Cofense Annual **Phishing Report**

2019

COFENSE.COM

COFENSE ANNUAL PHISHING REPORT 2019

When users report suspicious emails they become active defenders, a powerful force united to stop phishing attacks. Our new study shows why email reporting—human action, not mere awareness or technical controls—is the beating heart of a strong phishing defense.

Want to view this online?

VIEW WEBPAGE >

FAST-FORWARD THROUGH THE STORY

- 90 percent of the phish Cofense™ analyzes for customers are found in environments using secure email gateways (SEGs).
- Thus, user reporting of real phish is the true goal of phishing awareness.
- Customers using the Cofense Reporter™ button show strong phishing resiliency. In simulation exercises, their users report phishing more than twice as often as they fall susceptible.
- More frequent phishing simulations, in particular a monthly cadence, drive down susceptibility and improve reporting.
- Customers with 12 or more simulations per year have a 2.05 resiliency rate (the ratio of reporting to susceptibility), compared to 0.92 for those running fewer than 12.
- Real phish are the real problem, so simulations need to be relevant.
- Customers that include 'Active Threat' scenarios in their simulation mix have a resiliency rate of 2.72–versus 1.71 for those that don't include them.
- Frequent, relevant simulations and a focus on reporting = higher resiliency and a better phishing defense.

"When in doubt, report. Tell me. That's the biggest thing. Just hit the button, please, for the love of God."

- SOC Analyst, Regional Healthcare Company

Source: Cofense Customer Interview, Publication Pending

WHAT WE BELIEVE

For years, Cofense (formerly PhishMe) has been preaching the value of educating users to report suspicious emails. The idea is simple: with rigorous, frequent practice, any user in any department can learn to spot a phish and report it to security teams for faster investigation.

It's a myth, pure and simple, that humans are the weakest link. A workforce not educated in spotting and reporting phish will, of course, be vulnerable. But the same employees, when properly conditioned, are the best defense when perimeter controls, even the best, prove fallible.

Our approach stands in contrast to an over-reliance on security technology. Secure email gateways, an important layer of phishing defense, catch many but not all phishing emails. Cofense reported earlier this year that 90 percent of the phish we verify for customers are found in environments using one or more SEG. Check our blog: we're constantly reporting on SEG misses, examining the ingenious methods attackers devise to get past the perimeter.

90%

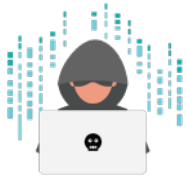
OF THE PHISH COFENSE VERIFIES FOR CUSTOMERS ARE FOUND IN ENVIRONMENTS USING **SECURE EMAIL GATEWAYS.**

74%

OF THESE ARE **CREDENTIAL PHISH.**

8.5%

ARE BUSINESS EMAIL COMPROMISE **(BEC).**



2%

ARE SCAMS **(INCLUDING SEXTORTION).**

Source: Cofense Phishing Defense Center™

Every phish in the stats above was reported by a human. A user reported an email to a security team, which used technology and expertise to verify and respond. In this way, user reporting links phishing awareness to response and remediation. Some approaches see awareness as the end goal. But what about taking action? Focusing on click rates instead of user reporting is like teaching people to see something without saying something. This approach often stems from compliance initiatives, where the idea is to check a box—"90 percent of employees took the annual CBT"—which isn't the same as preparing users to stop real attacks.

Reporting is a learned behavior, a kind of conditioning, which builds muscle memory so users won't think twice about raising a hand. As we'll see in the next section, when users report they also help the security awareness team quantify their program's impact.

"Building a culture where users can report phishing attempts (including ones that that are clicked on) gives you vital information"

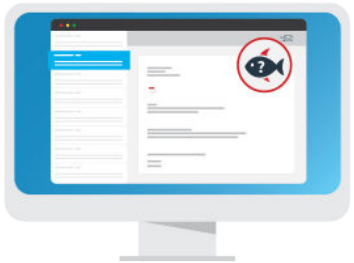
-

THE DIFFERENCE REPORTING MAKES

Ten million phishing simulations a month are sent through Cofense PhishMe™, our phishing awareness solution. And 20 million users are equipped to report phishing via Cofense Reporter™, our email toolbar button. The data we gather from these solutions sheds light on user susceptibility, reporting, and resiliency.

As a metric, reporting helps to track desired behavioral change. Since no one will ever achieve a zero click rate, awareness programs need to empower users to give the SOC visibility into threats, sometimes long before any threat intelligence feed alerts the organization.

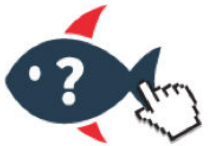
REPORTING BUTTON: MAKE IT EASY, MAKE IT BETTER



With Cofense Reporter, users can report suspicious emails with one click. The deployment of a reporting button, especially when integrated with the phishing simulation platform, provides two primary benefits:

1. It allows you to measure true behavioral change, along with user engagement in your phishing awareness programs. Remember, when it comes to susceptibility, or click rate, there is no certainty. There's simply no way of being 100 percent sure that a user who didn't click made a conscious decision. Perhaps the email wasn't read at all. Reporting a simulation is a conscious and deliberate action. It provides an unambiguous indicator: how well is the end user engaging in your programs? Is the user actively behaving in ways that improve overall security?

2. When phishing threats bypass perimeter controls and are delivered to a user's inbox, those controls have failed. The only sensors you have now are end users themselves. The presence of a reporting button in the email client reinforces the need to be mindful of phishing threats. It's a simple way for the user to take defensive action.



Deployment of a reporting button keeps security awareness teams happy—they gain valuable metrics that demonstrate the effectiveness of their programs. And SOC teams are happy to get visibility of threats they would otherwise be blind to.

Let's start with a couple of top-level views, comparing customers that use the Cofense Reporter button to those that don't.

Simulation Performance, Customers Using Cofense Reporter

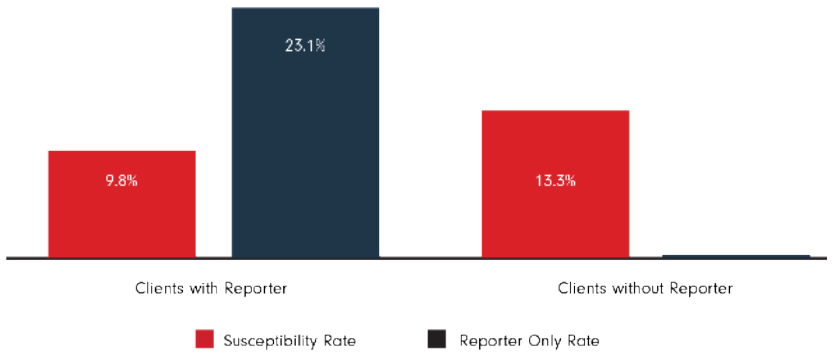
June 2018 - July 2019

Susceptibility: **9.8%**

Reported Only: **23.1%**

Resiliency: **2.35**

As you can see, the reporting button makes a positive difference: more than twice as many people reported instead of clicking. Customers not using it, who report emails manually, get an incomplete view of employee performance. If you tried to compare the stats above to those for customers that haven't deployed Cofense Reporter, the chart would look like this:



No button, no instant metrics. No reporting or resiliency rate for customers without the button. You get only part of the picture—the least helpful part, the 12-month susceptibility rate. The security awareness team is left to compile data manually, while the SOC and helpdesk have the unhappy task of rounding

up reported emails, during simulations and otherwise. The absence of a button means more work and mediocre metrics. Cofense Reporter, on the other hand, automatically feeds the metrics into the PhishMe platform for easy analysis.

"There are only so many ways to tell people what to look for in emails. The best way to help them is through reiteration. When they keep seeing simulations every month and practicing smart behavior, including reporting suspicious messages, they're going to be more on top of phishing."

- Security Awareness Manager, Global Manufacturing Company

Source: Cofense Case Study, Publication Pending

The next chart shows steady year-over-year improvement.

Year-Over-Year Performance, Customers Using Cofense Reporter

	Susceptibility	Reported Only	Resiliency
2016	12.6%	16.5%	1.32%
2017	11.0%	20.4%	1.86%
2018	10.5%	21.6%	2.06%
2019 *(through July)*	9.2%	24.1%	2.63%

It's interesting to see that Cofense Reporter appears to help lower susceptibility. We're not exactly sure why, but it could be that the button is simply a visual reminder to click with care. Or, as one customer told us, "users need something good to click on" and when you provide it, bad clicks drop. Regardless of the reason, Cofense Reporter drives better inbox behavior across the board.

The Cofense Reporter button is a game-changer. A large pharmaceutical company deployed it to a subset of users before rolling it out companywide.

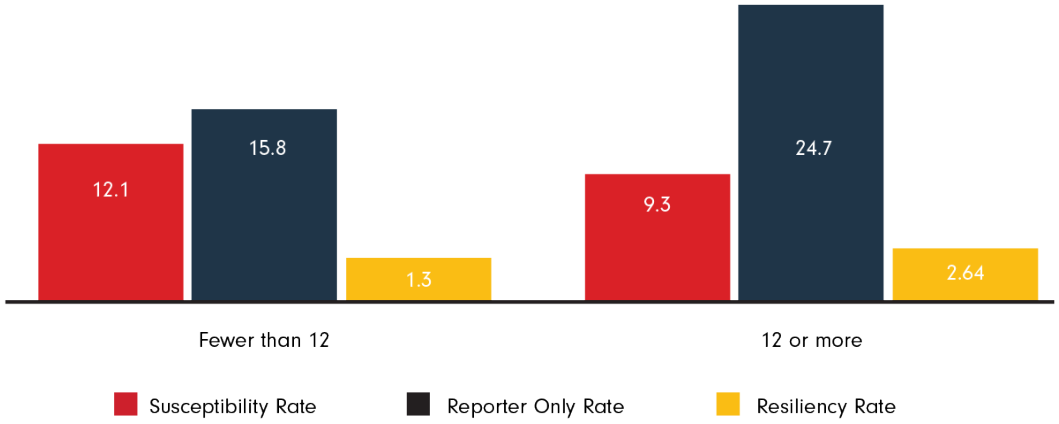
Their reporting rate was 11x higher than the rate for users without the button.

FREQUENT SIMULATIONS = BETTER REPORTING AND RESILIENCY

Practice makes better, as the following chart illustrates.

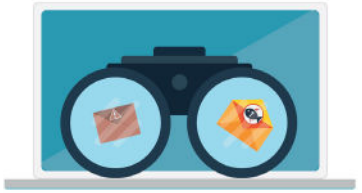
12 or More Simulations vs. Fewer than 12, Customers Using Cofense Reporter

June 2018 - July 2019



Customers running monthly simulations have a reporting rate nearly double that of customers that simulate less frequently. The resiliency score is more than double, with susceptibility a good deal lower.

A GLIMPSE AT 'JUST IN TIME' SCENARIOS



The following figures support the adage that timing is everything. It shows how Responsive Delivery, a new feature to Cofense PhishMe, is jump-starting engagement during simulations. Responsive Delivery sends simulations only when users are active in email—when they're more likely to pay attention, engage with the email, and learn something.

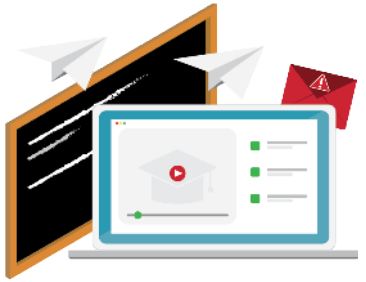
13%
SUSCEPTIBILITY

45%
REPORTED ONLY

3.44
RESILIENCY

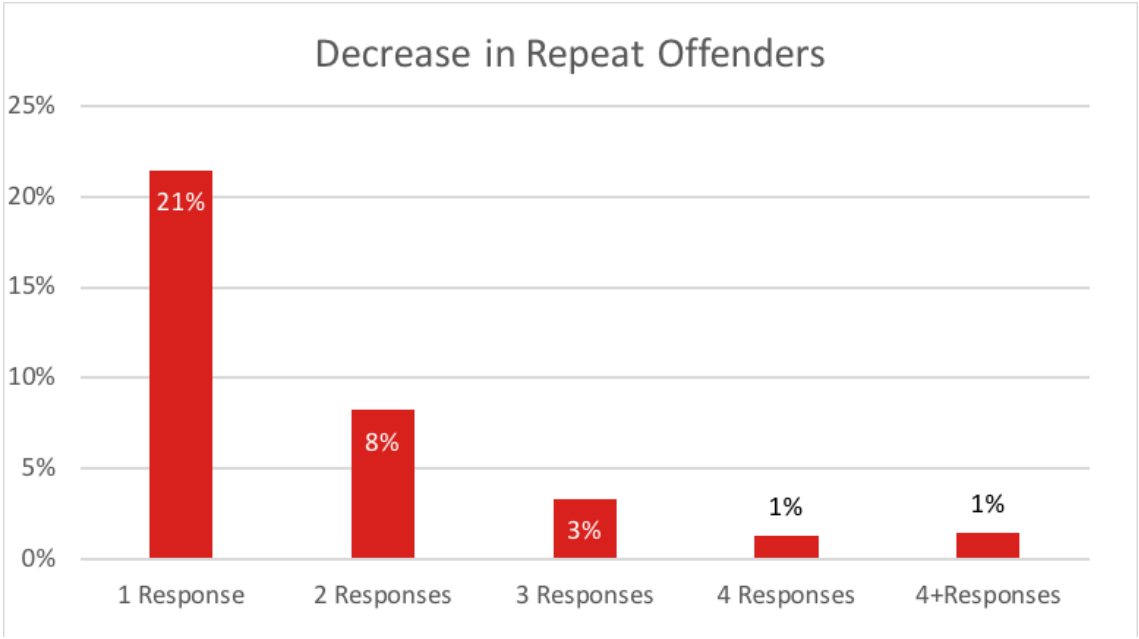
While these are preliminary numbers, compiled when Responsive Delivery was beta-tested and launched, they suggest the power of sending simulations at just the right time. While susceptibility during this period was a little over 10 percent, the reporting and resiliency rates were exemplary. Remember that the reporting rate for all Cofense customers using the Reporter button (June 2018 - July 2019) was 23.1 percent. The use of Responsive Delivery increased the reporting rate to 44.7 percent.

REPEAT OFFENDERS HAVE A LEARNING CURVE



For some users, it takes a few bad clicks before the "Aha!" moment happens. Repeat offenders—users that click during more than one simulation—need a little more practice, especially if they're in high-risk functions like finance or human resources.

One tactic some of our customers use: after running a companywide simulation, they follow up a few weeks later by targeting users that fell susceptible during the past few campaigns. This gives them a chance to flex muscle memory and apply what they've (hopefully) learned.



This pattern has held up over time. For example, our 2015 report showed that enterprises users went from a 26 percent click rate on the first simulation to well under 10 percent on their next couple of tries.

"I had a blinding flash of the obvious: I realized I was converting our clickers into reporters, that the behavior I wanted to reinforce was reporting... A machine cannot apply a non-linear approach to a problem, but a human being can make decisions that are a lot more intricate."

- Cyber-Security Awareness Evangelist, Regional Utility

Source: Cofense Customer Interview

THE DIFFERENCE RELEVANCE MAKES

Besides being frequent, phishing simulations should be relevant. Simulations ought to reflect both the attacks an organization sees and the overall threat landscape. And given time and budget constraints, every simulation ought to count.

Ideally, security awareness and operations teams collaborate and everyone wins. Awareness program managers have confidence that simulations ar relevant, while the SOC receives more useful reports from well-conditioned users. For further relevance, Cofense has rolled out Smart Suggest, a feature that uses an advanced algorithm and best practices to choose from nearly 2,000 Cofense PhishMe templates and recommend scenarios based on program and industry experience.

Most Popular Phishing Scenarios in Cofense PhishMe

June 2018 - July 2019

Year	Scenarios Launched
Account Security Alert	1,049
Package Delivery	1,043
File from Scanner	931
Order Confirmation	862
Social Media Invitation	832
Unauthorized Access	613
Inbox Over the Limit	609
Remote Work Policy	507
Verify Your Account	491
Undelivered Messages	433
Password Survey (Data Entry)	420
New Voicemail	376
Reset Your Password	361
Business Cards	292
Voicemail via Email	284
Summer Dress Code	280
Someone Has Your Password	261
Secure Email	254
Mandatory Compliance Training (Data Entry)	249

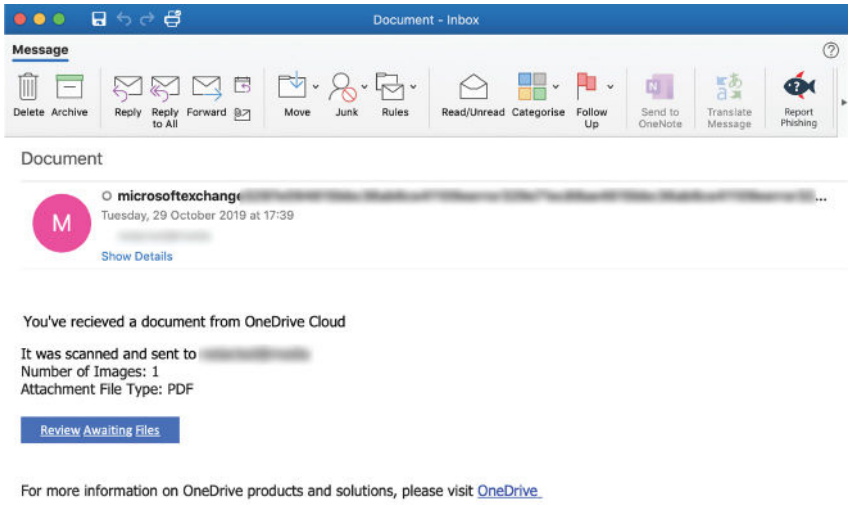
DON'T FORGET CREDENTIAL PHISH (ATTACKERS WON'T)

Most of the top scenarios in the chart above mimic click-only phish, designed to lure users to click on embedded links. A much lower percentage of scenarios ask users to enter credentials like their network passwords, a telltale sign of credential phishing.

> **74%** of Real Phish Are Credential Phish
>
> But Credential Phish Are Only **17.2%** of Simulations

During the first half of 2019, three out of four phish we saw in customers' environments were credential phish. With stolen user names and passwords, a threat actor has access to a corporate network and can pass for a legitimate user. It's one more reason to condition users to report the types of phishing your organization sees the most—real phish, not random possibilities.

Here's an example of credential phishing:



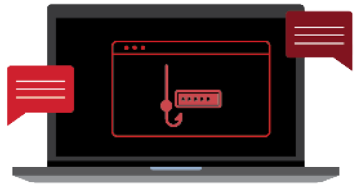
Source: Cofense Phishing Defense Center, January 1-July 31, 2019

A key part of our program is training our users to identify and react appropriately to real-world phishing attacks...We work in critical infrastructure and see nation-state attacks left and right. We can't rely on government to be our first line of defense, so our employees have to provide that."

- Cyber-Program Director, Multinational Utility

Source: Cofense Customer Interview, Publication Pending

BEC, SEXTORTION, AND FILE-SHARING PHISH



Besides wire fraud, BEC attacks have recently shifted to payroll diversion scams targeting HR and finance departments. This wrinkle hits employees where they live, in their wallets.

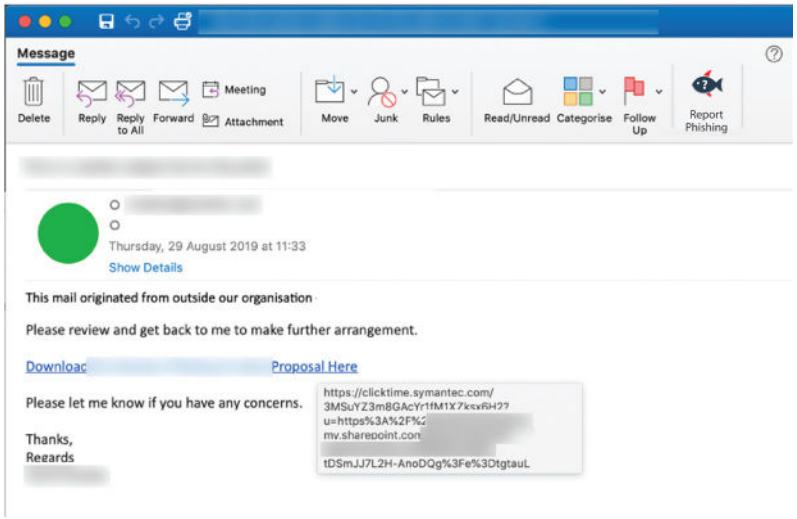
Likewise, sextortion scams are a growing problem. Sextortion emails use fear and panic to extort a ransom payment, usually in bitcoin. Cofense Labs is monitoring a sextortion botnet with over 300 million compromised accounts. In the first half of 2019 alone, our researchers analyzed over 7 million email addresses impacted by sextortion. Cofense Labs assessed that more than $1.5 million in payments were made to bitcoin wallets associated with sextortion campaigns.

Attackers are also following businesses to the cloud, with greater abuse of filesharing services like SharePoint and OneDrive. Why? Because they're legitimate and trusted, SEGs don't usually block them. Users receiving an email with a link to a SharePoint file often won't think twice before clicking.

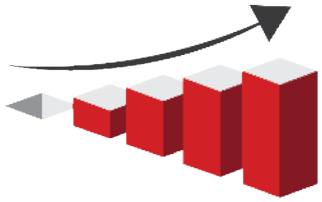
76%

OF FILE SHARING ATTACKS TARGET
SHAREPOINT AND ONE DRIVE.
March 2018 - March 2019

Below is an example of a phish that abuses Sharepoint:



'ACTIVE THREAT' SCENARIOS BOOST OVERALL PERFORMANCE

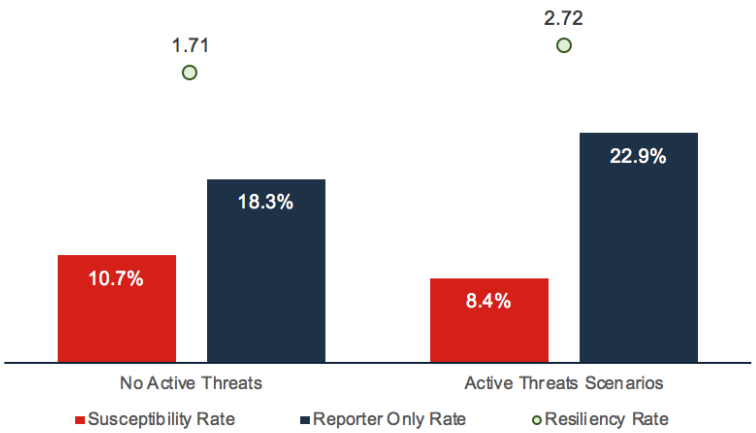


Another way our customers make their simulations relevant: using Active Threat scenarios based on input from Cofense Intelligence™, who along with Cofense Labs form our threat-intel and research arm. These teams have a unique perspective on phishing threats in the wild—campaigns and associated tactics, techniques, and procedures (TTPs)—as well as threats evading perimeter controls to reach users' inboxes.

The chart below compares overall performance across all simulations over a 12-month period: customers that use these scenarios in their mix versus those that don't.

Customer Performance: Mixing in 'Active Threat' vs. No 'Active Threat'

June 2018 - July 2019



Customers using Active Threat scenarios ran the table: the reporting rate was 4.6 percentage points higher, resiliency was 1.01 higher, and susceptibility was 2.3 lower. Threat actors study security controls, including secure email gateways, to adjust their tactics and keep a step ahead. This makes it urgent for awareness programs to simulate real threats. Use of Active Threat scenarios, versus random scenario selection, is the sort of refinement seen in mature programs .

"The awareness program has absolutely helped to stop real phishing attacks .... Because reporting suspicious emails is now centralized through Cofense Reporter, we can see patterns that signify phishing campaigns, versus dealing with reports as one-off incidents. We now know when we've got a real threat that we need to deal with right away."

- Chief Information Security Officer, National Healthcare Company

Source: Cofense Case Study

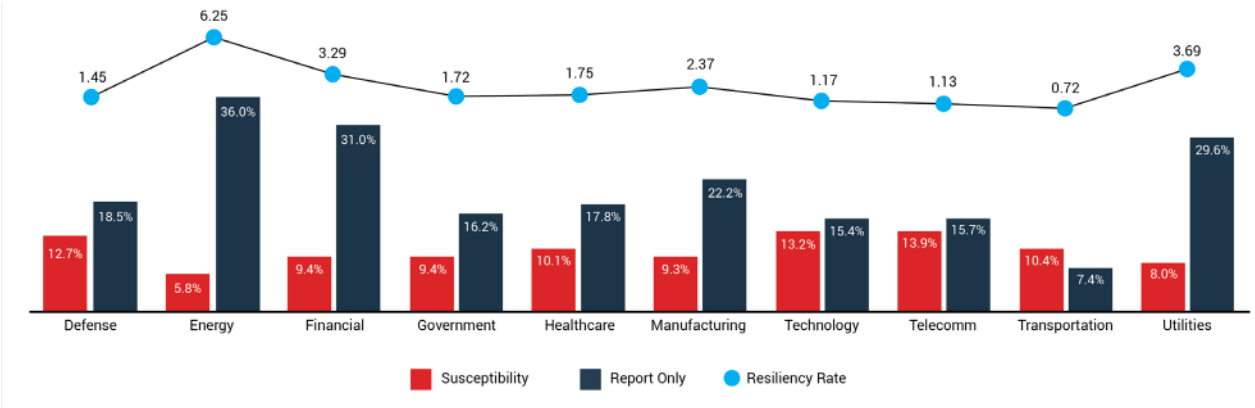
ANOTHER WAY TO BE RELEVANT: INDUSTRY BENCHMARKING

Boards of directors often ask: "How does our awareness program stack up within their industry? Cofense PhishMe provides industry benchmarks, in our Board Reports among other formats.

Below is a snapshot across industries classified as critical infrastructure. Because these industries have more regulatory pressure, they run more simulations. Moreover, industries like energy and finance are frequent targets of nation-state actors.

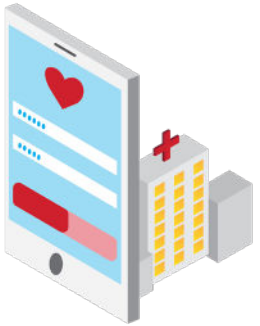
Performance in 10 Critical Infrastructure Industries

June 2018-July 2019



Comparing these numbers to 2018 performance, we see that energy is still tops, driving an already outstanding rate of 6.19 even higher, to 6.25. Manufacturing improved from 1.66 to 2.37 and financial services stepped up from 1.38 to 1.91. Healthcare, another industry threat actors train their sights on, showed a slight bump from 1.63 to 1.75. Continued public scrutiny and regulatory mandates will likely compel healthcare companies to raise their game in the coming year.

CASE STUDY SNAPSHOT: HEALTHCARE



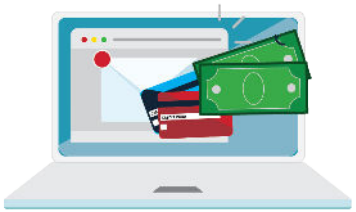
After suffering a phishing attack that led to a brief network shutdown, a healthcare CISO worked with Cofense to launch its awareness program.

Solutions and Results:

- Monthly companywide simulations
- Gamified tactics with rewards like Amazon gift cards
- In recent simulations, user reporting has been 3-7 times higher than susceptibility
- Real phish users have reported: credential attacks, malicious URLs, man-in-the-middle attacks

"People are getting the message," said the CISO. "They know how to report and why it's important." Read the full case study.

CASE STUDY SNAPSHOT: FINANCIAL SERVICES



To stop phishing attacks faster, a national financial services company turned to Cofense PhishMe, Cofense Reporter, and Cofense Triage™, our phishing analysis and response solution.

Solutions and results:

- Within a week of implementing the three Cofense solutions, the company used them to stop a phishing attack in just 10 minutes
- The attack was a credential phish that bypassed perimeter security to land in over 200 inboxes
- Multiple users reported the attack right away

"We were able to stop the attack in minutes, not days," said the security awareness manager. "It was a big win for our team." Read the full case study.

LOOKING AHEAD

Our data makes the case for key best practices: frequent simulations, relevant scenarios, and building a culture of reporting. Together, they add up to stronger phishing resiliency.

WHAT IS A GOOD RESILIENCY RATE?

It depends. At a minimum, we recommend aiming for a resiliency score of 1.0—for every user who clicks on a simulation, another reports it. But as you've seen, many industries have a much higher resiliency score. For example, mining has a score of 3.55. Imagine what that means during a real attack. If a targeted phish is delivered to 100 users at a mining customer, on average eight users would be expected to click. However, the SOC gets alerts from 29 users about a potential attack, visibility it might not otherwise have. The team can act before it's too late.

The true value of high resiliency comes when the SOC turns users' reports into actionable intelligence. When the SOC is able to prioritize, analyze, and understand the information users provide, it can take decisive action to neutralize the threat, cutting through the noise to "find bad" quickly. As organizations begin to track resiliency, they should ensure they're tracking other metrics, too:

- Volume of reported emails
- Volume of malicious emails/threats identified
- Time to respond – from initial report to analysis
- Time to analyze
- Time to mitigate

PHISH TESTING IS THE ENEMY OF PHISHING DEFENSE

In phish testing, the idea is to run occasional simulations and establish a baseline. The focus is almost exclusively on click rates, not reporting.

This practice is riddled with problems. The tests are a kind of vulnerability scan for users, but you can't patch users as you would machines. Moreover, due to variables such as timing and scenarios used, the baselines are only so helpful. And in a rapidly changing landscape, where phishing tactics evolve daily, trying for a zero click rate reflects an obsolete mindset. You need to drive reporting, not mere awareness, to give security teams visibility into real threats. If this isn't happening, you're building a false sense of security.

5 reasons why phish testing doesn't work:

1. An over-emphasis on click rates suggests that awareness is the real goal, an isolated activity unconnected to broader cyber-defense.
2. Stressing click rates turns phishing defense into a game of "Gotcha!" Users either pass or fail, with little educational benefit. No wonder too many users find their awareness programs punitive and stop engaging altogether.
3. The goal of higher user reporting gets lost. Instead of concentrating on helping users do the right thing—to say something when they see something—phish testing leads you to believe it's all about the metrics. Data is important, but there's more to phishing defense than obsessing over numbers.
4. Inattention to reporting means missing out on valuable intelligence. When security teams aren't able to operationalize human intel, they're blind to real threats that evade technical controls. Likewise, without steady reporting data, awareness managers can't operationalize click rates or, for that matter, compare results over time. It's pointless to compare one set of test results to another, since over time the users tested and circumstances will change.
5. Infrequent testing can't keep pace with the shifting threat landscape. It's impossible to prepare users for the latest attacker techniques when they only practice a few times yearly.

If your objective is to unite users and security teams against phishing, the better way is to stress reporting and overall phishing defense.

THE 'WEAKEST LINK' MYTH CAN WEAKEN YOUR SECURITY

To embrace the value of user reporting and build real phishing resiliency, security practitioners first need to free their minds. They need to bust the myth that humans are the weakest link, the most frequent point of failure in organizational defense.

Yes, phishing is a human problem. The whole idea is to trick someone. But the technology designed to stop attacks gets fooled itself, every day, by innovative tactics machines don't recognize. Again, if you don't believe this, peruse the Cofense blog, a catalog of technology misses and the active threats they trigger. Or view the Cofense Phishing Threat and Malware Review 2019, which details the cat-and-mouse game threat actors play so well.

Holding fast to the weakest-link myth will hold you back. It will limit the effectiveness of your phishing defense programs. After all, if you don't believe in your people, they can't possibly reach their potential. They won't learn to recognize and report phishing emails. Nor will they give your SOC the visibility it needs to stop a phishing attack before lasting damage is done.

When perimeter technology fails, people must step up. Given the right conditioning, they will. They'll unite to become a "Human Intrusion Detection System," a set of sensors intuiting threats your controls miss. It's human intelligence, not the artificial variety. And it's exactly what your security awareness program should provide.

Further Reading and Viewing

Case Studies

Customer Videos

White Papers and E-books

About Cofense

Cofense, formerly PhishMe, is uniting humanity against phishing. Our solutions empower users to recognize, report, and help stop phishing attacks in minutes, not days. By combining human intelligence with cutting-edge technology, we enable organizations to defend themselves from the inbox to the SOC. To learn how our solutions and expertise can protect your brand and bottom line, schedule a demo today.