PHISHME

Enterprise Phishing Susceptibility Report

An Inside Look at Employee Behavior Pertaining to Highly-Effective Phishing Scenarios

Special Acknowledgment for Contributing Analysis: University of Cambridge, London School of Economics and Political Science and PhishMe Managed Services Team.

Introduction

Welcome to the inaugural edition of PhishMe's Enterprise Phishing Susceptibility Report. PhishMe has been collecting and aggregating phishing threat and simulation data since the launch of the Simulator service in 2008. With this report, we hope to share our experiences and insights on employee behavior as it relates to the simulated phishing scenarios.

Phishing, to include spear phishing, persists as the No. 1 attack vector, and both continue to challenge IT security teams as threat actors evolve their tactics to gain access to corporate networks and assets as well as consumer data. Now, more than ever, it is critical to have the ability to identify the types of email attacks, themes and elements which cause your employees to respond. With this knowledge we can determine how best to prepare and condition them to identify attack emails and report them to your internal IT security teams.

To that purpose, this study examines data samples from more than 400 PhishMe customers who conducted over 4,000 training simulations during a period of 13 months. The simulation data illustrates the current state of phishing, highly successful attack vectors and prominent phishing themes as well as the factors that impact an employees' susceptibility to falling victim to an attack, such as time of day and email subject lines.

Report Data Demographics

- 8 million emails over a 13-month span
- 75% of organizations are training more than 1,000 employees
- Representing organizations from US (86%) and Europe (14%)
- Representing 23 industries
- Representing Fortune 500 and public sector organizations

Summary of Findings

After sending more than 8 million phishing-simulation emails to more than 3.5 million employees in 23 industries across the globe, PhishMe gathered the following insights:

- 87% of the employees who opened a phishing simulation email opened it the SAME DAY it was sent.
- Regardless of the time at which an email is sent, most employees responded to a phishing email in the morning hours, particularly at 8:00 AM local time.
- Employees who open a phishing email are 67% more likely to respond to another phishing attempt.
- The most effective phishing emails contain a business communication theme.
    - > 36% opened emails with the subject line "File from Scanner"
    - > 34% opened emails with the subject Unauthorized Activity/ Access
- Behavioral conditioning decreased susceptible employees' likelihood to respond to malicious email by 97.14% after just 4 simulations.

These results highlight the importance of understanding how the components of complexity and context impact the phishing susceptibility of employees in an organization and how a continuous security training program has been 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.

Easy Pickings

Phishing is the No. 1 attack vector today and with good reason—it often leads to success. An organization's employees are the primary target, the means to the attackers' end of gaining access to company systems. Employees are the easier targets due to their susceptibility to various emotional and contextual triggers. Thus, it follows that organizations are making behavioral conditioning and training a priority.

Phishing Themes or Categories of Communications

PhishMe themes and templates provide sample emails that match real-world scenarios and provide an opportunity to mimic a variety of attacks (see "Attack Methods" on page 3) and primary motivators. A theme accounts for the category topic of the communication such as business communications, package delivery, and IT communications. PhishMe templates provide specific communications within those themes.

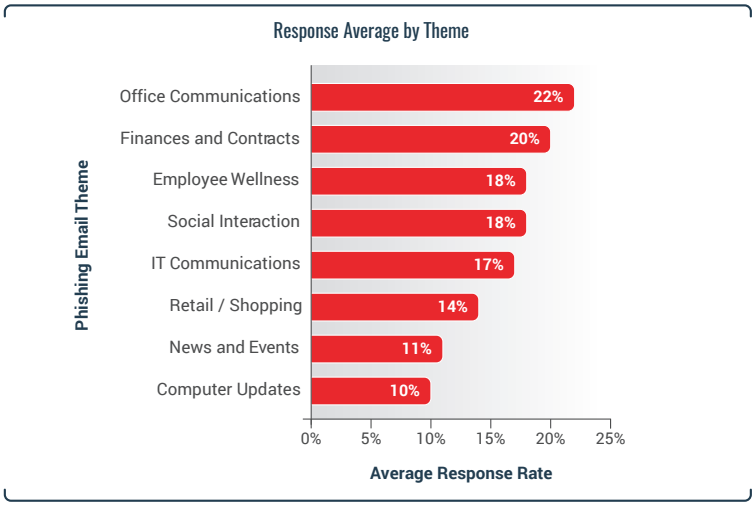


Figure1: Depicts training themes employees found most difficult to recognize as a phishing email.

Office Communications and Finances and Contracts theme garnered average response rates of 22% and 20%, respectively. Note the highest themes in Figure 1 (Office Communications) aligns with the highest benchmarking average in Figure 1A (File from Scanner). Computer Updates, as the lowest response rate in Figure 1, also aligns with the lowest simulation average in Figure 1A (Adobe Security Updates).

The correlation in results gives us some indication that business communication scenarios were more effective phishing emails than IT-related scenarios.

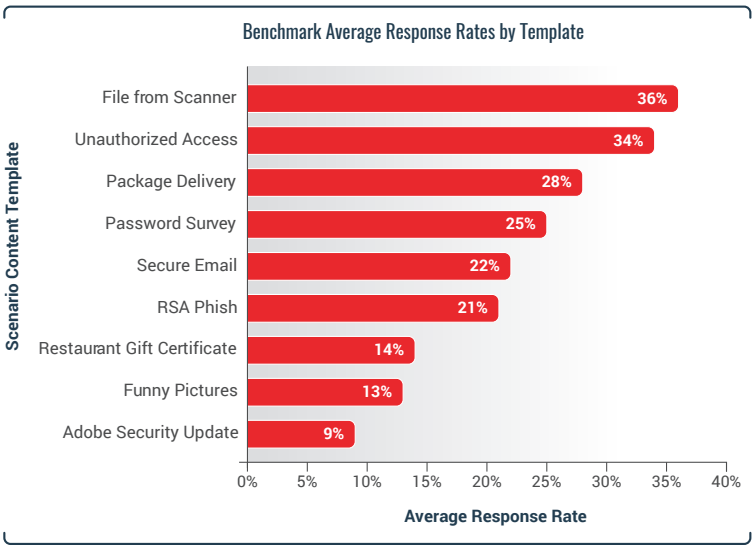


Figure 1A: Shows the different templates that were used in benchmark simulations across more than 10 industries.

An Aside on PhishMe's Patented Benchmarking

In benchmarking analysis, an aggregate performance of one group is compared with an aggregate performance of individuals from a second group, across separate companies.

Standardizing the simulated phishing attacks for individuals from both the first and second groups is necessary in order for the performance of the first group to be fairly or meaningfully compared to the performance of the second group.

To ensure uniformity in the simulated phishing attacks, messages thereof may be constructed from template messages, the template messages having placeholders for individual-specific and company-specific information.

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.

Note: These benchmarks are based on aggregate anonymized data; no personal or corporate specific data is used in the calculations.

Templates from the business communications theme, such as File from Scanner (36%) and Unauthorized Access (34%), proved to be approximately 4x more effective than IT-related emails at generating a response (fell for the phish) from employees.

> *Note: As with all averages, we need to exercise some caution with direct comparisons in the realm of phishing attacks. This is due to the wide variance in style and complexity of phishing simulations to which any given organization may be exposed.*

Industry and Gender Differences

PhishMe further analyzed data from the "Package Delivery" benchmark simulation to understand variances across industries and gender.

As we can see in Figure 1B, there is a wide variance in average response rates per industry, more than 40% (Agriculture, Education and Pharma/BioTech) to less than 15% (Travel). The results highlight the need to carefully consider a company's culture and background when viewing phishing simulation results.

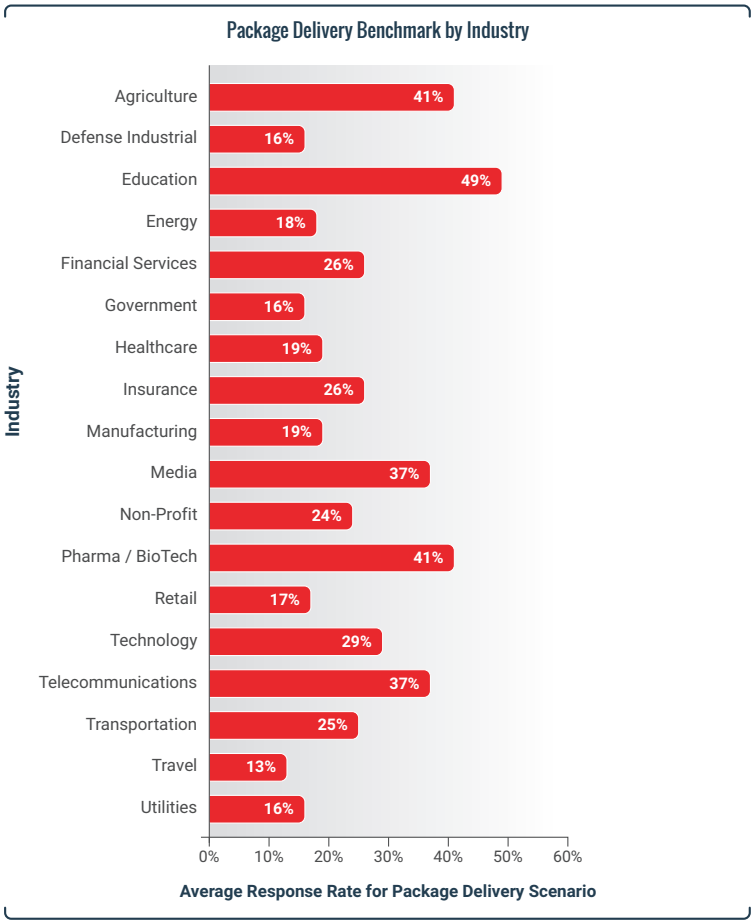


Figure 1B: Package delivery average results per industry.

We were also able to review and analyze gender response rates within the Package Delivery Benchmark results. This sample involved 26,942 verified recipients. 8,248 recipients were female, and 18,694 recipients were male. In this exercise, 1,841 female recipients and 3,697 male recipients clicked the link.

Figure 1C represents the percentage of responses by gender, indicating no significant difference since approximately 22% of females and 20% of males were susceptible to this type of attack scenario.

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.

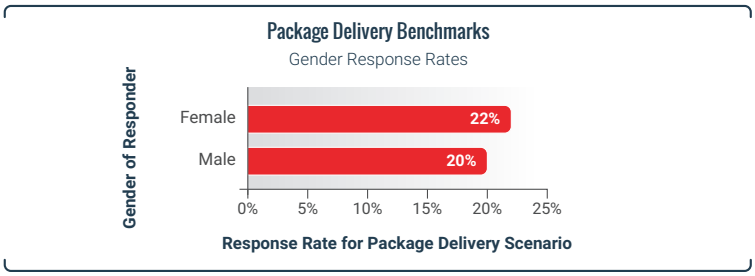


Figure 1C: No significant difference in response by gender.

Motivators

What Makes a Phish Difficult to Avoid?

Malicious actors and their targeted attack methods 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.

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

As you can see, the data in Figure 2 indicates the impact of emotional motivators on simulation outcomes. The strongest emotional motivators (above 20% average) were related to connection and reward (e.g., winning a prize).

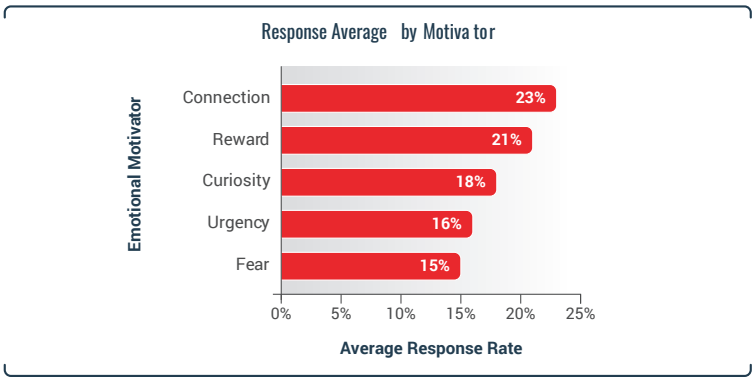
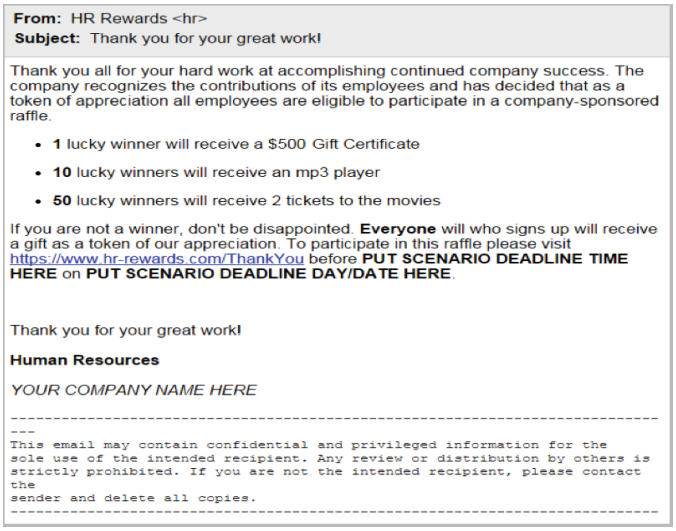


Figure 2: Average response rates by motivator.

Motivation: A Sample Use Case

To better understand the impacts of theme and motivation on responses, a sample PhishMe simulation is provided, below.



From: HR Rewards <hr>
Subject: Thank you for your great work!

Thank you all for your hard work at accomplishing continued company success. The company recognizes the contributions of its employees and has decided that as a token of appreciation all employees are eligible to participate in a company-sponsored raffle.

- **1** lucky winner will receive a $500 Gift Certificate
- **10** lucky winners will receive an mp3 player
- **50** lucky winners will receive 2 tickets to the movies

If you are not a winner, don't be disappointed. **Everyone** will who signs up will receive a gift as a token of our appreciation. To participate in this raffle please visit https://www.hr-rewards.com/ThankYou before **PUT SCENARIO DEADLINE TIME HERE** on **PUT SCENARIO DEADLINE DAY/DATE HERE**.

Thank you for your great work!

Human Resources

YOUR COMPANY NAME HERE

This email may contain confidential and privileged information for the sole use of the intended recipient. Any review or distribution by others is strictly prohibited. If you are not the intended recipient, please contact the
sender and delete all copies.

Figure 3: Example email of the employee raffle.

The average click rate for the employee raffle simulation was 38%. Despite obvious clues that this email is likely not from a employee's organization—containing both an *unknown sender and a URL not pointing to a known domain* —more than one-third of individuals tested found the content and context enough to override the technical warning signs.

This particular phishing email is a great example of how we can *combine appropriate context (Office Communications) and an emotional motivator (Reward) for greater response rates* . This is important for two reasons:

1. Presenting employees with difficult scenarios decreases overall training time by reaching more employees more quickly.
2. Identifying difficult themes allows companies the opportunity to remediate specific phishing risks through repetition of those difficult themes.

PhishMe Tip: *Identify what employees in your company respond to and focus your training efforts in those areas to more quickly reduce susceptibility.*

Timing is Everything

In real-life phishing attacks, companies have a small window to identify and respond to malicious email. The data sample analyzed showed that 87% of employees who clicked on the phishing simulation email did so on the day that it was sent, with most employees responding as soon as they opened their email inbox.

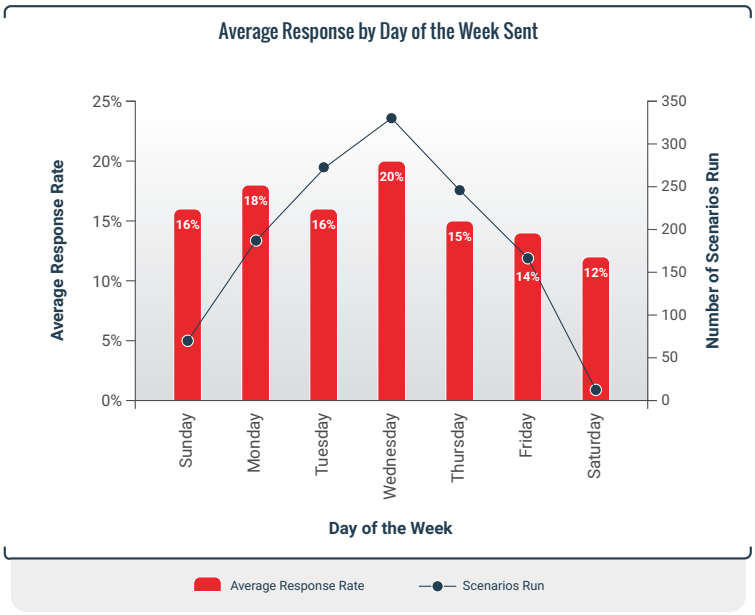


Figure 4A: Response by day sent.

An Approach to Phishing Training

- Start by sending phishing emails to all users in your entire population that mimic all attack methods and use a variety of themes and motivators.
- Include current "Premium Intel" (current real-world) themes in this cycle.
- Identify behavior trends such as susceptibility to particular attack methods, motivators, or themes, and plan future simulations to condition those employees to identify and report those simulations.
- Educate users about content and context, and teach them how to identify technical clues in phishing emails.
- Teach them to report suspected phishing emails to your designated teams.
- Use the reported phishing emails to mitigate actual threats to your organization and to develop new templates based on the real attacks reaching your employee inboxes.
- Measure improvement by tracking repeat offenders, repeat reporters, and decreases in susceptibility over time.

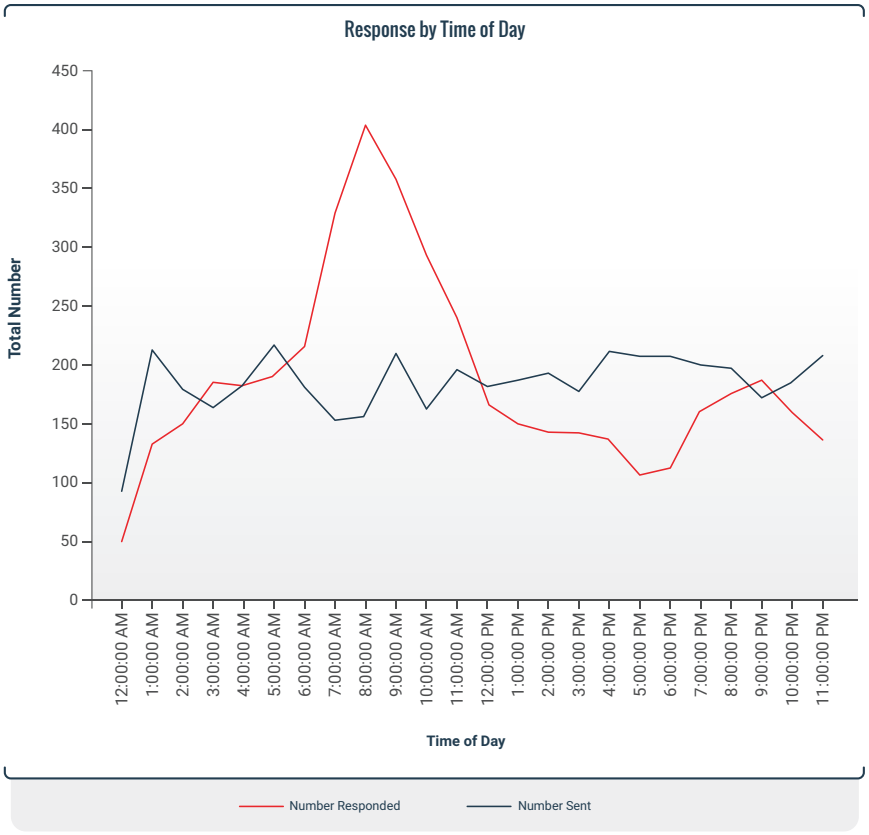


Figure 4B: Response by Time of Day.

In Figure 4B, we sampled 4,443 employee responses from 3 scenarios sent over several days and across 24 hours. The average send rate (blue line) was 183 emails per hour. The chart indicates that regardless of the time that the email was sent, most employees responded (red line) in the morning hours, with a peak at 8:00 am.

PhishMe Tip: *It is important for employees to report phishing attempts as soon as they are recognized in order to ensure that said suspicious email will be analyzed as quickly as possible to prevent the attack from spreading in a company's environment.*

Can You Reduce Employee Susceptibility?

While the task of reducing an organization's exposure to phishing may seem daunting, well-executed, continuous phishing simulations *will* improve the current security posture.

PhishMe's flexibility in the delivery of simulations allows for multiple program approaches (including the approach outlined in the sidebar), but more importantly, we can demonstrate what success looks like as employees improve and gain recognition.

The scenario responses shown in Figure 5 are based on a sample PhishMe client's results for phishing training conducted over a 7-month period. From the chart, the client has run several simulations while varying the theme, method, and sophistication. At first glance, this approach may not appear to yield a positive trend—yet it does.

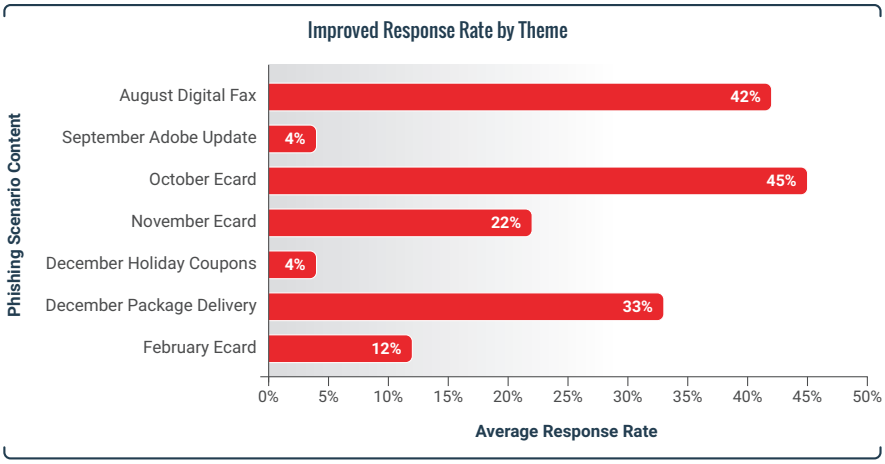


Figure 5: Sample client response rate by theme.

When we account for differences in theme, context and motivators, the positive trend emerges. Note the repetition of like simulations (Ecards) and the significant decline in response rates as employees began to recognize the theme.

To truly condition employees, programs should send several scenarios using the susceptibility traits identified during the initial phase of program development.

The higher the response on a theme, emotion, or scenario, the more often an organization should utilize that factor for its phishing training until an acceptable success rate is achieved. Organizations need to phish using themes their employees find difficult until they stop clicking—and repetition drives recognition.

In related studies conducted with the London School of Economics (LSE), we looked at differences in response rates across two simulations of varying theme and type to determine if the experience of a previous attack reduced one's susceptibility to future attacks.

In the data studied by LSE, employees received an attachment scenario followed by a click only scenario with a prior announcement. As expected, individuals who fell victim to the first simulation were much less likely to respond to the second simulation; only 15% of those that responded previously responded again.

Despite that significant drop in response rates, those that had responded to the first simulation were still 67% *more likely* to respond to the second scenario than those who did not fail the initial simulation.

The data suggests that once an employee has been identified as susceptible, they are more likely to repeat the behavior in the future.

Employees Learn Fast

In 2014, the average time employees spent on education after responding to a simulation was 2 minutes and 7 seconds.

As Figure 6 indicates, even highly-susceptible employees improve rapidly after 3-4 exposures to training.

> ***PhishMe Tip:*** *With less than 10 total minutes of exposure to immersive phishing training, employees can learn to change their behavior.*

Can Highly-Susceptible Employees Be Trained?

While the data in Figure 5 shows us the reduction of general susceptibility when repeating a specific theme, we also need to investigate a training program's impact at the employee level, specifically for repeat offenders.

An analysis of repeat offender data shows us that employee behaviors, even for those that are highly-susceptible, can be modified over time through repeated exposure to a variety of phishing simulations.

Figure 6 focuses attention on highly-susceptible employees (those that respond to more than 1 phishing simulation) and shows us that with repeated exposure, repeat offenders will begin to recognize phishing emails.

More importantly, these results demonstrate that organizations that continually train their employees reduce the risk of exposure to phishing attacks even as the tactics and themes of attackers in the real-world change.

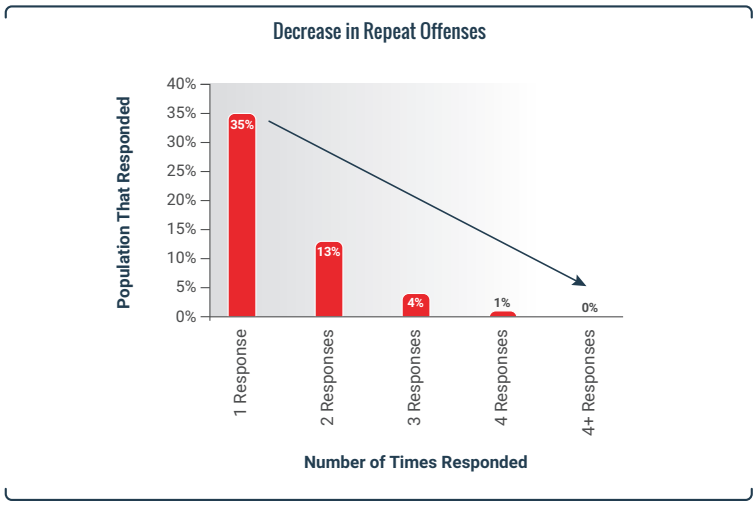


Figure 6: Decrease in repeat offenses.

Figure 6 also shows us that 35% of the population that received phishing simulations failed one time; 13% responded twice, with a drop to 4% and 1% for those responding 3 or 4 times to a simulation. The more times a population is exposed to a simulation, the fewer times they continue to click.

Another client sample shows us that when digging deeper into repeat responses based on number of simulation interactions, we can see that while the raw number of repeat offenders continues to drop over time, new responders and areas of susceptibility across the population become evident the more we phish.

Employees Can Learn to Detect Threats

Data in Figure 7 presents an overall view of the organizational response to a widespread phishing attack.

Analysis of this client's simulation shows that a well-educated workforce can exhibit greater resilience by reporting a scenario in larger numbers than those that fell susceptible.

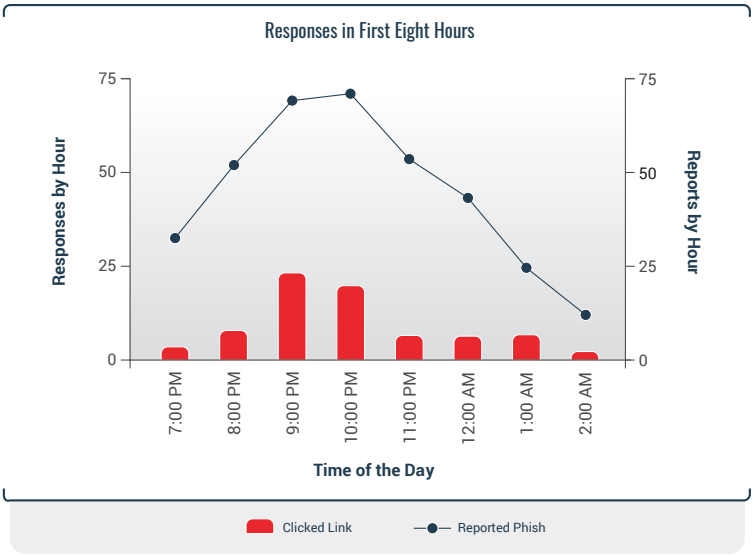


Figure 7: Reporting responses in the first 8 hours.

Analysis of the data from a different perspective, Figure 8 indicates that this client's employee base was capable of reporting a malicious attack a full 11 minutes prior to anyone downloading the associated attachment.

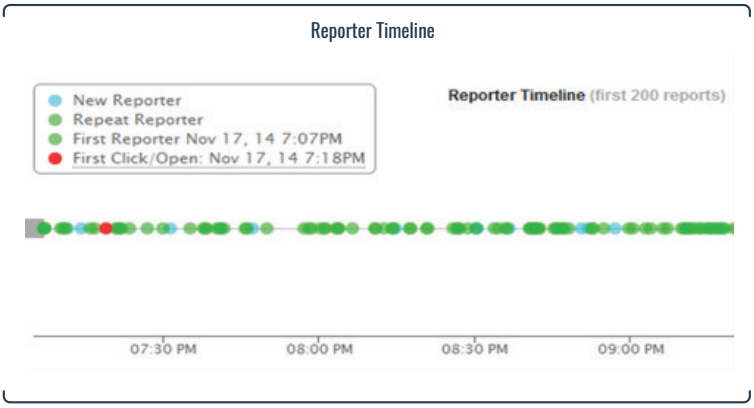


Figure 8: The Reporter timeline.

Habit Formation

According to James Clear, all habits form by the same three-step process:

1. **Reminder** – The cue that triggers a response.
2. **Routine** – The action you take or the habit itself.
3. **Reward** – The benefit gained from the habit.

In phishing training, the cue becomes recognition of a phishing attempt.

The routine becomes reporting a phish.

The benefit* gained by the organization is increased security.

* Rewarding employees for taking positive action reinforces this change in habit.

The Bottom Line

With repetition, a sustained and well-executed phishing simulation program provides a significant reduction in overall exposure to risk from this *ever-changing* attack vector and improves the security posture of an organization.

- 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.
- It is important to train employees to report phishing attempts as soon as they are recognized in order to offset the likelihood that a phishing attempt will be responded to in its first several hours in a network environment.
- By phishing across an entire employee base, an organization is able to quickly increase awareness, train more people, and identify key triggers that influence employee behavior.

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 not surprising 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

Course of activities designed to improve email employee knowledge, recognition, and response to spear phishing attacks.

Phishing Scenario

PhishMe's term for a simulation.

Phishing Template

Email content provided by PhishMe for use in scenarios.

Phishing Theme

PhishMe's term for a collection of email scenario templates that use the same context, motivation, or topic to elicit user action.

Repeat Offender

A person that has shown repeated susceptibility to spear phishing scenarios.

[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

About PhishMe

PhishMe® is the leading provider of human-focused phishing defense solutions for organizations concerned about their susceptibility to today's top attack vector—spear phishing. PhishMe's intelligence-driven platform turns employees into an active line of defense by enabling them to identify, report, and mitigate spear phishing, malware, and drive-by threats. Our open approach ensures that PhishMe integrates easily into the security technology stack, demonstrating measurable results to help inform an organization's security decision making process. PhishMe's customers include the defense industrial base, energy, financial services, healthcare, and manufacturing industries, as well as other Global 1000 entities that understand changing user security behavior will improve security, aid incident response, and reduce the risk of compromise.

Headquarters

PhishMe, Inc.
1608 Village Market Blvd.
Suite #200
Leesburg, VA 20175

New York Office

PhishMe, Inc.
817 Broadway, 4th floor
New York, NY 10003

San Francisco Office

PhishMe, Inc.
One Embarcadero Center
Suite# 510
San Francisco, CA 94111

London Office

PhishMe, Inc.
c/o Regus
London – Covent Garden
90 Long Acre
London, WC2E 9RZ

Dubai Office

PhishMe, Inc. (DMCC Branch)
Unit No: 30-01-449
Jewellery & Gemplex 3
Plot No: DMCC-PH2-J&GPlexS
Jewellery & Gemplex
Dubai
United Arab Emirates

Singapore Office

PhishMe, Inc. (Singapore Branch)
c/o Regus
1 Raffle Place
Level 24 Tower 1
Singapore, 048616. Singapore

www.PhishMe.com