Phishing with Friends and Frenemies

What we learned making a phishing cake from scratch

June 27, 2019
CME Group Background

Our Story of Innovation

WHERE FUTURES ARE MADE.
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
- Metrics & Reporting
- Executive Support
- Posters and Communications
- Key Partners
- Reward System
- Phishing Technology
- Key Partners
Training for Phishing and Social Engineering

Train, test, re-train.

Current phishing and social engineering course
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
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
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
Make it Easy to Report

Yep, that was easy.
Wait, there’s more?

**AUTOMATION!**

- 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

---

**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