

**MICHIGAN STATE**  

---

**U N I V E R S I T Y**

# Beta 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 2019



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

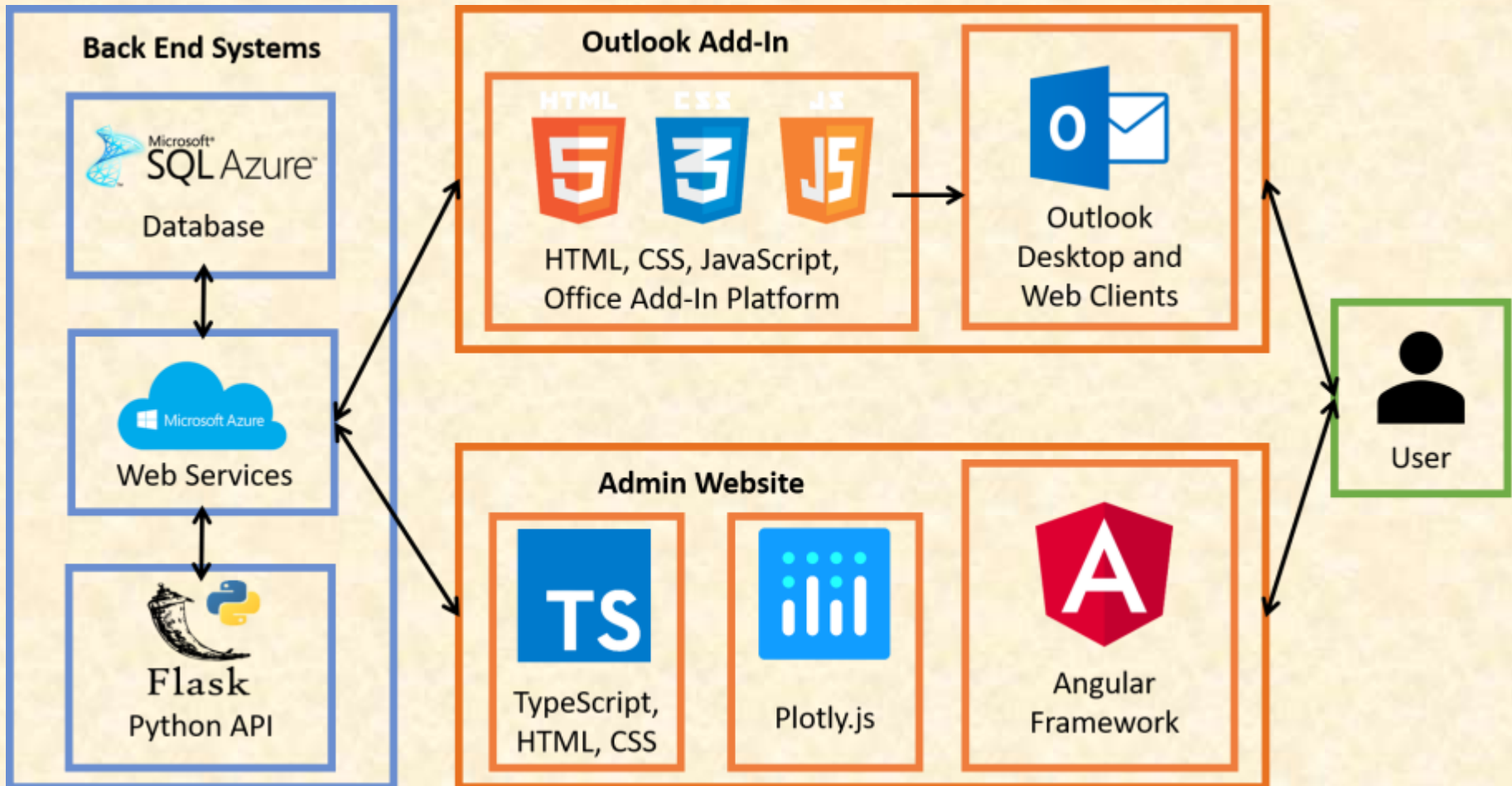
# Project Overview

---

- Every day, associates receive a multitude of phishing emails.
- Phish Phinder is an Outlook add-in that scans emails using a phishing detection algorithm.
- It 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

The screenshot displays the Microsoft Outlook interface. The top ribbon includes the 'Add-ins' section, where the 'Phish Phinder' add-in is highlighted with a red box and labeled 'Add-in Button'. The main content area shows an email from 'Singher, Gabrielle' with the subject 'Urgent! Recent Log-in to Your Gmail Account from a Different Device'. The email body contains a warning about a log-in from a different device and includes a link to the recipient's Gmail account. The right-hand pane shows the 'Phish Phinder' analysis results, which categorize the email as 'Suspected Phish' with a 100% confidence score. The analysis identifies features such as 'Links' and 'Urgency' that are characteristic of phishing attempts.

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

Singher, Gabrielle  
To: Bowden, Madison  
Sat 2/15/2020 8:48 AM

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 asap!

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.

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 inserting an

Email View  
Singher, singherg@msu.edu



# Suspected Phish in Outlook

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

 Singher, Gabrielle  
To: Bowden, Madison

[Reply](#) [Reply All](#) [Forward](#) [More](#)

Sat 2/15/2020 8:48 AM

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.

[Action Items](#) [+ Get more add-ins](#)

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 asap!

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

**Email View**  
Singher, [singherg@msu.edu](mailto:singherg@msu.edu)





# Suspected Phish in Outlook

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

**Email View**  
Singher, [singherg@msu.edu](mailto:singherg@msu.edu)

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**

*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.*

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



# Suspected Phish in Outlook

Phish Phinder

*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.

**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

### Email View

Singher, Gabrielle  
singherg@msu.edu

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

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.

Phish Phinder

*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.

**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

### Email View

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 asap!

Phish Phinder

Confidence Score **100 %**

### Identified Features

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

**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:

- 1

### Email View

Singher, Gabrielle  
singherg@msu.edu

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

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.

### Thanks for alerting us!

Thank you for pointing out this potentially malicious message. The IT security team looks into all possible



# Suspected to Confirmed Phish in Review System - Recategorized

The screenshot displays a phishing review system interface. On the left, a 'Filter By' sidebar includes options for 'Seems Harmless', 'Spam', 'Suspected Phish' (checked), 'Confirmed Phish', 'Processed', and 'Unprocessed' (checked). Below the filters are 'Start date' and 'End date' fields with calendar icons, and a 'Filter' button. The main list shows several emails from 'singherg@msu.edu' with subjects like 'Urgent! Recent Log-in to Your Gmail Account from a Different Device'. A detailed view of one email is shown in the center, including the subject, sender, received and scanned dates, and a 'Count: 1'. The email body contains a warning about a log-in from a different device and provides a link to log in and block the user. A green notification box at the bottom of the email view states 'The email was successfully recategorized'. On the right, an 'Email Overview' section shows the category as 'Confirmed Phish' with a 100% confidence rating. Below this is a 'Features' section with 'Subject' and 'Verify' details. An 'Associated Links' section includes a 'Scan All Again' button and two URLs: 'https://pypl.org/project/emaildata/' and 'https://urlscan.io/result/be719535-1665-4dc4-a6d8-1e703f6f6373/'. A green box at the top right, labeled 'Recategorization and Processing Action Box', contains a dropdown menu set to 'New category: Confirmed Phish' and two buttons: 'Recategorize' and 'Process'.



# Suspected to Confirmed Phish in Review System - Processed

The screenshot displays a phishing review system interface. At the top left is a search bar. Below it, a 'Sort by' section has 'Scanned' selected. On the left, a 'Filter By' sidebar includes checkboxes for 'Seems Harmless', 'Spam', 'Suspected Phish' (checked), 'Confirmed Phish', 'Processed', and 'Unprocessed' (checked). Below the filters are 'Start date' and 'End date' fields with calendar icons, and a 'Filter' button. The main list shows several emails from 'singherg@msu.edu' with the subject 'URGENT: Log in on Different Device!'. A green box highlights the top email. To the right, a detailed view of the selected email is shown, including the subject 'Urgent! Recent Log-in to Your Gmail Account from a Different Device', sender 'singherg@msu.edu', and a 'Date & Time' of 'Friday, January 31 12:00 PM ET'. The email body contains a warning about a log-in from a different device and a link to 'https://www.google.com/gmail/'. A green box at the bottom of the email view says 'The email was successfully processed.' Above the email view, a 'New category' dropdown is set to 'Confirmed Phish', with 'Recategorize' and 'Process' buttons. A green box highlights these buttons, with an arrow pointing to a text box that says 'Recategorization and Processing Action Box'. On the right, an 'Email Overview' section shows 'Confirmed Phish' and 'Confidence rating: 100%'. Below it, a 'Features' section includes 'Subject' and 'Verify' sections. At the bottom right, an 'Associated Links' section has a 'Scan All Again' button and a 'URL:' field containing 'https://pypl.org/project/emaildata/'.



# Confirmed Phish in Outlook

The screenshot displays an Outlook email interface. The main email content is on the left, and a 'Phish Phinder' analysis panel is on the right.

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

**Bowden, Madison**  
To: Singher, Gabrielle  
Mon 2/17/2020 6:00 PM

You forwarded this message on 2/18/2020 5:21 PM.

Action Items + Get more add-ins

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 **Confirmed Phish**

Confidence **100 %**

Score

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 information should be

**Email View**

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.



# Spam Email in Outlook

The screenshot displays an Outlook email interface. On the left, the email header shows the sender as 'msmr@broad.msu.esu' with a profile picture containing the letter 'M'. The recipient is 'To: msmr@broad.msu.esu'. Action buttons for 'Reply', 'Reply All', 'Forward', and a menu icon are visible. The email body contains a message from the 'MSU MSMR Student Research Team' inviting participation in a research study, with a link to a survey. On the right, a 'Phish Phinder' analysis panel is open, showing the sender as 'Phish Phinder' and the subject as 'Auto-Owners INSURANCE'. The panel indicates the email is categorized as 'Spam' with a 100% confidence score. It also lists 'Identified Features' such as 'Links' and 'Urgency'.

msmr@broad.msu.esu

msmr@broad.msu.esu  
To

Wed 4/1/2020 3:29 PM

Dear Spartans,

We would like to invite you to participate in an interesting research study where you can have an impact on a new dining app. If you would like to participate in the study, the link below will take you to the survey.

Thank you in advance for your help. Your opinions will help improve this app which might be available to MSU students shortly!

Please click the link to take the survey.  
[https://msu.co1.qualtrics.com/ife/form/SV\\_4HDHWidAvvrchil](https://msu.co1.qualtrics.com/ife/form/SV_4HDHWidAvvrchil)

Thank you,  
MSU MSMR Student Research Team

Phish Phinder

**Auto-Owners**  
INSURANCE

LIFE • HOME • CAR • BUSINESS

Category **Spam**

*This email is primarily marketing in nature but otherwise innocuous.*

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 inciting on

Email View



# Spam Email in Outlook

Phish Phinder

***Auto-Owners***  
**INSURANCE**

LIFE • HOME • CAR • BUSINESS

Category **Spam**

*This email is primarily marketing in nature but otherwise innocuous.*

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 inciting on...

Email View

Phish Phinder

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 inciting on...

Email View

**msmr@broad.msu.edu** msmr@broad.msu.edu

msmr@broad.msu.edu

Dear Spartans,

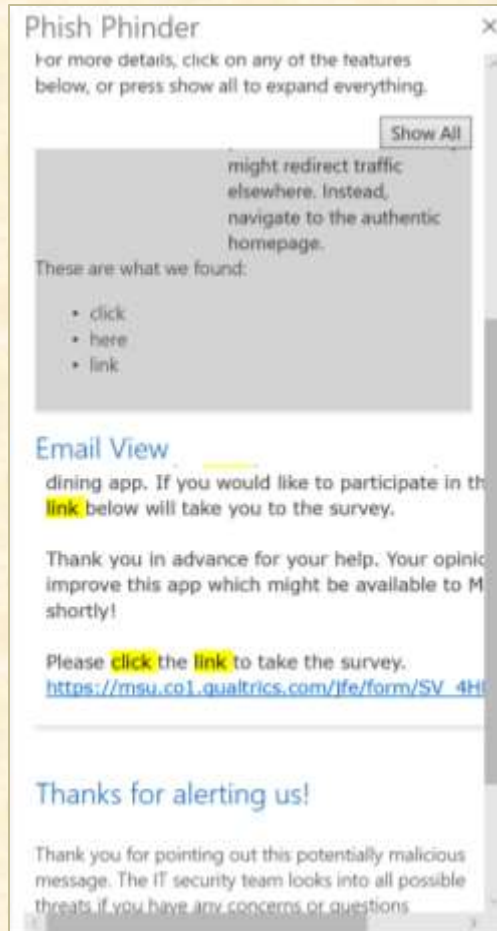
We would like to invite you to participate in a research study where you can have an impact on our dining app. If you would like to participate in the link below will take you to the survey.

Thanks for alerting us!





# Spam Email in Outlook



Phish Phinder

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

Show All

might redirect traffic elsewhere. Instead, navigate to the authentic homepage.

These are what we found:

- click
- here
- link

Email View

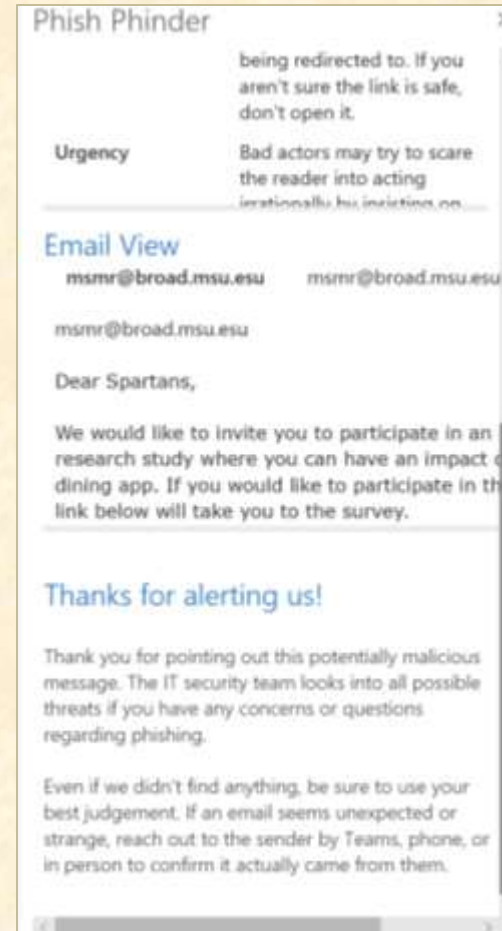
dining app. If you would like to participate in the **link** below will take you to the survey.

Thank you in advance for your help. Your opinion improve this app which might be available to M shortly!

Please **click** the **link** to take the survey.  
[https://msu.co1.qualtrics.com/jfe/form/SV\\_4H](https://msu.co1.qualtrics.com/jfe/form/SV_4H)

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



Phish Phinder

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...

Email View

msmr@broad.msu.esu msmr@broad.msu.esu

msmr@broad.msu.esu

Dear Spartans,

We would like to invite you to participate in a research study where you can have an impact on the dining app. If you would like to participate in the link below will take you to the survey.

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.

Even if we didn't find anything, be sure to use your best judgement. If an email seems unexpected or strange, reach out to the sender by Teams, phone, or in person to confirm it actually came from them.



# Harmless Email in Outlook

CSE 472 Projects and Exam

 Tong, Yiyong <ytong@msu.edu>  
To

Mon 3/30/2020 4:14 PM

Dear all,

Project 1 is online now. Please take a quick look even if you decide to start when it's closer to the deadline. The term project description is in the link provided in the grading document for Project 1. You can start filling out that part regarding what you wish to work on as the term project.

As mentioned in the class, we will have the in-class exam on April 15 during class time, which will be an open-book test.

BTW, the videos of the classes are uploaded to D2L. You may have to wait a bit for the processing to be done on mediaspace for the latest video.

Best,  
Yiyong

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 **89 %**

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



# Harmless Email in Outlook

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 **89 %**

---

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

Phish Phinder

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

---

Email View

Tong,Yiyong ytong@msu.edu

CSE 472 Projects and Exam

Dear all,

Project 1 is online now. Please take a quick look even if you decide to start when it's closer to the deadline. The term project description is in the link provided in the

---

Thanks for alerting us!

Phish Phinder

Identified Features

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

Show All

**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:

- now

---

Email View

In-class exam on April 15 during class time, which will be an open-book test.

BTW, the videos of the classes are uploaded to D2L. You may have to wait a bit for the processing to be done on mediaspace for the latest video.

Best,  
Yiyong

---

Thanks for alerting us!



# Phishing Net (Email Review System)

The screenshot displays the Phish Phinder web interface. At the top, the header includes the Auto-Owners Insurance logo, the Phish Phinder name with a fish icon, and navigation buttons for Dashboard, Review, and Manage. A user greeting "Hi Gabrielle!" and a Logout button are also present. The main content area features a search bar, a "New category" dropdown, and buttons for "Recategorize" and "Process". A status indicator shows "Unprocessed: 256".

On the left, a "Filter By" sidebar allows filtering by "Seems Harmless", "Spam", "Suspected Phish", "Confirmed Phish", "Processed", and "Unprocessed". Date filters for "Start date" (3/31/2020) and "End date" (4/4/2020) are also available.

The central email list shows several entries from "updates@email.whartoncenter.com" with the subject "Take It From The Top Summer 2020 is shaping up to be our most exciting yet". A detailed view of one email shows the sender "updates@email.whartoncenter.com", received and scanned timestamps, and a count of 1. The email content includes the Wharton Center eClub logo and a photo of a group of people celebrating.

On the right, an "Email Overview" panel displays "Spam" status, a "Confidence rating: 100%", and a "Features" section with a warning: "Always take extra caution when receiving emails external to the organization." Below this, "Personal information" and "Associated Links" sections are visible, including a URL and a scan link.





# Phishing Net (Email Review System)

The screenshot displays the Phishing Net interface. On the left, a list of emails is shown, sorted by 'Scanned'. The selected email is from 'updates@email.whartoncenter.com' with the subject 'Take It From The Top Summer 2020 is shaping up to be our most exciting yet'. The main panel shows the email content, including the sender's name, received and scanned dates, and a count of 1. Below the email content is a black banner with the text 'WHARTON Events / Donate / Gift Cards'. A green notification bar at the bottom of the main panel states 'The email was successfully processed'. On the right, the 'Email Overview' section shows a 'Spam' label and a 'Confidence rating: 100%'. Below this, the 'Features' section lists 'Urgency' and 'Links', both with descriptive text. The 'Associated Links' section shows the URL 'https://fonts.googleapis.com/css?family=Montserrat:300' and a scan result from 'https://urlscan.io/result/d75ce318-3cbf-43a4-925e-9233281c6789/'.

Sort by:  Scanned  Received

updates@email.whartonc... 04-02 15:21  
Take It From The Top Summer 2020 is shaping up to be our most exciting yet

updates@email.whartonc... 04-02 14:31  
Take It From The Top Summer 2020 is shaping up to be our most exciting yet

updates@email.whartonc... 04-02 14:29  
Take It From The Top Summer 2020 is shaping up to be our most exciting yet

updates@email.whartonc... 04-02 14:29  
Take It From The Top Summer 2020 is shaping up to be our most exciting yet

updates@email.whartonc... 04-02 14:28  
Take It From The Top Summer 2020 is shaping up to be our most exciting yet

msutoday@msu.edu 04-02 02:53  
New month, same Spartans Will. Read the MSUToday Weekly Update.

**Take It From The Top Summer 2020 is shaping up to be our most exciting yet**

updates@email.whartoncenter.com  
Received: 2020-04-02 14:12:11.173000  
Scanned: 2020-04-02 15:21:43.877000  
Count: 1

Wharton Center eClub

WHARTON  
Events / Donate / Gift Cards

The email was successfully processed

**Email Overview**  
Spam  
Confidence rating: 100%

**Features**

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

**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.

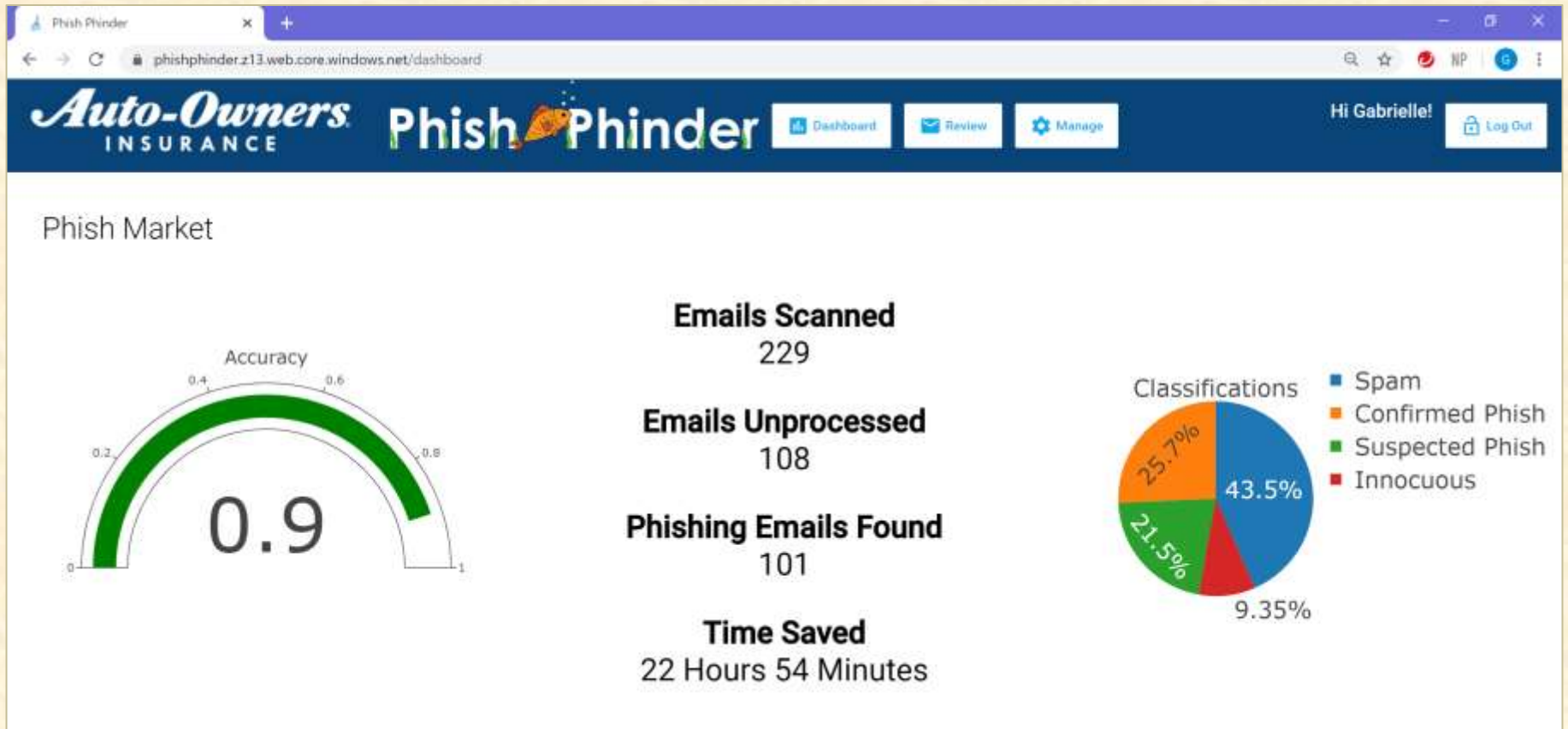
**Associated Links**

URL:  
<https://fonts.googleapis.com/css?family=Montserrat:300>

Scan:  
<https://urlscan.io/result/d75ce318-3cbf-43a4-925e-9233281c6789/>



# Phish Market (Analytics Dashboard)



# Safe Waters (Whitelist Webpage)

## Safe Waters

Filter

URL	ID	Delete
aoins.com	2	<a href="#">Delete</a>
schemas.microsoft.com	3	<a href="#">Delete</a>
w3.org	4	<a href="#">Delete</a>
google.com	5	<a href="#">Delete</a>
autoowners.com	10	<a href="#">Delete</a>
urldefense.com	23	<a href="#">Delete</a>

## Whitelist a url

URL  [Submit](#)



# What's left to do?

---

- User Testing and User Experience Testing
- Code Clean-up
- Fixing Bugs as They Arise





# Questions?

---

?

?

?

?

?

?

?

?

?

