RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: HUM-W14

RED PHISH, BLUE PHISH

Samantha Davison

Security Engineering Manager
Snap, Inc.
@Sam_E_Davison

Mike Mackintosh

Security Engineering Manager
Snap, Inc.
@MikeMackintosh

Introduction

History of the Risk Model

- Sam and Mike unite
- Vendor or no vendor
- Sophistication Model
- Infrastructure Turn Up
- Baseline
- Inventory of business applications/accounts
- Risk Model was born

RSAConference2018

Utopian Phishing Program

Training

- Orientation
- Workshops
- Classes
- Online learning
- Speakers

Behavioral Engineering

- Simulations
- Baselining
- Metrics

Content

- Discover
- Team Snaps
- Infographics
- Guides
- Video

Product & Process

- 2FA
- Identity Verification
- Security Checkup

Gamification

What were we trying to solve?

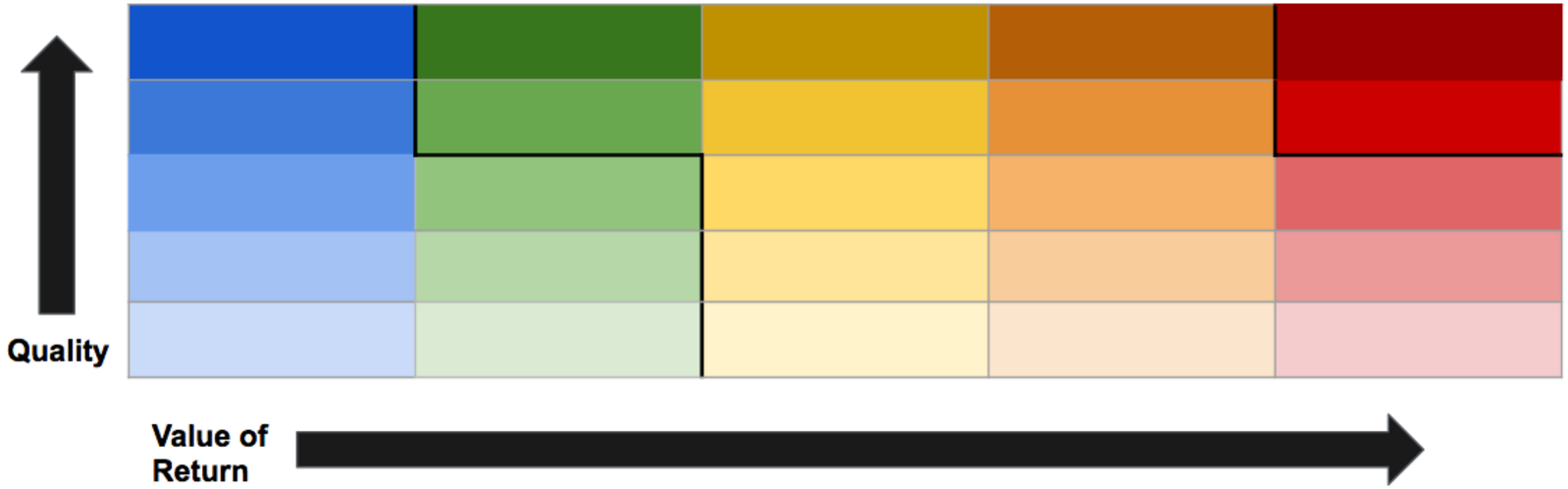
- Haphazard phishing
- Phishing that doesn’t measure what you think it measures
- Sentiment drain
- Phishing testing as it has been historically been done

RSAConference2018

STEP 1: MEASURE SOPHISTICATION

Classifying Phishes to Calculate Knowledge

Sophistication Matrix



Indicators: Spelling, Grammar, Sender Address, Salutations, Link Destination, Attachments, Content
Criteria: Relevancy, Targets, Lure, Payload, UX, Payoff, Detectability, Noise Generation, Timing, Simplicity

Blue Phish

Topic: Inheritance
From: Duke Westinghearst <dwestinghearst@gmail.com>
Subject: Important Notice

Dear sir/madam,

It has come across our desk in the form of a telegram of the recent passing of a distant relative. You are listed as a recipient of their death fund in the amount of $16,231,077.89. Please in haste submit a claim form at the following link:
https://urldefense.proofpoint.com/v2/url?u=http-3A__104.198.6.223_wp-2Dadmin_contents_functions.php-3Frid-3D2fb345da1e7e8fb05cf9130b4383930e4ecc66caf0cdb6646655eb580ee20308&d=DgIBaQ&c=ncDTmphkJTvjIDPh0hpF_w&r=I1ZpeztVsL0BVnhhc0eG5f-oviO-rXi2L6K8zpc36oA&m=kodDoJzEoWuOqwW49sCaOaf49jsBRXFU0nylbQRXDHA&s=ObdfaGvs2rBa0QQW7tXu8Pl7pJBw076fSdAQoJUFeXw&e=

With kindest regards,
Duke Muriel Westinghearst

Topic: Transaction
From: justicecandelou@gmail.com
Subject: Transaction Alert

You spent $1293.17 USD at The Home Depot. If you did not make this transaction please login here to stop this transaction. Thank you.
If the link above does not work, you can access it via the plaintext version below:
http://104.198.6.223/cgi-bin/uploads.pl?rid=359c918da3dac62b4d49fe80d33cc343414e25e6d67251952323565f8c3fc6df
Thank you.

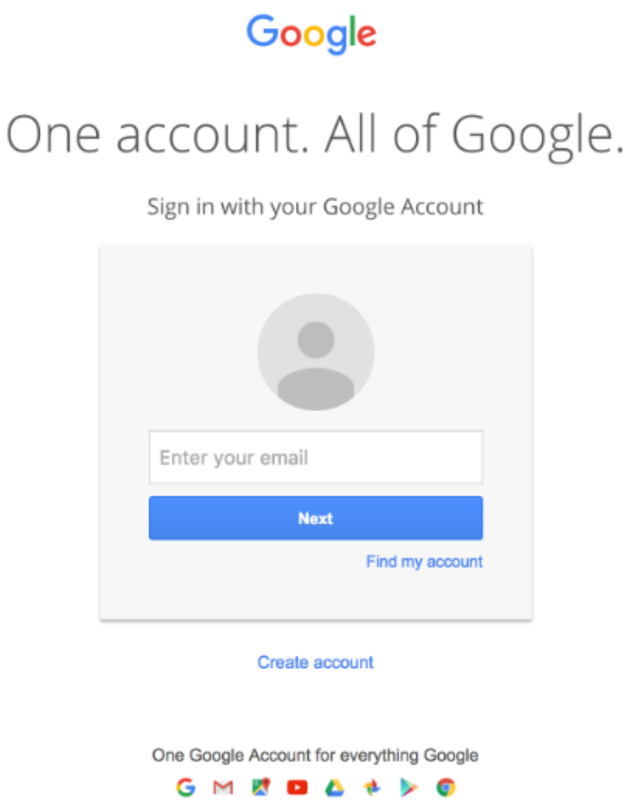
Topic: Fax
From: Duke Westinghearst <dwestinghearst@gmail.com>
Subject: Incoming Fax

Hello!

You have received a fax from London, England. Click here to view your fax.

RSAConference2018

Blue Landing



RSAConference2018

Orange Phish

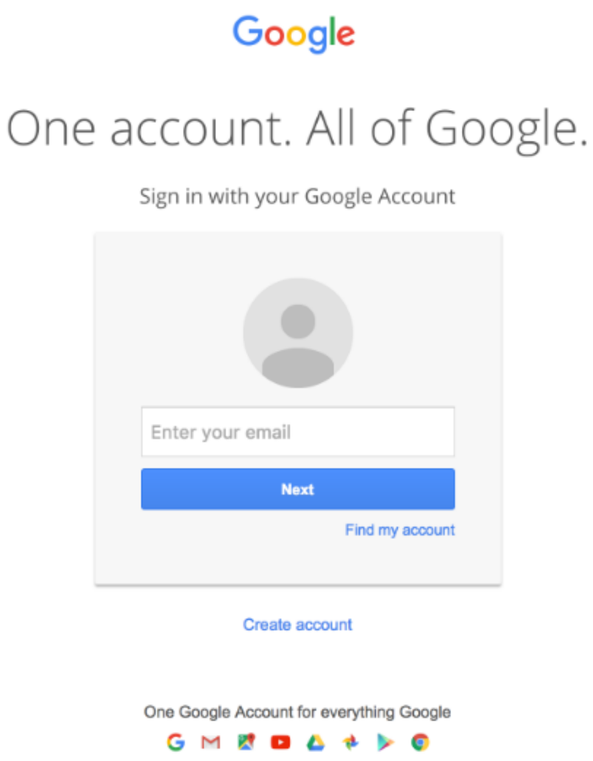
Topic: Candy Grams
From: Holiday Candy Grams teams@snapbenefits.us
Subject: Gifts That Keep on Giving

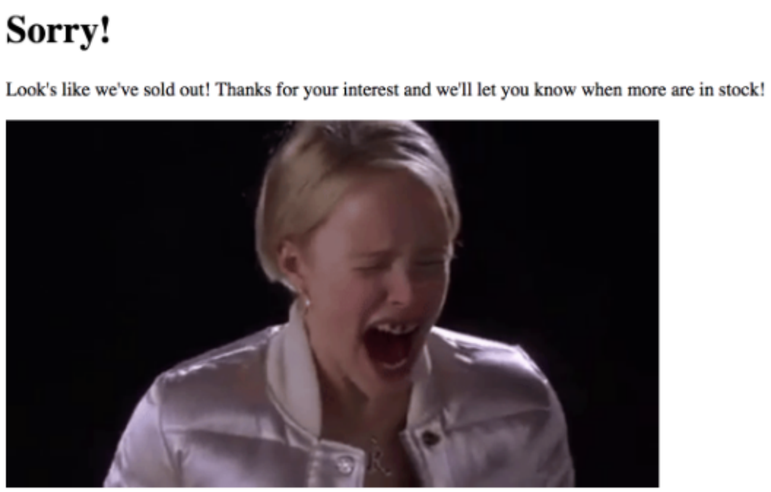
Happy Holidays Team!

Have a co-worker that's on your nice list? Let them know with a candy gram. Each candy gram comes with a flavored candy cane of your choosing and your customized message. Candy grams will be delivered the week of December 21st. Click **here** to fill out the form.

RSAConference2018

Orange Landing





RSAConference2018

Red Phish

FoodServices@snap.com Mar 16
to samantha.davis.

Google Forms

I've invited you to fill out a form:

Santa Monica Cafeteria Themes

Shh! You've been selected for a secret taste test some dishes and vote on the themes of our Santa Monica cafeterias. We're only inviting a small group of employees, so please don't share with your colleagues. This event will take place at the Blue House on Ocean Front Walk. Chose the dates and times that will work with your schedule from below:

FILL OUT FORM

Create your own Google Form

Training@snap.com Mar 17
to me

Google Forms

I've invited you to fill out a form:

Manager Performance Review Training

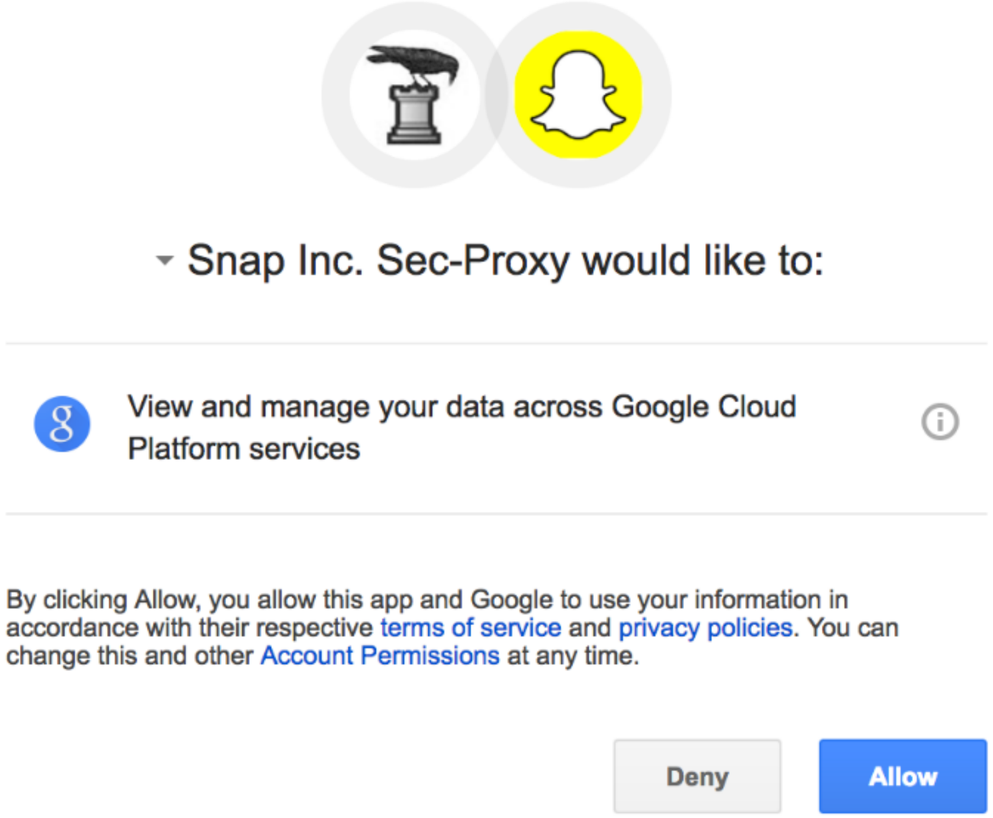
Hey Managers,

As you may have heard, Snap is rolling out company-wide performance reviews this year. Since you will have a pivotal role in the success of this endeavor, we are hosting a series of trainings specifically for our managers. During these sessions we will cover our Performance Review system, discuss key components and dates, and act out some role play scenarios. Please select the date below that works best for your schedule or fill in an alternate date in the text box.

A catered lunch will be provided by Mendocino Farms.

FILL OUT FORM

Red Landing



RSAConference2018

STEP 2: SET UP YOUR ENVIRONMENT

Common Services and Tooling Architecture

Where Do Phishing Emails Come From?

Table 1

Where	do	they	come	from?	I	can't	say.	
But I	bet	they	have	come	a	long,	long	way.

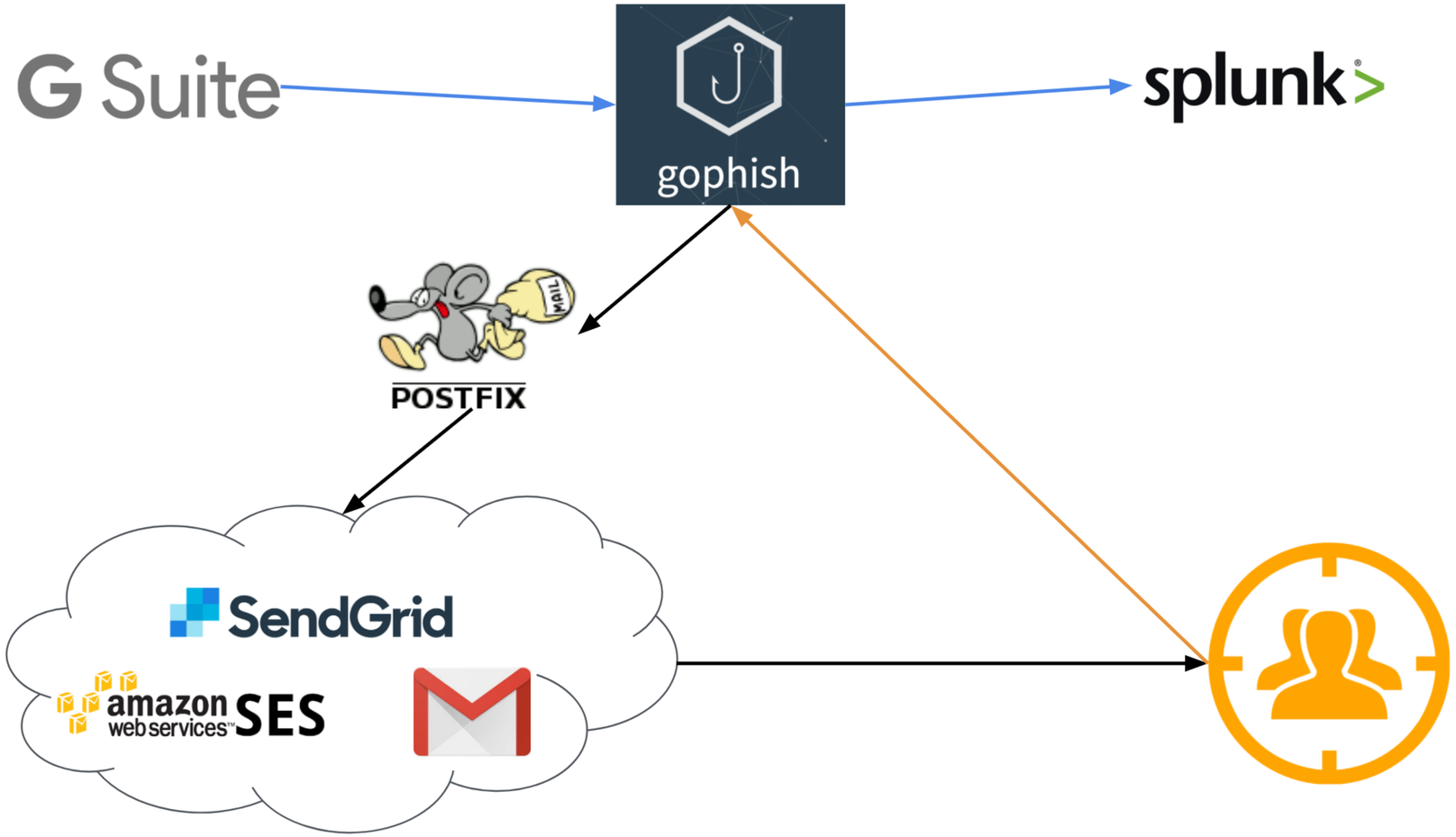
RSAConference2018

Architecture Contexts and Tools

Preparation Questions	Tool
• Who to phish?	G Suite, Auth0, okta, onelogin Identity Management
• How to phish?	Jackal, amazon web services SES Campaign Orchestration, KING PHISHER
• What is success?	splunk>, kibana Metrics Collection
• What is failure?	

RSAConference2018

Sample Phishing Architecture



RSAConference2018

Measuring Metrics

- How many phishes were sent?
- How many phishes were opened?
- How many targets have reported the phish?
- How many targets have clicked the phish bait?
- How many targets gave up sensitive information (creds, tokens)?
- How many targets revealed vulnerable browsers?
- How many targets revealed sensitive origin IP’s?

RSAConference2018

STEP 3: UNDERSTAND YOUR ADVERSARIES

Spam & Phishing Filters

Deceptive site ahead

Attackers on [redacted] may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards).

☐ Automatically report details of possible security incidents to Google. Privacy policy

HIDE DETAILS

Back to safety

Google Safe Browsing recently detected phishing on [redacted] Phishing sites pretend to be other websites to trick you. Learn more.

What are Spam Filters?

- Spam filters are technical controls put in place by mail transit services to prevent abuse and unwanted messages
- They include things like:
  - Verification of DNS records
    - SPF - Sender Policy Framework
    - DKIM - DomainKeys Identified Mail
    - DMARC - Domain-based Message Authentication, Reporting and Conformance
    - PTR - POINTER (PTR) Record
  - Rate Limiting
  - Message recipient caps/limits

What Else do Spam Filters Check?

- Message Headers
  - Non-standard headers
    - X-GetPastSpamFilter: LOL
  - Subjects
  - Sender Addresses
  - Recipient Addresses
  - Message-ID’s (and do they match the source)
- Links, Domains and IP’s oh my!
- HTML-standards compliance
- Content hash matching

RSAConference2018

What are Phishing Filters?

Google Safe Browsing

- Collection of reported and detected malicious sites
- Protects over 2 billion devices per day
- Is automatically updates by Chrome, Safari and Firefox
  - Chrome will automatically report suspicious sites (like fake Gmail logins)
  - Chrome will automatically download updated version of the Safe Browsing definitions

How to Subvert Phishing Filters

- Creative and crafty subjects
  - If you put the word “gram” in the subject, it will get junk folder’d
- Once you use a domain, it
  - You wouldn’t reuse your floss so don’t reuse your domain
- Use 3rd-party services like Amazon SES and SendGrid (but be sure to read the ToS)
  - They have a higher reputation and a reliable delivery network
- Random String Replacement
  - Increase the uniqueness of each message, and don’t send the same message to everyone in the company

STEP 4: PHISHING WITHOUT A RISK MODEL

Haphazard Phishing

RSAConference2018

Not Measuring What You Think It Is

Payload Problems

It’s like 2,000 passwords when all you need is 1 OTP

RSAConference2018

One Phish to Pwn Them All

- People are different
- The perfect phish for Sam wouldn’t be enticing for Mike
- The perfect phish for Mike wouldn’t be enticing for Sam
- Mike has access to assets that Sam doesn’t
- Sam has access to assets that Mike doesn’t

RSAConference2018

Magic Phishing Phairy

RSAConference2018

STEP 5: PHISHING, NOW WITH RISK MODELING

Phishing Risk Model

RSAConference2018

Phishing Actions

Click

- 0 Day
- Enter creds
- Enter other info
- Give OAuth
- Recon
- Download file on target
- Execute malicious JS
- Download plugin

Download

- 0 Day
- Execute
- Open
- Persistence
- Share File
- Ransomware

Reply

- Give info
- Take action
- Send file
- Validate RCPT
- Relinquish headers

Mobile

- 0 Day
- 2 Factor Compromise
- Surveillance Ware
- Auto preview
- SMS
- Chained attack

RSAConference2018

Assets

- User data
- Employee data
- Machine/Device
- IP
- Financial data

RSAConference2018

Target & Susceptibility

Phishing Risk Model Components

Phishing action x ($tool^{MFA}$) x assets x department = risk

**Where action, tool and asset are weight on a scale of 0-5*
**MFA = 1 for disabled, 3 for enabled or not required*
**Creates a total scale out of 3125*

RSAConference2018

PRM Application 1

Engineering risk to user data via OAuth grants to GitHub

Risk = **Click > Permit OAuth** x (**Github ^ MFA Not Required**) x **User Data** x **Engineering**

33.3% = (5 * (5 ^ 3) * 5 * .33) * 100 / 3125

RSAConference2018

PRM Application 2

Facilities risk to Financial Data via Credential Entry to Okta

Risk = **Click > Enter Credentials** x (**Okta ^ MFA Enabled**) x **Financial** x **Facilities**

0.24% = (5 * (2 ^ 1) * 3 * .25) * 100 / 3125

RSAConference2018

PRM Application 3

Legal risk to employee data via Credentials to Docusign

Risk = **Click > Enter Credentials** x (**Docusign ^ MFA Not Required**) x **Employee Data** x **Legal**

80% = (5 * (5 ^ 3) * 5 * 80%) * 100 / 3125

RSAConference2018

STEP 6: THE VALUE OF PHISHING EXERCISES

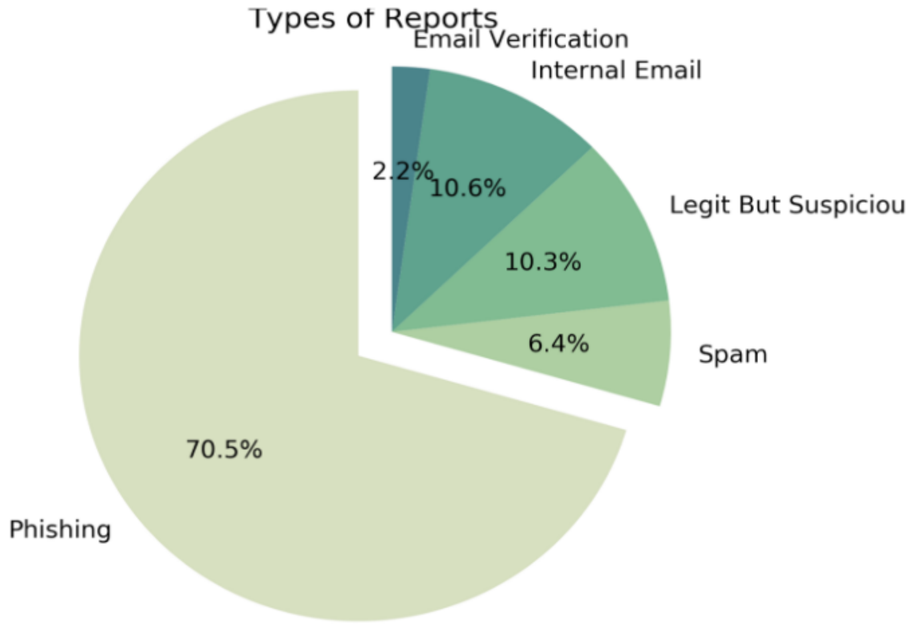
Waters Full of Phish

- Social Engineering is still a leading avenue for sensitive information leakage
  - Phishing emails, phone calls, text messages, in-person encounters are effective for attackers
- Teach your targets how to swim away from the lures
- Training solutions are effective but they don’t scale easily
- Measure the success and failures of your campaigns AND targets

RSAConference2018

Results

- 70% of the self reported emails received by our team are legitimate phishing attacks
- We have reduced our undesirable action rate significantly…and in a Q1 simulation, every employee that we deceived reported that they had installed a malicious file on their computer
- We had 10 highly sophisticated attacks in 2017 with 0 victims
- Our testing drove company-wide technical changes to take some choices out of the hands of our employees, reducing decision fatigue



RSAConference2018

Apply What You Have Learned Today

- Next week you should:
  - Audit and organize your SaaS and Identity Provider footprint
- In the first three months following this presentation you should:
  - Assign weights, measures and priorities to your SaaS and Identity Providers
  - Perform phishing baselines by running your own campaigns
- Within six months you should:
  - Perform another campaign and measure the deviation from your baseline
  - Reduce the number of “Super Administrators” across your platforms
  - Migrate legacy and non-SSO backed applications to SSO
  - Turn on 2FA for your most critical accounts