

# Team Baracuda: Let's Go Phishing

by Alauna Wheeler, Rhondene Wint, Lesly Lopez  
for NRT-ICGE Course  
4 May 2018



# The Problem

Congratulation!!! Facebook Lottery Winner

- Extensive Numbers of Phishing Emails received to UC Merced accounts
- Little to no training on how to recognize phishing emails
- Worried about undergraduates, in particular, clicking the links and compromising the system
- Some phishing attempts have been very sophisticated

\*\*\*STUDENT JOB OFFER\*\*\*

Dear Customer,

You will not be able to send/receive more emails until you visit the below help-desk portal link to restore [Click Here](#) to upgrade to Outlook 2018 to avoid suspension.

HelpDesk  
Copyright 2018  
[201.286.2331](#)

Attention:

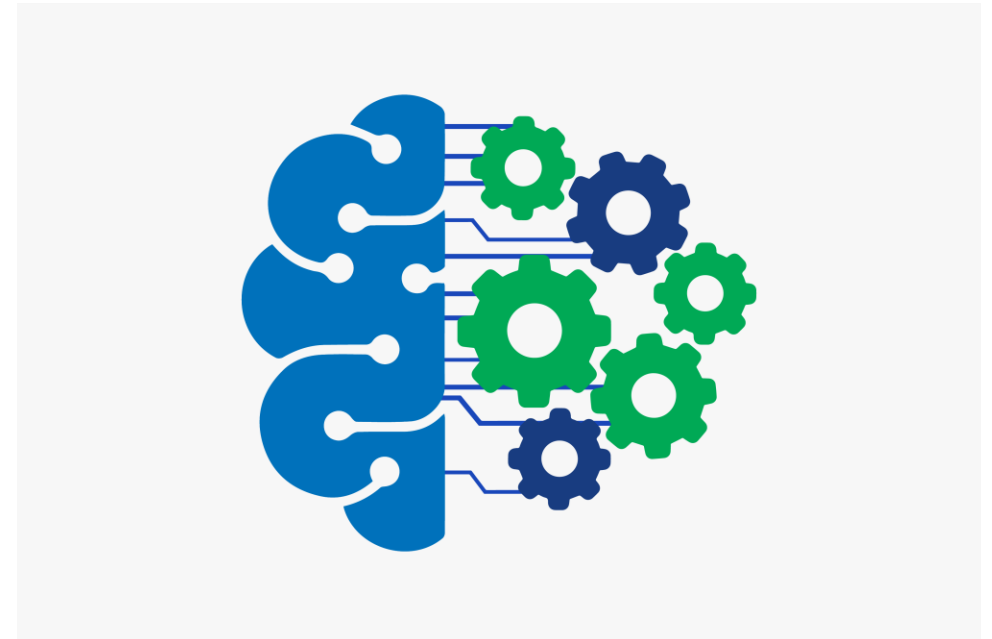
An Attempt has been made to Your Account from a new computer. Please kindly Update your account to prevent deactivation. To Confirm Your E-mail Account [CLICK HERE](#): to update.

System Administrator

# The Plan

---

- How can phishing emails be detected?
- Uncover what features of a phishing email are most likely to deceive receivers
  
- Two approaches:
  - Created a machine learning based phishing classifier
  - Simulated phishing attack to get human responses



# Evolution of the Plan

---

## Plan:

- Collaborate with IT to collect all the phishing emails the University had on file in order to create phishing classifier

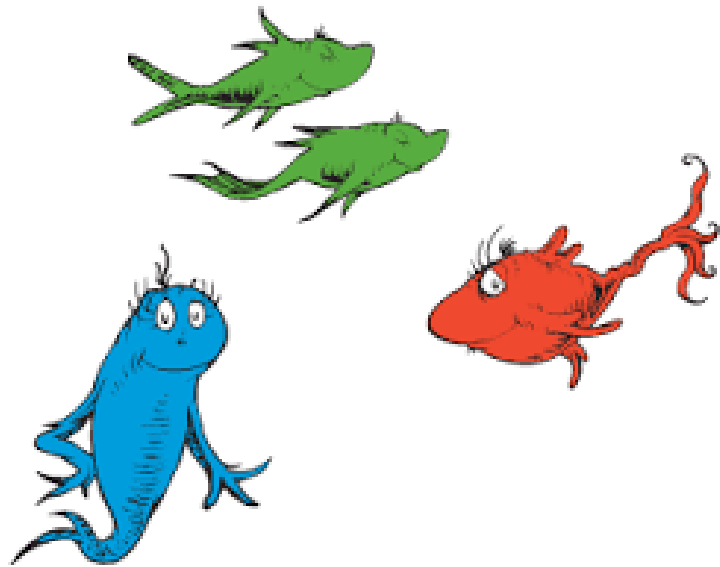
## Road Blocks:

- Initiating a Collaboration with IT Department
  - Suspected of being a phishing attack
  - Dean Zatz helped connect us with them
- Very small amount of data to work with
  - Collected more phishing emails



# Evolution of the Plan

---



## Plan Evolution:

- Planning Simulated Phishing Attack
  - Write a proposal and focus our goals
  - Create own phishing emails to send

## Road Blocks:

- IRB exception needed?
  - Course project versus research on human subjects
  - Consulted Dean Zatz on protocol

# Phishing Simulation

- Collaborated directly with Nick Dugan, Deputy CIO and Chief Information Security Officer from the IT Department
- Had software to create simulated phishing campaign
- 2 Base emails
  - Three alteration emails for each
- Variations on emails
  - Spelling Errors
  - Number of Links
  - Signature Block Errors
- Sent each email to 200 separate Undergraduates
- Gathered information on click rates for 1 week

Dear Customer,  
Due to a security update on our server, non-active accounts will be shut down. In order to keep your account active, please validate your email account by clicking on the link within 48 hours.  
Please [Click here to validate your UC Merced Email account.](#)  
This message will be available in your Secure Message Center until 04/18/2018.

Best Regards,  
Department of Information Technology  
University of California, Merced

## Mailing address changed successfully

Hello,  
We just wanted to let you know that your University mailing address was recently changed on Thursday, 12 April 2018 3:32 AM.

Don't recognize this activity?  
If you did not make this change, please contact us urgently for assistance.

### Students and applicants

- Contact our [Student Support Team](#)

### Staff, contractors, alumni and visiting academics

- Contact our [Staff Service Centre](#)

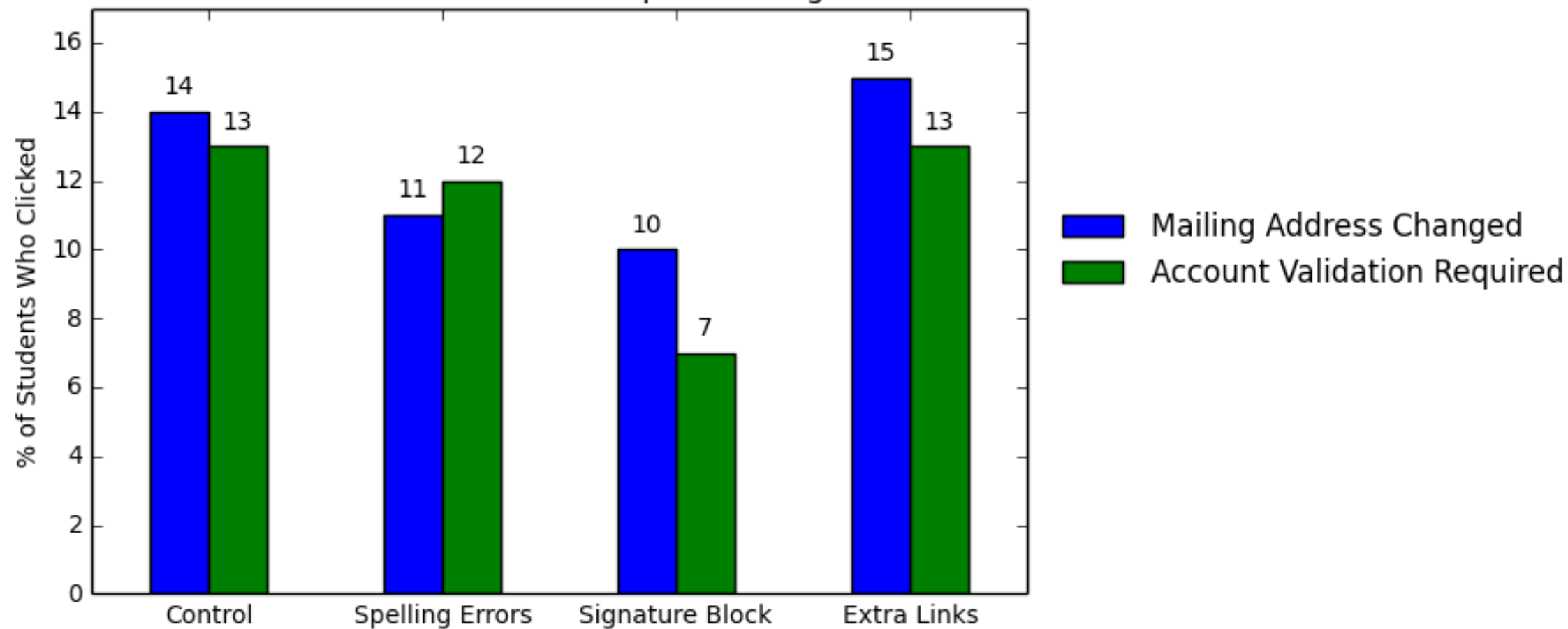
More contact details can be found [here](#).

Regards,  
Support Services Center  
Information Technology Department  
University of California, Merced

# Results of Simulated Phishing

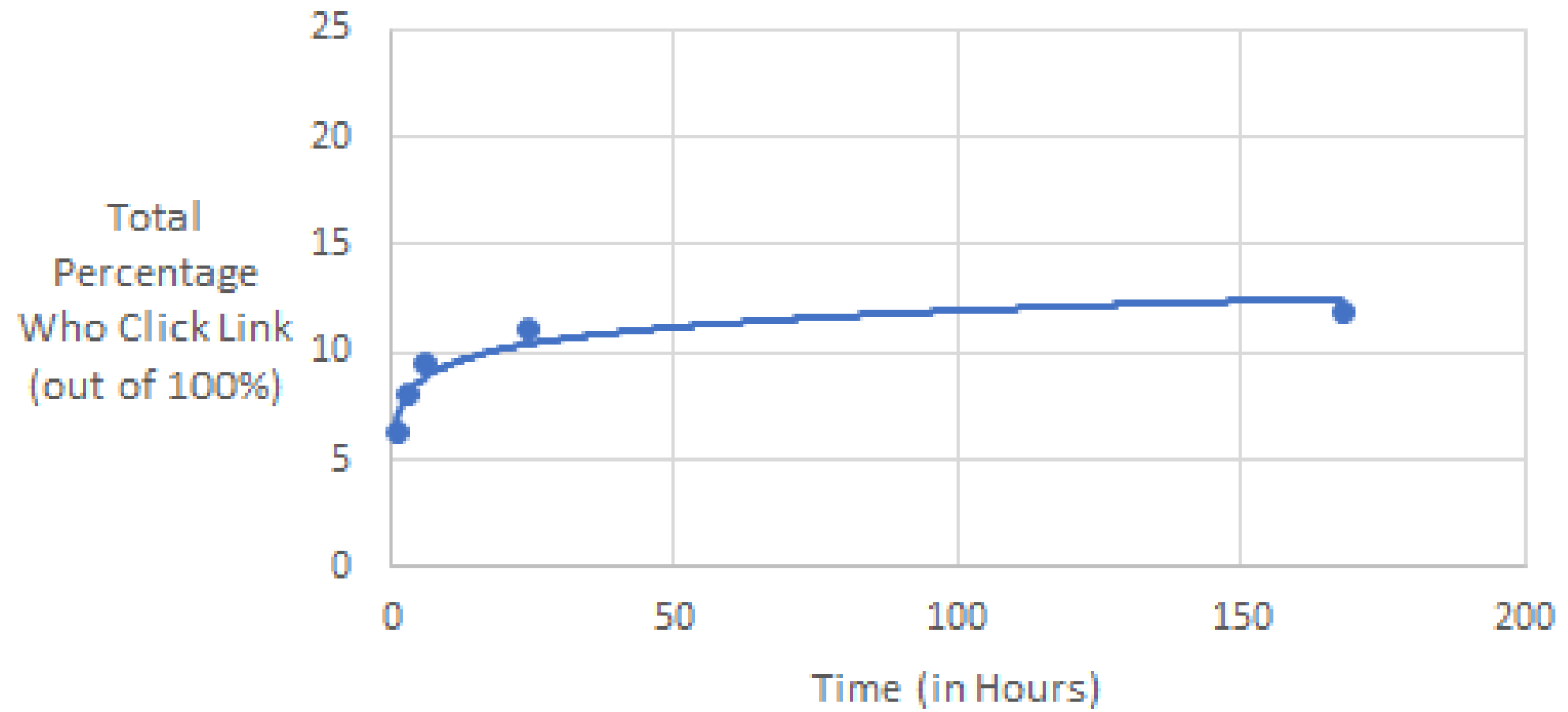
Title	Start	End	Created	Targets	Fail	Rate	Status
<b>Completed Campaigns</b>							
Mailing address changed - spelling errors	Apr 12, 2018 10:00 AM	Apr 19, 2018 10:00 AM	Apr 11, 2018 8:22 PM	200	22	11.00%	Complete
Mailing address changed - sig block	Apr 12, 2018 10:00 AM	Apr 19, 2018 10:00 AM	Apr 11, 2018 8:21 PM	200	20	10.00%	Complete
Mailing address changed - extra links	Apr 12, 2018 10:00 AM	Apr 19, 2018 10:00 AM	Apr 11, 2018 8:20 PM	200	30	15.00%	Complete
Mailing address changed - control	Apr 12, 2018 10:00 AM	Apr 19, 2018 10:00 AM	Apr 11, 2018 8:19 PM	200	28	14.00%	Complete
Account validation required - spelling errors	Apr 12, 2018 10:00 AM	Apr 19, 2018 10:00 AM	Apr 11, 2018 8:18 PM	200	24	12.00%	Complete
Account validation required - sig block	Apr 12, 2018 10:00 AM	Apr 19, 2018 10:00 AM	Apr 11, 2018 8:17 PM	200	14	7.00%	Complete
Account validation required - extra links	Apr 12, 2018 10:00 AM	Apr 19, 2018 10:00 AM	Apr 11, 2018 8:16 PM	200	26	13.00%	Complete
Account validation required - control	Apr 12, 2018 10:00 AM	Apr 19, 2018 10:00 AM	Apr 11, 2018 8:15 PM	200	26	13.00%	Complete

Percent of Students who Clicked per Phishing Features





# Percentage of People Who Have Clicked the Link as Time Passes



# Impact of Simulated Phishing Project

- Our involvement helped start the Simulated Phishing Campaign
- Happened just in time for a barrage of real phishing attacks on campus
- Community education about phishing attempts increased

9/19/2017

"Yeah, that link doesn't work." -Undergrad

UC Merced Classifieds  
Is this real? I don't want to click on the link 😬.. plus it's not an @ucmerced email

Reply-to: it-ops@securty.net  
@ucmerced.edu  
Date: Apr 12, 2018, 10:12 AM

**Mailing address changed successfully**

Hello,

We just wanted to let you know that your University mailing address was recently changed on Thursday, 12 April 2018 3:32 AM.

Don't recognize this activity?  
If you did not make this change, please contact us urgently for assistance.

**Students and applicants**

- Contact our **Student Support Team**

**Staff, contractors, alumni and visiting academics**

- Contact our **Staff Service Centre**

More contact details can be found [here](#).

4

11 comments

Like Comment

Scam

# Impact of Simulated Phishing Project

From: Ann Kovalchick <oitcommunications@ucmerced.edu>  
Date: Apr 25, 2018 11:10 AM  
Subject: Phishing Alert: Important Information About a Current Attack

- An email went out from Associate Vice Chancellor & Chief Information Officer warning students about phishing attacks

9/19/2017

Good morning and Thank you,  
  
This was a phishing attempt. Please disregard the email.  
  
We have posted alerts on Facebook and Twitter.

4/25/2018

Dear Campus Community,

In the last hour, the Office of Information Technology has received numerous reports of a sophisticated phishing attempt hitting UC Merced inboxes. The message appears to come from the Chancellor with the subject line "Updated Information on Policies and Practices."

Please note that THIS IS NOT A LEGITIMATE MESSAGE. If you receive it, please do NOT click on the .pdf attachment the message contains.

If you have already received the message and have attempted to open the .pdf, please contact the OIT Help Desk at 228-HELP so that we can assist you in reviewing your workstation and email account.

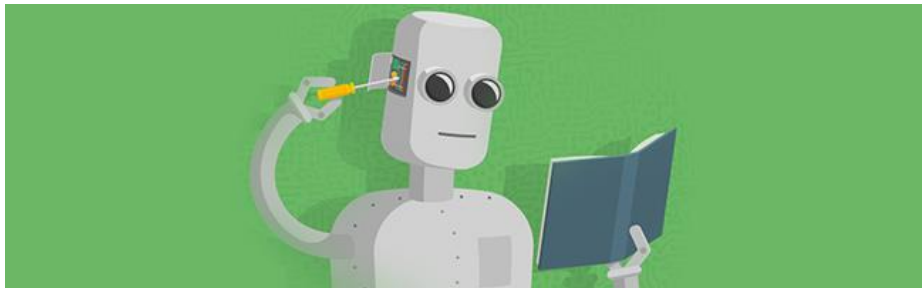
As the sophistication of these attempts increases, so must our campus community's vigilance about email security. In the case of this email, you can see that though the message appears to come from the Chancellor, it arrives via an external email address, has numerous punctuation mistakes, and is not typically formatted. These are all signs you should watch out for before clicking on attachments.

Thank you again for your assistance as we work together to limit the risk of these fraudulent messages to our campus.

Ann Kovalchick  
Associate Vice Chancellor and Chief Information Officer  
Office of Information Technology

# Phishing Classifier Code

---



# What We Learned Overall

---

- Projects Evolve
- If things don't work out, try something else
- Collaborate with outside sources
  - People are willing to help
- Sometimes you need someone higher up to help push through the road blocks
- We can be part of some small change and social awareness as we work together

*Thank  
you!*

# Acknowledgements

---

- Nick Dugan, Deputy CIO and Chief Information Security Officer, IT Department
- Ann Kovalchick, Associate Vice Chancellor & Chief Information Officer, IT Department
- Dean Marjorie Zatz, Vice Provost and Graduate Dean, and Professor, UC Merced
- Dr. Ashlie Martini, Professor of Mechanical Engineering, UC Merced
- Dr. Mukesh Singhal, Chancellor's Professor, UC Merced
- Dr. Sean Peisert, Lead Cybersecurity researcher, Computational Research Division, Berkeley National Lab

