Enterprise Phishing Susceptibility and Resiliency Report

2016

PHISHME

www.phishme.com

Introduction

Welcome to PhishMe's 2016 Enterprise Phishing Susceptibility *and* Resiliency report. The report we published in 2015 focused solely on susceptibility, only telling half of the story. Now, with over 5 million active installations of PhishMe Reporter™ across the globe, we can publish statistically significant metrics about the rate and accuracy of humans *reporting* phishing emails. We are excited to share this data as it has been missing from phishing studies in the past. Armed with this new data, we hope that security organizations focus their attention on the ratio of Report-To-Click instead of dwelling on susceptibility metrics.

PhishMe has been collecting and aggregating phishing threat, simulation, and reporting data since 2008. This report evaluates user susceptibility, analyzing why employees click on suspicious links and attachments including, for the first time, an additional area of analysis on the reporting of suspicious emails to measure the resiliency of conditioned employees.

Phishing and spear phishing remain the No. 1 attack vector threatening organizations world-wide, continuing to challenge IT security teams as threat actors evolve their tactics to gain access to corporate networks, assets, and consumer data. Now, more than ever, organizations must be able to understand and identify the successful types of email attacks, themes, and elements used to successfully phish employees so that we can determine how best to prepare and condition them to identify and report suspicious emails to internal IT security teams.

So Far in 2016...

- 91% of cyberattacks and the resulting data breach begin with a spear phishing email.
- Spear-Phishing Campaigns are up 55%.
- Ransomware Attacks are up 400%, and
- Business Email Compromise (BEC) Losses are up 1,300%.

To that purpose, this study examines data samples from more than 1,000 PhishMe customers who sent more than 40 million simulation emails from January of 2015 through July of 2016. Throughout this report, we will identify and highlight those phishing themes and emotional motivators that users find the most difficult to recognize and report and highlight how increased reporting impacts susceptibility.

Report Data Demographics

Based on PhishMe template/scenario response data:

- Over 1,000 PhishMe customers from across the globe
- Fortune 500 and public sector organizations across 23 verticals
- More than 40 million simulation emails
- 15 languages
- 18-month span (January 2015 through July 2016)

Phishing Simulations Explained

Unless you have run a phishing simulation program, the terms used throughout the report may not be familiar. At its core, a phishing simulation program allows organizations to assess, measure, and educate all employees about phishing threats. An ongoing, methodical program will provide sample emails ranging in complexity and topics that mimic real threats. The use of "scenarios" and "themes" allows for measurement and customization for better resiliency to those more successful phishes. Throughout the report, we will refer to scenarios and themes as we assess behavior across multiple industries.

Summary of Findings

After sending more than 40 million phishing simulation emails across 23 industries around the world, PhishMe gathered the following insights:

- Business-context phishing emails remain the most difficult for users to recognize.
- Top Themes: Office Communications, Finances, and Contracts.
- Top Emotional Motivators: Curiosity, Fear, Urgency.
- Susceptibility to phishing email drops almost 20% after just one failed simulation.
- Reporting rates significantly outweigh susceptibility rates when simple reporting is deployed to more than 80% of a company's population, even in the first year.
- Active reporting of phishing email threats can reduce the standard time for detection of a breach to 1.2 hours on average—a significant improvement over the current industry average of 146 days.

These results validate the importance of understanding how the components of complexity and context impact the phishing susceptibility of employees in your organization and how a continuous security training program has proven to significantly change employee security behavior. Improvement is driven by reducing susceptibility, reinforcing key principles, and increasing employee engagement to enhance threat detection rates and avoid costly incidents.

Why Behavioral Conditioning?

Phishing remains the No. 1 attack vector today **because it works**. Attackers are crafty and have many different tactics to entice a person to click or open an attachment. How is the executive assistant to the CEO supposed to recognize a phishing email if they have not seen that tactic used?

An organization's many employees in diverse roles offer a target-rich means to the attackers' end of gaining access to company systems. Employees are easier targets due to their susceptibility to various emotional and contextual triggers; and they might not be as focused on email security as they need to be.

Attack Methods

Click-only: An email that urges the recipient to click on the embedded link.

Data entry: An email with a link to a customized landing page that entices employees to enter sensitive information.

Attachment-based: Themes of this type train employees to recognize malicious attachments by sending emails with seemingly legitimate attachments in a variety of formats.

Double Barrel: A conversational phishing technique that utilizes two emails – one benign and one containing the malicious element.

Highly Personalized: Simulates advanced social engineering tactics by using specific known details about email recipients gathered from internal and public sources.

Which Topics or Themes are the Most Effective?

As part of its phishing simulation program, PhishMe provides its customers with themes and templates of sample emails matching real world scenarios that mimic a variety of attacks and primary motivators.

Our data has shown that the Office Communications and the Finance/Contracts themes garnered the highest susceptibility rates with 19.9% and 18.6%, respectively, which makes perfect sense if you are receiving a business-related email in your office inbox. Other themes that have increased in the last year include Retail/Shopping and External Communications.

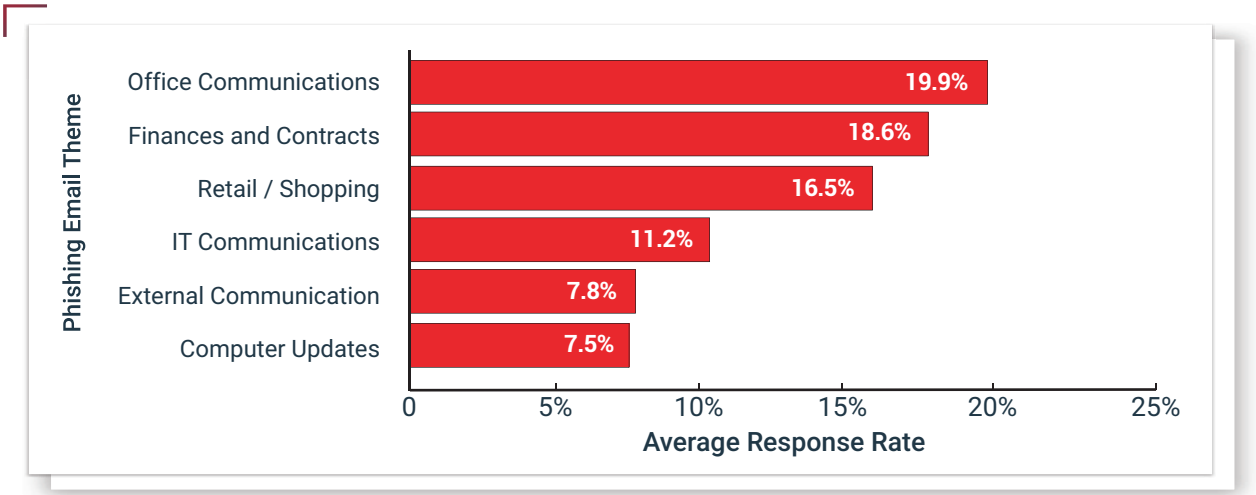

Figure 1: Training themes employees found most difficult to recognize as a phishing email

This correlation with last year's study results validates that Business Context/Communication scenarios make more effective phishing emails than other themes. This points to the need to fully understand and baseline your own internal communication standards to provide guidance to your users in the detection of malicious phishing attempts. This is particularly true, considering the increase in BEC style phish in the real world today.

Comparing Benchmark Scenarios and Customized Templates

PhishMe provides templates for benchmarking analysis, where an aggregate performance of one group is compared with an aggregate performance of individuals from a second group, across separate companies. To account for changes in variance across customizable themes, we compared average response rates for our benchmarks. This comparison provides greater confidence because the simulation variables are controlled.

The good news is that we see some significant improvements as compared to the last report in average response rates for the benchmark templates in **Figure 2**. Unauthorized Access, Secure Email (Attachment-based), and the RSA Phish (Click Only) dropped 7%, to 10%. The largest improvements in recognition were shown with a 12% drop in susceptibility for the Password Survey (Data Entry) scenario.

These changes point towards the value of a broad base of users being continually exposed to phishing themes over time. The best example in the real world of this same phenomenon is the well-known "Nigerian Prince"' scam. Because it is so widely and repeatedly used, it has become easily recognizable in multiple forms. The same can be said for the results below.

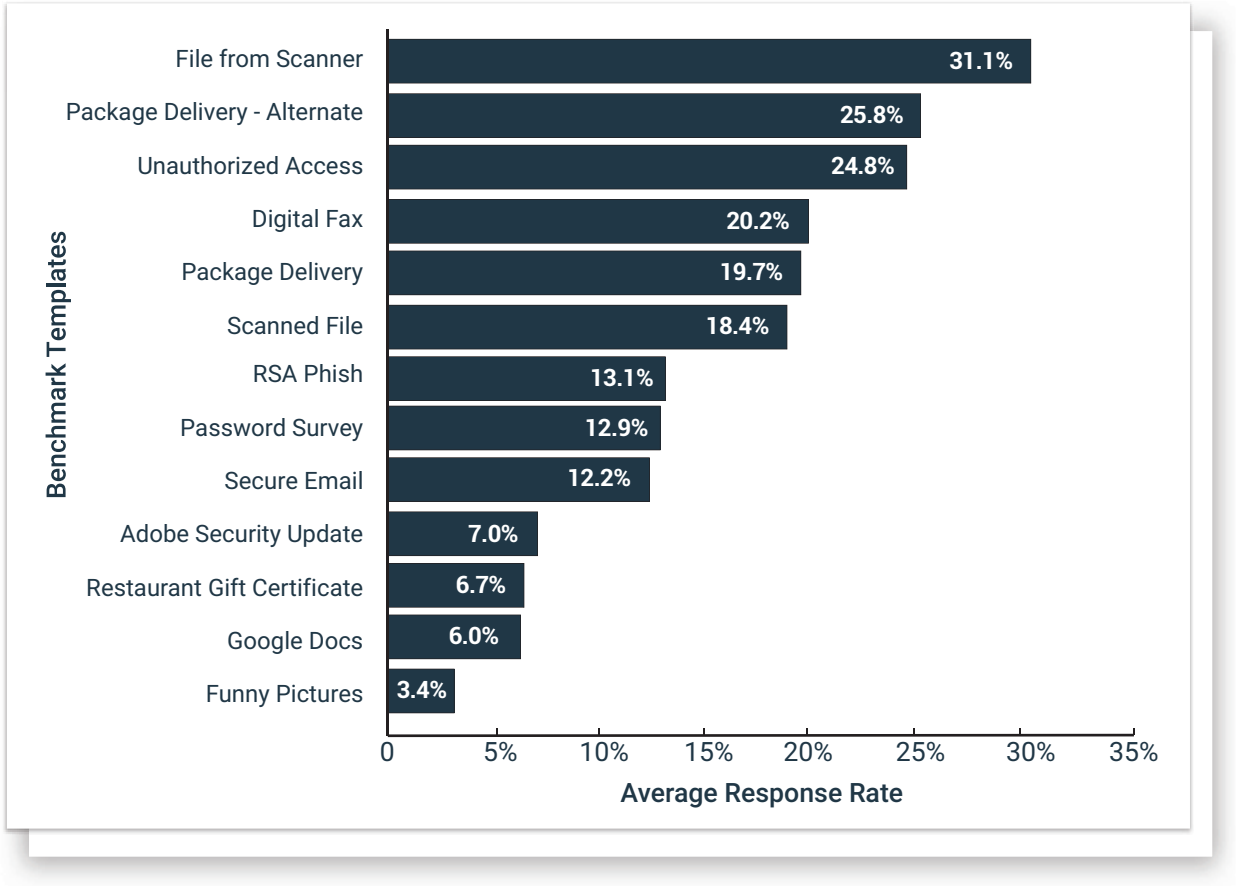

Figure 2: The different templates used in Benchmark simulations across more than 10 industries

To identify further trends and gain a closer look at correlations between our benchmark scenarios and customizable templates, we included average susceptibility for many of our most used templates in this study.

While these templates are less controlled (i.e. the phishing email can be customized by clients), we were able to tease out several findings in this year's study.

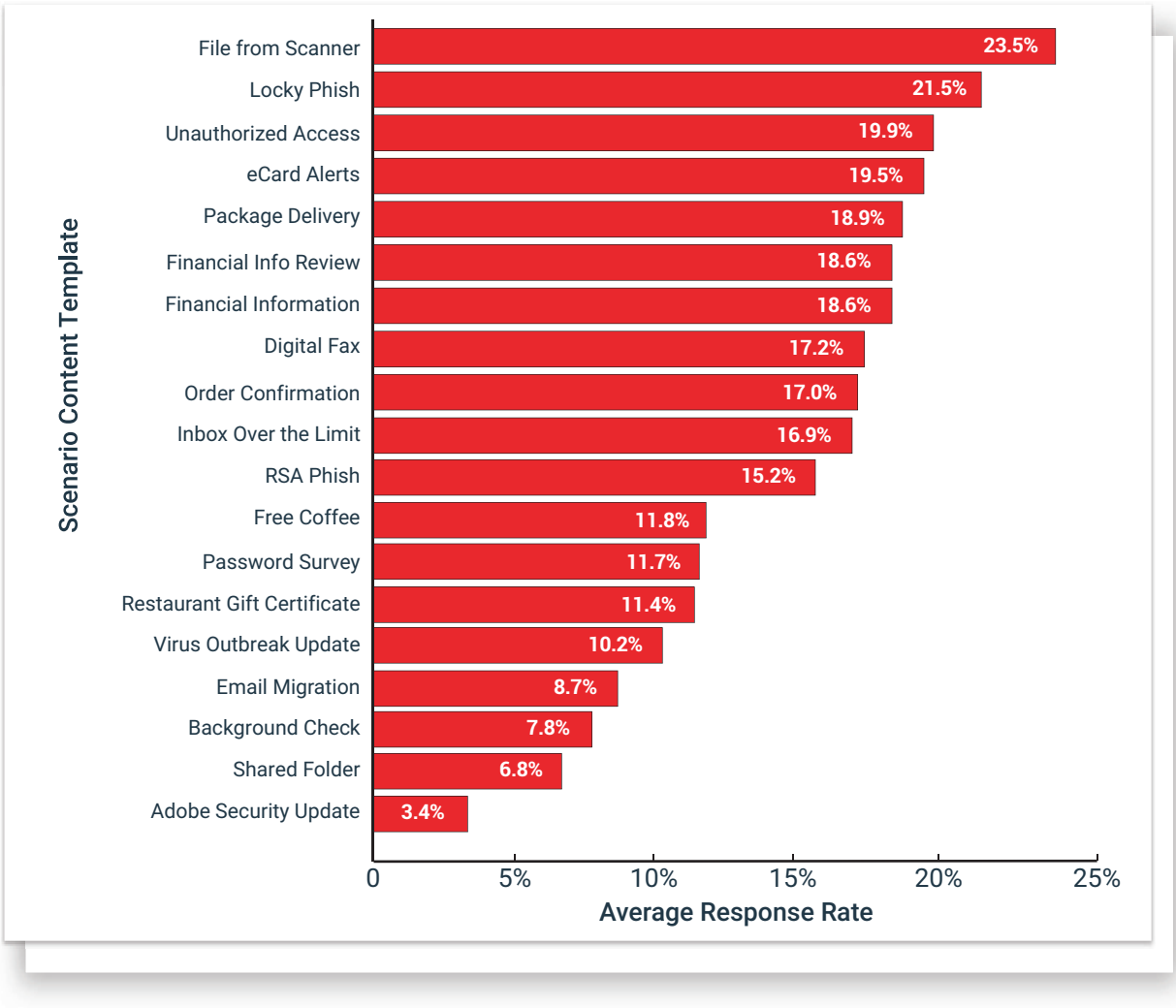

Figure 3: The different templates used in benchmark simulations across more than 10 industries

Notice that File from Scanner, Package Delivery, Unauthorized Access and others remain as the most difficult scenarios for users to recognize even though the templates in this sample can be edited. Further, we can see that the customizable templates average lower than their benchmarking counterparts. For example:

- The File from Scanner benchmark averages 31% while the customizable version averages 24%.
- The Unauthorized Access benchmark averages 25% compared to 20% for the editable version.

There are a few contributing factors to the lower rates on the customizable templates:

1. The volume of usage for the customizable version of these templates is higher, leading to broader recognition.
2. Many programs begin by customizing scenarios to include more visible errors, making them easier to recognize.
3. Differences between comparable benchmark and custom scenarios include differences in type. We will outline this further by taking a closer look at the File from Scanner templates.

Attachments Versus Links

The File from Scanner template reigns as the most difficult for users to recognize as both a benchmark and a customizable template; yet, as mentioned above, there are differences between the benchmark susceptibility rate and the average rate for the customized version:

- 31% average response as a benchmark
- 24% in customizable form

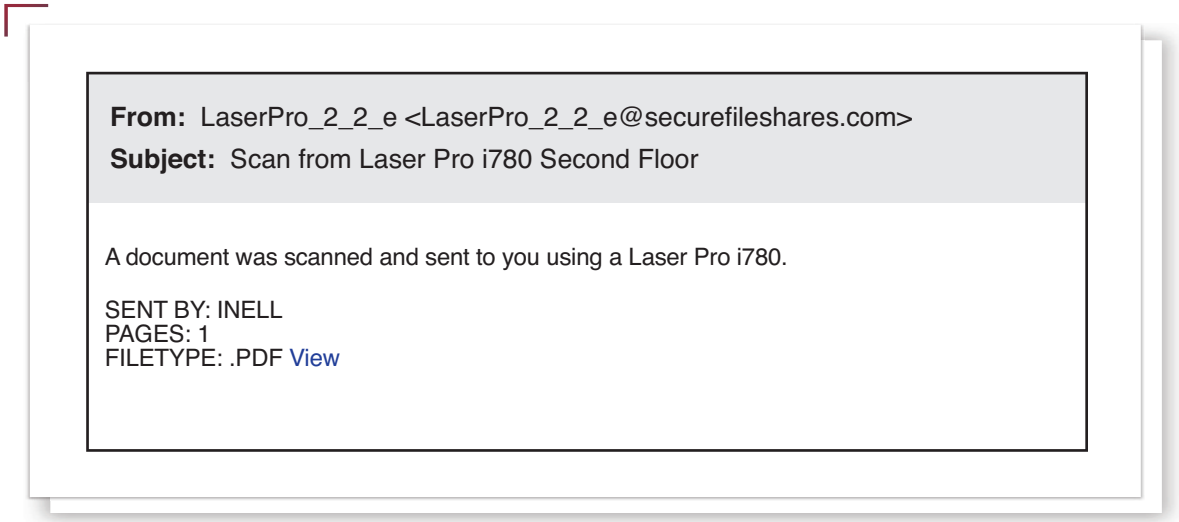

Figure 4: The file from scanner customizable template (Click Only)

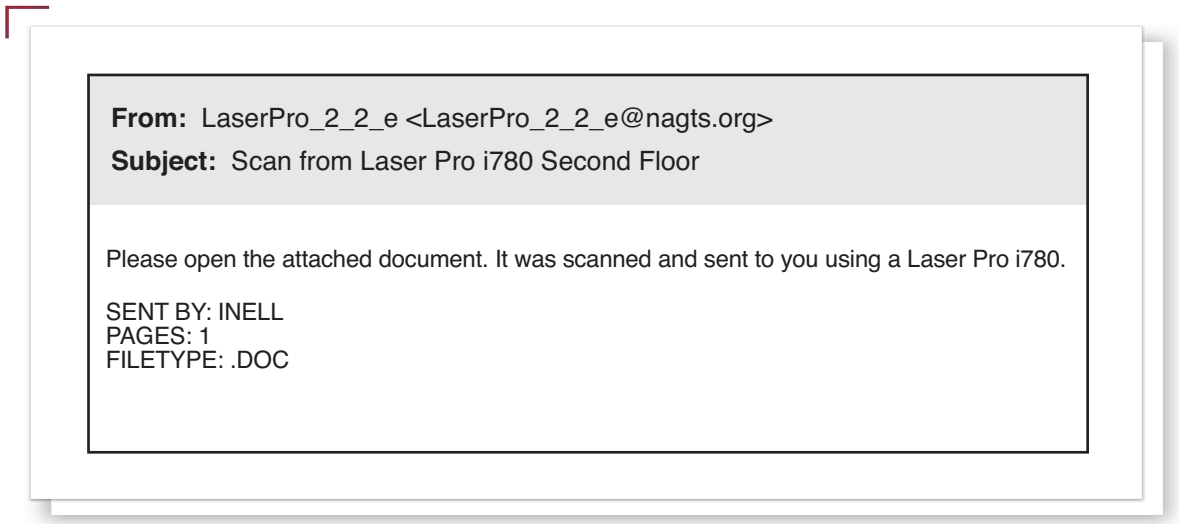

Figure 5: The file from scanner benchmark template (Attachment-based)

Figures 4 and 5 show the difference in the action needed in the benchmark scenario and customizable version: open versus a click. This suggests that because the attachment-based benchmark more closely mimics how an actual scan would work, it is more difficult for users to identify as suspicious.

PhishMe Tip

The results from the File from Scanner validates that business-context phish, in general, are the hardest for employees to recognize and report. It further emphasizes the need for organizations to baseline their operational procedures, particularly those involving internal and external business communications.

The existence of communication standards and policies allows an organization to improve phishing recognition by providing their users with a point of comparison. In other words, email communications that do not follow an understood standard format or appropriate process are easier to identify.

Variance by Industry

PhishMe further analyzed data from the "File from Scanner" benchmark simulation to understand variances across industries.

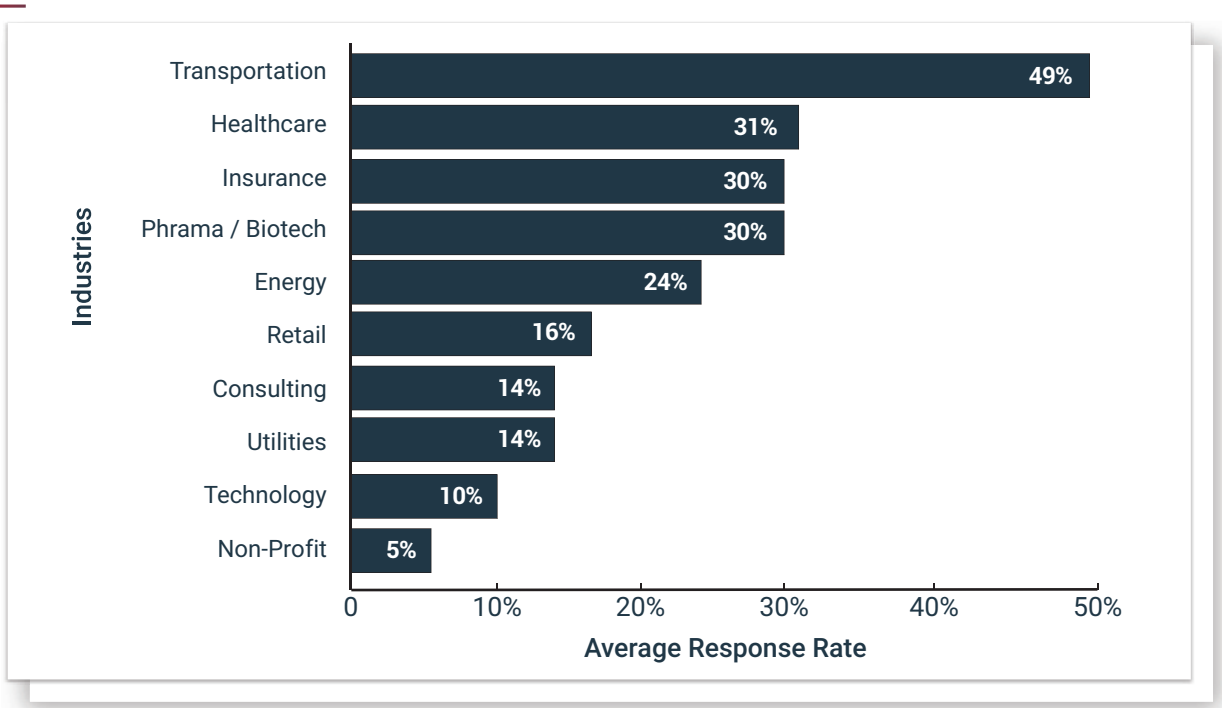

Figure 6: File from Scanner average results per industry

As we can see above, there is a wide variance in average response rates per industry, with almost a 50% response rate in Transportation, down to 5% for Nonprofits.

This further stresses the need to fully baseline your organization and processes so that your biggest phishing threats can be identified and mitigated through focused repetition of high response scenarios and additional awareness activities.

Targeted threat attackers and other malicious actors continue to mature, varying the types of phishing emails that enter the real-world environment. The complexity of the content and the emotional motivator often drives the success of a particular phish.

As we have already seen, business-context phish are more difficult for users to recognize and report. In addition to Context, we consider two other factors: Technical Difficulty (number of visible clues/errors in an email) and Emotional Motivators.

Components of Complexity	
Context	Business Personal
Emotional Motivators	Charity Curiosity Entertainment Fear Personal Connection Opportunity Reward Urgency
Technical Difficulty	Easy -- 3+ Visible Clues Med -- 1-2 Visible Clues Hard -- 0-1 Visible Clues

Figure 7: Components of Complexity

Emotional Motivations

Human nature influences our emotions and how they get the better of us. All of us come with an automated fight or flight response designed to protect us from danger. This leads to our emotions and feelings being triggered prior to our rational thought.

Consequently, we are at risk of increased susceptibility to phishes with a strong emotional pull, even at a subconscious level. To mitigate this natural reaction in users, it is important for us to understand those emotions that are most effective in bypassing critical analysis. With this level of understanding, we can condition our employees to be on the lookout for their natural reactions to malicious emails and to use those reactions as a trigger to look more closely for technical and process errors in what they are seeing.

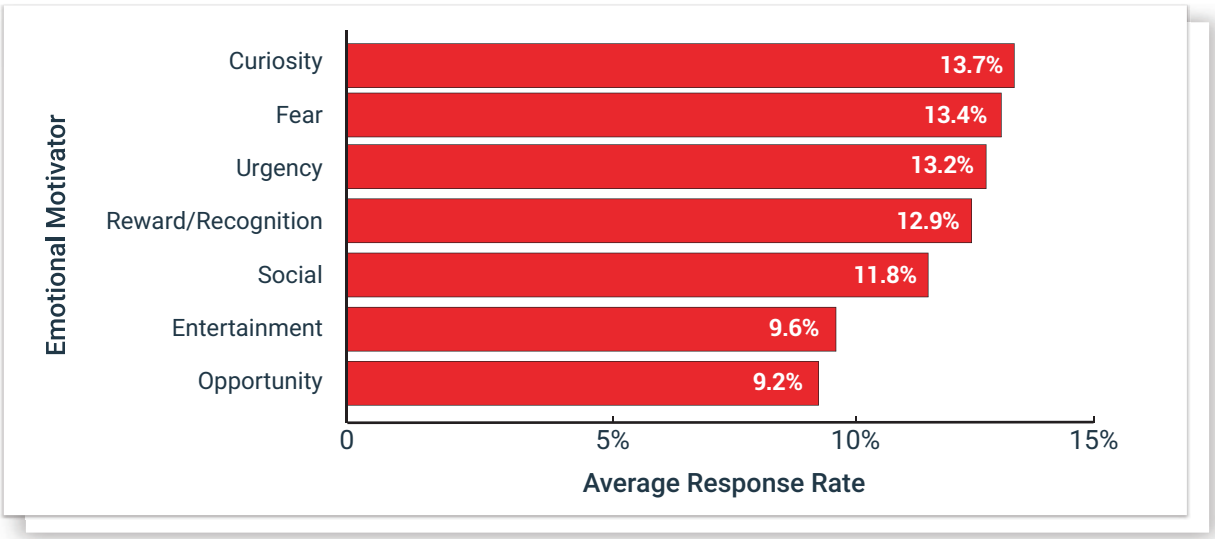

Figure 8: Average response rates by Motivator

In **Figure 8**, we analyzed our data set to determine the average response by emotional motivator. As you can see, Curiosity, Fear, and Urgency topped our list, with all coming in at averages higher than 13%.

It should be noted that Fear and Urgency are a normal part of everyday work for many users. Consider that most employees are conscientious about losing their jobs due to poor performance (fear) and are often driven by deadlines (urgency), leading them to be more susceptible to phish with these emotional components. Further, Curiosity replaced Social [interactions] at the top of our list of emotional motivators in this year's study. This is primarily due to maturing our model to assign multiple emotional motivator tags to our phishing templates.

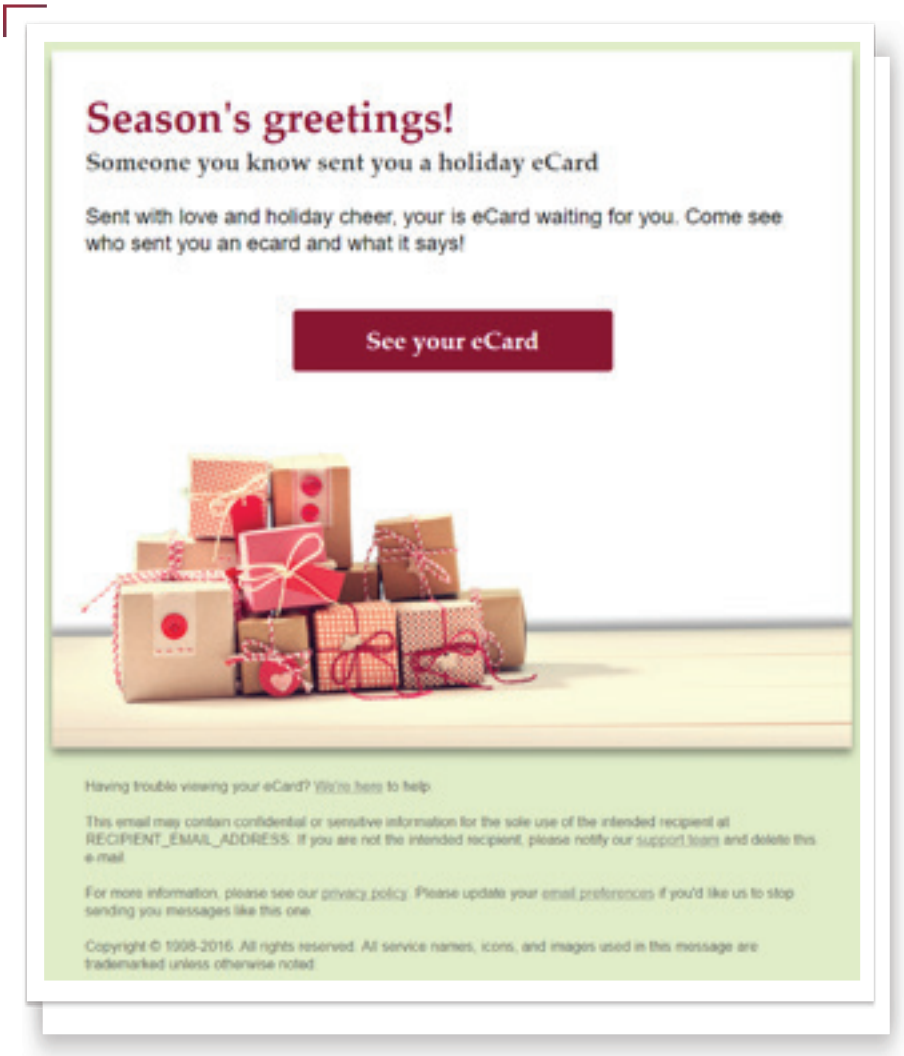

Figure 9: Holiday eCard template

This can best be seen by reviewing the average response rates for our customizable templates and noting that eCards remain difficult for users to avoid and that they are averaging 20% response rates. Our Holiday eCard template, shown above in **Figure 9**, includes multiple factors that make it difficult to avoid, such as personal context, curiosity, and social connection.

Ransomware and Active Threats

PhishMe strives to drive resiliency and reduce susceptibility to the wide range of phishing threats used today. However, some threats are more prevalent and disruptive to an organization and need a special focus by using Active Threat phishing scenarios.

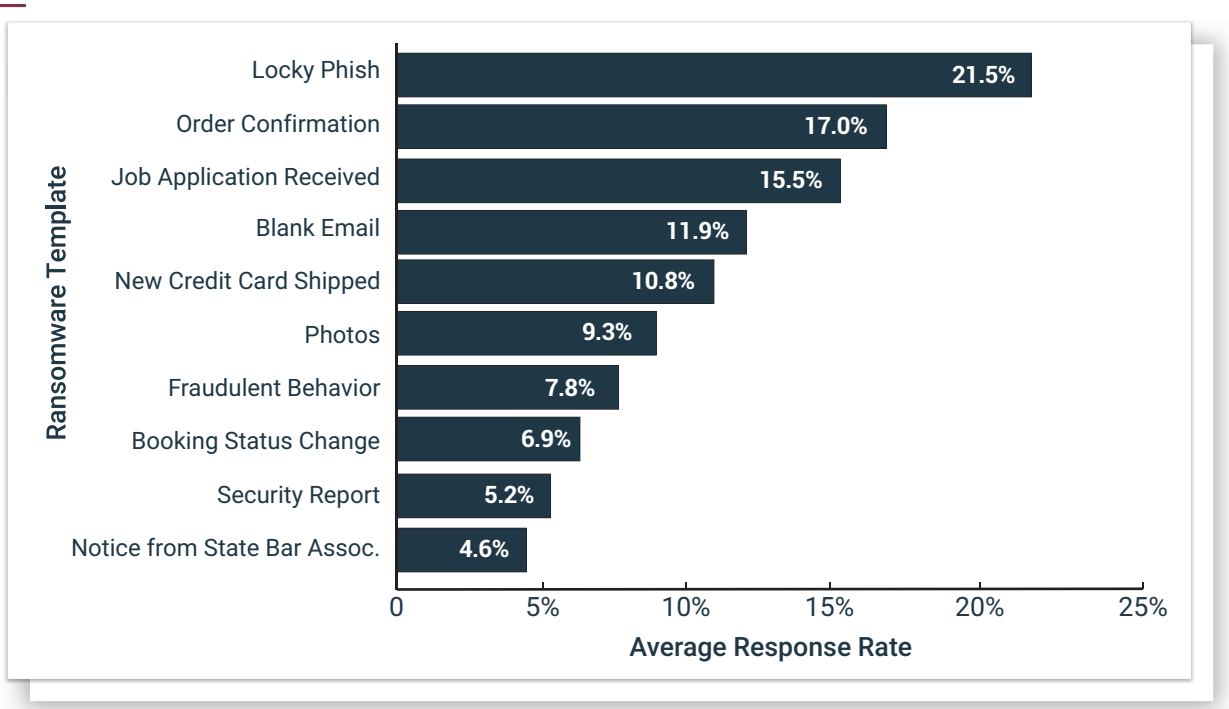

Figure 10: Ransomware template response rates

In **Figure 10**, the current average response rates for our templated scenarios that model today's active threats show an average 17% response rate across all Ransomware templates.

What is Ransomware?

Ransomware is a type of malware that prevents or limits users from accessing their system. This type of malware forces users to pay the ransom through certain online payment methods to grant access to their systems, or to get their data back.

According to PhishMe's Q3 Malware Review, **97.25%** of the samples analyzed contained a form of ransomware—making it the most utilized form of malware in phishing emails.

Locky Phish Analysis

On February 16, 2016, PhishMe's Intelligence team identified many significantly large sets of emails delivering Word documents that contained macro scripts used to download a malware payload known as Locky. The scope of Locky's delivery in its first full day of deployment was staggering with over 400,000 endpoints around the world affected by this encryption ransomware in mere hours. Locky distribution not only dwarfs most malware from 2016, but it also towers over all over other ransomware varieties, making it imperative to implement a phishing simulation using a Locky.

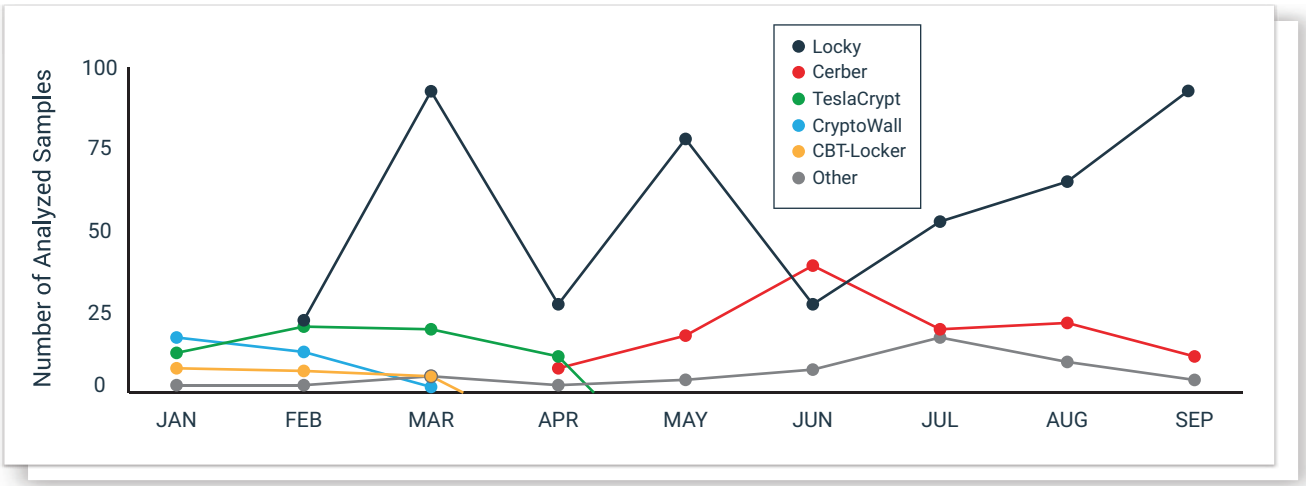

Figure 11: Relative proportions of ransomware varieties analyzed in 2016

In analyzing the susceptibility to the PhishMe Locky template, we can see the characteristics that lend to its effectiveness in both our anti-phishing programs and in the real world:

1. It is presented in a business context.
2. Its personalized to the recipient.
3. There are no noticeable errors in grammar or spelling.
4. It mimics many organizations' existing invoice processes.

From: Jill preston <jill.preston@lucrativehiring.com>
Subject: Unpaid invoice #4806

Dear RECIPIENT_NAME,

Please see the attached invoice (.doc) and remit payment according to the terms listed at the bottom of the invoice.

Let us know if you have any questions.

We greatly appreciate your business!
Jill preston

Figure 12: PhishMe's Locky Phish template

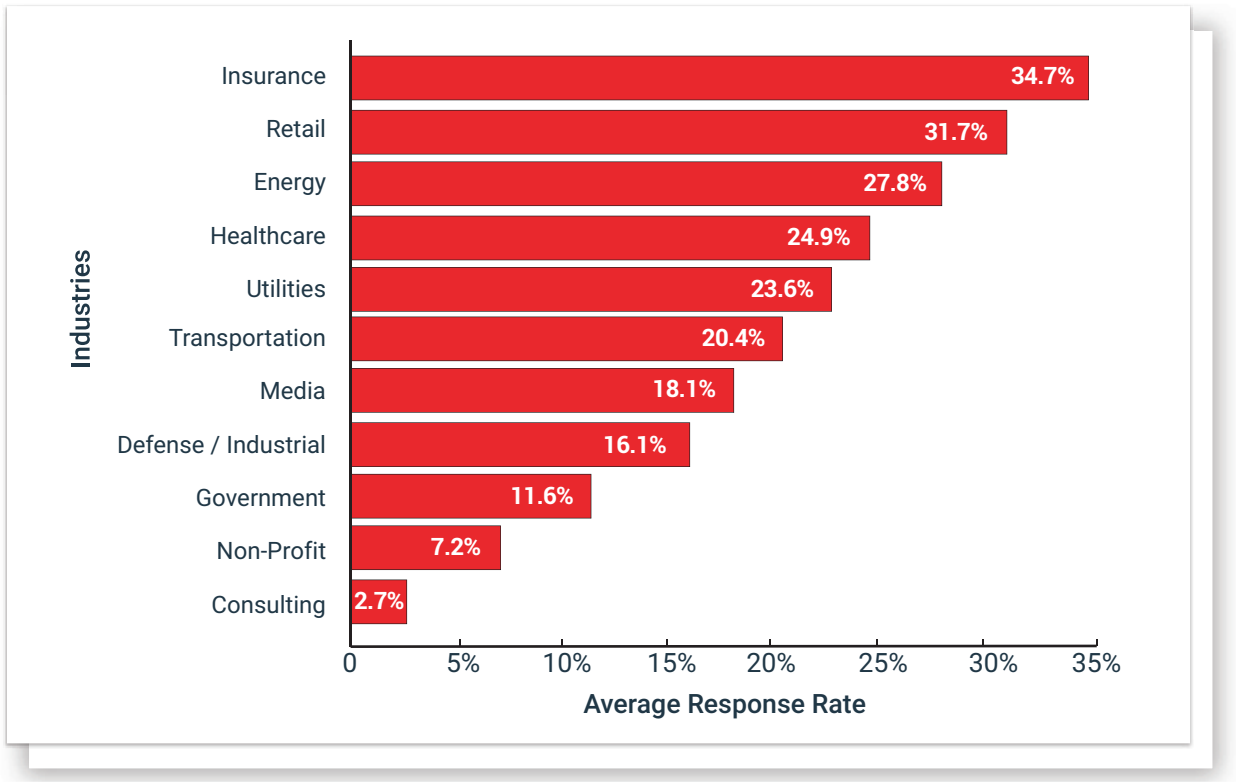

Figure 13: Locky Phish template averages by industry

As **Figure 13** shows, there is once again a wide variance in response to this real-world threat. From our data set, we find those organizations in the Insurance, Retail and Energy sectors most vulnerable with ranges in average response rates from 28% to 35%.

This underscores the need to ensure you understand how your company responds to any given phishing type and components complexity. This understanding will allow you to address your specific threats in your anti-phishing program. See the Appendix for more information on High Impact Scenarios and Scenario Response Rates by Industry.

No Links - The Challenge of Stopping BEC Emails

Business Email Compromise (BEC) is a sophisticated scam targeting businesses using familiarity and business activity requests such as performing a wire transfer payment or being asked to provide sensitive company information such as W2 data. The email appears to have come from an internal authority, but there are typically no links or attachments for technology to analyze and trigger an alarm, making these threats extremely difficult to detect.

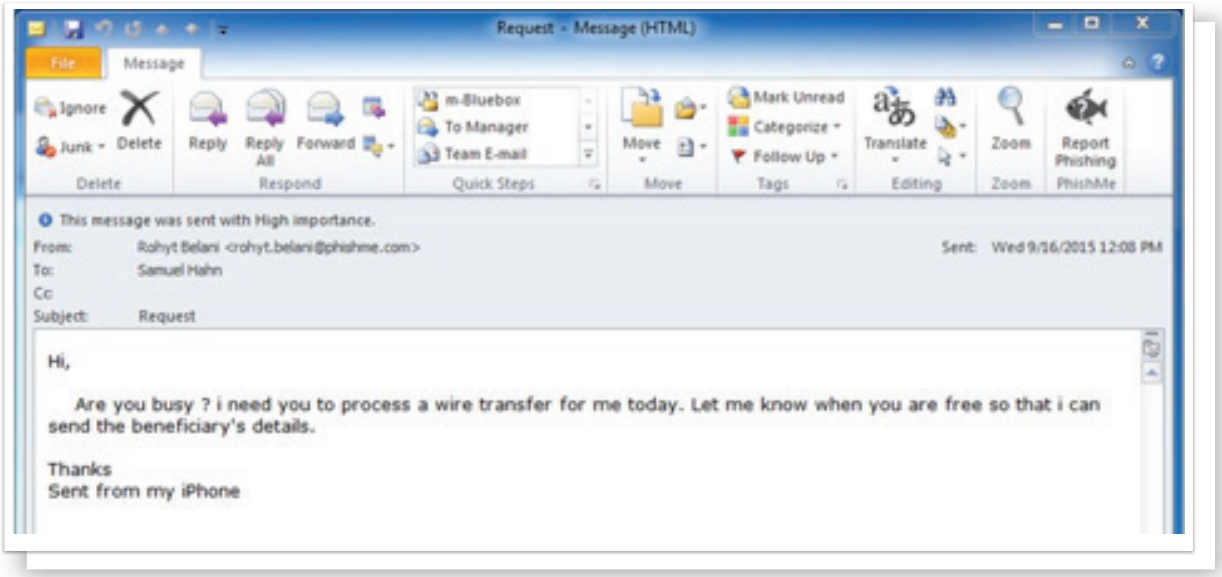

Figure 14: Example BEC email

BEC Style Average Susceptibility

Scenarios	Defense Industrial	Energy	Financial Services	Healthcare	Insurance	Media	Retail	Technology	Travel	Average
Wire Fraud			3.9%							3.9%
Wire Transfer Request		1.6%	2.0%	4.6%				2.2%	3.9%	2.6%
Wiring Money Process	15.5%	10.6%	10.2%	12.6%	19.6%	28.7%	4.4%			16.9%
Average	**15.5%**	**6.1%**	**6.1%**	**10.0%**	**19.6%**	**28.7%**	**4.4%**	**2.2%**	**3.9%**	**14.2%**

Figure 15: Average BEC susceptibility by theme

To help address the BEC threat, PhishMe added specific templates to mimic successful BEC attacks. Across our BEC templates, we found an average response rate of 14%. The Wiring Money Process was clearly the scenario with the highest susceptibility rate. It was particularly effective for Defense, Insurance, and Media industries.

PhishMe Tip

Incorporate feedback from your IR and Network teams into your anti-phishing program. Specifically, identify those real-world phishing scenarios that your organization receives on a regular basis, and incorporate them into your rotation.

The Phishing Kill Chain

To this point, our report has outlined and discussed the extent of the phishing risk and the factors that impact difficulty in recognition and reporting for users. It is now important to stress the differences between penetration testing results and an anti-phishing behavioral conditioning program. It is not enough to simply identify the breadth of the risk. We must answer the question: *how do we take susceptibility results and turn them towards mitigation of the phishing threat?*

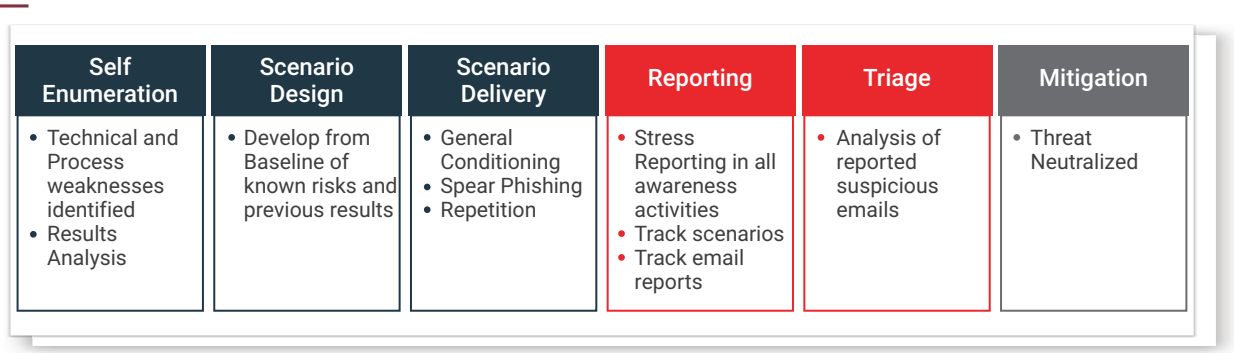

Figure 16: Phishing Kill Chain

The design of any anti-phishing program can be modeled on the Phishing Kill Chain in **Figure 16**. This model mimics the well-known Kill Chain process utilized in security organizations today. The difference is that the Phishing Kill Chain inserts Reporting by Users at the point at which the standard model indicates an exploitation of a breach. Incorporating the model above into any anti-phishing program can be accomplished via the steps outlined below:

1. Baseline your organization's technical and process weaknesses.
2. Analyze initial / previous phishing scenario results to identify the phishing models your users find most difficult to recognize.
3. Design future scenarios based on known deficiencies and analysis of results.
4. Deliver phishing scenarios and education to your general audience.
5. Stress the importance of reporting in all awareness activities including your scenario education.
6. Incorporate spear phishing for high-risk users and departments.
7. Repeat scenarios to increase recognition and reporting.
8. Track user progress for program reporting metrics and for reporting of suspected 'real' phishing attempts.
9. Route suspected phish reports to your IR teams for analysis and mitigation.

Improved Recognition and Reporting

When measuring the effectiveness of any anti-phishing program, we look across three (3) key metrics:

1. Reduced Susceptibility
2. Increased Recognition
3. Increased Reporting

In the charts below, we analyzed different sized organizations for trends in Repeat Offenses (falling for a phish) and for Reporting Rates. This sample included results from more than 300,000 users in organizations that have had PhishMe Reporter, a simple reporting tool, deployed for more than one (1) year.

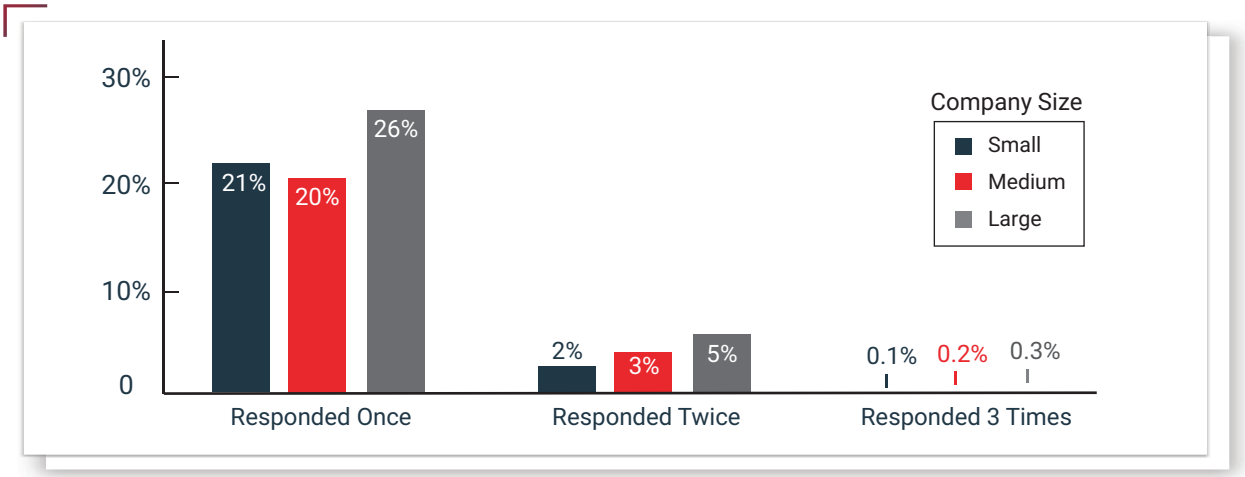

Figure 17: Reduction in repeat offense by company size

Figure 17 above shows an overall improvement in recognition of phishing attempts with and average drop of 19% in response rates after a single failure. This pattern holds true regardless of company size. In other words, users will improve performance with repetition and increased exposure to phishing templates.

In the Reporters Breakdown chart shown below, we can see that users will adopt a new habit as a result of stressing the importance of reporting in anti-phishing programs. For users in this sample with the PhishMe Reporter installed:

1. 12% to 20% have reported at least once.
2. 17% to 29% have reported multiple times.

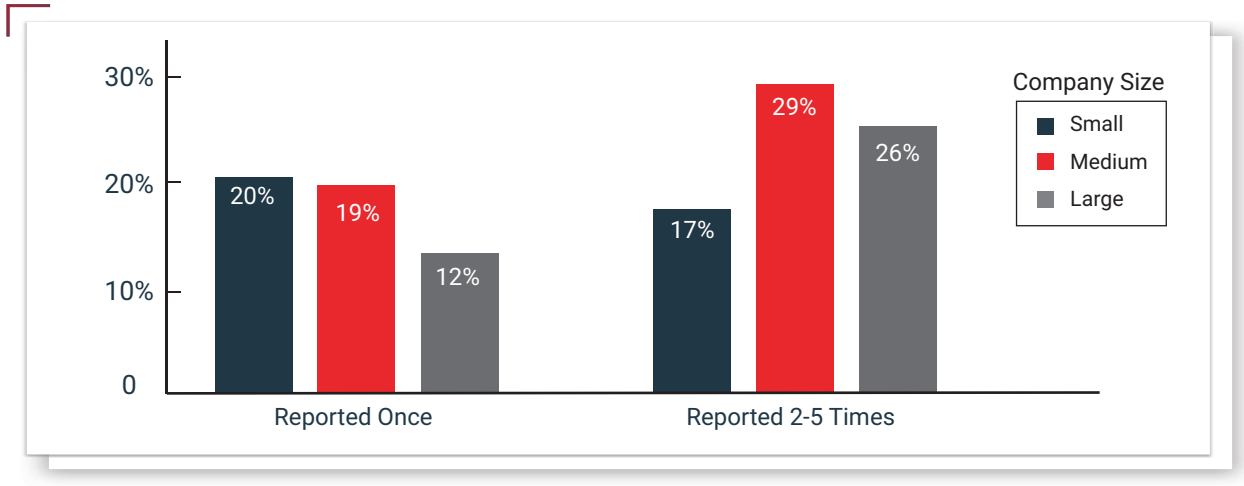

Figure 18: Increases in reporting by company size

In addition to these statistics, the organizations involved in this sample collected more than just simulated phishing reports. Over a twelve (12) to eighteen (18) month period, these organizations took in the following counts of "real" suspicious email reports from their users:

1. Large Company Size – More than 1 Million
2. Medium Company Size – More than 40,000
3. Small Company Size – More than 16,000

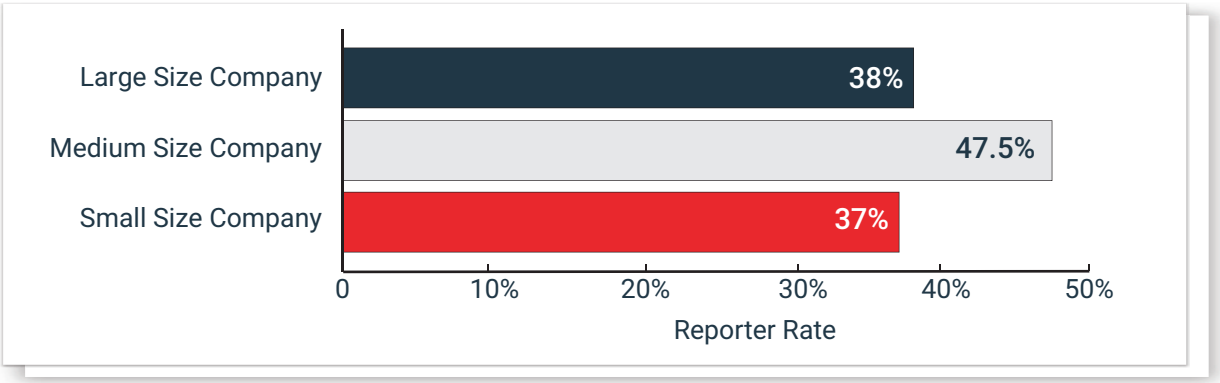

Figure 19: Reporting rates by company size

Our final chart from this sample in **Figure 18** shows us the percent of users—with PhishMe Reporter installed—who have reported at least one (1) simulated scenario or real phish. Again, regardless of company size, we see high percentages of users reporting, with a range of 37% to 40% of the population taking part. This is significant when compared to overall susceptibility rates that generally average 15% to 20% across all types and templates.

Having a higher rate of reporters than those susceptible provides an organization its best opportunity to "Get Left of Breach" as we previously discussed.

Measuring Anti-Phishing Program Effectiveness

When measuring the effectiveness of any anti-phishing program, we want to look at our results across the breath of an organization. Using the model below, we can provide a rating for an organization's current level of maturity and resiliency against phishing attacks.

Level	Description
Green	The Organization proactively responds to threats and mitigates them
Yellow	Users are alert ----> inspecting emails ----> reporting threats
Orange	Users are alert ----> inspecting emails for threats
Red	Users exhibit a complete lack of awareness of phishing threats

Figure 20: Organizational levels of effectiveness

The model moves from a complete lack of awareness to proactive response and mitigation of threats. The key to identifying your current state is to compare your organization's trends in susceptibility and reporting over time. The client sample in **Figure 21**, shows us an ideal pattern with divergence in susceptibility and reporting numbers. In other words, **as the susceptibility rates continue to decline, we see more users reporting suspicious emails**.

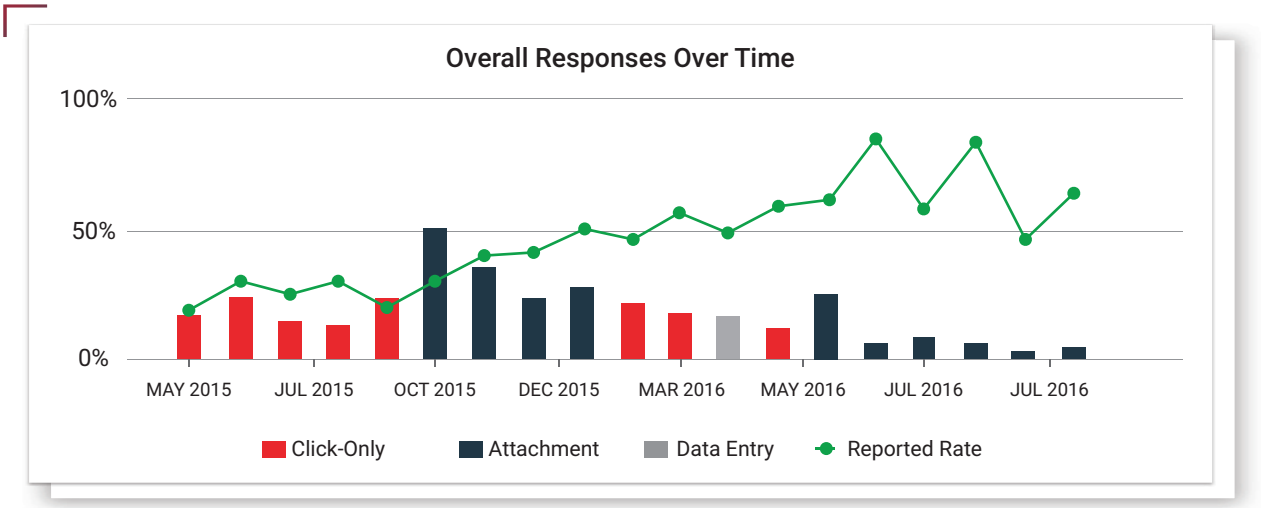

Figure 21: Diverging trends sample

As suggested by the Phishing Kill Chain model, this company stressed reporting from the very beginning of their program. Their program has been active for eighteen (18) months and is averaging between 11 or 12 anti-phishing scenarios per year.

Conditioning Users to Report

To further illustrate the importance of conditioning users to report a suspected phish, we analyzed data for clients who have had PhishMe's Reporter deployed over the past two (2) years. **Figure 22** shows the percent of users who were found susceptible versus the percent reporting and shown by the percentage of client users with the PhishMe Reporter feature deployed.

For example, in 2015, for clients who deployed Reporter to 10-20% of their population, the average susceptibility was ~15%, while the average reporting rate was ~7%. In 2016, those numbers change to 13% and 16%, respectively.

The client sample and trending charts in **Figure 22**, show the effectiveness of implementing a program with the Phishing Kill Chain model in mind. By stressing reporting, we see a consistent reduction in susceptibility and a correlating increase in reporting.

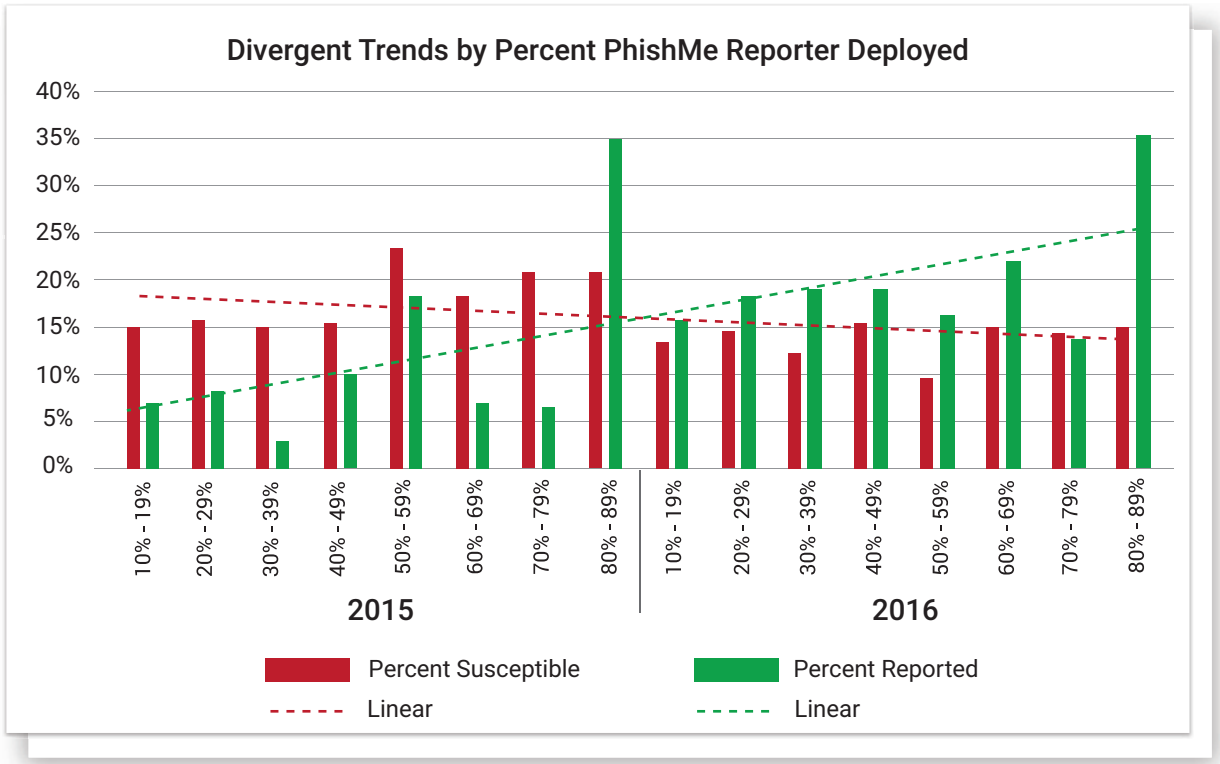

Figure 22: Diverging trends analysis

Figure 22 reveals a few important trends regarding the deployment of PhishMe Reporter:

1. Year over year, we see positive trends in reduction of susceptibility with Reporter deployed.
2. In the second year of Reporter deployment, we consistently see average reporting rates that are higher than average susceptibility rates.
3. **Reporting significantly outweighs susceptibility** when Reporter is deployed to more than 80% of a company's population, even in the first year.

Getting "Left of Breach"

Anytime we can get more users reporting a phish instead of falling susceptible to it, we provide our organization's Incident Response teams with a real opportunity to reduce the time to mitigate a potential breach or to eliminate the occurrence of a breach altogether.

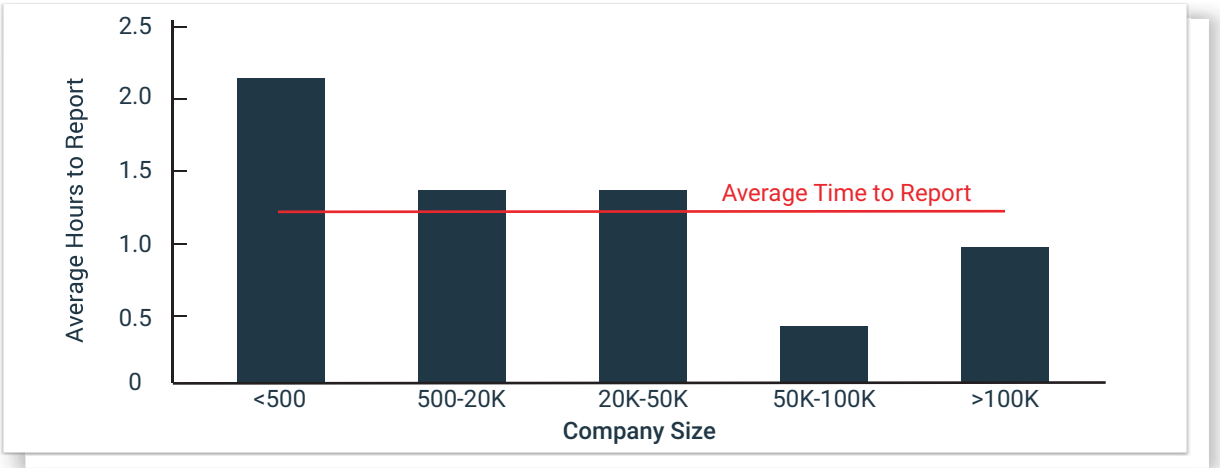

Figure 23: Average hours to report by size

Looking across our data at those organizations with PhishMe Reporter deployed, we could determine an average reporting time of 1.2 hours with a range of 2.1 hours on the high end and .4 hours on the low end. In cases such as this, we effectively reduce the standard time for detection of a breach to approximately 1.2 hours—a significant improvement over the current industry average of 146 days.

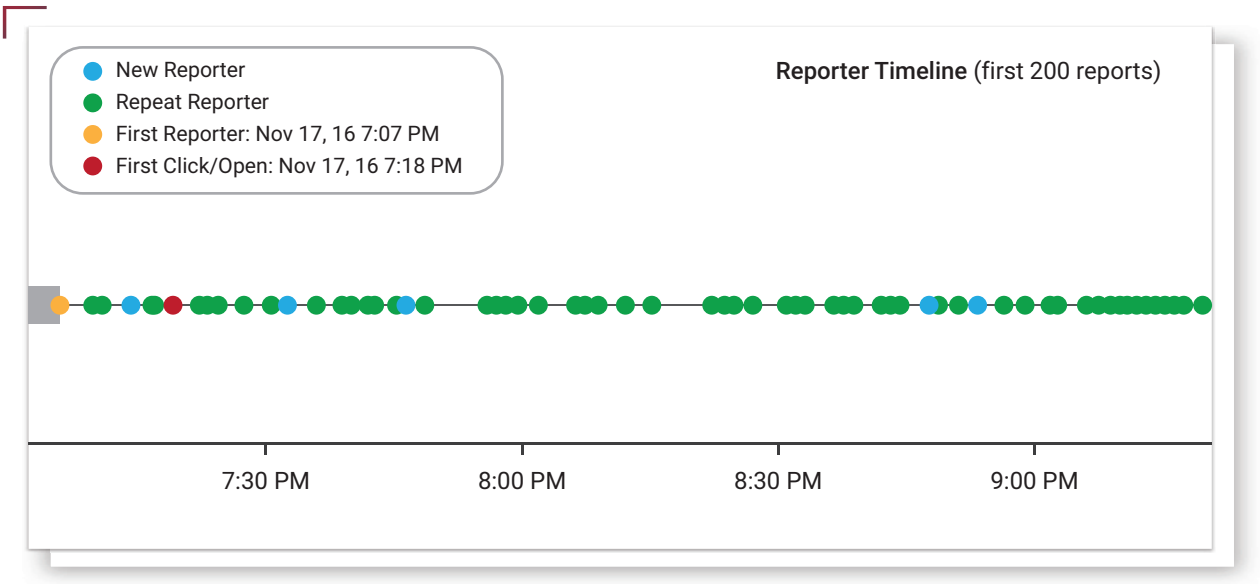

Figure 24: Left of Breach reporting

While the current average reporting time is 1.2 hours, we can see several instances in our data where the phishing scenario was **reported prior to any users falling susceptible**. For example, in **Figure 24**, we find an instance where the phishing scenario was reported a full 11 minutes prior to anyone falling for the phish and exposing company assets. In essence, this client was able to get "Left of Breach" in the Kill Chain for this scenario.

Phishing Incident Response for SOC and IR Teams

Instituting a formal reporting process for suspicious emails can fall short and overwhelm your SOC and IR resources. Without a way to organize, assess, and respond to the barrage of reported emails, the teams may not respond quickly enough to avoid an incident.

PhishMe Triage

PhishMe Triage is the first phishing-specific incident response platform that allows security operation (SOC) and incident responders to automate the prioritization, analysis and response to phishing threats that bypass your email security technologies. It gives teams the visibility and analytics needed to speed processing and response to employee-reported phishing threats and decrease the risk of breach.

Conclusions

Through baselining known weaknesses, identifying existing threats, and developing an understanding of an organization's difficulty in recognizing specifics types and components of a phish, companies can institute an anti-phishing program that significantly reduces the threat of a breach.

With repetition, a sustained and well-executed phishing simulation program, focused on conditioning employees to report, provides a significant reduction in overall exposure to risk from this ever-changing attack vector and improves the security posture of an organization. By analyzing our phishing simulation and reporting data over time, we have found:

- The combination of appropriate context and emotional motivators delivered greater response rates from employees to difficult scenarios which, in effect, decreased overall training time and allowed the organization to focus on remediating specific phishing risks with repetitive scenario training on those risks.
- By phishing across an entire employee base, an organization can quickly increase awareness, train more people, and identify key triggers that influence employee behavior.
- It is important to train employees to report phishing attempts as soon as they are recognized to offset the likelihood that a phishing attempt will be responded to in its first several hours in a network environment.
- It is possible to significantly reduce the standard time for breach detection from days to minutes with a conditioned workforce reporting suspicious activity.

Glossary

Phishing - Phishing is defined as any type of email-based social engineering attack, and is the favored method used by cyber criminals and nation-state actors to deliver malware and carry out drive-by attacks.

Phishing emails disguise themselves as legitimate communication, attempting to trick the recipient into responding by clicking a link, opening an attachment, or directly providing sensitive information. These responses give attackers a foothold in corporate networks, and access to vital information such as employee credentials, communications, and intellectual property. Phishing emails are often carefully crafted and targeted to specific recipients, making them appear genuine to many employees.

Email-based attacks are an effective, low-cost tool that can bypass many detection methods. The criminal organization benefits from this "tool", because there is little chance of capture or retribution. It is little wonder then that several prominent security firms have confirmed phishing to be the top attack method threatening the enterprise today:

- In their whitepaper, Spear Phishing Email - Most Favored Attack, security firm TrendMicro noted that spear phishing accounts for 91% of targeted attacks. [1]
- The Mandiant APT1 Report cites spear phishing as the Chinese hacking group APT1's most common attack method. [2]
- In their 2013 report, Verizon traced 95% of state-affiliated espionage attacks to phishing.[3]

Phishing simulation refers to a course of activities designed to improve employee knowledge, recognition, and response to phishing attacks. The emails are safe and contain links to educational content to help employees who have fallen for the simulation to understand why the email was potentially malicious.

Phishing scenario refers to a specific email used in a simulated phishing exercise.

Phishing template refers to email content provided for use in scenarios.

Phishing theme refers to a collection of email scenario templates that use the same context, motivation or topic to elicit user action

Repeat offender refers to a person that has shown repeated susceptibility to spear phishing scenario (has fallen for the simulations repeatedly)

1 http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf
2 http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
3 http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf

Appendix

High-response Scenarios

File from Scanner	
Transportation	49.2%
Healthcare	30.9%
Insurance	30.5%
Pharma / BioTech	30.4%
Energy	23.7%
Retail	15.8%
Consulting	14.4%
Utilities	13.6%
Technology	9.9%
Non-Profit	5.0%
Grand Total	**26.8%**

Locky Phish	
Insurance	34.7%
Retail	31.7%
Energy	27.8%
Healthcare	24.9%
Utilities	23.6%
Media	18.1%
Defense Industri	16.1%
Government	11.6%
Non-Profit	7.2%
Consulting	2.7%
Grand Total	**20.7%**

Unauthorized Access	
Defense Industri	46.1%
Consulting	29.9%
Insurance	25.3%
Telecommunicati	24.7%
Technology	24.4%
Utilities	17.6%
Travel	15.5%
Energy	14.6%
Manufacturing	14.6%
Legal Services	5.9%
Grand Total	**18.1%**

eCard Alerts	
Education	44.1%
Healthcare	30.9%
Insurance	27.1%
Financial Service	22.5%
Energy	22.0%
Technology	18.9%
Retail	16.5%
Consulting	12.2%
Manufacturing	9.7%
Government	7.0%
Grand Total	**19.7%**

Package Delivery	
Technology	28.0%
Pharma / BioTech	26.1%
Legal Services	25.5%
Manufacturing	21.3%
Healthcare	21.3%
Transportation	13.9%
Defense Industri	13.5%
Energy	13.5%
Non-Profit	13.3%
Media	7.1%
Grand Total	**19.9%**

Financial Information Review	
Healthcare	31.5%
Insurance	27.3%
Consulting	26.6%
Manufacturing	24.4%
Technology	19.7%
Energy	19.2%
Government	17.3%
Media	15.4%
Financial Service	14.6%
Retail	13.2%
Grand Total	**18.3%**

Financial Information	
Technology	36.1%
Legal Services	27.6%
Retail	25.3%
Manufacturing	24.9%
Healthcare	24.1%
Non-Profit	15.8%
Energy	15.1%
Financial Service	14.5%
Media	11.6%
Consulting	2.0%
Grand Total	**19.0%**

Digital Fax	
Legal Services	42.0%
Telecommunicati	32.9%
Defense Industri	28.0%
Consulting	22.1%
Healthcare	21.5%
Manufacturing	13.2%
Technology	10.2%
Retail	9.1%
Government	8.4%
Media	7.3%
Grand Total	**15.1%**

Order Confirmation	
Education	34.8%
Transportation	26.1%
Technology	24.8%
Insurance	19.6%
Media	19.0%
Manufacturing	13.8%
Consulting	13.5%
Pharma / BioTech	12.8%
Defense Industri	8.9%
Retail	6.4%
Grand Total	**17.8%**

Inbox Over the Limit	
Consulting	24.4%
Manufacturing	22.8%
Insurance	22.0%
Defense Industri	20.5%
Healthcare	19.5%
Energy	11.4%
Technology	11.3%
Education	10.6%
Legal Services	8.6%
Utilities	1.2%
Grand Total	**18.6%**

Scenario Response Rates by Industry

Media	
Bonus Agreement	42.9%
Manager Evaluation	42.6%
Cant Send, File Size Tc	41.3%
Corporate Rewards	31.3%
Free Lunch	30.9%
File from Scanner	18.1%
Locky Phish	18.1%
Dyre Campaign	18.0%
Brexit Impact on Oper	17.7%
Computer Refresh Pro	17.4%
Grand Total	**21.4%**

Energy	
Updated Organiz	41.8%
Cleaning Chemic	29.2%
Locky Phish	27.8%
Scanned File	26.6%
News Alert	25.9%
Word Documents	18.6%
Digital Fax	18.0%
Time Off Reques	17.8%
Bed Bugs Found i	17.6%
New Job Opportu	17.0%
Grand Total	**22.0%**

Transportation	
File from Scanne	49.2%
Pro-forma Invoic	31.3%
Order Confirmati	26.1%
Please Verify You	22.8%
eCard Alerts	21.4%
Euro 2016 Tickets	5.5%
Free Coffee	3.9%
Email Address Ve	3.6%
Adobe Security U	1.7%
Grand Total	**10.9%**

Government	
Financial Informa	23.4%
Tax Documents -	23.1%
Policy Memo - Su	23.0%
File from Scanne	22.7%
Brexit Impact on	20.7%
New Credit Card	13.5%
Superfish	13.2%
Pokémon GO Pol	13.0%
Inbox Over the Li	12.6%
Locky Phish	11.6%
Grand Total	**15.4%**

Financial Services	
Manager Evaluati	42.0%
Time Off Reques	29.0%
Halloween Costu	27.0%
Forgot Attachme	26.5%
Unauthorized Ac	26.3%
Scanned File	19.6%
Word Documents	19.1%
Valentine's Day e	17.7%
Digital Fax	17.5%
APT1	17.4%
Grand Total	**21.9%**

Healthcare	
Manager Evaluati	43.8%
Valentine's Day e	33.7%
Financial Informa	31.5%
eCard Alerts	30.9%
File from Scanne	30.9%
Unauthorized Ac	22.3%
Digital Fax	21.5%
Package Delivery	21.3%
Happy Valentine	20.8%
Inbox Over the Li	19.5%
Grand Total	**24.1%**

Manufacturing	
Unused Email Ac	40.7%
Notice to Appear	36.0%
Confirm Shipping	34.1%
Flash Update Rec	32.0%
Please Update Dr	31.3%
Company Newsle	21.9%
Inactive Email Ac	21.9%
Complaint Filed	21.4%
Package Delivery	21.3%
APT1	21.2%
Grand Total	**23.6%**

Legal Services	
Scanned File	46.4%
Digital Fax	42.0%
Unauthorized Ac	29.3%
Financial Informa	27.6%
Package Delivery	25.5%
Free Coffee	8.2%
Word Documents	8.0%
Shared Folder	7.9%
Secure Email	7.4%
Security Token C	7.2%
Grand Total	**14.4%**

Pharma / BioTech	
Sent From Phone	41.6%
Forgot Attachme	39.3%
Employee Satisfa	32.9%
File from Scanne	30.4%
Please Review Cc	28.6%
Forgot Attachme	16.1%
Build Your Own	13.2%
Order Confirmati	12.8%
Package Delivery	12.3%
Cease and Desist	10.5%
Grand Total	**19.6%**

Technology	
Free Lunch	49.4%
Financial Informa	36.1%
Time Off Reques	33.3%
Package Delivery	30.3%
Pro-forma Invoic	30.1%
Computer Refres	22.0%
Locky Phish	21.6%
Word Documents	21.2%
Build Your Own	21.0%
Please Verify You	20.9%
Grand Total	**23.4%**