Annual State of Phishing Report

2021

COFENSE

Table of Contents

SECTION 1:

Executive Summary

It's a staggering statistic - 70% of government cyberattacks start with a phish. And it's no secret that threat actors are escalating their efforts to breach networks and wreak catastrophic damage to our country.

In fact, the public sector is the second-most targeted industry (coming in just behind entertainment), with thousands of reported incidents and nearly 900 successful breaches.

The threats are so detrimental to our national security, the White House recently issued an Executive Order calling for "bold" and "significant" changes to the public sector cybersecurity posture to "defend the vital institutions that underpin the American way of life."

At Cofense we understand that your applications are mission critical and that is why we are passionate about identifying threats that seek to disrupt, infiltrate and steal from our federal, state, and local institutions.

2020 year in review

In 2020, Cofense stood alone actively discouraging sending COVID-19 themed phishing simulations at the outbreak of the pandemic. As information security experts grumbled about the need for realism, the Cofense customer community produced more REAL coronavirus/COVID-19 phishing email indicators than the entirety of the global cyber vendor landscape combined.*

Let that transpire for a bit. The inventors of phishing simulations blocked COVID-19 themed PhishMe templates, yet our customers' employees reported more real COVID-19 phish than anyone else.

What went wrong in 2020

Over 1.5 million simulated phishing emails leave our PhishMe infrastructure every Monday.

Unfortunately, some non-Cofense customers did not heed our cautionary tale of avoiding certain emotionally charged lures. 2020 claimed new victims whose "awareness programs" publicly blew up on social media when the promise of a bonus in a phishing simulation to an organization cutting budget was not well received. 2020 pawned a security awareness vendor, too. While they were busy creating naughty employee lists for their Computer Based Training sale, it was clear in their Incident Response webinar they didn't have a serious program in place to triage suspicious email reports.

Minimum effective dose

There is a problem in the awareness community and it boils down to this: Your organization isn't unique, and your security awareness program isn't special. You need just enough phishing simulations to produce enough employee reports to enable your operations team to stop a REAL phishing campaign.

Unfortunately, when it comes to phishing detection and response, I'm seeing partial information being reported that emphasizes the wrong data. If you are producing reports void of employee reporting metrics, you are doing it wrong. I'm still seeing awareness professionals playing gotcha games with individual departments, completely detached from how real phishing actually works. Let's not forget that organizations are taking these measures based on TRAINING data. All is not well in Security Operations Centers either. Everyone wants automation to do their job so they can be a threat hunter. The good news is, if you stop more phishing campaigns in progress, you have fewer alerts.

*as measured by the COVID-19 Cyber Threat Coalition.

Malware is dead. Long live phishing.
The vast majority of phishing campaigns are credential theft or conversational, where hackers insert themselves in e-mail conversations between known and trusted parties. They then exploit the trust to trick users into opening a malicious attachment. While malicious attachments still play a role in phishing, the frequency of this has dramatically declined over the years. In fact, most phish attachments these days are not even malware, but instead, conduits to open a browser to further credential theft. While malicious attachments on the decline, we have our finger on the pulse of phishing-related malware.

Our mission is to keep all federal, state, and local institutions safe. We have been working on this phishing problem for years, and our insight is only made possible by servicing a growing global population of the largest public and private organizations. This report wouldn't be possible without the data, and the data wouldn't exist without our amazing customers and their employees reporting phishing. Our teams burned the midnight oil organizing this data and we appreciate your interest in reading our annual report.

Aaron Higbee
Co-Founder & CTO

Setting the stage

While making the shift to a combined report, we also decided to take this opportunity to shift a few other notable mentions about the data. First, the time period covered in our research spans the calendar year. The next item relates to notifications to the user letting them know the security technology worked—"Invoice.docx was malicious and removed." While these alerts could appear suspicious to the end user, technically these messages are informational. Lastly, we adjusted how we make industry comparisons.

SECTION 2:

Let's Get Started

The Phishing Defense Center (PDC) Today

An enterprise customer asked us to manage their Cofense Triage application four years ago. This one-off project exploded into the Phishing Defense Center (PDC) staffed by a team of expert threat analysts, inside five locations across the globe, operating 24/7, processing millions of reported emails each year for large organizations. What started out as a way of helping a customer shaped how we look at phishing detection and response today.

With Managed Phishing Detection and Response (Managed PDR) delivered through the PDC, we've gained even greater insight into the phishing threat landscape. In fact, we have a larger pool of enterprise phishing threat intelligence data than anyone else in the world. What's even more remarkable is getting to see firsthand that well-conditioned users report real phish quickly and that reduces overall risk to an organization.

Cofense PDC Phishing Facts

In the millions of emails the Cofense PDC analyzed, they determined:

- **57% were credential phish**
- **12% delivered malware**
- **6% were business email compromise or CEO fraud**
- **45% of the credential phish were Microsoft-themed**
- **17% were finance-themed**
- **9.3% of the reported messages were malicious:**
  - **38% had a URL only**
  - **36% had attachments**
- **Of the 255,000 malicious emails, we found nearly 100 unique malware families**

The Cofense PDC analyzes suspicious emails reported by customers' users and stops the phishing attack or notifies their security teams when they need to act. Using the resources of the PDC, customers can rely on external expertise and have access to a global network — close to 30 million Cofense users who report suspected phishing emails—compared to a limited internal-only view. With Managed PDR, security teams are able to focus their attention on incident response instead of the time-consuming process of analyzing reported emails.

Percentage of Phishing Emails by Type and Industry

Industry	BEC (Business Email Compromise)	Malware	Credential
Administrative	6%	7%	58%
Construction	3%	31%	37%
Education	5%	2%	77%
Finance	6%	14%	57%
Healthcare	15%	5%	59%
Information	2%	4%	66%
Manufacturing	5%	10%	53%
Mining	4%	9%	59%
Professional	11%	12%	59%
Public	6%	8%	61%
Real Estate	3%	17%	58%
Retail	3%	2%	73%
Trade	9%	6%	71%
Transportation	9%	3%	67%
Utilities	3%	16%	48%

SECTION 3:

The Big Phishing Campaigns of 2020—Emotet and Ryuk

If we learned anything from 2020, it's that threat actors' abilities to quickly adjust their methods to world events can be lightning fast. From Emotet to Ryuk, and let's not forget COVID-19, Cofense and our Cofense Labs and Intelligence teams worked overtime.

Last year brought an unprecedented amount of disruption, directly leading to an increase in both volume and variety of threat activity. Threat actors continued to advance their tactics, techniques, and procedures to ensure their emails would reach end users throughout the year.

Here's what we saw:

Emotet

Cofense has been tracking the Emotet botnet for several years now. This insight has enabled us to collect a massive set of data on the templates, malicious payloads, tactics, and continuous evolution of this pervasive botnet.

Emotet has seen multiple iterations over the years and has consistently advanced, adapted, and been a threat to public and private organizations around the globe. The threat actors behind Emotet appear to spend a lot of time developing and advancing modules and overall functionality for their malware. Most of these modules focus on obtaining, stealing, and exfiltrating diverse types of data, including local and stored credentials, contact lists, and emails. Additionally, Emotet has also been known to drop multiple types of malware, such as: IcedID, QakBot, TrickBot, and Dreambot. In some cases, ransomware such as Ryuk and Conti have been deployed.

The Ryuk Threat: Why BazarBackdoor Matters Most

On October 28, 2020, media reports and US Government (USG) notifications emerged regarding an active "credible" Ryuk ransomware threat targeting the US Healthcare and Public Health sector. This was reportedly based on chatter observed in an online forum that allegedly included members of the group behind Ryuk.

Cofense investigated this threat and observed increased activity against the healthcare sector. Our team assessed with high confidence that BazarBackdoor is the primary delivery mechanism currently used for Ryuk operations. Also, the team identified that similar phishing campaigns used to establish a foothold for Ryuk infections targeted other sectors as well.

The Phish

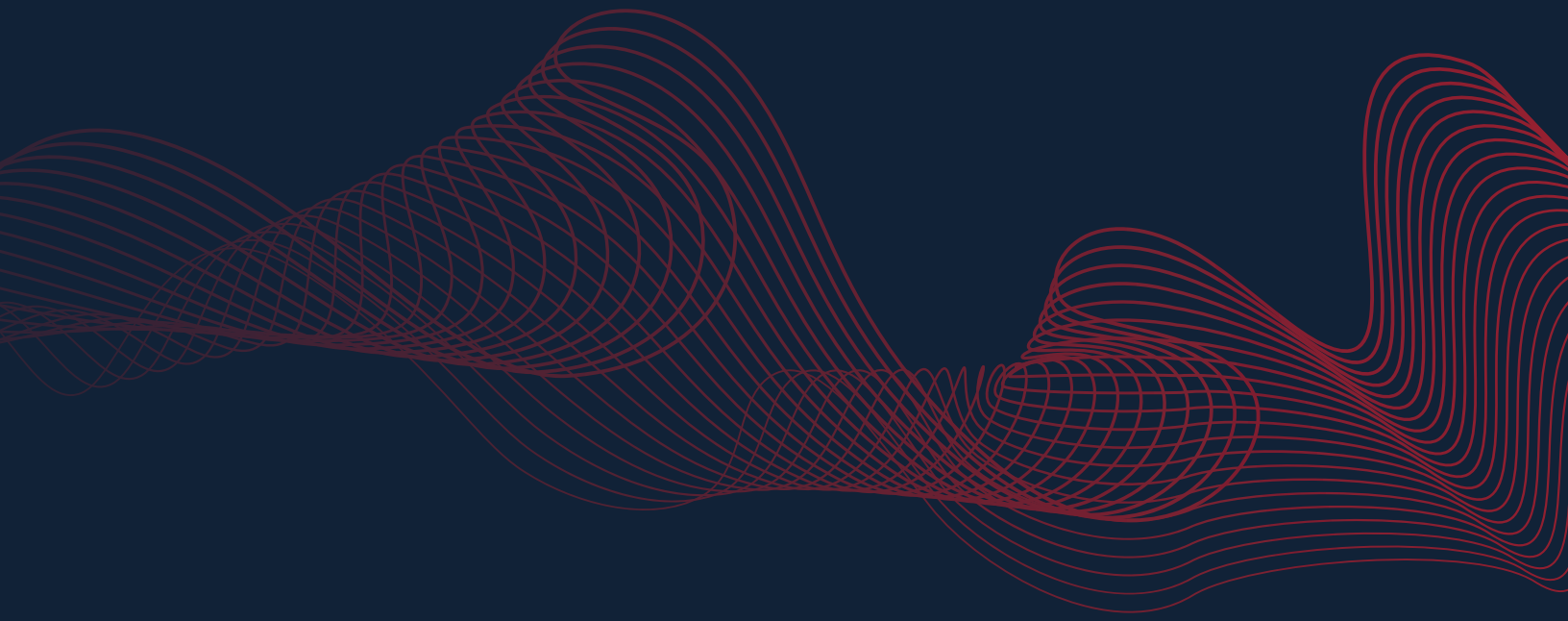
Cofense Intelligence has identified several campaigns, targeting multiple sectors, that share strong similarities to the phishing emails reportedly used as initial attack vectors in Ryuk campaigns, as outlined by FireEye. Two subject themes stand out across several industry verticals we have confirmed were targets of BazarBackdoor. These subjects relate A) to employment termination, almost always including the word "termination," or B) to payroll, almost always including the word "debit."

While the subjects remain the same, we observed two separate download services: via Google Docs or Constant Contact. Following is a list that highlights the different industries we have confirmed were targeted by such campaigns.

The sectors Cofense has directly observed targeted by Ryuk in these campaigns include:

- **Consumer Goods**
- **Healthcare**
- **Mining**
- **Energy**
- **Insurance**
- **Professional Services**
- **Financial Services**
- **Manufacturing**
- **Retail**

It is worth noting, these campaigns began in mid-September 2020, which corresponds with the timing of coordinated offensive operations to disrupt TrickBot.



SECTION 4:

How COVID-19 Changed the Threat Landscape

COVID-19 was certainly the source of the most disruption in 2020. During the peak of pandemic-themed campaigns, phishing emails predominantly delivered credential phishing and Agent Tesla keylogger, but threat actors also delivered ransomware, keyloggers, remote access Trojans, and information stealers.

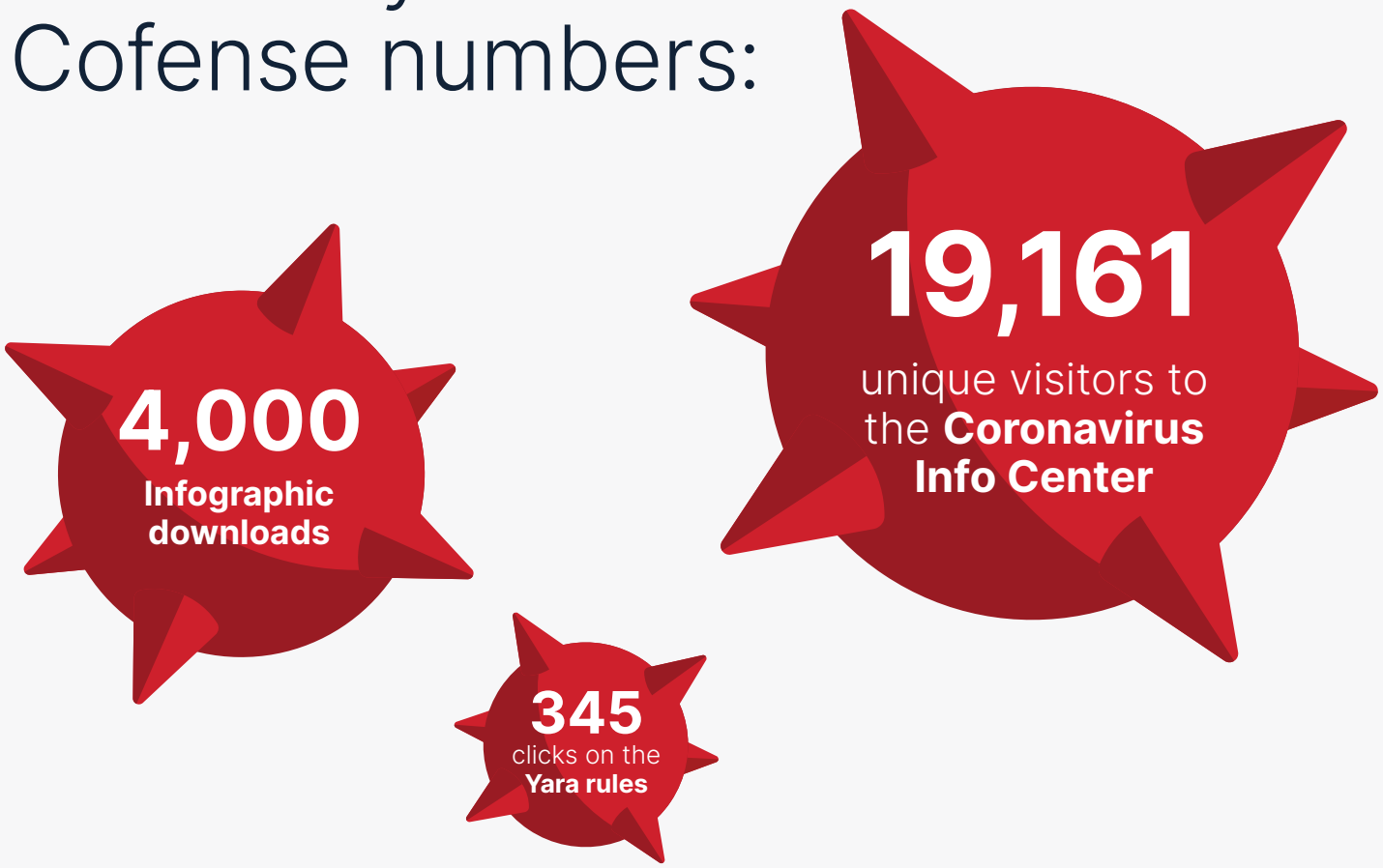
And, while overall phishing volume did not increase, numerous phishing campaign themes speak to the virus and its impact. Pandemic-themed campaigns picked up steam in February and March, peaking in April as much of the world adjusted to the concept of a "new normal." Following April, as the first shudders of the economic impact were felt and millions of people shifted to remote work, threat actors were quick to pounce.

6 Frequent COVID-related Phishing Themes

- Pandemic updates and guidance **purporting to be from global, federal, or local health organizations**
- **COVID-19 office infection data/contact tracing**
- **Updates on remote working changes**—organizational news and meeting invites
- Federal financial relief packages for **small or medium business loans**
- **Teleconferencing platform invites** or required updates related to platforms like Zoom, Teams, WebEx
- **Financial claims related to COVID-19**

Cofense has seen sophisticated and novice campaigns alike delivered with the above-mentioned themes. Similarly, we observed COVID-19 themes used to deliver different malware families as well as credential phishing attacks. Though campaigns dropped in volume after April's peak, themes continued to follow the news.

COVID by the Cofense numbers:



SECTION 5:

Fighting Crafty Humans—Malware in 2020

No matter how much automation drives a phishing campaign execution, behind every phishing attack is a threat actor. These adversaries understand what motivates and moves humans to action. They understand the power of social engineering, and how to outwit defense technologies and uneducated users.

Threat actors have improved at finding the "sweet spot" in social engineering and are identifying ways to make widespread campaigns appear targeted. Attackers are also diversifying the malware used in phishing campaigns and finding new ways to monetize phishing.

In 2020, Cofense Intelligence identified a major diversification in malware families prominent in phishing. We expect this trend of ransomware attackers leaking corporate data to force accelerated payment to continue, as it increases the pain for ransomware victims who may otherwise not pay. Organizations may be reputationally damaged by a data leak and, depending on laws and regulations, may be subject to fines and penalties. Data owners can potentially hold the organization liable and pursue litigation, exacerbating the cost.

New and Returning Malware in 2020:

Knowing your enemy is half the battle.
Here are the top trends Cofense saw in phishing-related malware throughout 2020. While a large percentage of commodity malware is detected every day, this is a listing of some of the more focused and continuously evolving malware families Cofense saw, impacting public and private organizations around the world.

New in 2020:

Avaddon Ransomware
Cheetah Keylogger
FireBird RAT
Gamorrah Bot
Grandoreiro
Hive RAT
LolKek Malware
Mass Logger
Matiex Keylogger
RedLine Stealer
STR RAT

Returning after 9+ month dormancy, often with updates:

Chanitor/Hancitor
Cobian RAT
Dharma Ransomware
Expiro
LatentBot
Proyecto RAT
Qarallax RAT
Remote Manipulator System (RMS)
Sality

Returned in 2020 after months of dormancy, in higher dissemination than in 2019:

Black RAT
Nemty Ransomware
Hakbit Ransomware
BetaBot
Iced-ID
KPOT
Kutaki
Loda
Pyrogenic Stealer
Valak
Vidar Stealer

SECTION 6:

The Need for Decreasing Dwell Time

When malicious emails reach the inbox, the chance of at least one erroneous click remains high. Average click rate for credential phishing simulations in PhishMe customers in 2020 is 10.7%—meaning that during a real attack, almost 11 users out of 100 will likely click on the phish, potentially leading to compromise of their credentials. The longer a malicious email stays in the inbox, the greater the chance of an erroneous click.

One metric of growing importance is dwell time—the elapsed time between an attacker gaining access to an environment and when they are detected, and the threat mitigated. Dwell time is composed of two key metrics—mean time to detect (MTTD) and mean time to remediate (MTTR). In their 2020 M-Trends report, Mandiant stated that global median dwell time is 56 days. Clearly, more work needs to be done. For phishing attacks, MTTD can be reduced through effective conditioning of end users to identify phishing threats and report them.

Mean time to remediate (MTTR) is currently impacted by:

- **The ability of security teams to effectively analyze today's phishing threats**
- **The ability of the same teams to hunt for, and eradicate, all copies of a malicious email within their environment**

SECTION 7:

Stopping Attackers with Human Analysis and Reporting—PhishMe in 2020

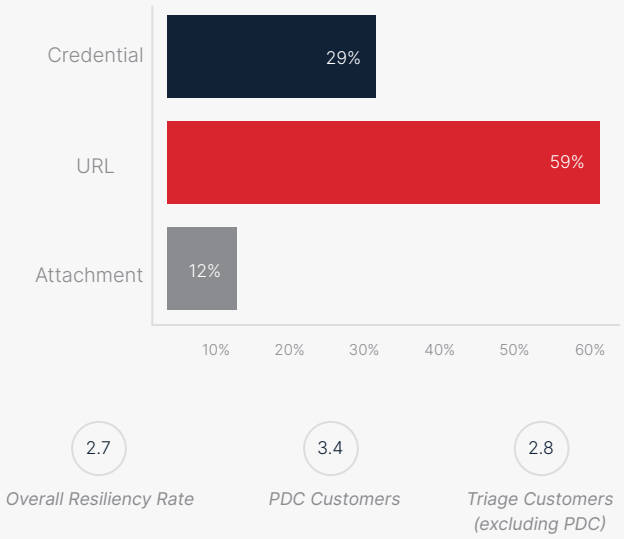
You can't stop human attackers without human reporting and analysis.

But what about training?
There is a reason we started with the phishing threat landscape and left the topic of training your users for the end. When it comes to training your users on threats leading to a data breach, simulating real threats is most effective.

We've mentioned the SEG throughout this report and it is just as relevant when it comes to training your users. In order to make training relevant to your organization and prepare your users for the items that are most likely to make it to their inbox, aligning your phishing simulation scenarios to what they will most likely experience will have a greater impact on your organization's overall resiliency when it comes to real phishing.

PhishMe Data—Simulations

Chart - Type of Simulations by Customers with Reporter



2.7	3.4	2.8
Overall Resiliency Rate	*PDC Customers*	*Triage Customers (excluding PDC)*

The Basics

As we highlighted earlier, Cofense customers who subscribe to our Managed PDR service delivered through our Phishing Defense Center have higher resiliency rates. While both subscribers to the service and customers who manage their own solutions show good resiliency rates, the Managed PDR customers outperform with a resiliency score of 3.4 (compared to 2.7 for overall customers) because Cofense responds to every reported message.

Chart - 2020 Resiliency

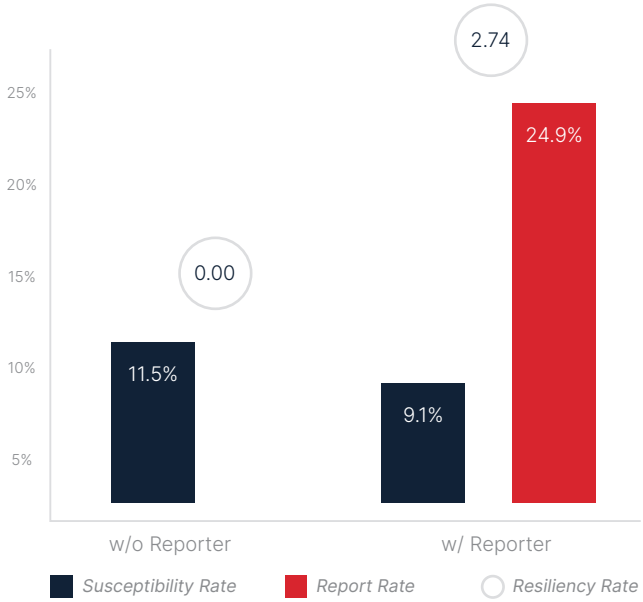
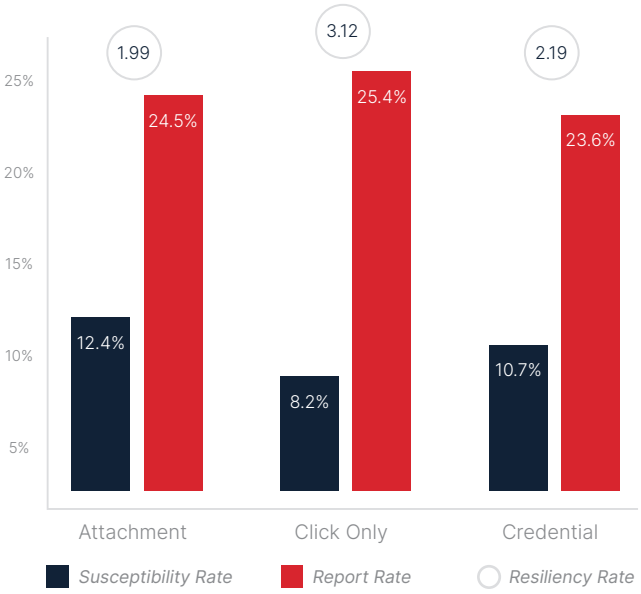


Chart - Resiliency By Scenario Type



Susceptibility Rate = [susceptible recipients ÷ emails delivered] This rate shows how many users were susceptible to the scenario versus the total number of emails delivered.

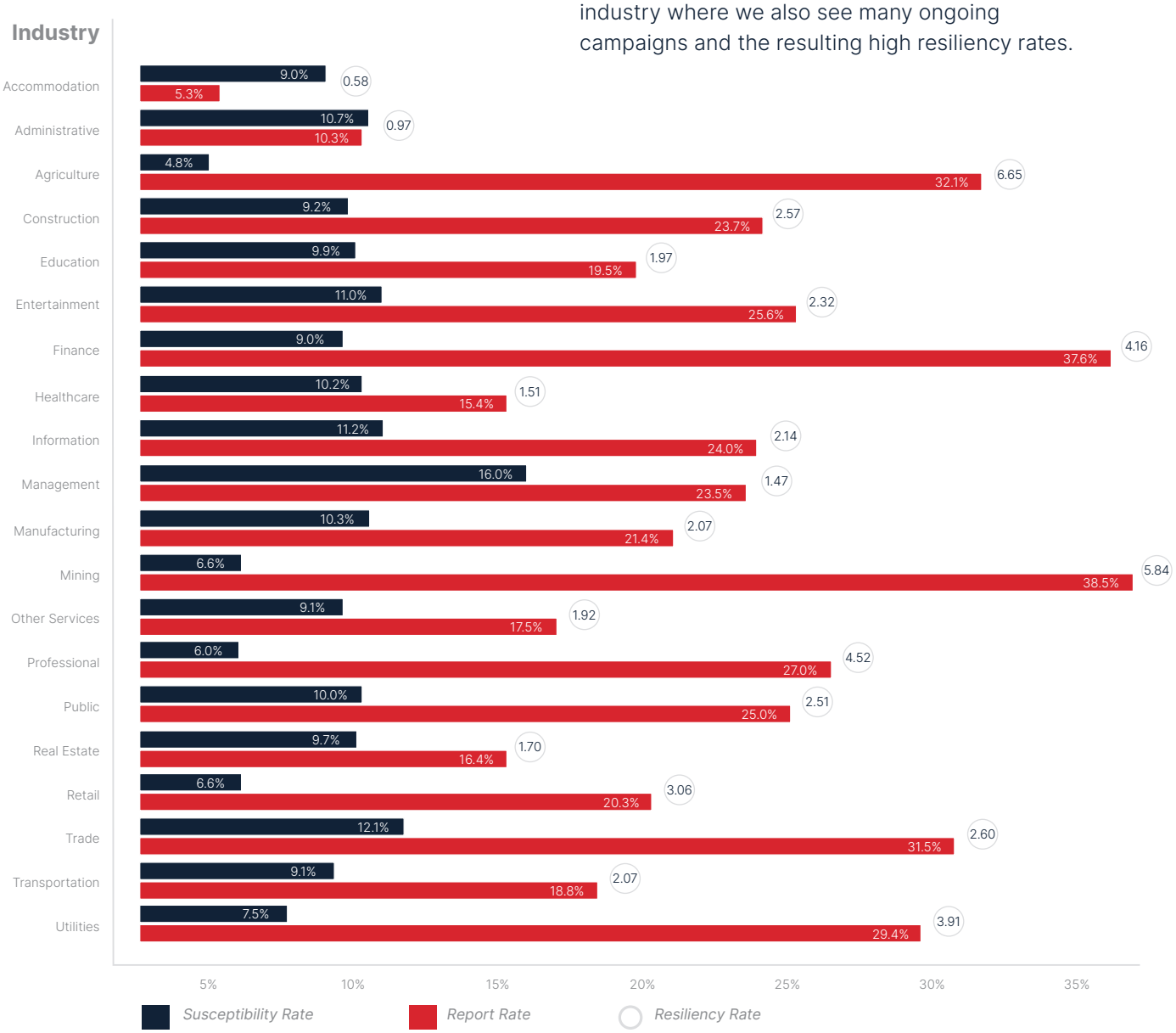
Report Rate = [users who reported ÷ emails delivered]
This is a percentage of users that reported the email, without being susceptible to it, compared to the total number of users who received the email.

Resiliency Rate = [reported on rate ÷ susceptibility rate]
This is the percentage of users who reported the email without being susceptible to it, compared to the percentage of users who fell susceptible.

When it comes to planning a simulation campaign, paging through the library of scenario templates is a daunting task. To help our Security Awareness operators in their planning process, we introduced “smart suggest,” which assists in selecting templates that are relevant to their organization. Since implementing these suggestions, 30% of organizations have adopted the templates to better align with the phishing landscape that most realistically aligns with what their users would experience.

How different industries stack up

Looking at the resiliency by industry, this year we continue to see Mining in the lead. The Mining category includes many customers in the broader Energy sector, which is highly regulated, and customers will often run monthly or multi-month campaigns. Finance is another highly regulated industry where we also see many ongoing campaigns and the resulting high resiliency rates.



Training works. Conditioning works. Take the 70:20:10 Model for Learning and Development[1] where 70% of knowledge comes from job-related experience, 20% from interactions with peers or mentors, and 10% from formal education. The developers of the model concluded that hands-on experience—in this case phishing simulations—is the most beneficial for employees as it enables them to discover, learn and refine their skills. Also, they learn from their mistakes and receive immediate feedback on their performance. With PhishMe, this holds true. Your users want to be able to identify and mitigate a potential threat to your organization and quickly report. With training, they can.

[1] Morgan McCall, Michael Lombardo and Robert A. Elchinger, Centre for Creative Leadership, a nonprofit educational Institution in Greensboro, N.C.

SECTION 8:

About Cofense

Cofense solves the problem of phishing emails that get past SEGs (Secure Email Gateways) and deliver threats to the inbox.

Combining automated response and human detection, our platform enables your teams to stop phishing attacks in minutes. While SEGs can validate an email's sender and to some extent its content, these technologies fail to stop phishing attacks every day. They simply cannot keep pace with threat actors' innovations, doomed to remain a step behind in the game of cat-and-mouse.

The Cofense Phishing Detection and Response (PDR) platform leverages a global network of over 26 million people actively reporting suspected phish, combined with advanced automation to stop phishing attacks faster and stay ahead of breaches. When an organization uses all of the Cofense solutions together, they can educate employees on how to identify and report phish, detect phish in their environment, and respond quickly to remediate threats.

Phishing solutions and products

Our Phishing Detection and Response platform catches the phishing emails that your secure email gateway inevitably misses.

We deliver the technology and insight needed to detect, respond, and stop phishing attacks.

Detection

Cofense PhishMe
Employee conditioning for resiliency against phishing

Cofense LMS
Streamlined employee computer-based training

Cofense Reporter
Real threats in real time from employees

Response

Cofense Triage
Identify, analyze, and mitigate threats

Cofense Vision
Auto-quarantine phishing threats

Integrations

Cofense Intelligence
Human-vetted phishing threat intelligence

Managed PDR

Managed PDR
Comprehensive managed phishing detection and response service

What Makes Cofense Unique

Automated Response + Human Detection
Cofense conditions end users to report suspicious emails. Automation accelerates the SOC's analysis of email reports and their ability to find and quarantine every phish in a campaign.

Patented technology delivers real-time detection and quarantine of phish. Our platform eliminates manual tasks like sifting through false positives to speed phishing response and lower the risk of breach. Purely focused on phishing, our phishing intelligence also enables your SOAR, SIEM, or TIP to get a holistic view of risk in your organization.

Network Effect
Nearly 30 million users are equipped with the Cofense Reporter button, forming the world's largest network of human phishing sensors. When users report phish, your SOC gains the visibility to remediate threats faster.

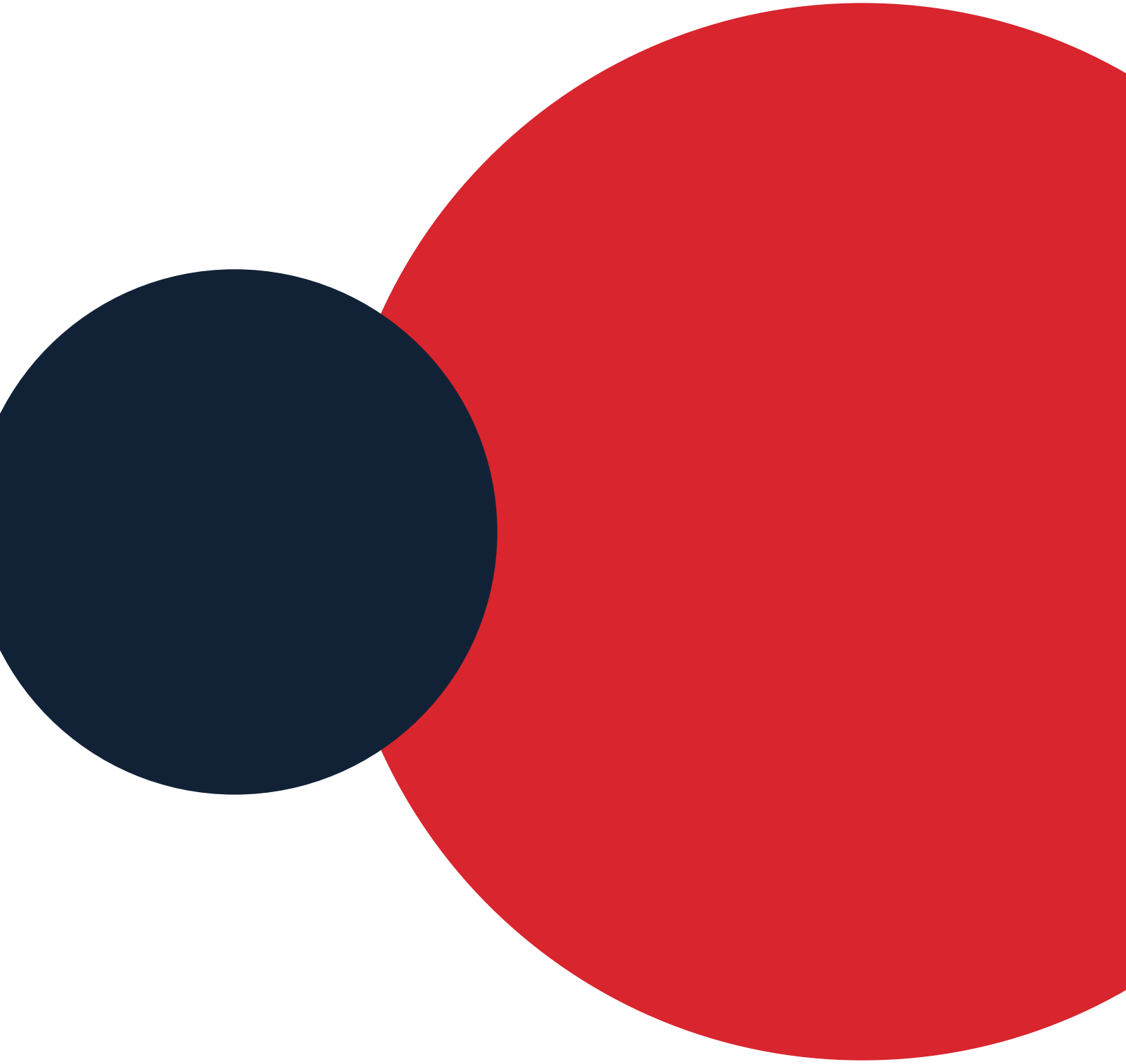
Phishing Intelligence

Cofense Intelligence maintains the largest, most accurate data set on phish that have hit the inbox.

Our Cofense Labs and Intelligence teams analyze millions of phish and malware samples annually. Their insights enable the SOC to prioritize threats and fine-tune perimeter controls.

Unbiased Insights
We are vendor agnostic. Cofense sees and shares the email threats evading all SEGs. Regardless of which SEG your company uses, you need a phishing defense to fill critical gaps.

Focus
100% of our R&D is focused on developing solutions to stop phishing attacks.



COFENSE