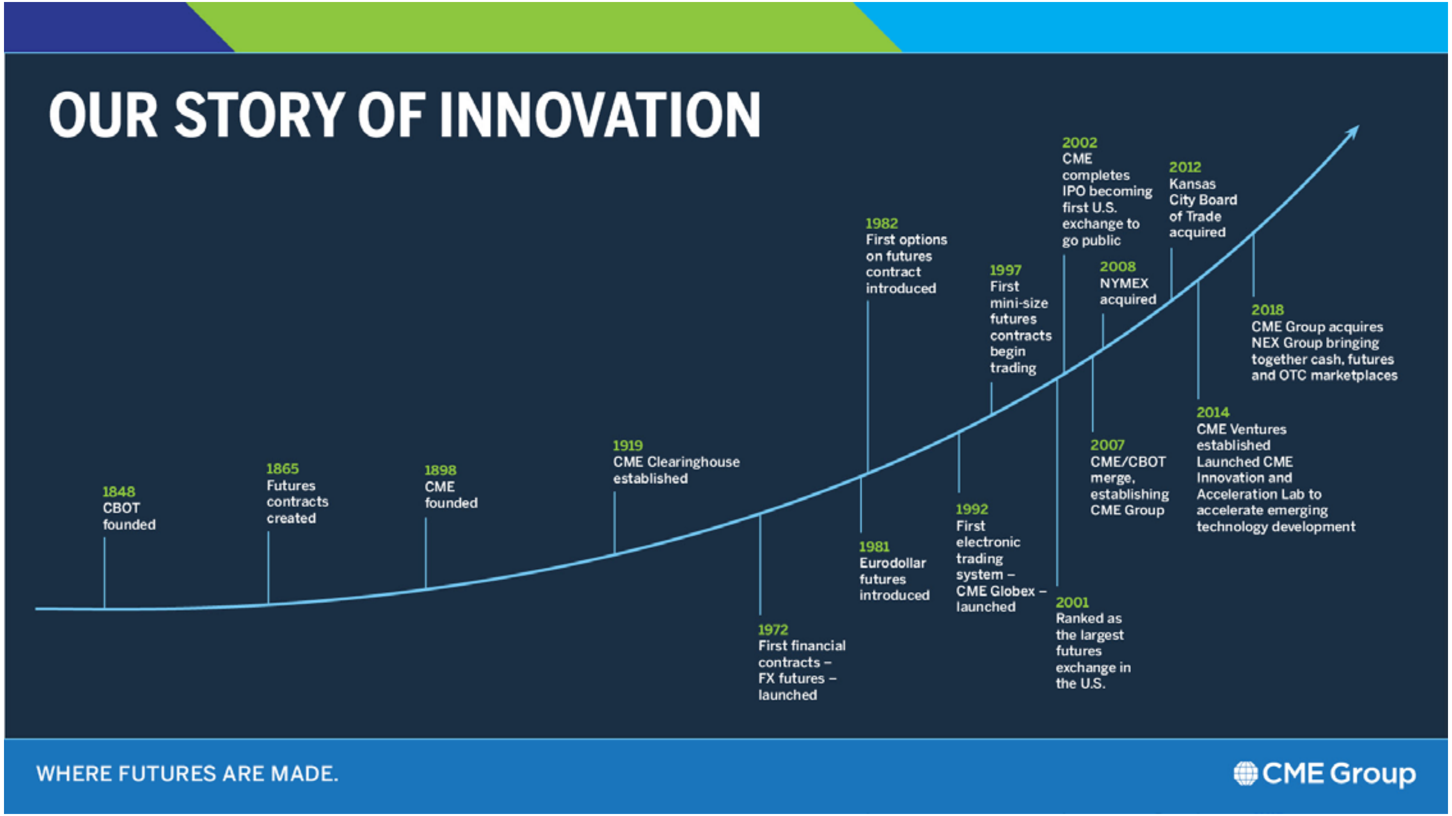
Phishing with Friends and Frenemies

What we learned making a phishing cake from scratch

June 27, 2019

CME Group Background



OUR STORY OF INNOVATION

1848
CBOT founded

1865
Futures contracts created

1898
CME founded

1919
CME Clearinghouse established

1972
First financial contracts – FX futures – launched

1981
Eurodollar futures introduced

1982
First options on futures contract introduced

1992
First electronic trading system – CME Globex – launched

1997
First mini-size futures contracts begin trading

2001
Ranked as the largest futures exchange in the U.S.

2002
CME completes IPO becoming first U.S. exchange to go public

2007
CME/CBOT merge, establishing CME Group

2008
NYMEX acquired

2012
Kansas City Board of Trade acquired

2014
CME Ventures established
Launched CME Innovation and Acceleration Lab to accelerate emerging technology development

2018
CME Group acquires NEX Group bringing together cash, futures and OTC marketplaces

WHERE FUTURES ARE MADE.

CME Group

Speakers

Brian Pope

Global Information Security
Sr. Technical Risk Management Analyst

Kevin Nicholl

Global Information Security
Technical Risk Management Analyst III

Agenda

- Phish Cake, but why?
- Required Ingredients
- Recipe for Success
- Icing on the Cake
- Lessons Learned

Phish Cake, but why?

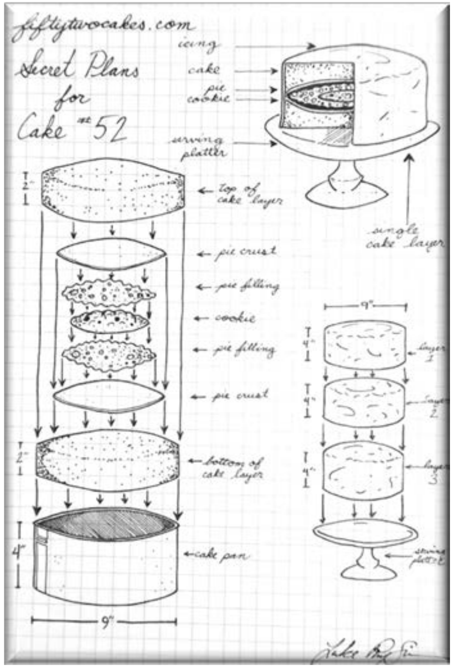
Phishing is a growing problem and has significant financial and reputational impacts

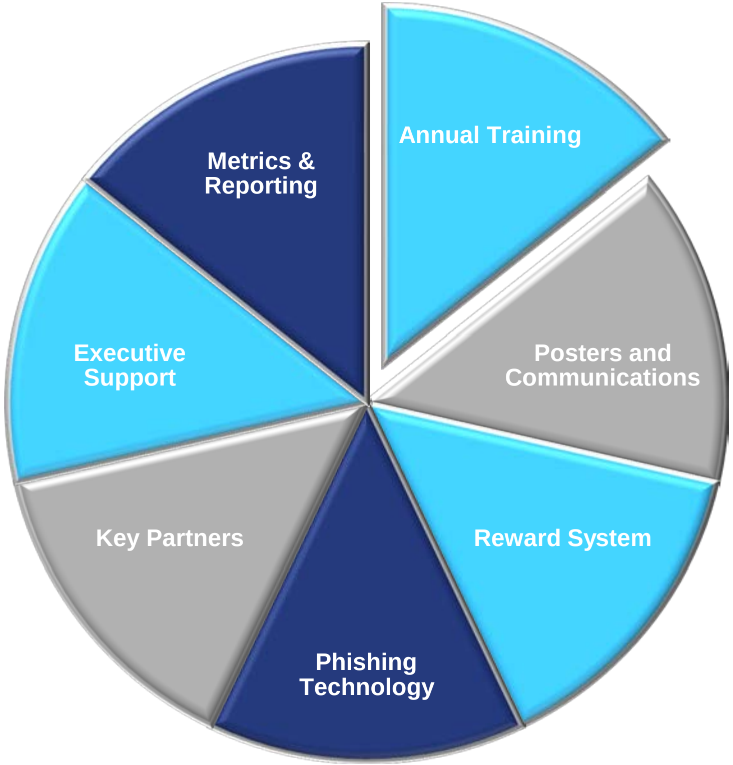
- Phishing is EFFECTIVE!*
  - Phish attempts increased 65% in 2018
  - 76% of businesses reported being a victim of a phishing attack in 2018
  - 95% of attacks on enterprise networks are the result of successful spear phishing
  - 1.5 million new phishing sites are created each month
- Breaches are EXPENSIVE!
  - The average breach costs $3.86 Million (Forbes 7/2018)

*Dashlane statistics retrieved from: https://blog.dashlane.com/phishing-statistics/

Required Ingredients

First collect the ingredients and plan the rollout of the program





Annual Training

Posters and Communications

Reward System

Phishing Technology

Key Partners

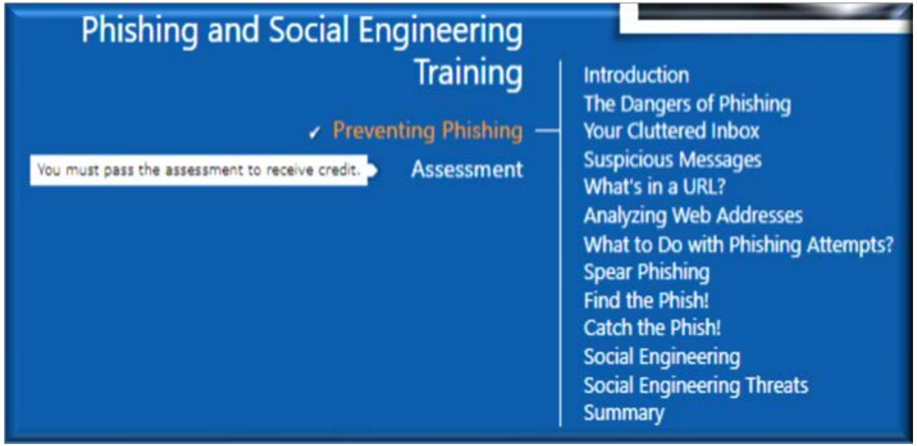
Executive Support

Metrics & Reporting

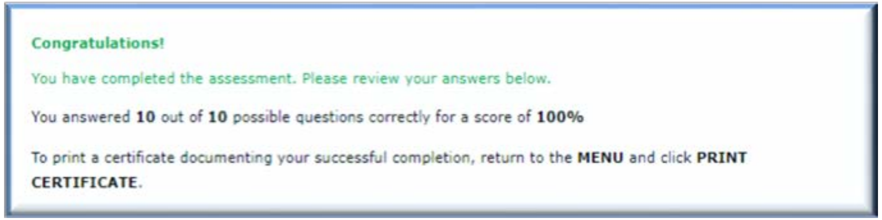
Training for Phishing and Social Engineering

Train, test, re-train.

Current phishing and social engineering course



You must pass the assessment to receive credit.



Congratulations!

You have completed the assessment. Please review your answers below.

You answered **10** out of **10** possible questions correctly for a score of **100%**

To print a certificate documenting your successful completion, return to the **MENU** and click **PRINT CERTIFICATE**.

Technical and Management Steps

Now let’s talk about how this all fits together

Technical Tasks

- Whitelist IP’s and sender emails
- Upload the user list
- Move users into distributed or location-based groups
- Deploy and compile metrics
- Design phishing emails

+

Management Tasks

- Senior Leader approvals
- Communication alerts to Cyber Defense Center
- Determine process for rewarding and re-training

Phishing Example - CEO

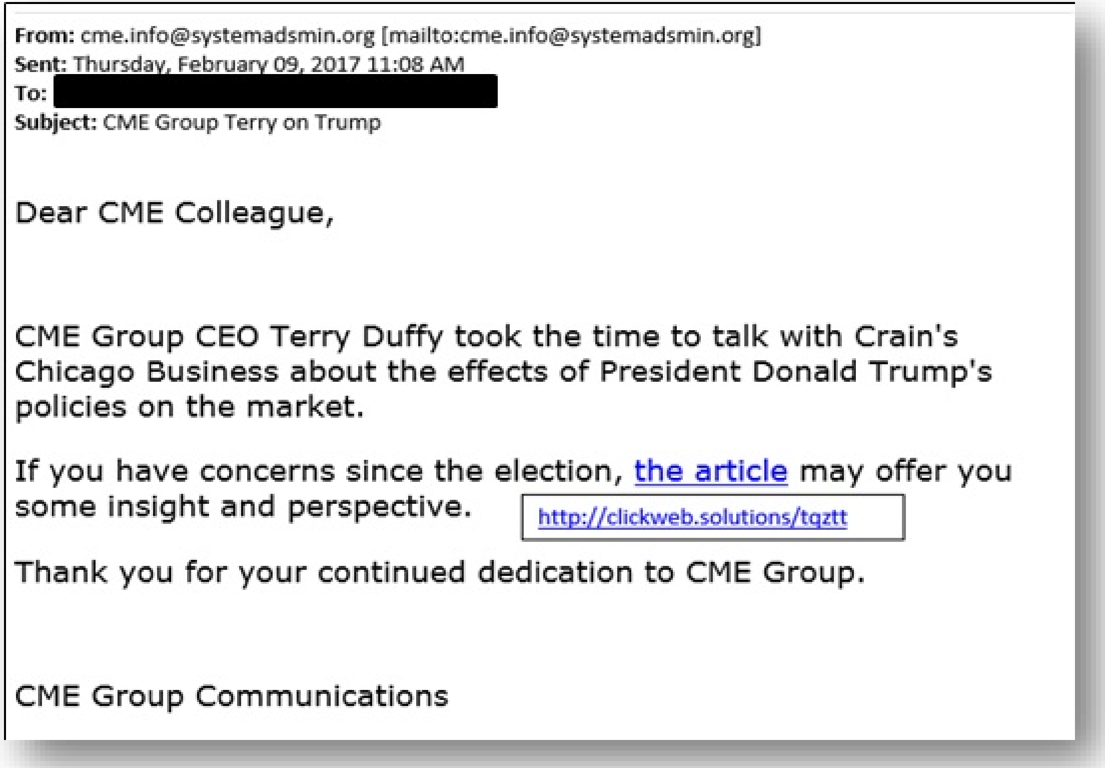
The Signs Were There…

Hard to Identify Phish Markers

- Seemingly legitimate sender
- Relative to recent events
- Intriguing to employees
  - Political topics illicit kneejerk reactions

Easy to Identify Phish Markers

- Link in email not valid
- No “CME Group Communications” team/department



From: cme.info@systemadsmin.org [mailto:cme.info@systemadsmin.org]
Sent: Thursday, February 09, 2017 11:08 AM
To: [redacted]
Subject: CME Group Terry on Trump

Dear CME Colleague,

CME Group CEO Terry Duffy took the time to talk with Crain's Chicago Business about the effects of President Donald Trump's policies on the market.

If you have concerns since the election, the article may offer you some insight and perspective. http://clickweb.solutions/tqztt

Thank you for your continued dedication to CME Group.

CME Group Communications

Phishing Example - Payroll

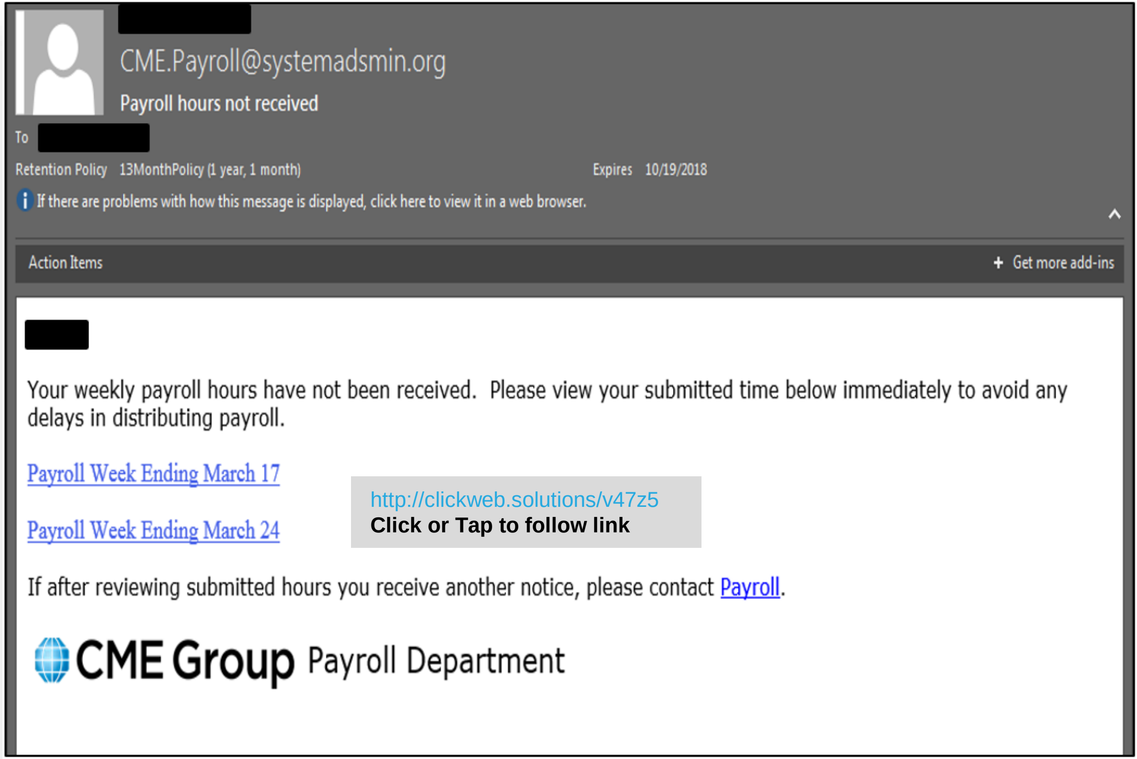
Use realistic topics

Difficult to Identify Phish Markers

- Seemingly legitimate sender
- Intriguing to employees
  - Potential missed paycheck

Easy to Identify Phish Markers

- Links in email not valid
- No “CME Group Payroll” department



[redacted]

CME.Payroll@systemadsmin.org

Payroll hours not received

To [redacted]

Retention Policy 13MonthPolicy (1 year, 1 month) Expires 10/19/2018

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

[redacted]

Your weekly payroll hours have not been received. Please view your submitted time below immediately to avoid any delays in distributing payroll.

Payroll Week Ending March 17

Payroll Week Ending March 24

http://clickweb.solutions/v47z5
Click or Tap to follow link

If after reviewing submitted hours you receive another notice, please contact Payroll.

CME Group Payroll Department

Phishing Example - Coffee

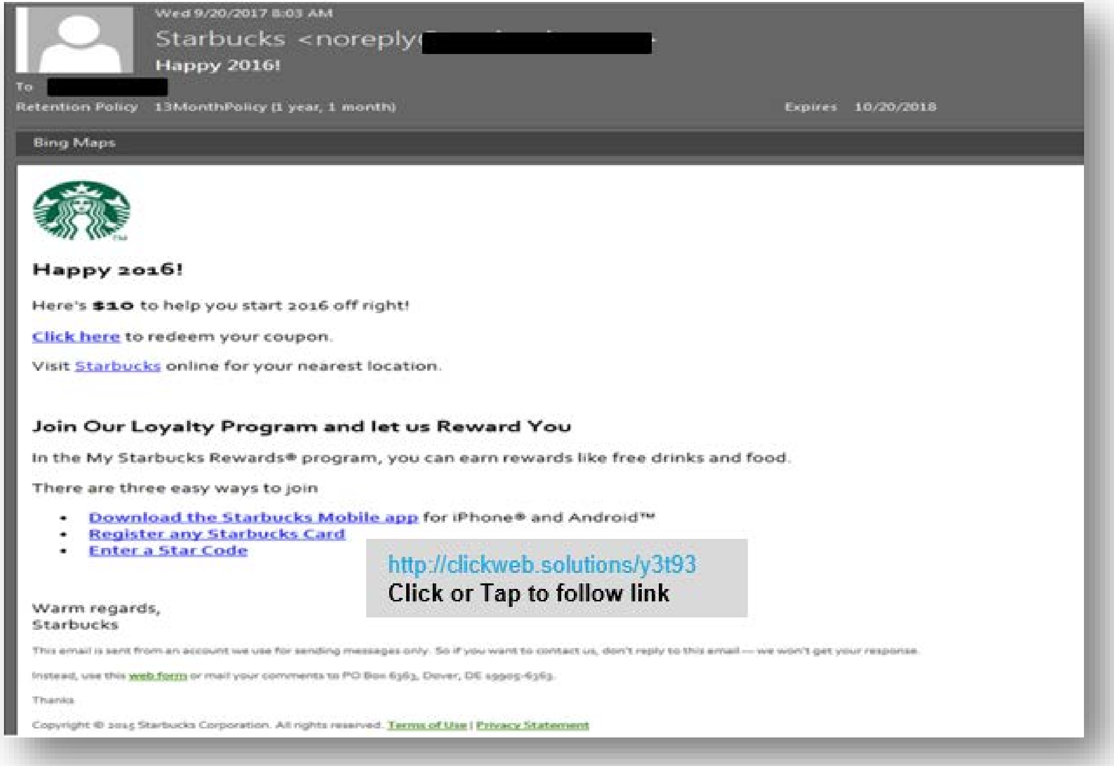
Try enticing offers – Gift Cards and Discounts

Difficult to Identify Phish Markers

- Seemingly legitimate sender
- Intriguing to employees
  - Free Starbucks

Easy to Identify Phish Markers

- Links in email not valid



Wed 9/20/2017 8:03 AM

Starbucks <noreply[redacted]>

Happy 2016!

To [redacted]

Retention Policy 13MonthPolicy (1 year, 1 month) Expires 10/20/2018

Bing Maps

Happy 2016!

Here's **$10** to help you start 2016 off right!

Click here to redeem your coupon.

Visit Starbucks online for your nearest location.

Join Our Loyalty Program and let us Reward You

In the My Starbucks Rewards® program, you can earn rewards like free drinks and food.

There are three easy ways to join

- Download the Starbucks Mobile app for iPhone® and Android™
- Register any Starbucks Card
- Enter a Star Code

http://clickweb.solutions/y3t93
Click or Tap to follow link

Warm regards,
Starbucks

This email is sent from an account we use for sending messages only. So if you want to contact us, don't reply to this email — we won't get your response.

Instead, use this web form or mail your comments to PO Box 6363, Dover, DE 19905-6363.

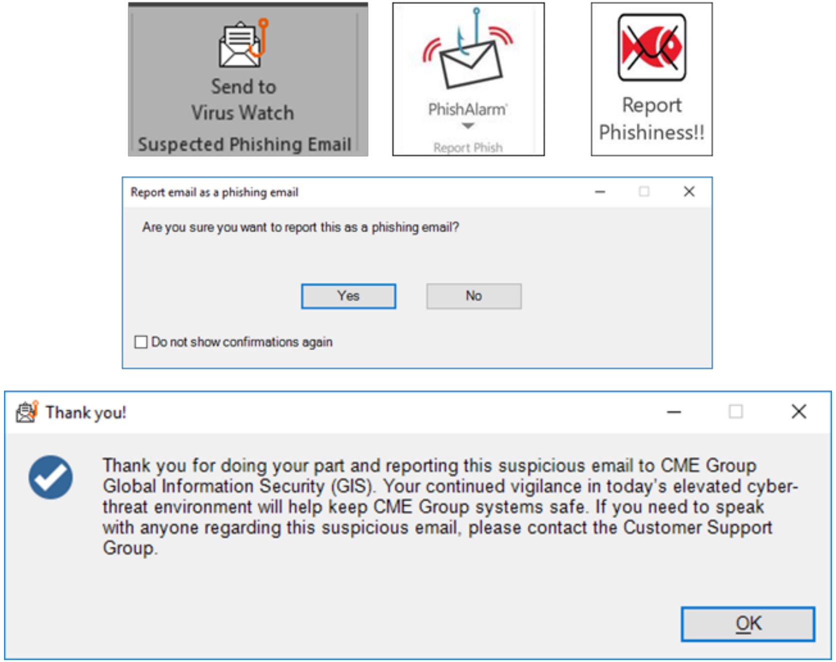
Thanks

Copyright © 2015 Starbucks Corporation. All rights reserved. Terms of Use | Privacy Statement

Make it Easy to Report

Yep, that was easy.

Easy method to report suspected phishing



Report email as a phishing email

Are you sure you want to report this as a phishing email?

□ Do not show confirmations again

Thank you!

Thank you for doing your part and reporting this suspicious email to CME Group Global Information Security (GIS). Your continued vigilance in today's elevated cyber-threat environment will help keep CME Group systems safe. If you need to speak with anyone regarding this suspicious email, please contact the Customer Support Group.

Wait, there’s more?

AUTOMATION!

Pitfalls

- Defense center overwhelmed with reported emails
- **300%** increase in reported emails after button implemented
- Average of **12** minutes to triage an email
- Department did not have enough headcount for new capacity

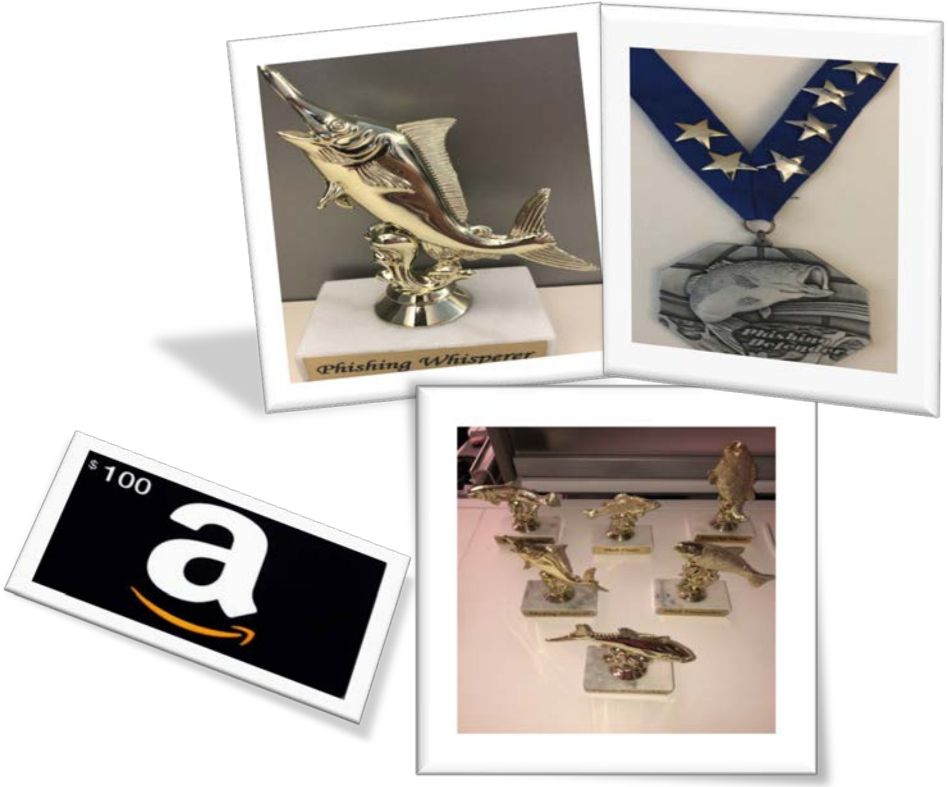
Solutions

- Department created an **Automation Filter** to streamline the process
- Email Triage time reduced from 12 minutes to **8-10 seconds** (including removing the emails from inboxes)
- Phishing button forced process evolution and allowed for better metric collection and reporting
- Users who end up failing phish are trained again

Icing on the Cake

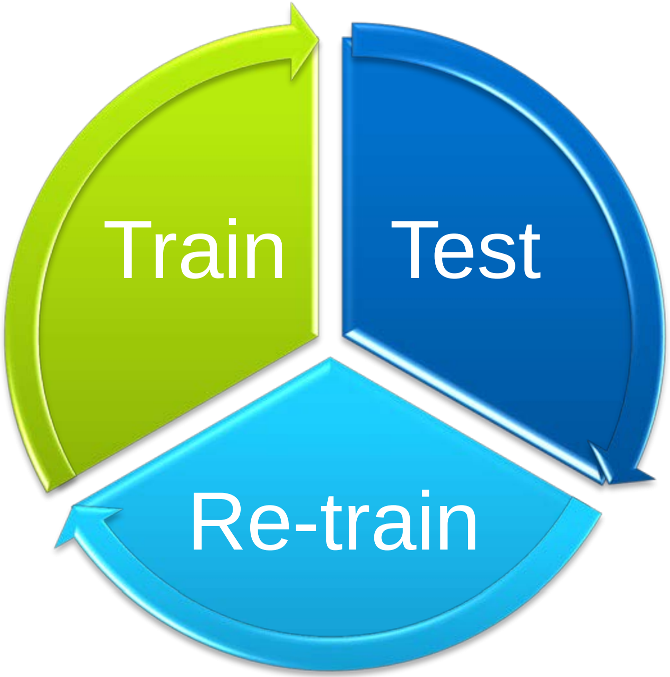
Positive reinforcement that transforms employee behavior

- **Recognition**
  - Trophies, medals and pins
  - $100 Gift Cards to 10 random users per quarter
  - Never publicly shame phishing simulation victims
- **Training**
  - Refresher training for clicking on real or simulated phishing emails
- **Welcome feedback from employees**
  - Make simulations harder – hackers don't pull punches
  - Include hot security topics to gain intrigue
  - Gift Cards or other desired rewards
- **Metrics!!**
  - Click Rate and Report Rate Trends to Sr Leadership and Board of Directors



Lessons Learned

- Define AND refine the rules of your program
  - Train, test then retrain
  - Have a phishing submission process already established
  - Confirm any “forbidden” topics
- Use key partnerships with other teams
  - Leadership backing is critical
  - Anticipate problems where possible
- Be prepared for the unexpected
  - Logos/branding – Can they be used and how…
  - Topics or individuals – Are the topics appropriate
  - You might make more work or problems for other users/teams
- Work to streamline processing
  - Code to prevent phish egress from corporate network
  - Inform information security staff of each pending simulation
- Make it easy for users to report a phishing email
- **Give rewards, they go a long way**



Phinal Phishing Questions?

Thank you

CME Group