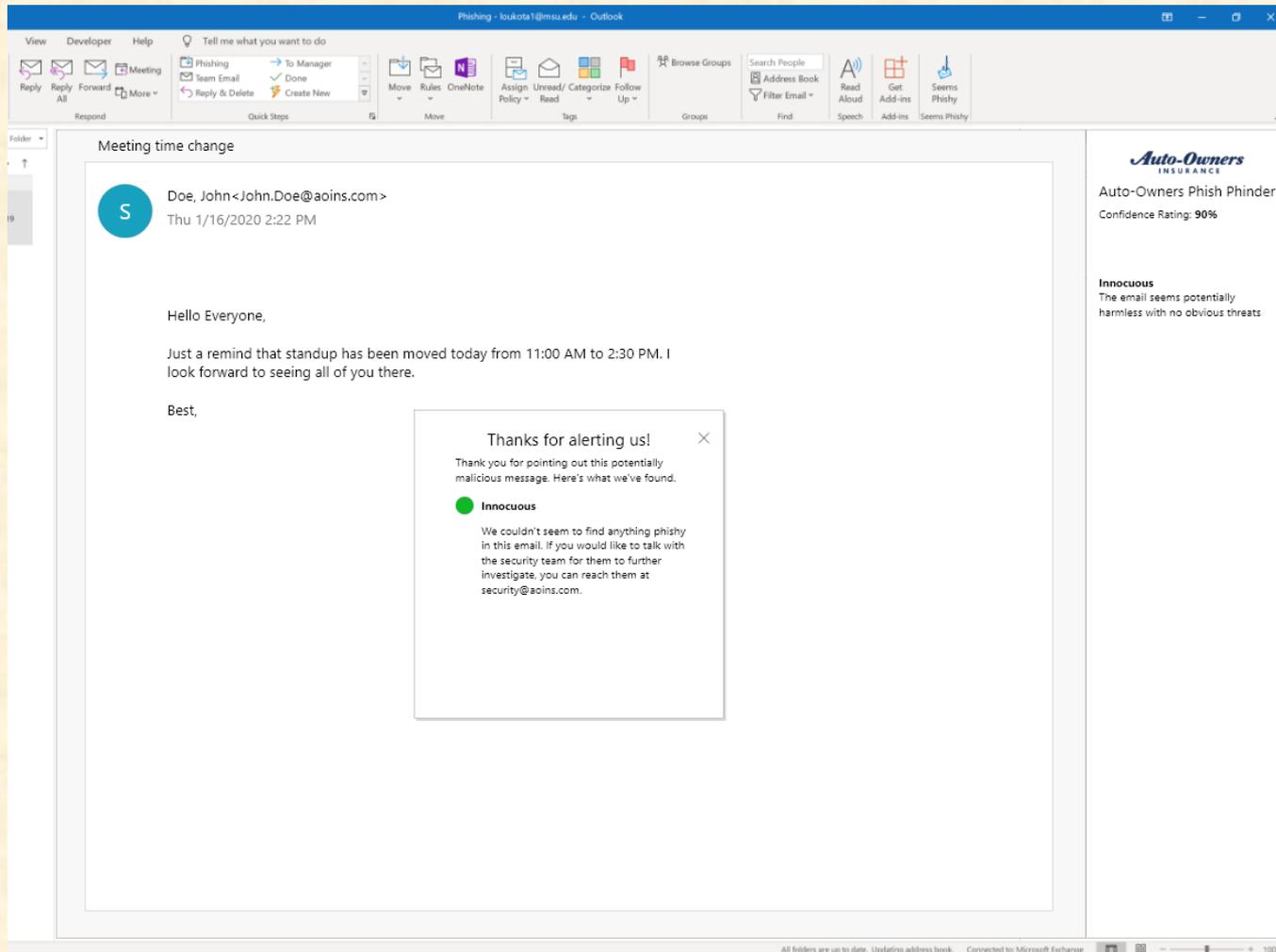
Thank you for pointing out this potentially malicious message. Here's what we've found.

- Suspicious Address** @autoownersinc.net
It appears as though the sender's email address is external. This can oftentimes be a good indicator of malicious activity especially if they are also asking for personal information.
- Offering of Free Service** "free"
It appears as though the sender mentioned the opportunity of free goods and services which is normally a good indication that the sender is malicious. It is common for the sender to also

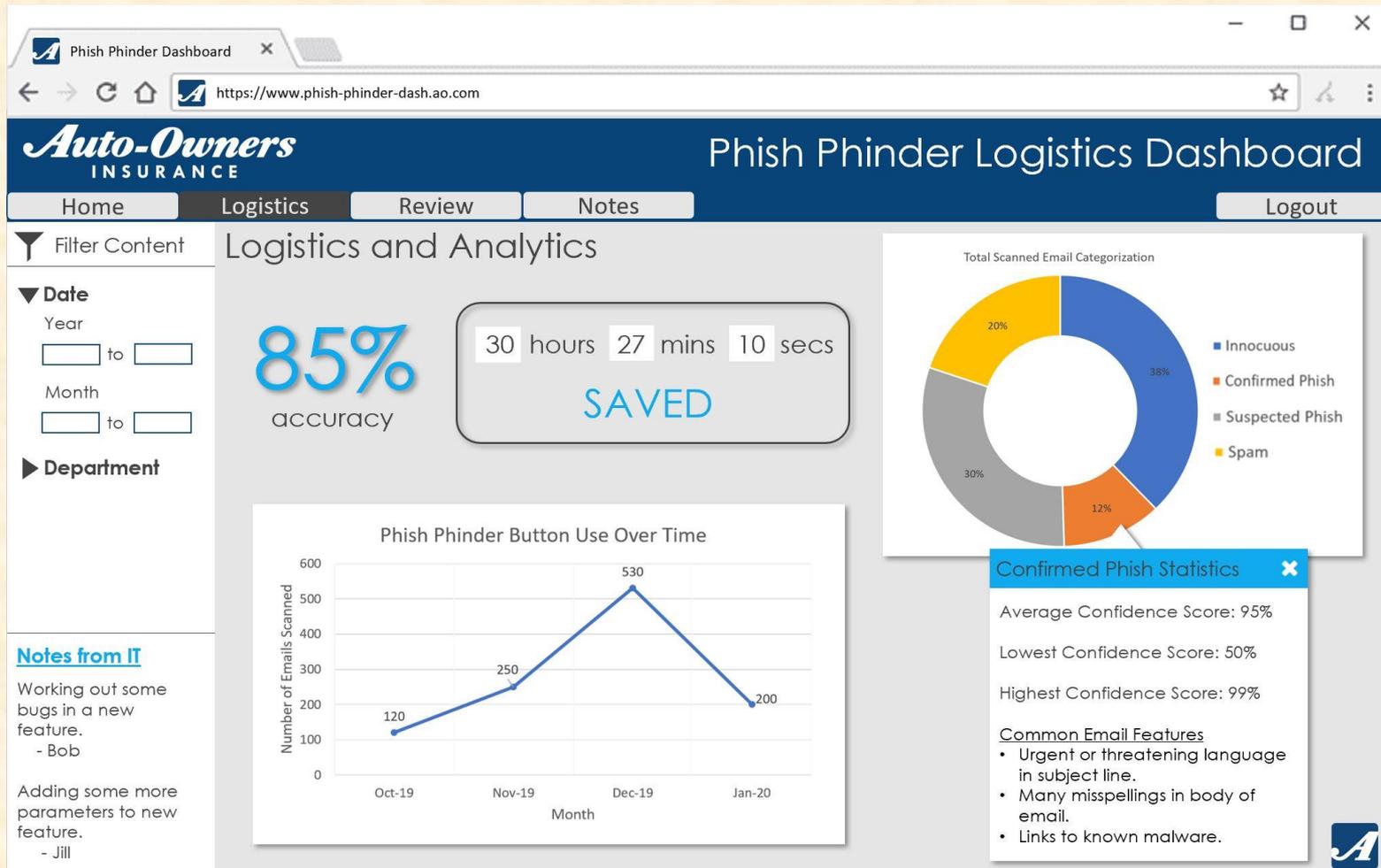
Auto-Owners INSURANCE
Auto-Owners Phish Finder
Confidence Rating: **95%**
Suspected Phish
The email contains elements that indicate a bad actor is attempting to gain information or engage in malicious behavior against the recipient.



Screen Mockup: Outlook Add-in (Innocuous Email)



Screen Mockup: Logistics Dashboard Webpage



Screen Mockup: Email Review Webpage

The screenshot displays the 'Phish Phinder Email Review' interface. The top navigation bar includes 'Auto-Owners INSURANCE' and 'Phish Phinder Email Review'. Below this, there are tabs for 'Home', 'Logistics', 'Review', and 'Notes', along with a 'Logout' button. The main content area is divided into two sections: a list of emails on the left and a detailed view of the selected email on the right.

Left Panel - Email List:

Category	Sender	Time	Subject
Innocuous	No Sender	11:55 PM	Your information compromised! Confirm...
Suspected Phish	No Sender	12:00 PM	Sales numbers
Confirmed Phish	No Sender	3:25 PM	Act Now to save 10% on services
	No Sender	10:30 PM	Act by the end of the day to receive...
	No Sender	7:50 PM	Let's connect to help you save hundreds!
	No Sender	2:45 PM	Important! Your password will expire...
	No Sender	3:22 PM	Click to save time and money!!!

Right Panel - Detailed View:

No Sender <unknown email> Tue 1/21/2020 3:25

Act Now to save 10% on services

Alex,

We are offering many specials at different times of year. Please click the link below to see how you could save 10% on our services now!

www.amazon.com/specialOffers

- Customer Care Team

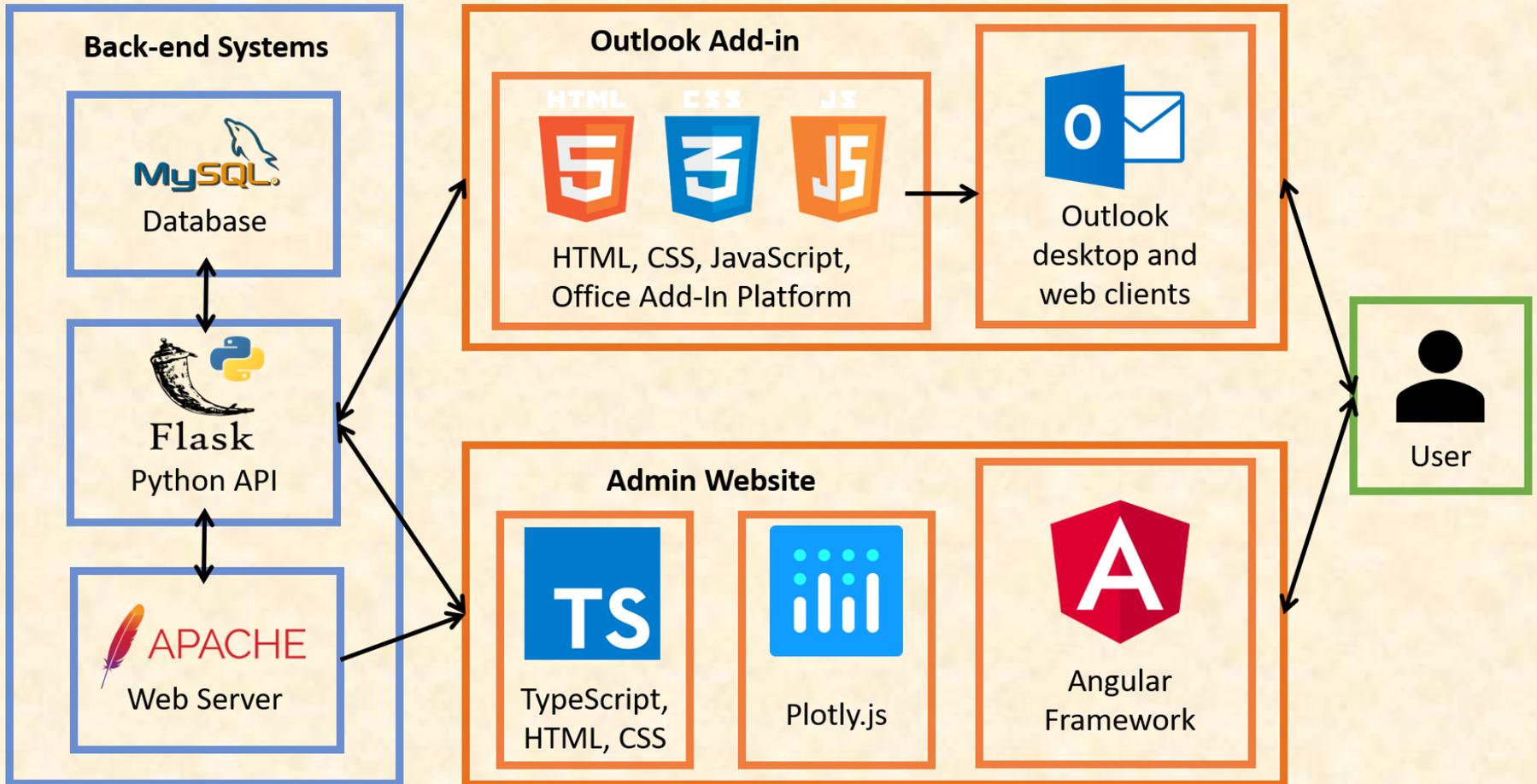


Technical Specifications

- Frontend User Interface
 - Outlook Add-in
 - Angular framework for website for analytics dashboards and suspicious email reviews
- Backend Phishing Analysis
 - MySQL server retaining information from email scans
 - Python Flask
 - Apache Web Server
 - Phishing analysis algorithm based on common phish features



System Architecture



System Components

- Hardware Platforms
 - Rack-mounted server running Ubuntu 18.04
 - iMacs running Windows 10 through VMWare Fusion
 - MySQL Database
- Software Platforms / Technologies
 - Outlook
 - HTML, CSS, JavaScript, Plotly.js, Angular
 - Python Flask
 - Apache Web Server



Risks

- **Phishing Detection Algorithm | Difficulty: High | Priority: High**
 - **Description:** The algorithm needs to catch all variations of phishing emails and differentiate between Spam, Suspected Phish, Confirmed Phish, and Innocuous.
 - **Mitigation:** Create varying testing emails having aspects ranging from obvious phishing tactics to subtle ones and make sure our algorithm catches all instances.
- **Security Issues with Handling Associate Emails | Difficulty: Medium | Priority: High**
 - **Description:** Associate information is important to protect, and it is imperative that our solution handles the protection and security of the information accordingly. This is a scalability issue as well because of the handling of all emails received by all associates.
 - **Mitigation:** Have log-ins for everything that is publicly facing and do not move data unless needed.
- **Creating an Effective and Useable Outlook Add-in | Difficulty: Medium | Priority: High**
 - **Description:** The team has not had experience creating Outlook add-ins before. We need to find the right way to create one that will supplement the goal of its function. It also needs to be in a good location in the Outlook application and something that users would utilize.
 - **Mitigation:** Research and ask contacts about the creation of good Outlook add-ins. Create prototypes and have users test the experience.



Questions?

?

?

?

?

?

?

?

?

?

