ENTERPRISE PHISHING RESILIENCY and DEFENSE REPORT

2017

ANALYSIS OF SUSCEPTIBILITY, RESILIENCY AND DEFENSE AGAINST SIMULATED AND REAL PHISHING ATTACKS.

PHISHME®

Human Phishing Defense

EXECUTIVE SUMMARY

Phishing in 2017 — Alive and Well

For hackers, phishing is easy. And profitable. The average phishing attack costs a mid-sized company $1.6 million.[1] No wonder the number of phishing attacks shot up 65% worldwide last year.[2]

For many years, organizations have invested in technology to keep them safe from malicious emails. Yet ransomware, CEO fraud/business email compromise (BEC) and breaches stemming from phishing emails inflict a heavy toll. According to the FBI, BEC alone cost businesses worldwide over $5 billion from 2013 to 2016.[3]

Here's the disconnect: phishing skirts technology by targeting human beings. That's why it's critical to educate employees to recognize and report all manner of phishing attacks.

In empowering their workforce, more than 1,400 organizations, including over half the Fortune 100, use PhishMe to simulate phishing and boost resiliency to attacks. They also use insights drawn from PhishMe's analysis and response platform and our intelligence feed to make sure their simulations reflect the latest attack methods. This kind of anticipatory action helps to disrupt phishing as soon as it occurs.

About This Report

With more than a decade of human-focused anti-phishing data, PhishMe has a keen perspective on what makes phishing successful. We offer deep insights on who clicks, why they click, what emails work best for attackers and how to engage employees as part of the solution.

This is our third annual report on controlled phishing activity. Our first report, the 2015 Enterprise Susceptibility Report, focused on just that—what makes people most susceptible to phishing emails. With more data to support engagement, the 2016 Enterprise Susceptibility and Resiliency Report focused on how reporting impacted susceptibility. Now the 2017 Enterprise Phishing Susceptibility and Defense Report adds another dimension—data on how resiliency and reporting help organizations quickly respond to and mitigate attacks in progress, moving from chronic defense to proactive offense.

For this report, we've aggregated data across phishing simulation, phishing reporting and, in a few cases as noted, phishing response solutions. The data reflects the experiences of some 1,400 PhishMe customers across the globe, including Fortune 500 and public-sector organizations across 23 industries.

In some instances, the data goes back to 2014 or 2015 to show longer-term trends or may focus on a specific time frame. In other cases, the data is from the past eight months, January through August 2017. The foundation of this data is 52.4 million simulation emails. As in the past, the emails were written in numerous languages, 15 to date.

THE DATA

- Reflects the experiences of 1,400 clients in 23 industries and more than 50 countries
- 52.4 million phishing simulations
- 7.5 million emails reported in 2017 alone
- 3,000 campaigns analyzed
- Simulation data is from January 2015 – July 2017
- Triage (real-attacks) data is from January 2017 – August 2017

KEY FINDINGS

Among the key take-aways from the research:

- In simulations, overall susceptibility dropped to as low as 5% (individual companies may have experienced greater changes).
- As reporting or engagement increased, susceptibility decreased.
- Employees are most susceptible to phishing emails that target them as consumers.
- Emails with malicious URLs are the most reported.
- Almost 15% of the emails employees reported in this study were found to be malicious.

How Do We Get This Data?

For those unfamiliar with PhishMe, we offer a suite of solutions from which we gather data:

PhishMe Simulator™ educates and conditions employees to recognize phishing emails by delivering a safe, simulated phish to their inbox with context and education if the phish is successful. By conditioning employees on what real phishing looks like, they become more cautious and critical in their email habits.

PhishMe Reporter® is an easy plug-in to email clients which allows users to immediately alert IT and security teams about suspicious emails. If the reported email was, in fact, a simulation the employee receives immediate positive feedback and is encouraged to stay vigilant.

PhishMe Triage™ ingests all reported suspicious emails for the security team and enables it to quickly process and analyze potential threats—providing visibility and response to an attack in progress within minutes of the first report.

PhishMe Intelligence™ provides human-vetted, phishing-specific threat intelligence analysis. PhishMe Intelligence integrates with various security solutions and is a valuable source of content on the latest threats for PhishMe customers.

GLOSSARY

Key Terms to Know:

Active Threat
A term for simulations using a recent phishing tactic or malware type that is new, frequent or dangerous.

Attachment-based Phish
Emails with seemingly legitimate attachments, in diverse formats, but which when opened unleash malware to steal data or paralyze systems.

CEO Fraud or Business Email Compromise (BEC)
BEC is among the most effective scams. The email appears to have come from an internal authority—say, someone requesting W2 data or a transfer of funds—but typically has no links or attachments for technology to analyze and trigger an alarm. A must-have model for your simulation program.

Phishing Simulation
A safe, controlled phishing email sent with the intent of educating the user on how to identify a real phishing email.

Ransomware
This malware type prevents or limits users from accessing their system, then demands a ransom, often in Bitcoin, in return for "freeing" business operations. It's the most popular form of malware today.

Reporting
The second simulation metric. How often are employees reporting fake phishes to incident responders?

Resiliency
Number of reported / Number of susceptible. Lower susceptibility + higher reporting = better resiliency.

Susceptibility
The first metric measured in simulations. How susceptible are employees to different mock phishes?

A FEW WORDS ABOUT SUSCEPTIBILITY

Many organizations focus on measuring and lowering susceptibility to phishing attacks. It's an unfortunate reality that there will always be a day when someone will be caught off guard – in a rush or a moment of weakness – and fall for a phish. It can happen to the best of us. Individually, we may fail. But together we can form a collective defense – reporting critical threat information to IT Security in time to stop attacks in progress.

Good News: Susceptibility Rates are Steadily Declining

The tendency to fall for a phishing email, or susceptibility, is best addressed with conditioning employees to recognize and understand phishing emails. Repeated phishing simulations—including those based on relevant, emerging threats—have shown a shrinking susceptibility rate for three years running. It's proof that a progressive, mature anti-phishing program keeps organizations safer.

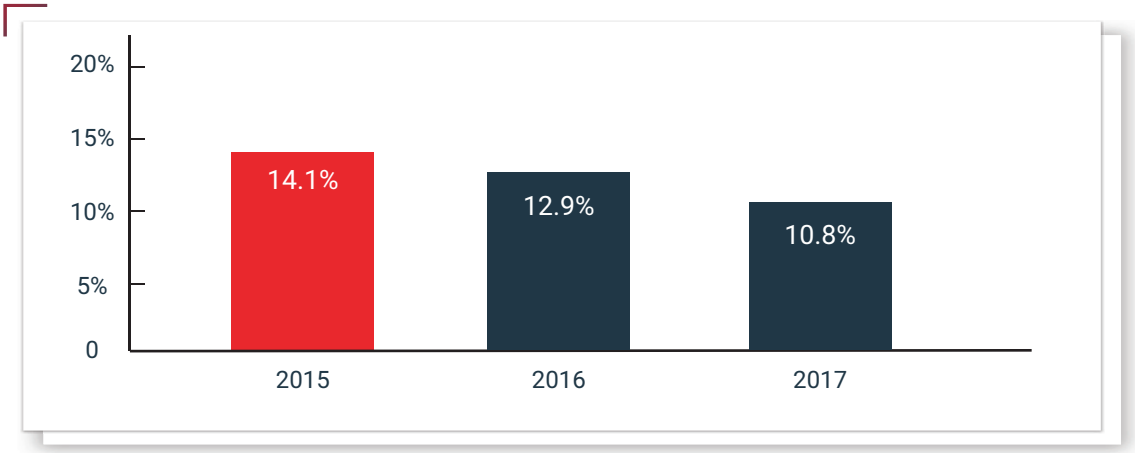


Figure 1: Aggregated Organizational Susceptibility Rates.

What Makes a Program Mature?

A mature conditioning program will provide ongoing, immersive training that is targeted, specific and increasingly difficult. Simulations should progress over time to challenge employees and keep them aware of emerging threats.

Example: one PhishMe client had reduced organizational susceptibility across 4,500 employees in multiple countries to just above 5%. The client concluded that employees could recognize phishing emails, but it was time to raise the bar. It adopted a phishing simulation program targeted by department, which brought some departments to over 40% susceptibility. Success! No pain, no gain. This client continued to evolve its program, increase the difficulty and keep up with today's complex phishing attacks.[4]

WHAT "GETS" US?

Employees are (*successfully*) being targeted as consumers

As Internet behavior changes, so do cyberattacks. In previous years, PhishMe reported that fear, urgency and curiosity were the top emotional motivators behind successful phishes. Now they're closer to the bottom, replaced by entertainment, social media and reward/recognition.

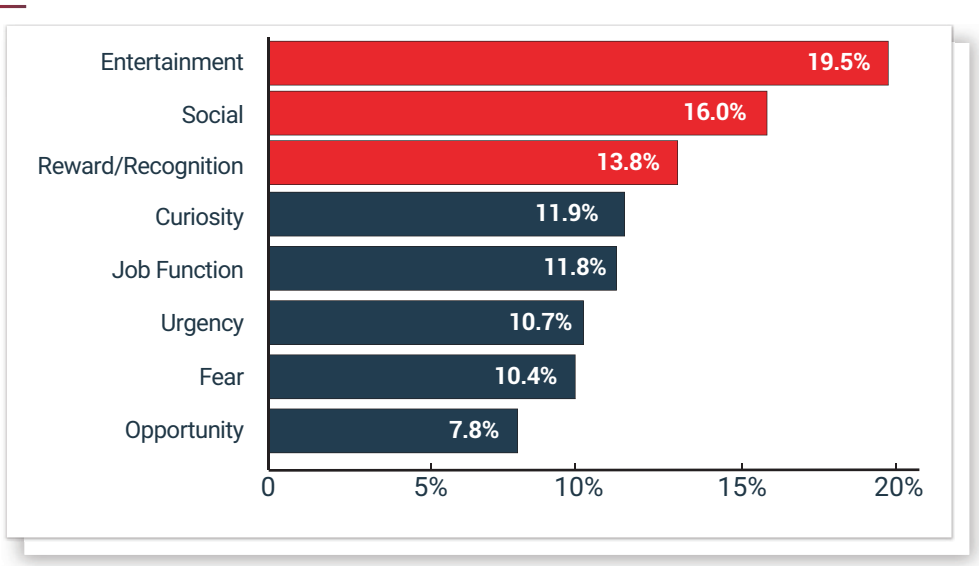


Figure 2: Response Average by Motivator.

It's possible that mature anti-phishing programs have conditioned employees to spot work-related scams: "Delivery Issue" or "Parking Ticket"(fear), "Urgent Order" or "Canceled Transaction" (urgency) and "Final Version of the Report" or "Refund for Purchase"(curiosity). But most programs don't focus on consumer scams, which are cropping up more in the workplace, targeting employees with personal vs. business messages.

Employees will always take a break to do personal business online, so you can expect work and home email to continue blurring. Personal devices in the workplace often have multiple email accounts—the source of an email may not be distinguished as it should. However, to sustain morale, communication and collaboration, among other reasons, companies are unlikely to restrict BYOD or access to social media, news and entertainment sites.

At a high level, the issue is how consumers/employees get their news and interact. Many news and social feeds are now subscription based; they're common in email and mobile device alerts. This explains the rise in phishing attacks via social media links and fake news sites. Because they're accustomed to them, people think it's safe to click.

When creating simulations, remember consumer scams—those phony Netflix or LinkedIn emails sent to busy employees, who are glad to switch gears and click on something fun. Through repetition, train employees to be less gullible. The best way to combat a knee-jerk response: teach your people to be aware of their emotional reactions to emails and see them as phishing triggers. You can be sure attackers are paying attention.

Holidays and office fun… *gee, what could wrong?*

We thought it would be useful to see which simulations match the top emotional motivators. You'll notice that simulated e-card phishes appear across the top three: social, entertainment and reward/recognition. They're an old ruse but a goodie. Internal promotions (raffles, ticket giveaways, free lunches, etc.) performed strongly, too.

Several financial and compliance scenarios also had strong "take" rates. These suggest that fear is still a compelling motivator. Who wants to get the blame for losing money?

A Few More Tips

- Understand the dynamics of entertainment or social phishing (think uncritical social acceptance and shortened URLs).
- Stress vigilance when it comes to emails promising rewards. If its sounds too good to be true…well, you know the rest.
- Take note of internal reward programs in danger of being mimicked. If you know how legitimate emails look and read and who they ought to come from, you stand a better chance of catching counterfeits.

Top Phishing Scenarios per Emotional Motivator

Entertainment

Scenario Name	Rate
Holiday eCard Alerts	24.8%
St. Patrick's Day eCard Alert	19.7%
Lunar New Year	17.8%
Halloween Costume Guidelines	16.7%
Cricket Big Bash Ticket Giveaway	14.6%
Office Gambling: College Basketball	14.2%
Flash Update Required	13.4%
Cricket International Series Tickets	13.4%
Streaming Football Match	11.6%
Funny Pictures	9.7%

Job Function

Scenario Name	Rate
Customs Charges	20.9%
Financial Information Review (Attachment)	20.9%
New Fax	19.2%
Please Sign Online	18.7%
Expense Denied	17.9%
Financial Information Review (Click Only)	17.6%
Compliance Training (Click Only)	17.2%
Gmail Attachment Scam	15.7%
Compliance Training (Data Entry)	12.6%
Mailinator Scam	12.4%

Reward/Recognition

Scenario Name	Rate
Holiday eCard Alerts	24.8%
New Rewards Program	23.6%
eCard Alerts	22.2%
Employee Satisfaction Survey	17.2%
Life Insurance Policy Documents	16.0%
Free Coffee	15.8%
Employee Raffle	15.5%
Cricket Big Bash Ticket Giveaway	14.6%
Valentines Day eCard	14.4%
Free Lunch	14.3%

Social

Scenario Name	Rate
Holiday eCard Alerts	24.8%
eCard Alerts	22.2%
St. Patrick's Day eCard Alert	19.7%
Thanksgiving Recipe	14.5%
Valentines Day eCard	14.4%
Funny Pictures	9.7%
Brexit Forwarded Email	7.3%
Shared Folder	6.8%
New Chat App	6.2%
Forward From Manager	6.2%

Top Phishing Scenarios per Emotional Motivator (continued)

Opportunity

Scenario Name	Rate
New Rewards Program	23.6%
Employee Satisfaction Survey	17.2%
Employee Raffle	15.5%
Email Migration (Data Entry)	11.8%
Corporate Rewards	9.2%
Google Docs	7.8%
Summer Flex Hours	7.3%
Email Migration (Click Only)	6.7%
Tax Refund	6.5%
Thanksgiving Deals and Coupons	6.5%

Fear

Scenario Name	Rate
State Bar Assoc.: Grievance Filed	44.0%
Board of Accountancy: Complaint Filed	34.2%
Ebola Outbreak	27.9%
Mold Found in Office!	24.1%
Notice to Appear	24.0%
Money Transfer Reversed	21.7%
HSA Customer Service Email	18.6%
Browser Update Required	18.0%
Expense Denied	17.9%
Bed Bugs Bulletin	17.6%

Urgency

Scenario Name	Rate
State Bar Assoc.: Grievance Filed	44.0%
Open Enrollment	39.2%
Board of Accountancy: Complaint Filed	34.2%
Ebola Outbreak	27.9%
Mold Found in Office!	24.1%
Notice to Appear	24.0%
New Rewards Program	23.6%
Customs Charges	20.9%
Order Tracking Information	19.7%
Please Sign Online	18.7%

Curiosity

Scenario Name	Rate
State Bar Assoc.: Grievance Filed	44.0%
Board of Accountancy: Complaint Filed	34.2%
Ebola Outbreak	27.9%
Holiday eCard Alerts	24.8%
Proforma Invoice	24.5%
Locky Phish	24.2%
Mold Found in Office!	24.1%
Notice to Appear	24.0%
Updated Organizational Chart	23.9%
New Rewards Program	23.6%

"Funny Pix" and "Bed Bugs." Email Content Matters.

Besides emotional motivators, certain types of content make for irresistible phishes. Thus, we also sorted simulations by content theme.

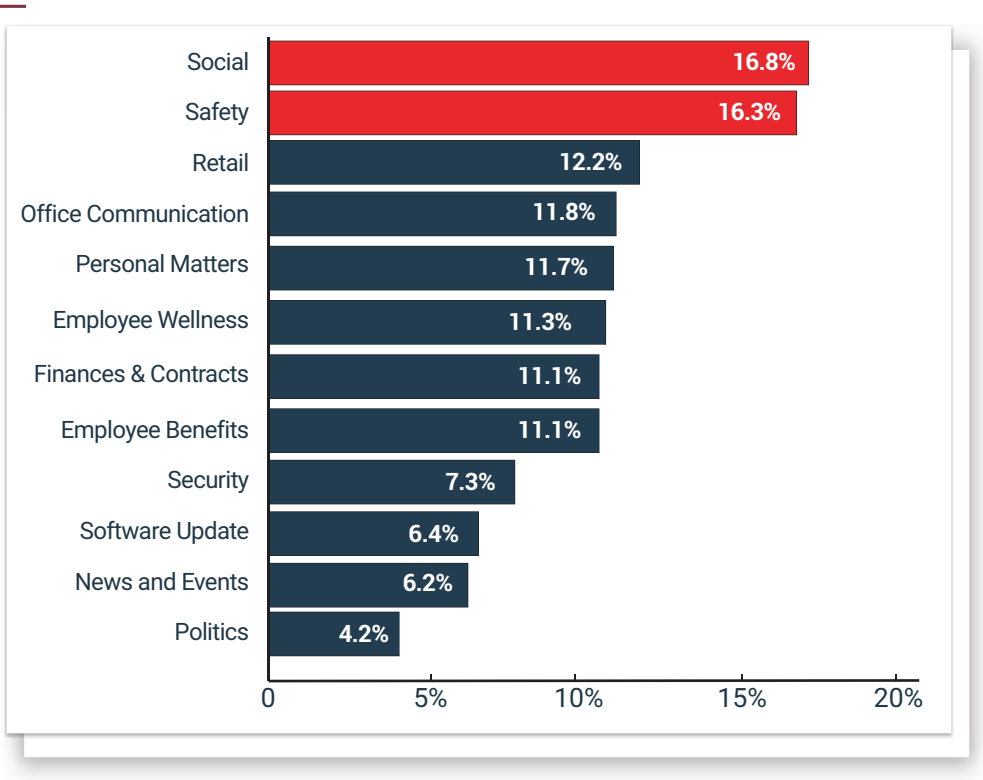


Figure 3: Response Average by Theme.

Social and personal safety content rose to the top, followed by retail promotions. The charts below echo that business and personal life are merging. For example: "Bed Bugs Found in Office."

Retail

Scenario Name	Rate
Courier Service	18.5%
Lunar New Year	17.8%
Order Confirmation	15.4%
Package Delivery	14.8%
Holiday Order Confirmation	13.8%
Restaurant Gift Certificate	7.8%
Thanksgiving Deals and Coupons	7.3%
Holiday Coupons (Click Only)	6.7%
Mothers Day Flowers	6.5%
Holiday Coupons (Attachment)	6.5%

Safety

Scenario Name	Rate
Mold Found in Office!	24.1%
Bed Bugs Bulletin	17.6%
Workplace Safety Training	16.8%
Cleaning Chemical Concerns	7.5%
Background Check	6.3%
Mold Found in Office! (Click Only)	3.1%
Health Alert? Bed Bugs	2.5%
Local Crime Bulletin	1.4%
Bed Bugs Found in Office!	1.1%

Security

Scenario Name	Rate
Please Sign Online	23.6%
Internet Privileges Suspended	17.2%
Security Report	15.5%
Password Survey (Click Only)	11.8%
Data Breach (Attachment)	9.2%
PhishMe's CNBC Phish	7.8%
Password Survey (Data Entry)	7.3%
Data Breach (Click Only)	6.7%
Security Token Compropmised (Data Entry)	6.5%
Security Token Compropmised (Click Only)	6.5%

Computer/Software Update

Scenario Name	Rate
Browser Update Required	18.0%
Email Accounts to be Deleted	17.3%
Flash Update Required	13.4%
Email Migration (Data Entry)	11.8%
Computer Refresh Program	11.7%
Email Accounts to be Deleted (Data Entry)	7.4%
Email Migration (Click Only)	6.7%
Please Update Drivers	6.5%
Free OS Upgrade	6.3%
Required Mobile App	5.5%

Finances and Contracts

Scenario Name	Rate
Pro-forma Invoice - Indonesian	24.5%
Locky Phish	24.2%
Money Transfer Reversed	21.7%
Financial Information Review (Attachment)	20.9%
Macro-Enabled Scanned Image	19.6%
Pro-forma Invoice	18.5%
Financial Information Review (Click Only)	17.6%
Bonus Agreement	16.4%
Attached Life Insurance Policy Documents	16.0%
Macro-Enabled Attached Invoice	15.1%

Social

Scenario Name	Rate
Holiday eCard Alerts	24.8%
eCard Alerts	22.2%
St. Patrick's Day eCard Alert	19.7%
Thanksgiving Recipe	14.5%
Valentine's Day eCard	14.4%
Funny Pictures	9.7%
Brexit Forwarded Email	7.3%
Shared Folder	6.8%
New Chat App	6.2%
Forward From Manager	6.2%

Employee Benefit

Scenario Name	Rate
Open Enrollment	39.2%
New Rewards Program	23.6%
HSA Customer Service Email	18.6%
Employee Satisfaction Survey	17.2%
Free Coffee	15.8%
Employee Raffel	15.5%
Cricket Big Basg Ticket Giveaway	14.6%
Free Lunch	14.3%
Cricket International Series Tickets	12.8%
Macro-Enabled Paid Time Off Request	11.9%

Employee Wellness

Scenario Name	Rate
Open Enrollment	39.2%
Mold Found in Office!	24.1%
Summer Flex Hours	7.3%
Employee Wellness	3.8%
Mold Found in Office! (Click Only)	3.1%

Personal Matters

Scenario Name	Rate
Internet Privileges Being Suspended	13.0%
Mobile Game Receipt	4.0%

News and Events

Scenario Name	Rate
Ebola Outbreak	27.9%
Lunar New Year	17.8%
Halloween Costume Guidelines	16.7%
Cricket International Series Tickets	12.8%
News Alert	12.3%
Streaming Football Match	11.6%
Presidential Inauguration Live Streaming	8.9%
Brexit Impact on Operations	8.9%
Women's Euro 2017 Tickets	8.3%
Breaking News	7.9%

Politics

Scenario Name	Rate
Rising Tensions in Korea	5.5%
Tension in the Crimean Peninsula	5.2%
Polling Center	3.8%
Election Polling (Click Only)	1.3%
Election Polling (Attachment)	0.5%

Office Communications

Scenario Name	Rate
Mold Found in Office!	24.1%
Updated Organizational Chart	23.9%
New Rewards Program	23.6%
New Fax	19.8%
Browser Update Required	18.0%
File From Scanner	17.2%
Employee Satisfaction Survey	17.2%
Workplace Safety Training	16.8%
Halloween Costume Guidelines	16.7%
Signature Needed	16.5%

BREAKING DOWN SUSCEPTIBILITY

Organizations in Key Industries Should Simulate these Active Threats.

What's happening in your industry is important to your organization. This PhishMe Simulator data on threats in different verticals can help you decide which phishing tactics to add to simulations. Each of these threats is active and considered high-risk.

Government

SIMULATION	SUSCEPTIBILITY RATE
Canceled ACH Transaction - Mimics a real-world Sage Ransomware attack	66.7%
Delivery Issue - Mimics a real-world Locky and Kovter attack	50.0%
Urgent Order - Mimics a real-world Pony attack	31.6%
Parking Ticket	28.5%
Wire Fraud	27.0%

Healthcare

SIMULATION	SUSCEPTIBILITY RATE
Payment Notification - Mimics a real-world TrickBot attack	36.6%
Canceled ACH Transaction - Mimics a real-world Sage Ransomware attack	33.9%
Budget Report - Mimics a real-worldLocky attack	27.2%
Parking Ticket	25.4%
Refund for Purchase	22.2%

Insurance

SIMULATION	SUSCEPTIBILITY RATE
Health Insurance Contract	52.8%
Canceled Order - Mimics a real-world Sage Ransomware attack	50.0%
Urgent Statement - Mimics a real-world Viotto Keylogger attack	25.0%
Payment Notification - Mimics a real-world TrickBot attack	22.0%
New Fax - Mimics a real-world TrickBot	21.3%

Financial

SIMULATION	SUSCEPTIBILITY RATE
New Fax - Mimics a real-world TrickBot attack	36.2%
Customs Charges - Mimics a real-world Ursnif attack	30.6%
Online Order	28.9%
Delivery Issue - Mimics a real-world Locky attack	28.3%
Order Tracking Information	27.4%

Legal Services

SIMULATION	SUSCEPTIBILITY RATE
Parking Enforcement Notification	73.7%
Tax Evasion - Mimics a real-world Zeus Panda attack	42.9%
Canceled Order - Mimics a real-world Sage Ransomware attack	41.8%
New Fax - Mimics a real-world TrickBot attack	29.2%
Locky Phish	25.0%

Education

SIMULATION	SUSCEPTIBILITY RATE
Delivery Issue - Mimics a real-world Locky attack	62.5%
Canceled Order - Mimics a real-world Sage Ransomware attack	50.0%
Delivery Issue - Mimics a real-world Locky and Kovter attack	50.0%
Macro-Enabled Scanned Image	41.2%
Parking Ticket	40.4%

Energy

SIMULATION	SUSCEPTIBILITY RATE
Request for Quotation	75.0%
Customs Charges - Mimics a real-world Ursnif attack	37.0%
Parking Ticket	33.3%
HSA Customer Service Email	31.3%
Attached Invoice	30.2%

Manufacturing

SIMULATION	SUSCEPTIBILITY RATE
Parking Ticket	61.5%
Final Version of the Report - Mimics a real-world Locky attack	37.9%
Gmail Attachment Scam	28.5%
New Fax - Mimics a real-world TrickBot attack	21.9%
Booking Status Change	21.7%

Besides addressing active threats, simulations should condition users to spot these vintage attacks.

When a phishing type disappears for awhile, be afraid. Be very afraid. It will likely come back and you need to be ready.

So be proactive. Baseline your risks before attackers do (for more on this, read this blog post) and then run simulations using the phishing tactics below.

To repeat: condition users to be aware of their emotional responses to emails. Note the emotional motivators that make employees susceptible to these top-ranking phishes.

Government

SIMULATION	SUSCEPTIBILITY RATE
Open Enrollment	75.0%
Canceled ACH Transaction - Mimics a real-world Sage Ransomware attack	66.7%
Please Update Drivers	60.0%
Ebola Outbreak	55.4%
At the Airport	50.0%

Healthcare

SIMULATION	SUSCEPTIBILITY RATE
Brand Registration Confirmation	66.7%
Suspicious Activity	50.0%
Airline Mileage	50.0%
Payment Notification - Mimics a real-world TrickBot attack	36.6%
Canceled ACH Transaction - Mimics a real-world Sage Ransomware attack	33.9%

Insurance

SIMULATION	SUSCEPTIBILITY RATE
Health Insurance Contract	52.8%
Canceled Order - Mimics a real-world Sage Ransomware attack	50.0%
Password Survey	49.8%
Email Migration	40.5%
Voice Message Attached - Mimics a real-world TrickBot, WSC Downloader	40.1%

Financial

SIMULATION	SUSCEPTIBILITY RATE
Guest Speaker	75.0%
Flash Update Required	66.7%
Operation Ghoul	66.7%
Open Enrollment	46.8%
Package Delivery	46.0%

Legal Services

SIMULATION	SUSCEPTIBILITY RATE
Parking Enforcement Notification	73.7%
Data Breach	71.4%
Office Gambling: Football Playoffs	47.6%
Internet Privileges Being Suspended	45.9%
Notice from State Bar Association: Grievance Filed	44.6%

Energy

SIMULATION	SUSCEPTIBILITY RATE
Request for Quotation	75.0%
Notice from the Board of Accountancy: Complaint Filed	50.0%
Build Your Own	50.0%
Google Docs	50.0%
Customs Charges - Mimics a real-world Ursnif	37.0%

Education

SIMULATION	SUSCEPTIBILITY RATE
Verify Transaction	75.0%
Delivery Issue - Mimics a real-world Locky	62.5%
Free Lunch	52.6%
Canceled Order - Mimics a real-world Sage Ransomware	50.0%
Delivery Issue - Mimics a real-world Locky and Kovter	50.0%

Manufacturing

SIMULATION	SUSCEPTIBILITY RATE
Parking Ticket	61.5%
Security Breach	49.5%
Email Migration	47.1%
Inbox Over the Limit	45.5%
Urgent Order	42.9%

HEY! Are you trying to trick me?

We've seen reports and social comments accusing employers (and PhishMe) of trying to trick them with simulated emails. We get it. When employees see only tricky emails coming in, they feel "tested." But the best way to turn the dial from simple awareness to real defense is by empowering them in the fight against phishing. A reporting process/tool and feedback on their efforts can turn employee opinion from "tricky IT program" to "protecting my company." It's essential to creating a network of human phishing sensors.

Reporting Rates Have Climbed a Healthy 6% in Three Years

In 2015, PhishMe introduced PhishMe Reporter, an easy way to engage employees and measure progress. Since then, we've seen a steady increase in reporting across all active customers. Being able to recognize a phishing attempt is only half the battle—instilling a culture of "see something, say something" helps to lower overall organizational susceptibility.

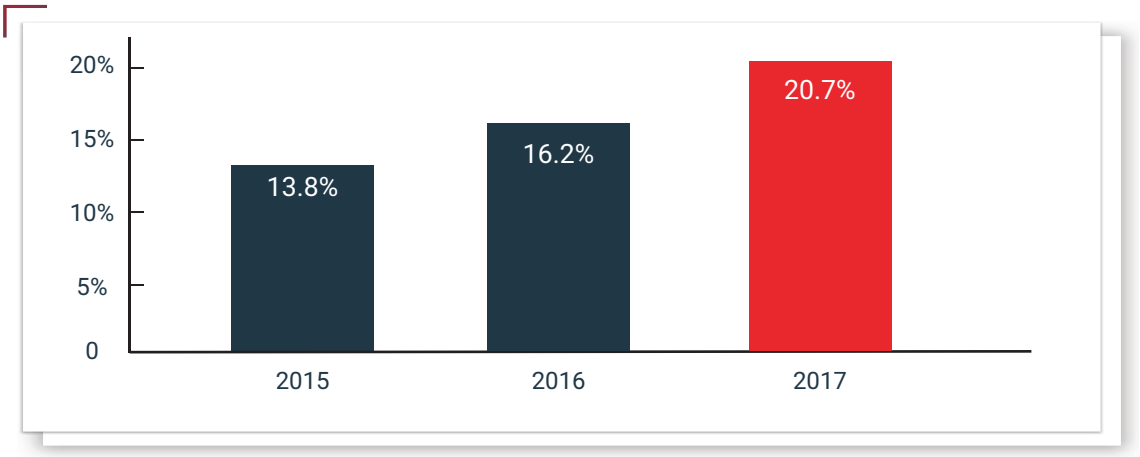


Figure 4: Increased Reporting Rates

In fact, easier reporting lowers susceptibility rates.

Over a three-year period, users of PhishMe Reporter, which offers one-click email reporting, were markedly less susceptible than users lacking it. There's a clear correlation between using a reporting button added to email toolbars and lowering phishing susceptibility. When employees have a way to act against threats, not simply recognize and avoid them, they're more involved and more likely to maintain a state of vigilance.

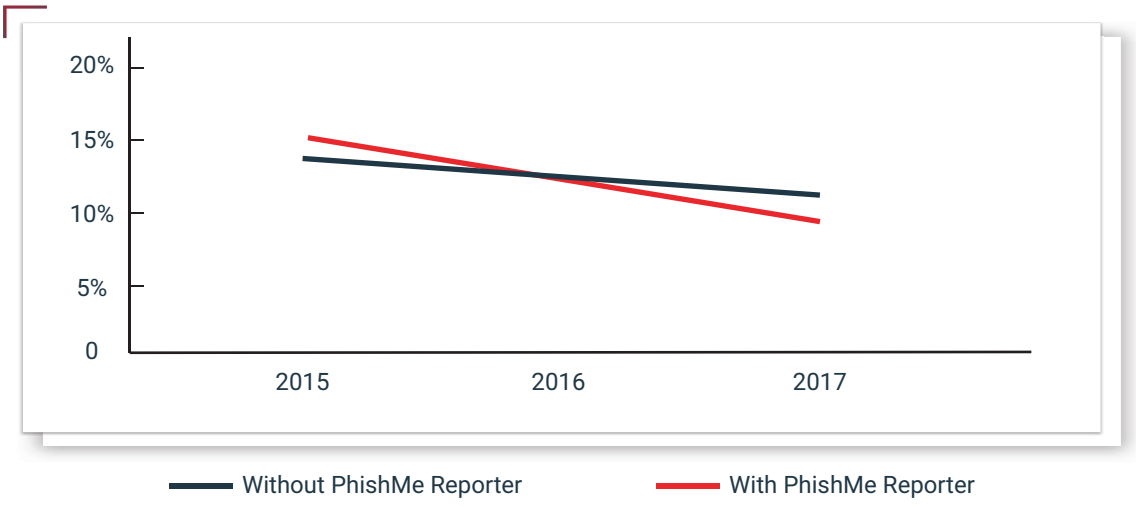


Figure 5: Susceptibility Rate Trend

RESILIENCY IS HARDENING

Top indicators of resiliency improved at a steady pace.

Resilient companies develop a toughness. In the case of simulations, it's developing an immunity to phishing attacks, as measured by the combined metrics of susceptibility and reporting. When susceptibility lowers and reporting rises, resiliency improves.

Key take-aways from our data: (1) clients of all sizes and from all industries are improving and (2) resiliency can grow quickly. In fact, over three years we've seen a 2-1 ratio in resiliency rates when comparing users with PhishMe Reporter to those who work without it.

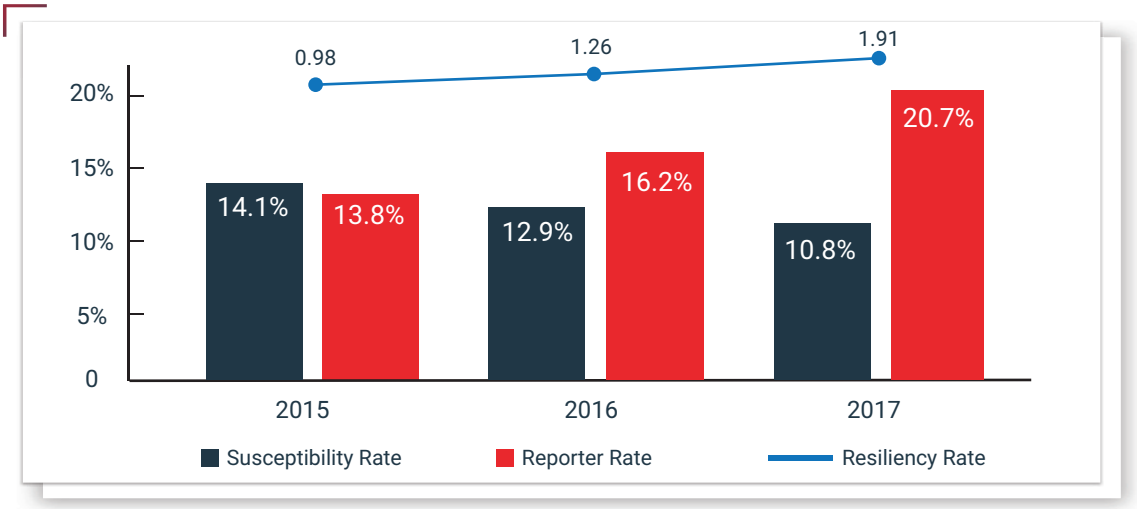


Figure 6: Overall Resiliency Trends

Resiliency has improved against all types of attacks.

Across all types of simulations, susceptibility is down, reporting is up and resiliency is gaining. Regardless of attack type, you can cultivate resiliency.

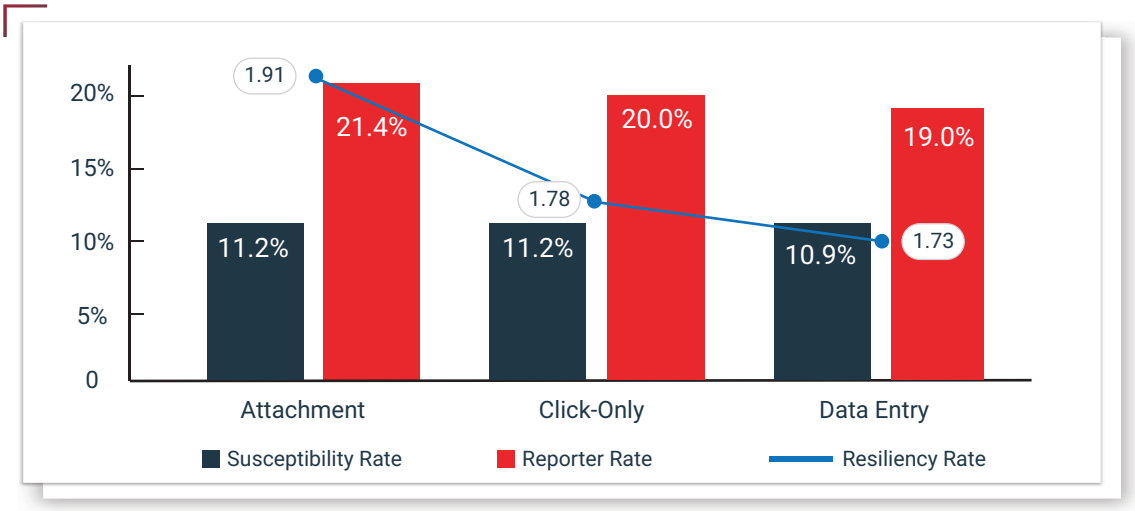


Figure 7: Resiliency by Attack Type

Do trickier simulations hurt resiliency rates? No.

Programs improve resiliency even as they become harder, using targeted attacks, personalization and other attacker tricks. As shown in the chart below, more complex simulations may cause resiliency to dip, but it rebounds over time as repetition sharpens learning.

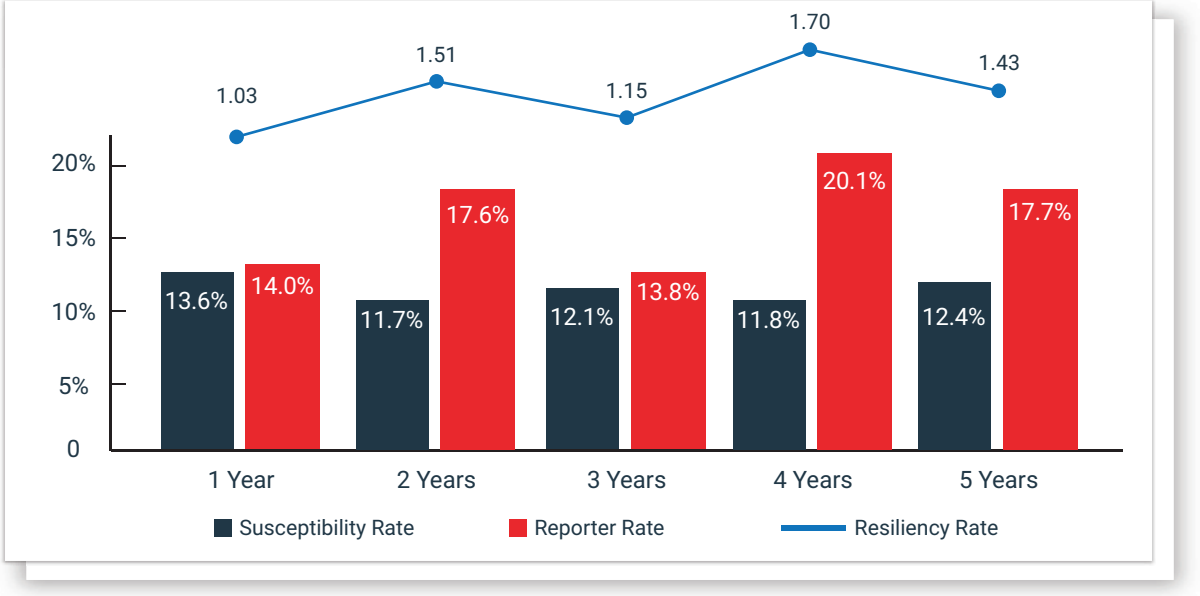


Figure 8: Rates Based on Program Longevity

Practice makes resilience.

Running more frequent simulations, rather than one or two a year, unsurprisingly drives up resiliency. While the capacity of each organization is different, it's important that anti-phishing programs stay as active as possible. This is particularly true when it comes to developing recognition and reporting of active threat models.

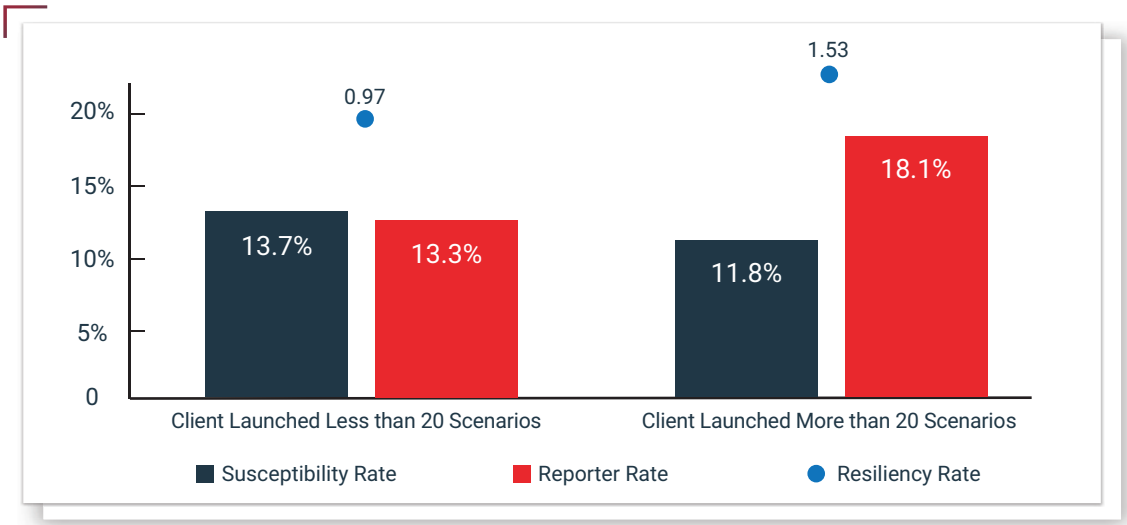


Figure 9: The Effect of Frequent Simulations

In 7 out of 8 industries, resiliency has hardened.

As with susceptibility and reporting, resiliency is improving throughout major industries. Education is the exception. Possible reasons: tighter security budgets compared to other industries, lack of central control and typically open environments that encourage users to "bring your own device."

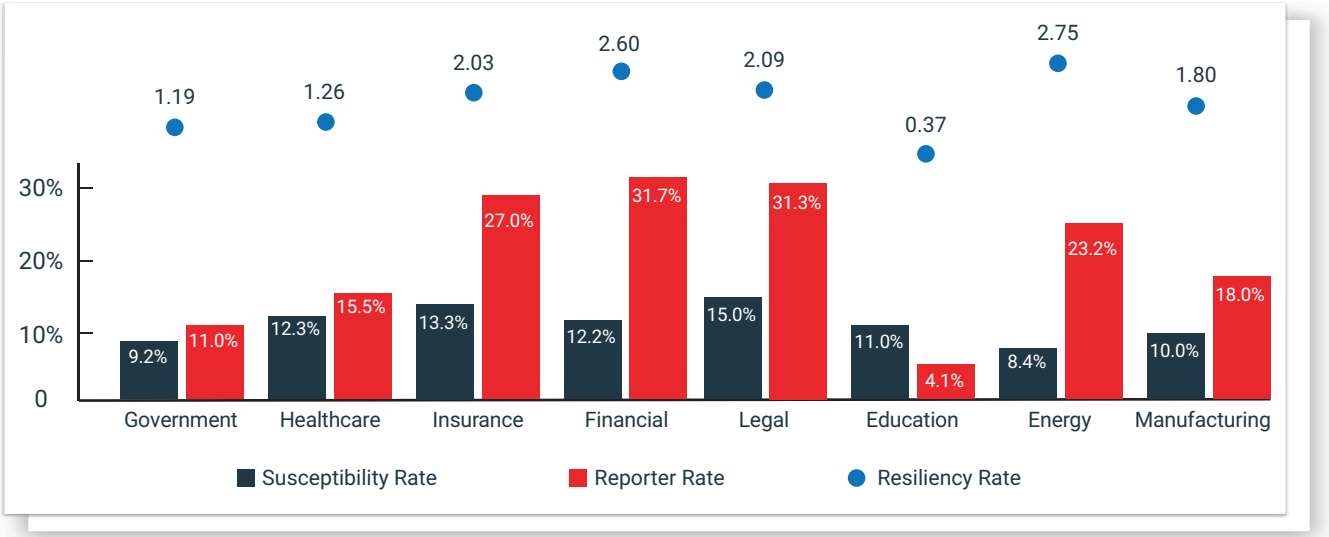


Figure 10: Resiliency Across Industries

WHAT SUCCESS LOOKS LIKE

Users are reporting real threats.

Most of the data in this report is from phishing simulations. But what about real attacks—how do conditioned employees react?

They report real threats, that's how.

Over the first eight months of 2017, our Managed Triage users identified over 216k emails, 15% of which were malicious, containing malware and bad links.

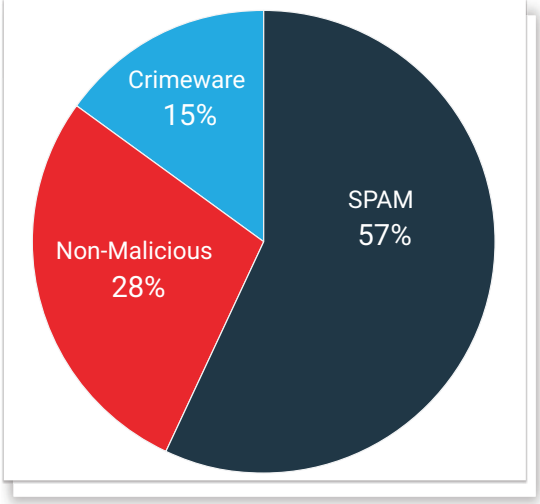


Figure 11: Reported Malicious vs. Non-Malicious

Further, clients of PhishMe Managed Triage are catching the most prevalent types of phishing. Business email compromise (BEC) account for 5% of reported attacks, while 24% contain attachments and potentially Office Macros.

Identified malware includes DELoader, Pony and Loki and other widespread threats. The top threats from compromised internal sources were "fakery" such as account checks or IT Help Desk messages; the top external threat was bogus order payment.

Drawing from phishing intelligence, simulations of new attacks can be quickly crafted and run. The attack methods incident responders see, along with fresh phishing intelligence, should be regularly woven into simulations. This keeps anti-phishing programs relevant and potent.

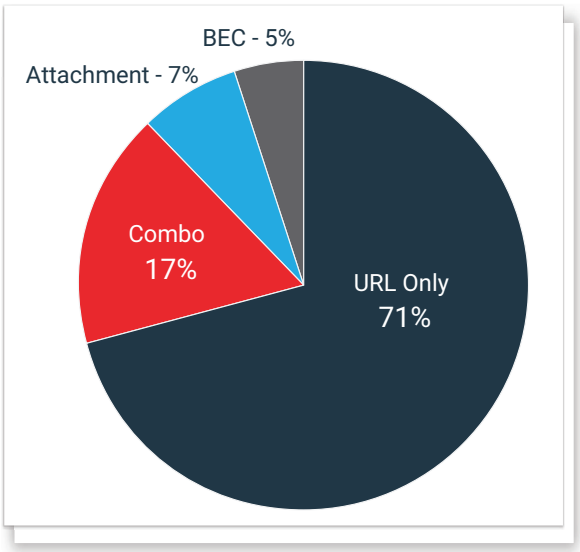


Figure 12: Malicious by Email Content

Each week, the PhishMe Intelligence team sends the Simulator team a report on new threats. Often the same day, the Simulator team recreates the most urgent threats and adds them as simulation templates for PhishMe clients to use.

Below is an example based on a real phish that uses Office Macros to distribute the Smoke Loader Downloader and Monero Minor Bot (and previously the Zyklon HTTP Trojan).

From: Gladys Fernandez <Gladys.Fernandez@lucrativehiring.com>
Subject: Job Application

Good day

I visited your website recently..
I'm currently looking for work either full time or as a intern to get experience in the job field. Please review my CV and let me know what you think.

Thank you for your assistance in this matter,

--
FROM_FRIENDLY_NAME

Figure 13: Office Macro Phishing Example

The threats listed to the right, identified by PhishMe Intelligence over the course of one year, are good candidates for simulations PhishMe clients can customize.

Office Macro is a good example. Resiliency against it has increased.

Office Macro is a malware attackers plant in attachments like Microsoft Word or Excel files. Through dogged simulations, PhishMe clients have become notably more resilient to it.

TOP 10 MALWARE THREATS

Malware Family	Count
• OfficeMacro	564
• Remote Access Trojan	378
• Pony	311
• Credential Phishing	184
• Keylogger	161
• Lock	132
• Kolter	126
• WSF Downloader	95
• Cerner Ransomware	81
• JAR Downloader	76

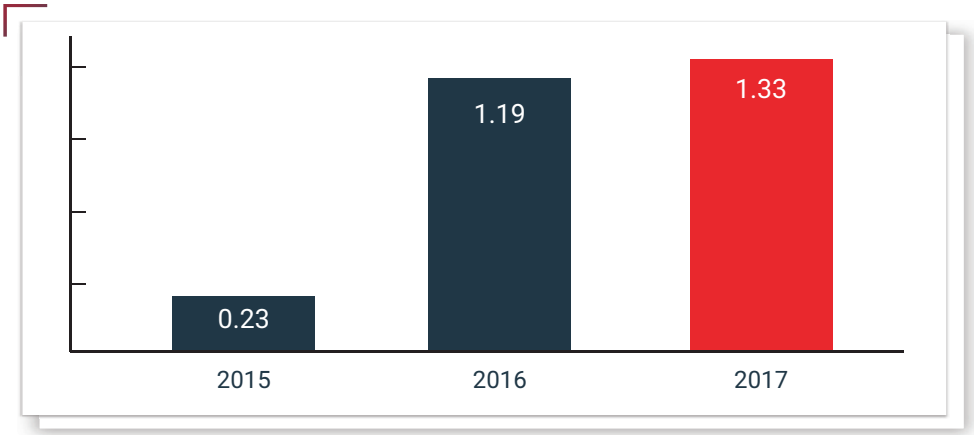


Figure 14: Office Macro Simulation Resiliency

Ditto for resiliency against BEC attacks. BEC is the most frequent phishing threat identified by PhishMe Triage. By adding BEC tactics to the simulations we create for clients, we've helped increase resiliency to BEC 2.3% during the past three years.

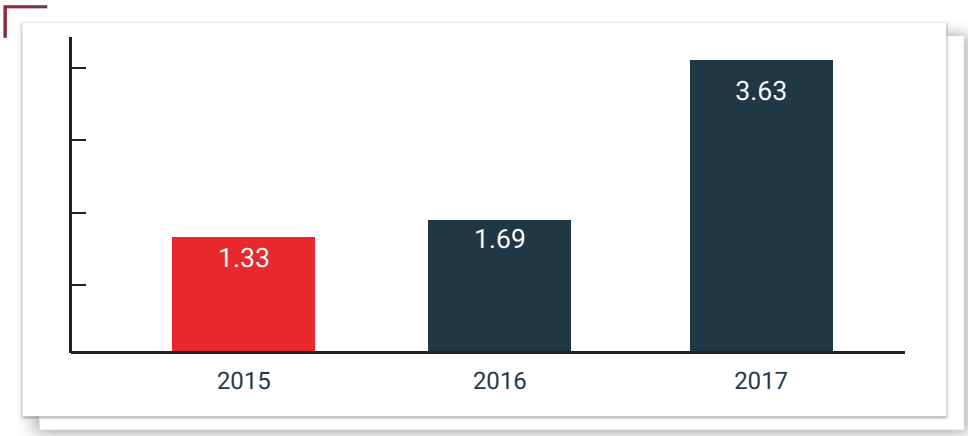


Figure 15: BEC Simulation Resiliency

"Our leadership wants to know that we're always getting better."

A PhishMe client with global operations in consumer package goods (CPG) has seen anti-phishing metrics steadily improve. But, "We can't just do the same basic simulations over and over," said their head of security awareness.

"Our leadership wants to know that we're always getting better. With PhishMe Simulator, it's easy to customize more complex phishing scenarios. Over time, we've made the exercises more advanced, personalizing emails by name and company logo, to reflect what's happening in the real world."[5]

| Read More >>

CONCLUSIONS

Our data supports a proactive approach.

It's well known that phishing, like all forms of cyber-crime, constantly evolves as attackers seek an edge. The data in this report points to another evolution: that of organizations refining anti-phishing programs to blunt the attacker's advantage.

In simulation training, users learn to recognize phishing and report it right away. Incident responders not only use such human intelligence to hunt and stop threats—they also loop it back to the training, so simulations mirror ongoing real-world dangers. When users train routinely and remain engaged, anti-phishing programs become proactive and more effective.

- Among PhishMe customers, simulations over time are decreasing organizational susceptibility.
- The more employees report phishing—in other words, the more engaged employees are—the faster susceptibility decreases.
- Employees are quite susceptible when targeted as consumers. Be on guard against phishing emails that use e-cards, rewards programs and similar lures.
- BEC/CEO fraud emails without a link or attachment are the most effective simulated phishes. This reflects what PhishMe observes in our phishing response and intelligence services.
- An anti-phishing program that decreases susceptibility while increasing reporting and resiliency is a very good start.
- A program that proactively defends by mirroring the newest, most dangerous phishes is even better. To help you stay out in front of attacks, simulations must be relevant.

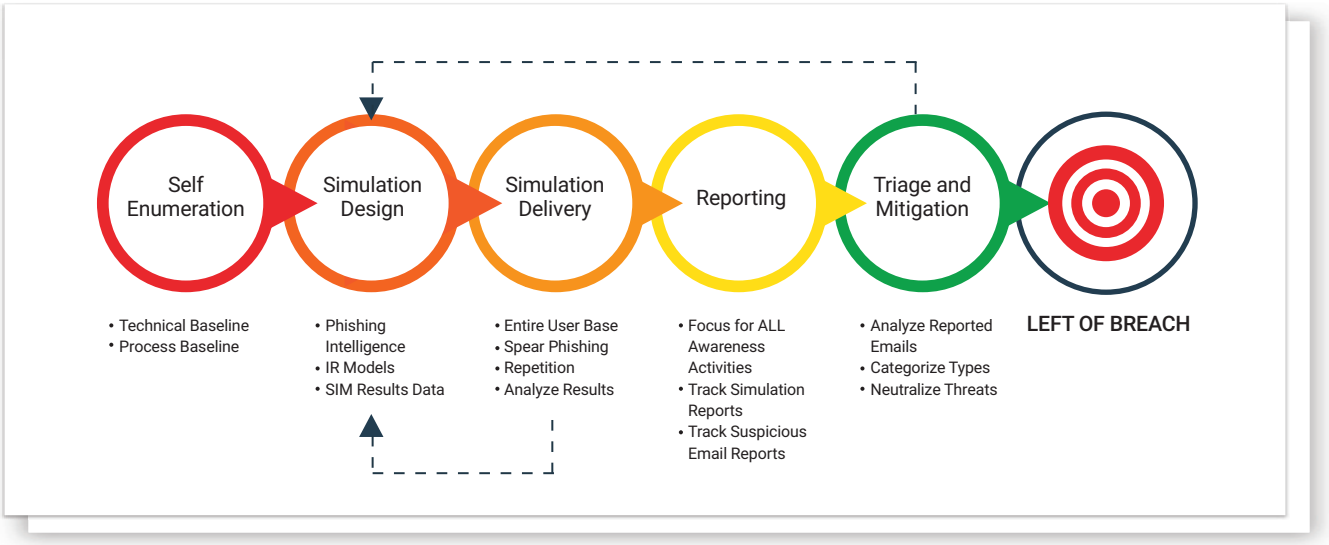
RECOMMENDATIONS

Go on offense: model your program on the phishing kill chain.

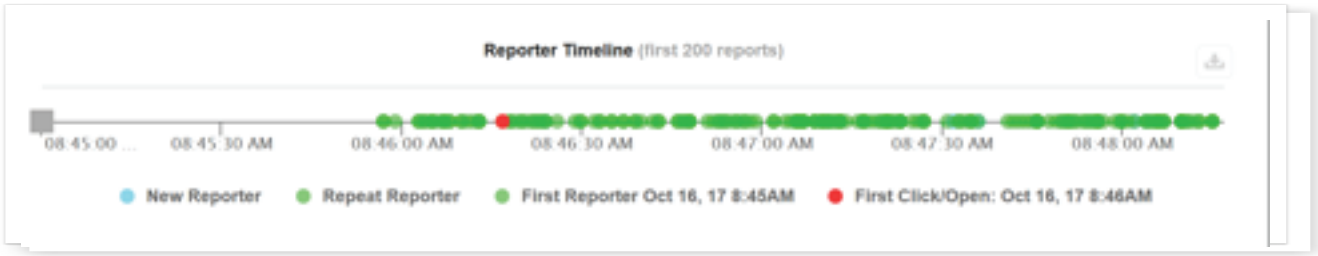
The "kill chain" is a well-known model among security professionals. The idea is to outline, link by link, the chain leading to a security incident and take all steps to prevent it.

In the phishing kill chain, you want to stay "left of breach" (see illustration below). In short, here's how to utilize this model:

- Be transparent and educate users on standard phishing clues and the purpose of the program.
- Baseline your organization's technical and business process weaknesses, so you can target them during initial simulations.
- Run diverse simulations and analyze each for high susceptibility to active threats.
- Design follow-up simulations based on known deficiencies and analysis of first results.
- Stress the importance of reporting in all simulations and awareness activities.



An Example of the Reporting Response to a Phishing Simulation



Imagine this was a real attack.

By 8:45 am, your IT Security team would have already gotten a notification about this attack in progress and been able to respond quickly. This highly conditioned organization had only a single initial fail and many engaged reporters.

It's a picture of success—a proactive phishing defense.

CITATIONS

1. Cloudmark, "Spear Phishing: The Secret Weapon Behind the Worst Cyber Attacks," 2016.
2. The Anti-Phishing Work Group, "Phishing Activity Trends Report," 2016.
3. FBI, "Business E-Mail Compromise/E-Mail Account Compromise the 5 Billion Dollar Scam," 2017.
4. PhishMe, Financial Services Case Study, 2016.
5. PhishMe, "Global CPG Leader Accelerates Incident Reporting and Response," 2017.