PHISHING DEFENSE GUIDE
2017

With more than 90% of breaches attributed to successful phishing campaigns, it's easy for organizations to point to the everyday employee as the root cause of the problem.

We disagree. In our comprehensive Phishing Defense Guide, you’ll learn how to empower humans as part of the solution to help strengthen defenses and gather real-time attack intelligence to stop attacks in progress.
Executive Summary

The Phishing Defense Guide 2017 is a compilation of select PhishMe research and reports covering a variety of security topics from phishing threat analysis to ransomware trends and industry surveys, all to assist in developing a comprehensive phishing defense strategy for your organization.

In 2016, 91% of cyberattacks were caused by phishing emails. These malicious messages trick employees into clicking links or attachments or responding in some way that inadvertently gives cybercriminals access to business networks. Because employees – real people – are the targets of these attacks, PhishMe empowers employees to be part of solution. We do that by gathering behavioral data from phishing victims, reviewing phishing threat intelligence and arming employees with training and conditioning to help them recognize threats and report them.

This guide provides an overview of our methods and insight into what drives phishing victims and the criminals threatening them.

In this report, we:
• Share key user susceptibility statistics
• Describe what behavior conditioning is and why it’s effective
• Observe phishing prevention techniques and market trends
• Review malware samples and ransomware findings
• Explain how PhishMe measures return on investment

How do phishing emails trick people into clicking links, allowing bank account access or sharing secure information? They play on victims’ emotions – namely, curiosity, fear and urgency. In this report, we discuss how understanding these underlying motivations is key to PhishMe’s phishing defense strategy, which involves employees conditioned to recognizing threats through simulated phishing email scenarios. Employees use their reactions as triggers to later scrutinize and report real threats, generating a unique stream of human-vetted phishing threat intelligence that incident responders and security operations teams can take advantage of to stop active threats in real time.

In this guide, we also review specific threats – malicious software that has skyrocketed in use. Last year saw increases of over 400% in ransomware, 51% in non-ransomware spear-phishing and 1,300% in business email compromise (BEC) scam losses.

Ransomware is the “give me your money or lose your computer files” software that’s loud and proud in communicating its intentions to victims. Non-ransomware malware, on the other hand, is quiet, stealthy and designed to avoid detection. BEC scams may be the sneakiest malware of all because threat actors use the software to infiltrate internal email networks and then email employees, pretending to be their co-workers. Instead of including links or attachments (like in non-ransomware), BEC messages request business-related payments or sensitive company information.

PhishMe’s human phishing defense solutions empower humans to recognize and report attacks, speeding incident response and fueling human-vetted threat intelligence for security operations. Our clients see their return on investment when there’s:
• A drop in the number of phishing emails bypassing security perimeters
• A decrease in time spent identifying and responding to compromised systems
• A reduction in employees clicking suspicious emails because they’ve been previously conditioned by simulated phishing emails.

We hope this guide inspires you to look at the human solutions within your ranks. In PhishMe’s own client pool, representing more than half of the Fortune 100, a growing number of security professionals are acknowledging employees as valuable, untapped resources in the fight against phishing. As an example, there’s significant value in our clients’ employees reporting threats in progress. PhishMe found that employees phishing reports reduced the average time of detecting a breach from 146 days to 1.2 hours. Detecting breaches quickly is critical in stopping threats before money or information is stolen or compromised, and only people can make that happen.
BEHAVIORAL CONDITIONING, NOT AWARENESS, IS THE ANSWER TO PHISHING

By Aaron Higbee and Scott Greaux
You don’t stop phishing attacks by raising user awareness. A recent study conducted by a German university confirms what we at PhishMe have known all along: Focusing on awareness isn’t the point. The real solution is behavioral conditioning.

The study, conducted by Friedrich-Alexander University (FAU) of Erlangen-Nuremberg, Germany, used 1,700 students to simulate spear phishing attacks. An August 31 Ars Technica article published preliminary results of the study showing at least 50% of students clicked simulated phishes, even though they understood the risks.

With its headline, “So Much for Counter-Phishing Training: Half of People Click Anything Sent to Them,” the article appears to suggest training is pointless. But we see it differently. While the article confirms what our own research has revealed – that awareness isn’t the problem – the proper conclusion to draw isn’t that training is futile. PhishMe tends to agree with this sentiment and encourages organizations to focus on conditioning their employees to identify and report security risks.

We focus our training on conditioning human behavior, and the results speak for themselves. Our customers spend 22 seconds reviewing phishing education, and yet their susceptibility to phishing decreases significantly. Why? It’s the experience we put them through that changes behavior. Even when they are aware of the risks, as studies show, they are susceptible to opening email from unknown users and clicking suspicious links. But conditioned through the real-world examples we provide in our simulations, users are much less likely to click.

**Enterprise Relevance**

The FAU study focused on students, who were sent emails and Facebook messages with links purporting to be for photos from a New Year’s Eve party held a week before the study. “Links sent resolved to a webpage with the message ‘access denied,’ but the site logged the clicks by each student.”

It’s dangerous to use research results conducted on a student population to Enterprise workers. We have several problems with the approach as described. For starters, it wasn’t created by people in the trenches who understand real-world threats, but by academics in a computer science department. We already know the bait used by the study’s authors works on students, as well as consumers, but is far less effective with enterprise users. Yet, readers of the Ars Technica article are concluding the study’s results apply to enterprise environments.

We know that because we’ve started to get messages with their reactions. So we feel an obligation to point out the study didn’t use a realistic scenario, from an enterprise point of view. Real-world enterprise phishes are more likely to be emails pretending to be files from a scanner, a document with a job evaluation, or a message that someone has signed for a package addressed to the user.

There’s also a difference of perspective between students and enterprise users. Students, whose primary experience with computing revolves around mobile devices such as tablets and smartphones, don’t worry about cyber risks. Clicking a link from a smartphone isn’t going to compromise the device because such devices are nearly impervious to attacks. But click the link from a computer, and the story is quite different.
It also appears the FAU study focused only on clicking links, but phishing threats aren't limited to one vector. Others include data entry, password credentials, clicking attachments, and email conversations that don't involve links or attachments. Replicating some of these vectors in a real-world simulation is a bigger challenge than the method used by the study.

**Focus on Reporting**

A PhishMe-commissioned study found 94% of office workers know what phishing is and the risk it presents to organizations. The study also found that 94% of office workers know how to report suspicious emails in their organization. And that's where the focus of training needs to be – reporting. When users are conditioned to report suspicious email, even if they do so after already clicking on it – maybe they had a lapse – the reporting is still valuable because it helps your security operations teams.

Learning to identify suspicious emails through conditioning is far more effective than general efforts to raise awareness. PhishMe simulator provides customers with templates that include the exact content used by threat actors. By deriving content from our Phishing Intelligence platform we provide experiences that are relevant to enterprise users. This method allows customers to condition users to spot potential phishes, avoid interacting with them, and report them to their security teams.

While we appreciate the FAU’s study's confirmation of what our own research has shown about awareness, we fear it may lead enterprises to make decisions based on the erroneous conclusion that training doesn't matter. This perspective could lead to the compromise of a network with disastrous results. To avoid such an outcome, we at PhishMe stand ready to work with any academic institution or researcher that could benefit from our experience in the trenches to produce meaningful research about phishing.
Techniques for Dealing with Ransomware, Business Email Compromise and Spearphishing

An Osterman Research White Paper

Published January 2017
EXECUTIVE SUMMARY

Phishing, spearphishing, CEO Fraud/Business Email Compromise (BEC) and ransomware represent a group of critical security threats that virtually every organization will encounter at some point – and most already have. While phishing actually started in the 1995-1996 time frame, it became a much more serious problem in the mid-2000s. The logical evolution of phishing – spearphishing (targeted against a group, a company or individuals within that company) and CEO Fraud/BEC (which targets senior executives within a single company) – are increasing rapidly and costing organizations hundreds of millions of dollars each year. Add to this the fact that ransomware is reaching epidemic proportions and increasing at an even faster pace, growing from an impact of "just" $24 million in 2015, but increasing to approximately $1 billion in 2016.

KEY TAKEAWAYS IN THIS PAPER

• The vast majority of IT decision makers are highly concerned about phishing, malware infiltration, spearphishing and ransomware…and for good reason: most organizations have been the victim of these types of attacks and exploits, as well as others, during the last 12 months.

• The cyber security solutions that are in place today are somewhat effective, but a significant proportion of decision makers report that their problems with phishing, spearphishing, CEO Fraud/BEC and ransomware are getting worse over time (although the proportion reporting that their ransomware problem is staying the same or getting better increased from our 2016 survey). For most of the cyber security capabilities that organizations have deployed to combat these threats, the majority of decision makers report they are not highly effective.

• Users continue to be the weak link in most organizations’ cyber security infrastructure because they have not been adequately trained to deal with phishing, spearphishing and CEO Fraud/BEC attempts.

• IT decision makers’ confidence in their users’ ability to deal with phishing, spearphishing, CEO Fraud/BEC and ransomware is low, in part because of the lack of training their users receive, but also because organizations are not performing sufficient due diligence to address these problems.

• Problems with phishing, spearphishing, CEO Fraud/BEC and ransomware are getting worse as cyber criminals become more sophisticated, better funded and are outpacing many prospective victims’ spending on new cyber security solutions and security awareness training.

• Despite the escalating threat level, there are a number of steps that organizations can take to significantly improve their defenses against phishing, spearphishing, CEO Fraud/BEC and ransomware that will dramatically reduce their chances of falling victim to these attacks.

ABOUT THIS WHITE PAPER

A primary research survey was conducted specifically for this white paper, some of the results of which are included herein. The complete set of survey results will be published in a separate Osterman Research survey report. This white paper was sponsored by PhishMe – information about the company is provided at the end of this paper.

LEADING CYBER SECURITY CONCERNS

The research conducted for this white paper found that a wide range of cyber security problems have occurred within the organizations surveyed. As shown in Figure 1, 37 percent of organizations have been the victim of an email phishing attack that successfully infected systems with malware, 24 percent of have been the
victims of a successful ransomware infection, and 22 percent have had sensitive or confidential information leaked through email. In fact, only 25 percent of the organizations we surveyed have not been the victim of at least one of the cyber security incidents shown or, more importantly, are not aware they are victims.

Figure 1
Cyber Security Problems That Have Occurred During the Previous 12 Months

<table>
<thead>
<tr>
<th>Incident</th>
<th>% of Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>An email phishing attack was successful in infecting systems on our network with malware</td>
<td>37%</td>
</tr>
<tr>
<td>One or more of our endpoints had files encrypted because of a successful ransomware attack</td>
<td>24%</td>
</tr>
<tr>
<td>Malware has infiltrated our internal systems, but we are uncertain through which channel</td>
<td>22%</td>
</tr>
<tr>
<td>Sensitive / confidential info was accidentally leaked through email</td>
<td>22%</td>
</tr>
<tr>
<td>One or more of our systems were successfully infiltrated through a drive-by attack from employee web surfing</td>
<td>21%</td>
</tr>
<tr>
<td>An email as part of a CEO Fraud/BEC attack successfully tricked one or more senior executives in our organization</td>
<td>12%</td>
</tr>
<tr>
<td>An email spearphishing attack was successful in infecting one or more of our senior executives’ systems with malware</td>
<td>10%</td>
</tr>
<tr>
<td>Sensitive / confidential info was maliciously leaked through email</td>
<td>7%</td>
</tr>
<tr>
<td>Sensitive / confidential info was accidentally or maliciously leaked through a cloud-based tool like Dropbox</td>
<td>6%</td>
</tr>
<tr>
<td>Sensitive / confidential info was accidentally or maliciously leaked through a social media / cloud application</td>
<td>2%</td>
</tr>
<tr>
<td>Sensitive / confidential info was accidentally or maliciously leaked, but how it happened is uncertain</td>
<td>2%</td>
</tr>
<tr>
<td>None of the above has occurred or are aware it has occurred</td>
<td>25%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.

RECENT PHISHING, SPEARPHISHING, CEO FRAUD/BEC AND RANSOMWARE EXAMPLES
Here are some recent examples of the types of attacks discussed in this white paper:

- The GoldenEye ransomware is targeting German speakers in HR departments using a two-part attack. The first attachment is a PDF file delivered in email that contains a cover letter, while the second attachment is an Excel file that uses malicious macros to load ransomware by asking the victim to click a link.

- In early 2017, organizations with MongoDB databases in which access control had not been configured properly were deleted and were being held for ransom. On January 2nd, 200 databases had been deleted, but by January 6th the number of deleted databases reached 10,500.

- A new ransomware technique employs a twist on social engineering by offering free decryption for victims’ files if they send a link to their contacts and if at least two of these new victims pay the ransom of one Bitcoin.
Some notable victims of CEO Fraud/BEC over the past couple of years include Crelan Bank in Belgium (victimized for $75.8 million); FACC, an Austrian manufacturer of aircraft components, which ($54 million); Mattel, ($3 million); The Scoular Company, a commodities trading firm, ($17.2 million); Ubiquiti Networks, ($46.7 million); and the Romanian factor of German firm Leoni AG ($44 million).

PROBLEMS THAT CONCERN DECISION MAKERS MOST

Not surprisingly, there is a wide range of cyber security issues about which IT decision makers and influencers are concerned. As shown in Figure 2, the top three issues of concern are focused on email as the primary threat vector: phishing, malware infiltration and spearphishing. However, a number of other cyber security threats are also of significant concern, including malware infiltration through Web browsing, ransomware, and CEO Fraud/Business Email Compromise (BEC).

Figure 2
Level of Concern Over Various Types of Security Threats

<table>
<thead>
<tr>
<th>Threat</th>
<th>Low Concern</th>
<th>Moderate Concern</th>
<th>High Concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing through email</td>
<td>2%</td>
<td>24%</td>
<td>74%</td>
</tr>
<tr>
<td>Malware infiltration through email</td>
<td>6%</td>
<td>27%</td>
<td>67%</td>
</tr>
<tr>
<td>Spearphishing through email</td>
<td>2%</td>
<td>32%</td>
<td>65%</td>
</tr>
<tr>
<td>Malware infiltration via web browsing</td>
<td>2%</td>
<td>36%</td>
<td>61%</td>
</tr>
<tr>
<td>Ransomware infiltration</td>
<td>4%</td>
<td>40%</td>
<td>56%</td>
</tr>
<tr>
<td>CEO Fraud/Business Email Compromise (BEC)</td>
<td>10%</td>
<td>50%</td>
<td>40%</td>
</tr>
<tr>
<td>Insider, accidental disclosure of data</td>
<td>10%</td>
<td>53%</td>
<td>36%</td>
</tr>
<tr>
<td>Phishing through social media</td>
<td>12%</td>
<td>53%</td>
<td>36%</td>
</tr>
<tr>
<td>Insider, malicious disclosure of data</td>
<td>20%</td>
<td>49%</td>
<td>31%</td>
</tr>
<tr>
<td>Physical theft of laptops and mobile devices</td>
<td>17%</td>
<td>55%</td>
<td>28%</td>
</tr>
</tbody>
</table>

Source: Osterman Research, Inc.

CYBER SECURITY SPENDING IN 2016 AND 2017

To address these cyber security issues, organizations are spending significantly on security. Our research found that the median expenditure in 2016 focused on phishing, malware, ransomware and related types of threats was $58.33 per employee for the year, increasing slightly to $58.85 per employee for 2017. More significantly, while 36 percent of organizations planned to spend the same amount in 2017 addressing these issues as they did in 2016, 62 percent will increase their cyber security budget, while only two percent will spend less.

However, we found that larger enterprises (more than 1,000 employees) are actually planning to spend slightly less on cyber security in 2017 than they did in 2016, dropping from $23.86 per employee in 2016 to $21.53 per employee in 2017. Smaller organizations, on the other hand will see an increase from $66.67 per employee in 2016 to $70.00 per employee in 2017.

The significant difference in per-employee spending between larger and smaller organizations highlights one of the perennial problems of the latter: they lack the
WHY ARE PHISHING, SPEARPHISHING, BEC AND RANSOMWARE SUCCESSFUL?

Phishing, spearphishing, CEO Fraud/BEC, ransomware and other cyber security threats have proven to be highly successful in stealing funds and causing other problems. Consider the following:

- The World Economic Forum places the global cost of cyber crime at $445 billion in 2016v.
- The Ponemon Institute estimates that the typical 10,000-employee company spends $3.7 million per year dealing with just phishing attacksvi.
- Vade Secure estimates that the cost of one spearphishing attack against a company with $100 million in revenue that suffers a breach of 50,000 records will be $7.2 millionvii.
- The FBI estimates that for the two years ended June 2016, CEO Fraud/BEC attacks have cost the more than 22,000 businesses that have fallen victim to it a total of $3.09 billionviii.
- Ransomware attacks netted cyber criminals approximately $1 billion in 2016ix.

These are staggering figures that cost organizations of all sizes enormous amounts of money in direct costs, but also lost employee productivity, lost revenue, lost goodwill with customers, and damage to their corporate reputations.

So, why are these attacks so successful?

USERS ARE THE WEAK LINK IN THE CHAIN

One of the fundamental problems with cyber security – and the primary reason that these attacks are so successful – is users themselves. Most users are not adequately trained about how to recognize phishing, spearphishing, CEO Fraud/BEC, or ransomware attempts, and so often fall prey to them by clicking on links or opening attachments in emails that they receive without considering the potential for harm that can result. For example, our research found that six percent of users never receive any security awareness training, while 52 percent receive training no more than twice per year. The result is that users are not trained to be sufficiently skeptical of suspicious emails or other potential threats, such as short URLs in Twitter or Facebook advertisements, primarily because they have never been trained to be skeptical about these threat venues. Moreover, organizations do not provide the infrastructure that would adequately support better user-focused security, such as notifications, reminders, or opportunities for users easily to query IT about suspicious emails or attachments.

The result of this poor training is that IT is not at all confident in their users’ ability to recognize incoming threats or in their organizations’ ability to stop phishing and related incursions. For example, as shown in Figure 3, fewer than one in five IT decision makers or influencers is “confident” or “very confident” that their employees are adequately trained to recognize ransomware attacks.
Further complicating the problem is that organizations are not performing enough due diligence to address the problems of phishing, spearphishing, CEO Fraud/BEC and ransomware.

**ORGANIZATIONS ARE NOT PERFORMING SUFFICIENT DUE DILIGENCE**

Further complicating the problem – and enabling cyber criminals to be successful – is that organizations are not performing enough due diligence to address the problems of phishing, spearphishing, CEO Fraud/BEC and ransomware. For example:

- Many organizations have insufficient backup processes that would enable them to rapidly revert content on servers, user workstations and other endpoints to a known good state following a ransomware attack or other incursion.
- Most organizations do not adequately test their users to determine which are most susceptible to interacting with malicious emails.
- Many organizations lack strong internal control processes that require checks and balances in an effort to prevent CEO Fraud/BEC attacks. For example, many organizations do not require that a wire transfer request from a senior executive delivered through email be verified through some sort of “backchannel”, such as a text message or voice call.
- Many organizations have not implemented technologies that are sufficiently sophisticated to reduce the threats that they face.
- Many organizations have not adequately addressed the “Bring Your Own” phenomenon in the context of the devices, mobile apps and cloud applications that users employ, allowing corporate data and system resources to be accessed through insecure means.

**CRIMINAL ORGANIZATIONS ARE WELL FUNDED**

The criminal organizations that are perpetrating cyber crime are generally very well funded and they have the technical resources to publish new and increasingly more capable variants of their malware. For example, ransomware has evolved from locker-type variants that were the norm just a few years ago to more sophisticated, crypto-based variants like CryptoWall (2014), CTB-Locker (2014), TeslaCrypt (2015), Samas...
(2016), Locky (2016) and Zepto (2016). Add to this the fact that ransomware-as-a-service is becoming more commonplace – as just one example, the Cerber service had infected 150,000 endpoints as of July 2016 and is generating profits of nearly $200,000 per monthx. Because of their robust funding, criminal organizations can readily adapt to changing requirements in an effort to stay ahead of less capable cyber security solutions and processes.

**CYBER CRIMINALS ARE SHIFTING THEIR FOCUS**

Cyber crime has been so successful over the past few years, data breaches have been so numerous, and the number of sellers on the "Dark Web" and in underground hacking forums have increased so much, that stolen credentials, credit card numbers, health records and other content are no longer as valuable as they once were. For example, the price of a payment card record in 2016 was $6, down from $13 in 2014 and $25 in 2011xi. The cost of a health record on the black market dropped from $75 to $100 in 2015 to just $20 to $50 in 2016xii.

In effect, cyber criminals have flooded the market with so much stolen data that supply is exceeding demand, resulting in a significant drop in prices for this information. This means that cyber criminals will need to steal more data in order to generate the same level of revenue as they did in the past. Moreover, there is now a shift in emphasis from stealing information that then needs to be sold on the black market, where prices are declining, to stealing information directly from information-holders themselves. Cyber criminals will more frequently use phishing and spearphishing that will install malware like keyloggers that can enable them to transfer money out of corporate financial accounts, ransomware that will extort money from victims, and CEO Fraud/BEC that will trick senior managers into making large wire transfers directly to cyber criminals' accounts. This will effectively reduce the need to steal and sell something of value, and instead is moving cyber criminals to steal the funds directly.

**WIDESPREAD AVAILABILITY OF LOW-COST PHISHING AND RANSOMWARE TOOLS**

There is a growing number of tools designed to help amateurs with minimal knowledge of IT to become “hobbyist” phishers and ransomware authors. As noted in a FraudWatch International blog post from September 2016, "Gone are the days where only the most skilled hackers could develop a phishing site and scam users into divulging their personal information. Nowadays, any Joe Shmo, can create one and they do it with the help of a Phishing Kit." The result has been an explosion of ransomware and other exploits coming from a large and growing assortment of amateur cyber criminals, adding to the problem from professional cyber criminal organizations driven by the onset of Ransomware-as-a-Service (RaaS)xiv.

**MALWARE IS BECOMING MORE SOPHISTICATED**

Over time, phishing and various types of malware have become more sophisticated. For example, the early days of crude phishing attempts that tried to trick gullible users into clicking on a malicious link or open a malicious attachment have evolved into sophisticated CEO Fraud/BEC attacks in which hackers infiltrate an organization’s network and learn business processes with the goal of crafting potentially lucrative attacks aimed at specific senior executives. Ransomware has evolved from variants that simply prevented an individual from accessing his or her files to those that use sophisticated encryption capabilities. Jonathan Whitley of WatchGuard Technologies believes that 2017 will see the development of even more sophisticated threats, such as self-propagating ransomware (what he dubs "ransomworms"), as well as the use of machine learning to get around cyber security solutions that also rely on machine learningxv.

In short, the problems of phishing, spearphishing, CEO Fraud/BEC and ransomware are simply going to get worse without appropriate solutions and processes to defend against them.
CYBER SECURITY MUST GET BETTER

The simple answer to the problem of increasingly sophisticated phishing, spearphishing, CEO Fraud/BEC and ransomware is that practices, processes, solutions and the overall mindset toward cyber security must improve. However, our research found that while there are some improvements in cyber security, they are not keeping pace with threats.

SECURITY SOLUTIONS ARE IMPROVING ONLY SLIGHTLY IN SOME AREAS AND GETTING WORSE IN OTHERS

Our research found that for many organizations, phishing/spearphishing, ransomware and CEO Fraud/BEC solutions actually are improving by being better able to detect and thwart these threats before they can reach end users or have an impact on an organization. However, as shown in Figure 4, the majority of organizations report that their cyber security solutions either are not improving or are getting worse, while many are simply unsure whether or not they are seeing any change.

![Figure 4: Perceptions About Changes in the Effectiveness of Cyber Security Solutions](image)

Source: Osterman Research, Inc.

HOW EFFECTIVE ARE CURRENT SOLUTIONS?

Our research also asked organizations to rate the effectiveness of their various cyber security solutions and training practices. As shown in Figure 5, 56 percent of those surveyed believe that their current solutions to eliminate malware before it reaches end users are either "very good" or "excellent", but things deteriorate from there: fewer than one-half of respondents indicated that their solutions against ransomware, phishing or mobile device threats rate this highly. Even worse, the effectiveness of current end user training practices was considered "very good" or "excellent" by only a minority of organizations.
However, we found that organizations with more frequent security awareness training (where employees are trained at least twice per year) rate their cyber security effectiveness more highly than organizations in which security awareness training is either less frequent or non-existent, as shown in Figure 6.

Source: Osterman Research, Inc.
THREATS ARE GETTING WORSE

WHAT DO WE MEAN BY “GETTING WORSE”? Cyber security threats are getting worse, but what exactly does that mean? In short, it means that while cyber criminals are becoming more adept at their craft, many cyber security solutions and the level of security awareness training are not keeping pace. For example:

• Cyber criminals are shifting from consumer to corporate victims with very targeted strategies aimed at the latter, as noted below.

• Phishing, spearphishing and related types of attacks are becoming more advanced, making it harder for intrusion prevention systems, DLP and other defenses to detect a breach.

• The cost of data breaches, ransomware demands, and threat remediation continue to climb.

STATISTICS TO PROVE THE POINT Compounding the problem of ineffective cyber security solutions and inadequate training is the fact that phishing, spearphishing, CEO Fraud/BEC and ransomware are becoming more common threats than they already are. For example:

• The Anti-Phishing Working Group reports that the number of unique phishing sites it detected grew from 0.39 million in 2014 to 0.79 million in 2015 to 1.49 million in 2016.

• The FBI reported that identified, exposed losses from CEO Fraud/BEC increased by 1,300 percent from January 2015 to June 2016.

• Symantec reports that the average ransom amount has increased from $294 in 2015 to $679 in 2016.

• The FBI reported that ransomware victims paid $24 million in ransom in 2015, but $209 million in just the first quarter of 2016 and was on-pace to be a $1 billion problem for all of 2016.

• The Identify Theft Resource Center reported that the number of data breaches increased from 614 in 2013 to 783 in 2014 and dropped only slightly to 781 in 2015.

A GROWING VARIETY OF THREAT VECTORS Osterman Research anticipates that phishing, spearphishing, CEO Fraud/BEC and ransomware – and the resulting data breaches and financial losses they can cause – will continue to get worse over the next few years in several key ways:

• Businesses will increasingly be the target for phishing and ransomware, not individuals. Because businesses are more likely to have mission-critical data that must be recovered, will have the means to purchase Bitcoin or other digital currencies to pay the ransom, and are more likely to pay higher ransom amounts, cybercriminals will focus more of their efforts on infecting these higher value targets. The increasing emphasis on businesses as targets of ransomware is borne out by data from Kaspersky, which found that corporate users comprised 6.8 percent of ransomware victims in the 2014-2015 timeframe, but 13.1 percent of victims in 2015-2016.

• The healthcare industry will be a key target for ransomware because of the success that cyber criminals have enjoyed so far in 2016 targeting hospitals and other healthcare facilities, and because healthcare organizations have demonstrated that they will pay significant amounts to recover their data. Among
the healthcare organizations successfully attacked in 2016 were the Chino Medical Center (Chino, CA), Ottawa Hospital (Ottawa, ON), the National Health Service's (NHS’) Lincolnshire and Goole Trust (three locations in England), University of Southern California’s Keck and Norris Hospitals (Los Angeles, CA), the New Jersey Spine Center (Chatham, NJ), Alvarado Medical Center (San Diego, CA), Professional Dermatology Care (Reston, VA), Lukas Hospital (Neuss, Germany), Hollywood Presbyterian Medical Center (Los Angeles, CA), Marin Healthcare District (Greenbrae, CA), King’s Daughters’ Health (Madison, IN), Urgent Care Clinic of Oxford (Oxford, MS), Kansas Heart Hospital (Wichita, KS), MedStar Health (Washington, DC), Desert Valley Hospital (Victorville, CA) and Methodist Hospital (Henderson, KY).

Underscoring the tremendous vulnerability of the healthcare industry to cyber attack, one firm found that, as of mid-2016, 88 percent of ransomware attacks had been in the healthcare industry. Many healthcare organizations have been hit with malware multiple times, such as Leeds Teaching Hospital (Leeds, England) that suffered five attacks during 2016, part of the NHS’ growing problem in which 30 percent of NHS Trusts have been hit with ransomware.

• CEO Fraud/BEC will become a primary focus area for cyber criminals because of the lucrative nature of this activity. While these types of attacks require significantly more effort than, for example, ransomware attacks because of the need to determine key staff members in the target companies, the victims’ suppliers, their payment practices, and so forth, the payoff is much larger. Trend Micro has determined that the typical CEO Fraud/BEC exploit results in a net payoff of $140,000 per incident compared to $30,000 from a successful ransomware attack on an enterprise.

FOURTEEN BEST PRACTICES AND TECHNIQUES TO CONSIDER

Osterman Research recommends that decision makers consider the following 14 steps that will help to improve an organization’s cyber security posture in the context of protecting against phishing, spearphishing, CEO Fraud/BEC and ransomware.

1. **Appreciate the risks that your organization faces**
   Decision makers must understand the risks that their organizations face from phishing, spearphishing, CEO Fraud/BEC and ransomware and address them as a high priority. While that may seem like an obvious recommendation, many decision makers understand problems intellectually, but they fail to put that understanding into action by training users appropriately and implementing the right cyber security infrastructure. Cyber crime is an industry with sophisticated technical expertise, huge funding, and a rich target environment of potential victims and it must be dealt with as such.

2. **Conduct a complete audit of current cyber security tools, training and practices**
   Organizations should conduct a thorough audit of their current cyber security infrastructure, including their security awareness training regimen, the security solutions they have in place, and the processes they have implemented to remediate security incidents. This is an essential element in identifying the deficiencies that may (and probably do) exist, and it can be used to prioritize spending to address problems.

3. **Establish policies**
   It is important to develop policies for all of the email, Web, collaboration, social media, mobile and other solutions that IT departments have deployed or that are allowed for use as part of “shadow IT”. As a result, Osterman Research recommends that a key step should be the development of detailed and
thorough policies focused on the tools that are or probably will be used in the future. Policies should focus on legal, regulatory and other obligations to encrypt emails if they contain sensitive or confidential data; monitor all communication for malware that is sent to blogs, social media, and other venues; and control the use of personal devices that access corporate systems that contain business content.

Policies, in and of themselves, will not provide cyber security per se, but they can be useful in limiting the number of solutions that employees use when accessing corporate systems. These limitations can be helpful in reducing the number of ingress points for ransomware, other forms of malware, phishing and spearphishing attempts, and other content that might pose a cyber security risk.

4. **Deploy alternatives to the solutions that employees use as part of “Shadow IT”**

   It is important for IT to offer good alternatives to the solutions that employees have deployed, or might want to deploy, to be more effective in their work. This includes solutions for file-sync-and-share, voice-over-IP, cloud storage, real-time communications and other capabilities that employees download and install because they do not have an equivalent capability from IT, or because the IT-provided solution is not as good as the free or freemium solution they have chosen. Providing an IT-approved solution that is as good as the solutions that employees have deployed on their own can significantly enhance cyber security and give IT control over corporate content.

5. **Implement and/or update company procedures**

   Every organization should implement, and periodically update, their company procedures with regard to how sensitive and confidential data, as well as business-critical systems, are protected and accessed. For example, every organization needs an effective set of backup, restoration and testing procedures for all of its data assets so that it can quickly recover from a ransomware infection. Moreover, dual-control procedures should be implemented for access to critical data assets, particularly those focused on financial transactions, so that a single, rogue employee cannot create a data breach or breach of cyber security.

6. **Implement best practices for user behavior**

   Organizations should establish a number of best practices to address whatever cyber security gaps may exist in the organization. For example:

   - Employees should be tested on a regular basis to determine if their security awareness training has been effective, and to identify those employees that might need additional training.

   - Employees should use passwords that match the sensitivity and risk associated with the corporate assets they are accessing. These passwords should be changed on an enforced schedule established by IT.

   - Create communication “backchannels” for staff members that will be involved with corporate finances or sensitive information. For example, if a CEO sends a request to his CFO to transfer funds to an established vendor, the CFO should have a means of verifying the authenticity of the CEO’s request before initiating the transfer, such as texting or calling the CEO’s smartphone.

   - Employees should be reminded and required to keep software and operating systems up-to-date to reduce the potential for a known exploit to infect a system with malware. IT can help through management and enforcement on behalf of users.
Employees, particularly senior executives who are more likely to be the target of a CEO Fraud/BEC attack, should be reminded regularly about the dangers of oversharing information on social media. Employees’ friends might be interested in the latest personal information that gets posted on social media, but this information might give cybercriminals the information they need to create a believable spearphishing email.

- Make sure that every employee maintains good anti-malware defenses on their personal devices if there is any chance that these devices will access corporate resources like corporate email or databases with sensitive corporate information.

7. **Train all users and senior executives**

   Develop a good security awareness training program that will help users to make better judgments about the emails they receive, how they use the Web, the links they click in social media, and so forth. The goal of security awareness training is to help users to be more skeptical about what they view and what they consider to be safe to open. While security awareness training alone will not completely address an organization’s cyber security problems, it will bolster the ability for users to be more aware of cyber security issues and make the organization less susceptible to phishing, spearphishing, CEO Fraud/BEC and ransomware attacks. It is critical to invest adequately in employee training so that this “human firewall” can provide a solid first line of defense against increasingly sophisticated phishing and other social engineering attacks. Senior executives should have additional training to deal with spearphishing and CEO Fraud/BEC, since they are higher value targets to cyber criminals and the consequences of their failure can be dramatically greater.

8. **Keep systems up-to-date**

   Vulnerabilities in applications, operating systems, plug-ins and systems can allow cybercriminals to successfully infiltrate corporate defenses. Every application and system should be inspected for vulnerabilities and brought up-to-date using the latest patches from vendors, a key mitigation technique to reduce the effectiveness of exploit kits. One source estimates that 99 percent of computers are vulnerable to exploit kits because almost all computers run Oracle Java, Adobe Flash and/or Adobe Reader.

9. **Ensure there are good and recent backups**

   An effective way to recover from a ransomware attack, as well as from other types of malware infections, is to restore the infected endpoint(s) from a known, good backup taken as close as possible to the point before the infection occurred. With a recent backup, an endpoint can be reimaged and its data restored to a pre-infection state with minimal data loss. While this strategy will probably result in some data loss because there will normally be a gap between the most recent backup and the time of reimaging, recent backups will minimize data loss if no other remedy can be found.

10. **Deploy anti-phishing and anti-ransomware solutions**

    There are very good solutions that can be deployed on-premises or in the cloud that can detect phishing and spearphishing attempts, ransomware, data exfiltration and a variety of other threats. Every organization should implement solutions that are appropriate to its cyber security infrastructure requirements, but with an emphasis on the ability to detect, isolate and remediate phishing, spearphishing, CEO Fraud/BEC and ransomware threats. DLP is a key element in any cyber security infrastructure because of its ability to reduce or prevent data breaches.

11. **Use good threat intelligence**

    The use of historical and real-time threat intelligence to reduce the potential for infection can be an effective way to reduce the likelihood of an attack or infection. Real-time threat intelligence can offer a strong defense to protect
against access to domains that are known to have a poor reputation and so are more likely to be used by cyber criminals for phishing, spear phishing, ransomware and other forms of attack. Threat intelligence can also be used proactively by cyber security analysts to investigate recent attacks and discover previously unknown threat sources. Plus, historical threat intelligence – such as a record of Whois data that includes information on who has owned domains in the past – can be of use in conducting cyber crime investigations.

12. **Implement data-centric protection of all high value data**
   At the end, no matter the cyber security precautions taken by an organization to stop an intrusion, a sophisticated cyber attack may get through cyber defenses. Organizations should implement data-centric protection of their most valuable data so that if attackers get through, the information captured will be unusable. New encryption technologies such as Format-Preserving Encryption (FPE) are easy to use and simple to maintain and can protect high value data at rest, in-use or in-motion, ensuring protection in all use cases. Recently, FPE was standardized by the National Institute of Standards and Technology (NIST) of the US Department of Commerce.

13. **Encrypt sensitive email communications**
   The disclosure of sensitive email communications has been central to some of the most high-profile data breaches in recent memory. Corporations should broadly leverage email encryption for protection of all internal and external emails. Either by the automated trigger of a DLP or by user initiation, email encryption should be added as a standard tool for fighting phishing by making sensitive data useless to the attackers. Look for a solution that encrypts email end-to-end, from originator to recipient on any desktop or mobile device. Some email encryption solutions can also be used to encrypt all data flowing into a cloud-office application provider, including files used in collaboration.

14. **Consider the use of behavior analytics**
   Behavior analytics examines the normal behavior patterns of employees across an organization and, when a divergence is noted – for example, when the user account accesses applications not previously accessed, accesses data at unusual times of the day or night or from foreign locations, or there is an increase in some other unusual activity – an exception is raised for further investigation, or access is immediately blocked. Unusual behavior could signal an employee going rogue, a malware attack, the presence of compromised credentials or some other problem, thereby enabling early detection and risk mitigation.

**SUMMARY**

Phishing, spear phishing, CEO Fraud/BEC and ransomware represent serious threats to any organization because they can be used to steal finances, extort ransom payments, exfiltrate intellectual property, disrupt business operations and, in extreme cases, actually put a company out of business. These problems are getting worse over time because cyber criminals can easily exploit organizations that have not deployed appropriate cyber security solutions and that have not adequately trained their users about best practices for dealing with email, social media and other business systems. However, there are robust cyber security solutions and best practices that can be implement to reduce dramatically the chance that a phishing, spear phishing, CEO Fraud/BEC or ransomware attack will be successful. Deploying these solutions and implementing best practices must be a high priority for every organization.
SPONSOR OF THIS WHITE PAPER

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. Visit https://phishme.com/ to learn more.
No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader’s compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, “Laws”) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

REFERENCES

ii http://www.techrepublic.com/article/hr-managers-beware-ransomware-could-be-your-next-job-applicant/
iii http://arstechnica.com/security/2017/01/more-than-10000-online-databases-taken-hostage-by-ransomware-attackers/
iv http://www.information-age.com/new-ransomware-offers-victims-free-decryption-key-123463585/
xi Source: Intel Security as noted in the Verizon 2016 Data Breach Investigation Report
xiii http://fraudwatchinternational.com/all/what-are-phishing-kits/
xiv http://www.enterprisetimes.co.uk/2016/05/20/clever-cerber-ransomware-attack-spotted/
xv http://www.itproportal.com/features/7-security-predictions-for-2017/
xvi Osterman Research extrapolation based on January-September 2016 APWG data
xviii Source: An ISTR Special Report: Ransomware and Businesses 2016
xxi http://www.healthcareitnews.com/slideshow/ransomware-see-hospitals-hit-2016?page=1
xxii https://www.helphousesecurity.com/2016/07/27/ransomware-healthcare-industry/
xxiv http://betanews.com/2017/01/17/uk-health-ransomware/
xxv http://www.trendmicro.co.uk/vinfo/uk/security/research-and-analysis/predictions/2017
xxvi https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/
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.
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.

Report Data Demographics

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.

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 phishing attempts. Throughout the report, we will refer to scenarios and themes as we assess behavior across multiple industries.

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%.
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. 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.

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

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.

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.

### 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 7: Components of Complexity](image)

<table>
<thead>
<tr>
<th>Components of Complexity</th>
<th>Business</th>
<th>Personal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>Charity</td>
<td>Fear</td>
</tr>
<tr>
<td>Emotional Motivators</td>
<td>Curiosity</td>
<td>Personal Connection</td>
</tr>
<tr>
<td></td>
<td>Entertainment</td>
<td>Opportunity</td>
</tr>
<tr>
<td>Technical Difficulty</td>
<td>Reward</td>
<td>Reward</td>
</tr>
<tr>
<td></td>
<td>Urgency</td>
<td>Urgency</td>
</tr>
</tbody>
</table>

![Figure 8: Average response rates by Motivator](image)
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.

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.

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 other ransomware varieties, making it imperative to implement a phishing simulation using a Locky.

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:

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:

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
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.
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](image)

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 an 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

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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>The Organization proactively responds to threats and mitigates them</td>
</tr>
<tr>
<td>Yellow</td>
<td>Users are alert ----&gt; inspecting emails ----&gt; reporting threats</td>
</tr>
<tr>
<td>Orange</td>
<td>Users are alert ----&gt; inspecting emails for threats</td>
</tr>
<tr>
<td>Red</td>
<td>Users exhibit a complete lack of awareness of phishing threats</td>
</tr>
</tbody>
</table>

Figure 19: Reporting rates by company size

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.

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.
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.

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.  
- The Mandiant APT1 Report cites spear phishing as the Chinese hacking group APT1’s most common attack method.  
- In their 2013 report, Verizon traced 95% of state-affiliated espionage attacks to phishing.

**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).

---

### High-response Scenarios

<table>
<thead>
<tr>
<th>Scenario Response Rates by Industry</th>
<th>File from Scanner</th>
<th>Locky Phish</th>
<th>Unauthorized Access</th>
<th>eCard Alerts</th>
<th>Package Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare</td>
<td>48.9%</td>
<td>48.7%</td>
<td>48.4%</td>
<td>48.2%</td>
<td>49.1%</td>
</tr>
<tr>
<td>Insurance</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
</tr>
<tr>
<td>Pharma/Biotech</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
</tr>
<tr>
<td>Energy</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
</tr>
<tr>
<td>Retail</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
</tr>
<tr>
<td>Utilities</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
</tr>
<tr>
<td>Technology</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
</tr>
<tr>
<td>Non-Profit</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
</tr>
<tr>
<td>Grand Total</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
<td>48.9%</td>
</tr>
</tbody>
</table>

### Financial Information

<table>
<thead>
<tr>
<th>Scenario Response Rates by Industry</th>
<th>Healthcare</th>
<th>Insurance</th>
<th>Consulting</th>
<th>Manufacturing</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Info</td>
<td>31.5%</td>
<td>27.3%</td>
<td>26.6%</td>
<td>24.4%</td>
<td>19.7%</td>
</tr>
<tr>
<td>Technology</td>
<td>31.5%</td>
<td>27.3%</td>
<td>26.6%</td>
<td>24.4%</td>
<td>19.7%</td>
</tr>
<tr>
<td>Legal Services</td>
<td>31.5%</td>
<td>27.3%</td>
<td>26.6%</td>
<td>24.4%</td>
<td>19.7%</td>
</tr>
<tr>
<td>Retail</td>
<td>31.5%</td>
<td>27.3%</td>
<td>26.6%</td>
<td>24.4%</td>
<td>19.7%</td>
</tr>
<tr>
<td>Government</td>
<td>31.5%</td>
<td>27.3%</td>
<td>26.6%</td>
<td>24.4%</td>
<td>19.7%</td>
</tr>
<tr>
<td>Financial</td>
<td>31.5%</td>
<td>27.3%</td>
<td>26.6%</td>
<td>24.4%</td>
<td>19.7%</td>
</tr>
<tr>
<td>Media</td>
<td>31.5%</td>
<td>27.3%</td>
<td>26.6%</td>
<td>24.4%</td>
<td>19.7%</td>
</tr>
<tr>
<td>Media</td>
<td>31.5%</td>
<td>27.3%</td>
<td>26.6%</td>
<td>24.4%</td>
<td>19.7%</td>
</tr>
<tr>
<td>Consulting</td>
<td>31.5%</td>
<td>27.3%</td>
<td>26.6%</td>
<td>24.4%</td>
<td>19.7%</td>
</tr>
<tr>
<td>Consulting</td>
<td>31.5%</td>
<td>27.3%</td>
<td>26.6%</td>
<td>24.4%</td>
<td>19.7%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>31.5%</td>
<td>27.3%</td>
<td>26.6%</td>
<td>24.4%</td>
<td>19.7%</td>
</tr>
<tr>
<td>Technology</td>
<td>31.5%</td>
<td>27.3%</td>
<td>26.6%</td>
<td>24.4%</td>
<td>19.7%</td>
</tr>
<tr>
<td>Non-Profit</td>
<td>31.5%</td>
<td>27.3%</td>
<td>26.6%</td>
<td>24.4%</td>
<td>19.7%</td>
</tr>
<tr>
<td>Technology</td>
<td>31.5%</td>
<td>27.3%</td>
<td>26.6%</td>
<td>24.4%</td>
<td>19.7%</td>
</tr>
<tr>
<td>Grand Total</td>
<td>31.5%</td>
<td>27.3%</td>
<td>26.6%</td>
<td>24.4%</td>
<td>19.7%</td>
</tr>
</tbody>
</table>

### Scenario Response Rates by Industry

<table>
<thead>
<tr>
<th>Scenario Response Rates by Industry</th>
<th>Bonus Agreement</th>
<th>Manager Eval.</th>
<th>Can't Send, File Size</th>
<th>Corporate Reward</th>
<th>Free Lunch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media</td>
<td>42.9%</td>
<td>42.6%</td>
<td>41.3%</td>
<td>31.3%</td>
<td>30.9%</td>
</tr>
<tr>
<td>Energy</td>
<td>42.9%</td>
<td>42.6%</td>
<td>41.3%</td>
<td>31.3%</td>
<td>30.9%</td>
</tr>
<tr>
<td>Word Documents</td>
<td>42.9%</td>
<td>42.6%</td>
<td>41.3%</td>
<td>31.3%</td>
<td>30.9%</td>
</tr>
<tr>
<td>File from Scanner</td>
<td>42.9%</td>
<td>42.6%</td>
<td>41.3%</td>
<td>31.3%</td>
<td>30.9%</td>
</tr>
<tr>
<td>View Point</td>
<td>42.9%</td>
<td>42.6%</td>
<td>41.3%</td>
<td>31.3%</td>
<td>30.9%</td>
</tr>
<tr>
<td>Digital Fax</td>
<td>42.9%</td>
<td>42.6%</td>
<td>41.3%</td>
<td>31.3%</td>
<td>30.9%</td>
</tr>
<tr>
<td>Time Off Request</td>
<td>42.9%</td>
<td>42.6%</td>
<td>41.3%</td>
<td>31.3%</td>
<td>30.9%</td>
</tr>
<tr>
<td>File from Scanner</td>
<td>42.9%</td>
<td>42.6%</td>
<td>41.3%</td>
<td>31.3%</td>
<td>30.9%</td>
</tr>
<tr>
<td>View Point</td>
<td>42.9%</td>
<td>42.6%</td>
<td>41.3%</td>
<td>31.3%</td>
<td>30.9%</td>
</tr>
<tr>
<td>Word Documents</td>
<td>42.9%</td>
<td>42.6%</td>
<td>41.3%</td>
<td>31.3%</td>
<td>30.9%</td>
</tr>
<tr>
<td>File from Scanner</td>
<td>42.9%</td>
<td>42.6%</td>
<td>41.3%</td>
<td>31.3%</td>
<td>30.9%</td>
</tr>
<tr>
<td>View Point</td>
<td>42.9%</td>
<td>42.6%</td>
<td>41.3%</td>
<td>31.3%</td>
<td>30.9%</td>
</tr>
<tr>
<td>Grand Total</td>
<td>42.9%</td>
<td>42.6%</td>
<td>41.3%</td>
<td>31.3%</td>
<td>30.9%</td>
</tr>
</tbody>
</table>

### Scenario Response Rates by Industry

<table>
<thead>
<tr>
<th>Scenario Response Rates by Industry</th>
<th>Unauthorized Access</th>
<th>eCard Alerts</th>
<th>Package Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Nwsl.</td>
<td>22.3%</td>
<td>21.9%</td>
<td>21.3%</td>
</tr>
<tr>
<td>Digital Fax</td>
<td>21.5%</td>
<td>21.9%</td>
<td>21.3%</td>
</tr>
<tr>
<td>Package Delivery</td>
<td>21.5%</td>
<td>21.9%</td>
<td>21.3%</td>
</tr>
<tr>
<td>Happy Valentine</td>
<td>20.8%</td>
<td>21.9%</td>
<td>21.3%</td>
</tr>
<tr>
<td>Inbox Over Limit</td>
<td>19.5%</td>
<td>21.9%</td>
<td>21.3%</td>
</tr>
<tr>
<td>Grand Total</td>
<td>24.1%</td>
<td>21.9%</td>
<td>21.3%</td>
</tr>
</tbody>
</table>

### Scenario Response Rates by Industry

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Info</td>
<td>23.4%</td>
<td>20.5%</td>
<td>18.0%</td>
<td>17.5%</td>
<td>16.5%</td>
<td>15.6%</td>
</tr>
<tr>
<td>Time Off Request</td>
<td>23.4%</td>
<td>20.5%</td>
<td>18.0%</td>
<td>17.5%</td>
<td>16.5%</td>
<td>15.6%</td>
</tr>
<tr>
<td>Halloween Cost</td>
<td>23.4%</td>
<td>20.5%</td>
<td>18.0%</td>
<td>17.5%</td>
<td>16.5%</td>
<td>15.6%</td>
</tr>
<tr>
<td>Forgot Attach.</td>
<td>23.4%</td>
<td>20.5%</td>
<td>18.0%</td>
<td>17.5%</td>
<td>16.5%</td>
<td>15.6%</td>
</tr>
<tr>
<td>Unauthorized Act.</td>
<td>23.4%</td>
<td>20.5%</td>
<td>18.0%</td>
<td>17.5%</td>
<td>16.5%</td>
<td>15.6%</td>
</tr>
<tr>
<td>Scanned File</td>
<td>19.6%</td>
<td>17.9%</td>
<td>17.2%</td>
<td>16.5%</td>
<td>16.5%</td>
<td>15.6%</td>
</tr>
<tr>
<td>Word Documents</td>
<td>19.6%</td>
<td>17.9%</td>
<td>17.2%</td>
<td>16.5%</td>
<td>16.5%</td>
<td>15.6%</td>
</tr>
<tr>
<td>Pokèmon Go Pol.</td>
<td>19.6%</td>
<td>17.9%</td>
<td>17.2%</td>
<td>16.5%</td>
<td>16.5%</td>
<td>15.6%</td>
</tr>
<tr>
<td>Black Hat</td>
<td>19.6%</td>
<td>17.9%</td>
<td>17.2%</td>
<td>16.5%</td>
<td>16.5%</td>
<td>15.6%</td>
</tr>
<tr>
<td>Digital Fax</td>
<td>19.6%</td>
<td>17.9%</td>
<td>17.2%</td>
<td>16.5%</td>
<td>16.5%</td>
<td>15.6%</td>
</tr>
<tr>
<td>APT1</td>
<td>19.6%</td>
<td>17.9%</td>
<td>17.2%</td>
<td>16.5%</td>
<td>16.5%</td>
<td>15.6%</td>
</tr>
<tr>
<td>Grand Total</td>
<td>19.6%</td>
<td>17.9%</td>
<td>17.2%</td>
<td>16.5%</td>
<td>16.5%</td>
<td>15.6%</td>
</tr>
</tbody>
</table>
THE PHISHME ADVANTAGE – ROI

Measuring the return on investment (ROI) from your PhishMe solution is simple and easy. The most obvious and significant impact is the dramatic reduction you will see in the overall risk of a phishing attack both getting past your perimeter protection and your skilled users but there are other ways to measure your investment:
Measuring the return on investment (ROI) from your PhishMe solution is simple and easy. The most obvious and significant impact is the dramatic reduction you will see in the overall risk of a phishing attack both getting past your perimeter protection and your skilled users but there are other ways to measure your investment:

**Monetary ROI**

Customers can realize monetary ROI from PhishMe by reducing their overall risk to phishing and other security threats. Adversaries have successfully employed phishing tactics to steal intellectual property, personally identifiable information, and other sensitive information that can harm an organization's competitive advantage and reputation. The costs of a data breach vary and can range from hundreds of thousands to billions of dollars. The costs of incident response and mitigation will be, at a minimum, a few hundred thousand to millions of dollars. While the loss of intellectual property and sensitive information can have a severe financial and legal impact on an organization. PhishMe's solutions lower the likelihood of users being susceptible to various security risks while also increasing your IT Security team's ability to quickly and accurately identify and mitigate an attack in progress. PhishMe's experience sending simulated phishing attacks to over 20 million unique users has shown that prior to training, organizations show a reduction in repeat "clicker" susceptibility to phishing of 95%. Download our Phishing Susceptibility Report for the full details.

**Time ROI**

There is also the opportunity cost view of measuring the ROI from PhishMe. Specifically, this includes the amount of time and resources your IT organization must commit when responding to user reports of falling for phishing attacks, resetting passwords, slow computer performance caused by malware, and unwinding the damage caused by such incidents. The internal cost to identify, respond, triage and recover compromised systems can place an unbearable strain on the IT service organization. Most firms find that cutting the need for this effort by 50% to 80% results in significant savings of time, labor and energy, all of which can be focused on core business operations that can help your business grow.

PhishMe's innovative training solutions will save your entire organization time and resources while increasing employee productivity. On average, PhishMe simulated training exercises conducted periodically takes 1/30th as much time as traditional computer-based training (CBT).
Final Thoughts for Phishing Defense

Phishing emails, the No. 1 form of cyberattacks today, are often carefully crafted and targeted to specific employees. If employees respond by clicking on a link or an attachment or allowing access to secure information, attackers gain a foothold in corporate networks and have the potential to cause catastrophic damage.

Employees who have never seen the carefully worded requests and demands in phishing emails can’t be expected to identify and ignore them, let alone report them to IT teams attempting to stop threats.

PhishMe believes employees should be armed with knowledge, behavioral conditioning and the ability to easily report threats as key components of a comprehensive phishing defense program. We implement these strategies by blending malware intelligence with behavioral data from actual and potential victims. Our customers believe in our programs because they know that understanding and conditioning employee behavior around email phishing attacks improves cybersecurity, shortens incident response time and reduces the risk of compromising company assets and information.

To educate your employees and protect your company from cyberattacks, sign up for our free threat alerts or check out our library of complimentary computer-based (CB) training.

For more information about our anti-phishing programs or questions about our Phishing Defense Guide, contact PhishMe at info@phishme.com.

You can also sign up for a risk-free demo of our phishing defense solutions on our website.

Contact

w phishme.com/contact
p 703.652.0717
a 1608 Village Market Blvd, SE #200 Leesburg, VA 20175
e info@phishme.com

Our Global Locations

New York | San Francisco | Birmingham
London | Dubai UAE | Singapore | Melbourne