

MICHIGAN STATE

U N I V E R S I T Y

Alpha Presentation

Phish Phinder

The Capstone Experience

Team Auto-Owners

Gabrielle Singher

Jacob Loukota

Madison Bowden

Hunter Hysni

Alex Larson

Department of Computer Science and Engineering

Michigan State University

Spring 2020



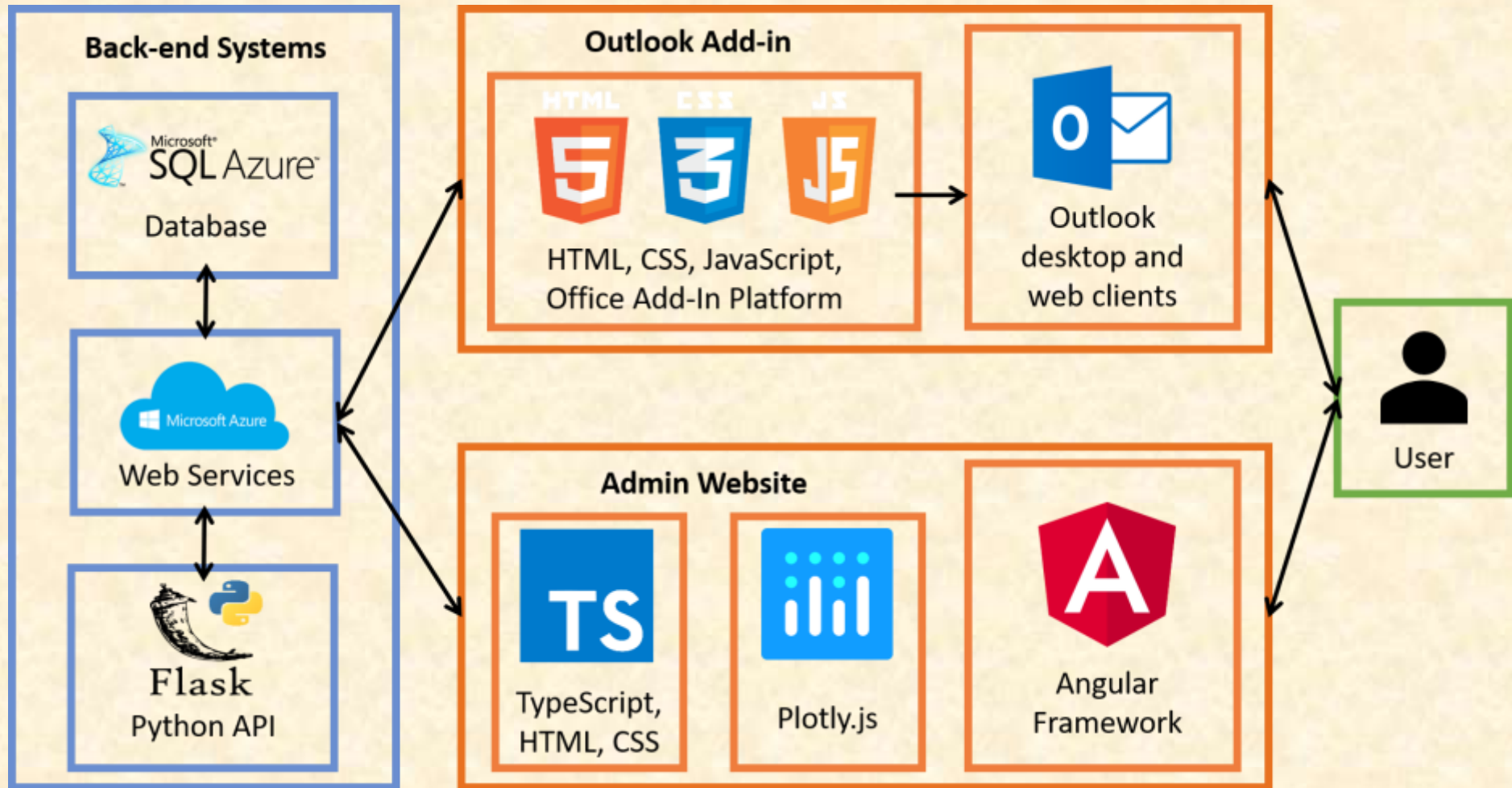
*From Students...
...to Professionals*

Project Overview

- Auto-Owners Insurance offers life, home, auto and business insurance.
- Every day, associates receive multiple phishing emails.
- Phish Phinder is an Outlook add-in that scans emails using a phishing detection algorithm.
- Provides a categorization, confidence score, and an educational tutorial about suspicious features.
- A dashboard and email review system are available to administrators and executives.



System Architecture



Suspected Phish in Outlook

Urgent! Recent Log-in to Your Gmail Account from a Different Device

Singher, Gabrielle
To: Bowden, Madison
Thu 2/13

Bob,

We noticed that there was a log in from a different device. Please review the information below about the device used to log in.

Date & Time: Friday, January 31 12:00 PM ET
Browser: Chrome
Operating System: Linux
Location: Paris, France

If this does not seem like it was you, go to this link <https://www.google.com/gmail/> to log into your account and block this other user. We encourage you to do this as soon as possible!

Gmail Team

Phish Phinder

Auto-Owners INSURANCE
LIFE • HOME • CAR • BUSINESS

Category **Suspected Phish**

This email contains elements that indicate a bad actor is attempting to gain information or engage in malicious behavior against the recipient. It's probably best to delete this email.

Confidence Score **100 %**

Identified Features

For more details, click on any of the features below, or press show all to expand everything.

Show All

Links	Take caution before opening any links. Hover over a link before clicking it to see where you're being redirected to. If you aren't sure the link is safe, don't open it.
Urgency	Bad actors may try to scare the reader into acting irrationally by insisting on urgent behavior or negative consequences.
User information	Requests for personal user, customer, or client



Suspected Phish in Outlook

Category

Suspected Phish

This email contains elements that indicate a bad actor is attempting to gain information or engage in malicious behavior against the recipient. It's probably best to delete this email.

The category and the text color indicate to the user that this email is not safe.

The description below the category explains to the user that they were right in reporting it, and that it would be safest for the user to delete the email.

The user should view the “Identified Features” to further educate themselves on what to look out for in future phishing attempts.



Phish Phinder

Auto-Owners
INSURANCE
LIFE • HOME • CAR • BUSINESS

Category **Suspected Phish**

This email contains elements that indicate a bad actor is attempting to gain information or engage in malicious behavior against the recipient. It's probably best to delete this email.

Confidence Score **100 %**

Identified Features

For more details, click on any of the features below, or press show all to expand everything.

[Show All](#)

Links	Take caution before opening any links. Hover over a link before clicking it to see where you're being redirected to. If you aren't sure the link is safe, don't open it.
Urgency	Bad actors may try to scare the reader into acting irrationally by insisting on urgent behavior or negative consequences.
User information	Requests for personal user, customer, or client



Suspected Phish in Outlook

Phish Phinder

Hide All

Links
Take caution before opening any links. Hover over a link before clicking it to see where you're being redirected to. If you aren't sure the link is safe, don't open it.

These are what we found:

- **Domain Disparity**
 - <https://www.google.com/gmail/>
 - <https://security.berkeley.edu/education-...>
 - <https://security.berkeley.edu/education-...>
 - <https://www.google.com/gmail/ to log..>
- **Tinyurl or Bit.ly**
 - <https://www.google.com/gmail/>
 - <https://security.berkeley.edu/education-...>
 - <https://security.berkeley.edu/education-...>
 - <https://www.google.com/gmail/ to log..>
- **Link Text**
 - <https://security.berkeley.edu/education-...>

Urgency
Bad actors may try to scare the reader into acting irrationally by insisting on urgent behavior or negative consequences.

These are what we found:

- !
- soon

List of suspicious links in the email.

“Show All” function is active and “Hide All” button is visible. Allows user to view all features at once.

“Show All” button is inactive, and users can view features one at a time by selecting each.

Phishing adversaries tend to incite urgency through the wording on their emails to get the user to act quickly.

Phish Phinder

Identified Features

For more details, click on any of the features below, or press show all to expand everything.

Links
Take caution before opening any links. Hover over a link before clicking it to see where you're being redirected to. If you aren't sure the link is safe, don't open it.

Urgency
Bad actors may try to scare the reader into acting irrationally by insisting on urgent behavior or negative consequences.

User information
Requests for personal user, customer, or client information should be handled with caution.

These are what we found:

- user

Show All



Suspected Phish in Outlook

Personal information

Never send personal information like passwords or usernames over email. If you think you need to confirm any personal information, do not click on links in the email or phone number listed - they might redirect traffic elsewhere. Instead, navigate to the authentic homepage.

These are what we found:

- log
- here
- link

Phishing emails aim to gather information. Personal Information is a feature set of words that aim to collect credentials belonging to the recipient.

The sidebar shows this “Thanks for alerting us!” message every time an email is scanned. IT security personnel are able to review every email if desired and take actions on them.

Certain key words are searched for in the subject as was done for the body of the email. The features found are listed. Phishing attempts tend to introduce urgency in the subject line.

Subject

Be careful of subject lines that are designed to make the reader act with urgency and not to think. Offerings of free services or requests for personal information are also characteristic of phishing attempts.

These are what we found:

- Urgency
- Verify
- Personal information

Thanks for alerting us!

Thank you for pointing out this potentially malicious message. The IT security team looks into all possible threats if you have any concerns or questions regarding phishing.



Spam Email in Outlook

The screenshot shows the Outlook interface with a blue header bar. The main window displays an email from Grubhub with the subject "Study Break: \$7 off your first Grubhub delivery order of \$10+". The email body features a photo of food and the Grubhub logo. To the right, a "Phish Phinder" window is open, displaying the "Auto-Owners INSURANCE" logo and a "Spam" category. The Phish Phinder window also shows a confidence score of 80% and a list of identified features such as Links, Urgency, and Update.

Help Tell me what you want to do


Capstone To Manager
Team Email Done
Reply & Delete Create New

Move Rules OneNote
Assign Policy Categorize Follow Up
Unread/Read
Search People Address Book Filter Email
Read Aloud Get Add-ins Report Message Insights Phish Phinder

Study Break: \$7 off your first Grubhub delivery order of \$10+

Grubhub <Grubhub@imleagues.com> (Grubhub via mail42.suw15)
To: Bowden, Madison Thu 2/13

You forwarded this message on 2/14/2020 11:36 AM.
If there are problems with how this message is displayed, click here to view it in a web browser.
The actual sender of this message is different than the normal sender. Click here to learn more.


GRUBHUB
\$7 off your first delivery order of \$10+!

Phish Phinder

Auto-Owners
INSURANCE
LIFE • HOME • CAR • BUSINESS

Category **Spam**

This email is primarily marketing in nature but otherwise innocuous

Confidence Score **80 %**

Identified Features

For more details, click on any of the features below, or press show all to expand everything.

Links **Show All**
Take caution before opening any links. Hover over a link before clicking it to see where you're being redirected to. If you aren't sure the link is safe, don't open it.

Urgency
Bad actors may try to scare the reader into acting irrationally by insisting on urgent behavior or negative consequences.

Update
Emails requesting information, updates, or confirmation might be suspicious, especially if it's



Spam Email in Outlook

Words in the body that indicate an account, whether a membership, rewards, or other.

Verify

Be careful whenever an email asks you to verify account information. Make sure you check the sender and inspect any links before clicking.

These are what we found:

- account

Personal information

Never send personal information like passwords or usernames over email. If you think you need to confirm any personal information, do not click on links in the email or phone number listed - they might redirect traffic elsewhere. Instead, navigate to the authentic homepage.

These are what we found:

- click
- here

Sender

Always take extra caution when receiving emails from external to the organization.

These are what we found:

- Your domain: msu
- Sender's domain: imleagues

Sender email address does not match recipient's address which is expected for spam.



Innocuous Email in Outlook

The screenshot shows the Outlook interface for a user named 'Demo - bowdenm1@msu.edu'. The email being viewed is titled 'Team Auto-Owners: Project Plan Presentation Evaluation' and is from Wayne Dyksen (DW). The email content includes a PDF attachment named 'team-auto-owners-project-plan-evaluation.pdf' (145 KB) and text regarding project plan presentation feedback. On the right side of the interface, a 'Phish Phinder' notification is displayed, indicating that the email is categorized as 'Seems Harmless' with a 90% confidence score. The notification also includes a thank you message for reporting the potentially malicious message.

Help Tell me what you want to do

Reply Forward More -

Respond

Quick Steps

Move

Phish Phinder

Team Auto-Owners: Project Plan Presentation Evaluation

DW Dyksen, Wayne

To: Bowden, Madison; Hysri, Hunter; Larson, Alex; Loukota, Jacob; Singhet, Gabrielle

Cc: Johnson, Ryan

2/5/2020

You forwarded this message on 2/14/2020 11:35 AM

team-auto-owners-project-plan-evaluation.pdf
145 KB

Team Auto-Owners,

Attached is feedback for your Project Plan Presentation.

Recall that, with respect to your team grade, the project plan presentation and project plan document together are worth 10 points. The grade in the attached is strictly for the presentation, so it's out of 5 points. The remaining 5 points are associated with the document itself and will be assigned later in the semester.

James and Ryan will be providing you with written feedback on your project plan document. You will be able to incorporate that feedback and resubmit it at a due date later in the semester for grading by James and Ryan

Keep up the good work,

Dr. D.

Phish Phinder

Auto-Owners
INSURANCE

LIFE • HOME • CAR • BUSINESS

Category **Seems Harmless**

We didn't find anything! This email seems potentially harmless with no obvious threats. But if you're still concerned, being cautious is always a good plan.

Confidence Score **90 %**

The features in this email determine the confidence rating for the categorization above. Confidence ratings go from 0 to 100% based on the features and number of features found. The classification above is determined by the highest confidence per category (Seems Harmless, Spams Suspected Phish, or Confirmed Phish). However, it's always a good idea to be cautious if you think something is suspicious.

Thanks for alerting us!

Thank you for pointing out this potentially malicious message. The IT security team looks into all possible threats if you have any concerns or questions regarding phishing.



Innocuous Email in Outlook

Category

Seems Harmless

We didn't find anything! This email seems potentially harmless with no obvious threats. But if you're still concerned, being cautious is always a good plan.

Information icon has been clicked and information is expanded below confidence score.

Confidence Score

90 % ⓘ

The features in this email determine the confidence rating for the categorization above. Confidence ratings go from 0 to 100% based on the features and number of features found. The classification above is determined by the highest confidence per category (Seems Harmless, Spam, Suspected Phish, or Confirmed Phish). However, it's always a good idea to be cautious if you think something is suspicious.

Thanks for alerting us!

Thank you for pointing out this potentially malicious message. The IT security team looks into all possible threats if you have any concerns or questions regarding phishing.

Phish Phinder

Auto-Owners
INSURANCE
LIFE • HOME • CAR • BUSINESS

Category

Seems Harmless

We didn't find anything! This email seems potentially harmless with no obvious threats. But if you're still concerned, being cautious is always a good plan.

Confidence Score

90 % ⓘ

The features in this email determine the confidence rating for the categorization above. Confidence ratings go from 0 to 100% based on the features and number of features found. The classification above is determined by the highest confidence per category (Seems Harmless, Spam, Suspected Phish, or Confirmed Phish). However, it's always a good idea to be cautious if you think something is suspicious.

Thanks for alerting us!

Thank you for pointing out this potentially malicious message. The IT security team looks into all possible threats if you have any concerns or questions regarding phishing.



Phish Market (Analytics Dashboard)



Phish Market (Analytics Dashboard)

Auto-Owners
INSURANCE

Phish  Phinder

Dashboard

Review

Phish Market

Enter Date Range

mm/dd/yyyy

mm/dd/yyyy

Allows the ability to filter the data being represented in the graphs based off date.

Navigation buttons to go between the dashboard (“Phish Market”) and the review system (“Phishing Net”).

The graphics and diagrams visual on the dashboard are used for analyzing the accuracy of the phishing algorithm and monitoring the effectiveness of it in the company.



Phishing Net (Email Review System)

The screenshot shows the Phishing Net web application interface. At the top, there is a navigation bar with the "Auto-Owners INSURANCE" logo, the "Phish Phinder" title, and buttons for "Dashboard" and "Review". The user is logged in as "Hi Alex!" with a "Log Out" button. Below the navigation bar, the main content area is titled "Phishing Net" and features a search bar. On the left, a "Filter By" sidebar includes checkboxes for "Seems Harmless", "Spam", "Suspected Phish" (checked), "Confirmed Phish", "Processed", and "Unprocessed", along with a "Filter" button. The central "Message List" displays several email entries, with the top one selected: "Urgent! Recent Log-in to Your Gmail A...". The selected email details show the sender "bowdenm1@msu.edu" and a timestamp of "2020-02-17 23:00:03.457000". The email body text reads: "Bob, We noticed that there was a log in from a different device. Please review the information below about the device used to log in. Date & Time: Friday, January 31 12:00 PM ET Browser: Chrome Operating System: Linux Location: Paris, France If this does not seem like it was you, go to this link https://www.google.com/gmail/ to log into your account and block this other user. We encourage you to do this as soon as possible! Gmail Team". Below the email text is a "Processing" modal with a "Recategorize" dropdown and a "Done" button. On the right, an "Email Overview" panel displays a "Suspected Phish" status with a "Confidence rating: 100%". It includes sections for "User Information" (Requests for personal user, customer, or client information should be handled with caution), "Urgency" (Bad actors may try to scare the reader into acting irrationally by insisting on urgent behavior or negative consequences), and "Verify" (Be careful whenever an email asks you to verify account information. Make sure you check the sender and inspect any links before clicking).



Phishing Net (Email Review System)

Email Review System

Search

Filter By

- Innocuous
- Spam
- Suspected Phish
- Confirmed Phish

- Unread
- Read

Sender	Message Subject
alert@messages.alert.msu.edu	MSU Timely Warning: Burglary
noreply@github.com	[GitHub] A third-party OAuth application has been added to your account
noreply@github.com	[GitHub] A third-party OAuth application has been added to your account
service@co-operativebank.co.uk	The Co-operative Bank p.l.c. Attention (Needed Update Account Information)
service@nafcu.org	[NOTIFICATION] - Confirm Your Federal Credit Union Credit/Debit Card Information
service@paypal.com	IMPORTANT: Notification of limited accounts
	Your Barclays Online Account

Allows the ability to search for key words to find emails easily.

List of emails scanned by Phish Phinder algorithm. The list can be filtered and searched.

Allows the ability to filter the emails listed to the right.



Phishing Net (Email Review System)

Urgent! Recent Log-in to Your Gmail Account from a Different Device



bowdenm1@msu.edu

2020-02-17 23:00:03.457000

Bob, We noticed that there was a log in from a different device. Please review the information below about the device used to log in. Date & Time: Friday, January 31 12:00 PM ET Browser: Chrome Operating System: Linux Location: Paris, France If this does not seem like it was you, go to this link <https://www.google.com/gmail/> to log into your account and block this other user. We encourage you to do this as soon as possible! Gmail Team

Processing

Recategorize

Done

Confirm Status

The scanned emails are viewable in full for administrators to IT security personnel to analyze and confirm.

Email Overview

Suspected Phish

Confidence rating: 100%

User information

Requests for personal user, customer, or client information should be handled with caution.

Urgency

Bad actors may try to scare the reader into acting irrationally by insisting on urgent behavior or negative consequences.

Verify

Be careful whenever an email asks you to verify account information. Make sure you check the sender and inspect any links before clicking.

Allows administrators and IT security personnel with access to recategorize scanned emails and process them by confirming correct status. Emails can be recategorized to Confirmed Phish, Suspected Phish, Spam and Seems Harmless.

The educational tutorial of the identified features within the email are shown here. It is like what is visible in the Outlook sidebar to users.



What's left to do?

- Improve the classification algorithm
- Finish email review system functionalities
- Dashboard data analysis
- User testing
- Unit testing



Questions?

?

?

?

?

?

?

?

?

?

