COFENSE

# 2022 Annual State of Phishing Report

IT'S ALWAYS A PHISH

# Contents



It's Always a PHISH

# Executive Summary

**f there is anything I hope the industry takes away from the Cofense 2022 State of Phishing Report, it is that threat actors are innovating but Secure Email Gateway vendors (SEGs) are not. I believe the number of real phish, reported by real users, found in all major SEG environments speaks for itself.**

And speaking of numbers, 99% is a magical number in marketing, isn't it? The great thing about touting 99% is it mentally brings the buyer to the conclusion that something is nearly perfect. Secure Email Gateway vendors (SEGs) artfully deploy the 99% claim because it gives them the insurance policy needed when their customers find phishing emails that made it past their layered defense.

Thinking through the 99% claim at face value, that would imply they have a way to detect and measure what sneak's past. But, if you know about the 1% that side-steps your filtering wouldn't you block it to begin with?

For example, "we block 99% of malware" sounds pretty good, right? But what if you knew that malware comprises less than 3% of the phishing emails reported by employees? We've been tabulating and reporting on the state of phishing for years now. In this report you will see exactly what percent of phishing emails are conversational (BEC), credential theft, and lastly malware. You block 99% of *malware*? Great! I'll start polishing your participation trophy.

Another word of advice, beware of self-serving-SEG bakeoffs. It starts with "let us show you what we catch that Microsoft™ misses". This bakeoff consists of a secret stash of contrived emails they know will make their solution look good. That game is over. Cofense builds, curates, and maintains *real* phishing samples that have been reported by humans. For the first time ever, we have brought a solution to market that lets you use Cofense data to test your vendors. Are you spending your budget on multiple layers of email defense? Do you have to?

Also, the phishing simulation awareness mission is finished. Employees know what phishing is. Phishing simulations create a prepared workforce. Prepared to do what? Recognize and Report suspicious email. The data in this report wouldn't be possible without the Cofense customers who have prepared their workforce to recognize and report suspicious email. We would not be able to blow the lid off the 99% claim without humans clicking the 'Report Phishing' button coupled with Security Operations professionals responding to those reports.

**WARNING** to the '*we block 99% of phishing*' SEG sales professionals: **DO NOT READ THIS REPORT**. If you read this report, it will shatter your confidence. You will not meet your quota. You will not go on the President's Club Trip.

Aaron Higbee
Co-Founder and CTO

*"The data in this report wouldn't be possible without the Cofense customers who have prepared their workforce to recognize and report suspicious email. We would not be able to blow the lid off the 99% claim without humans clicking the 'Report Phishing' button coupled with Security Operations professionals responding to those reports."*

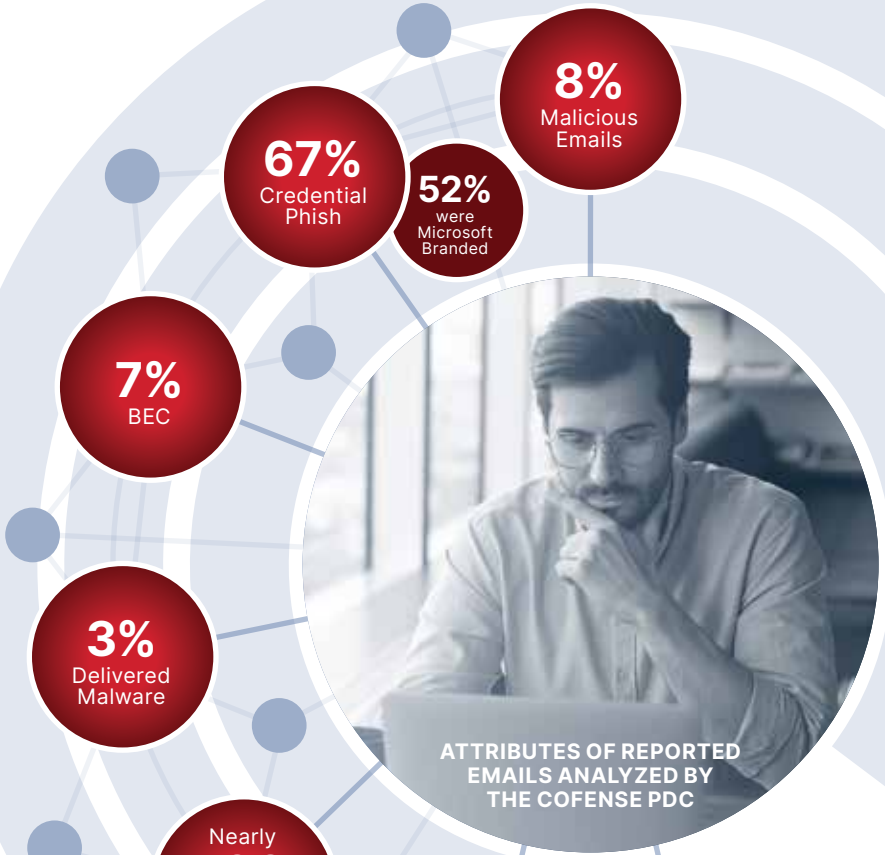
Aaron Higbee
Cofense Co-Founder and CTO

# 2022 State of Phishing – What's in Your Inbox?

**There's no question that the last year was filled with vulnerabilities that drained already exhausted security operations teams.** Pile pandemic burnout and the impacts of the Great Resignation on top of that and we can all agree that it was a difficult year. Especially when it comes to having a clear understanding of, and defending against, evolving threats.

The level of visibility Cofense has thanks to our extensive portfolio of email security solutions puts us in a unique position to understand the most prevalent threats and trends. This report dives into the three main phishing threat types we have seen over the last year – credential theft, business email compromise (BEC), and malware – and analyzes how these are affecting specific industries as well as the approach organizations are taking to defend themselves against them.

Most of the data in this report has been collected from the Cofense Phishing Defense Center (PDC), the hub for our specialized, fully managed email security service. The Cofense PDC analyzes millions of phishing emails annually and provides insights like what you see to the right. Insights related to the tactics and techniques of threat actors using email as the vector to reach unsuspecting recipients. You'll also find anecdotes gleaned from other parts of our portfolio that provide additional perspectives and insights that could be indicative of wider trends or things to come. As you dig into this data, it's worth noting all emails analyzed have made their way into the inbox after bypassing email security controls – sometimes multiple layers.



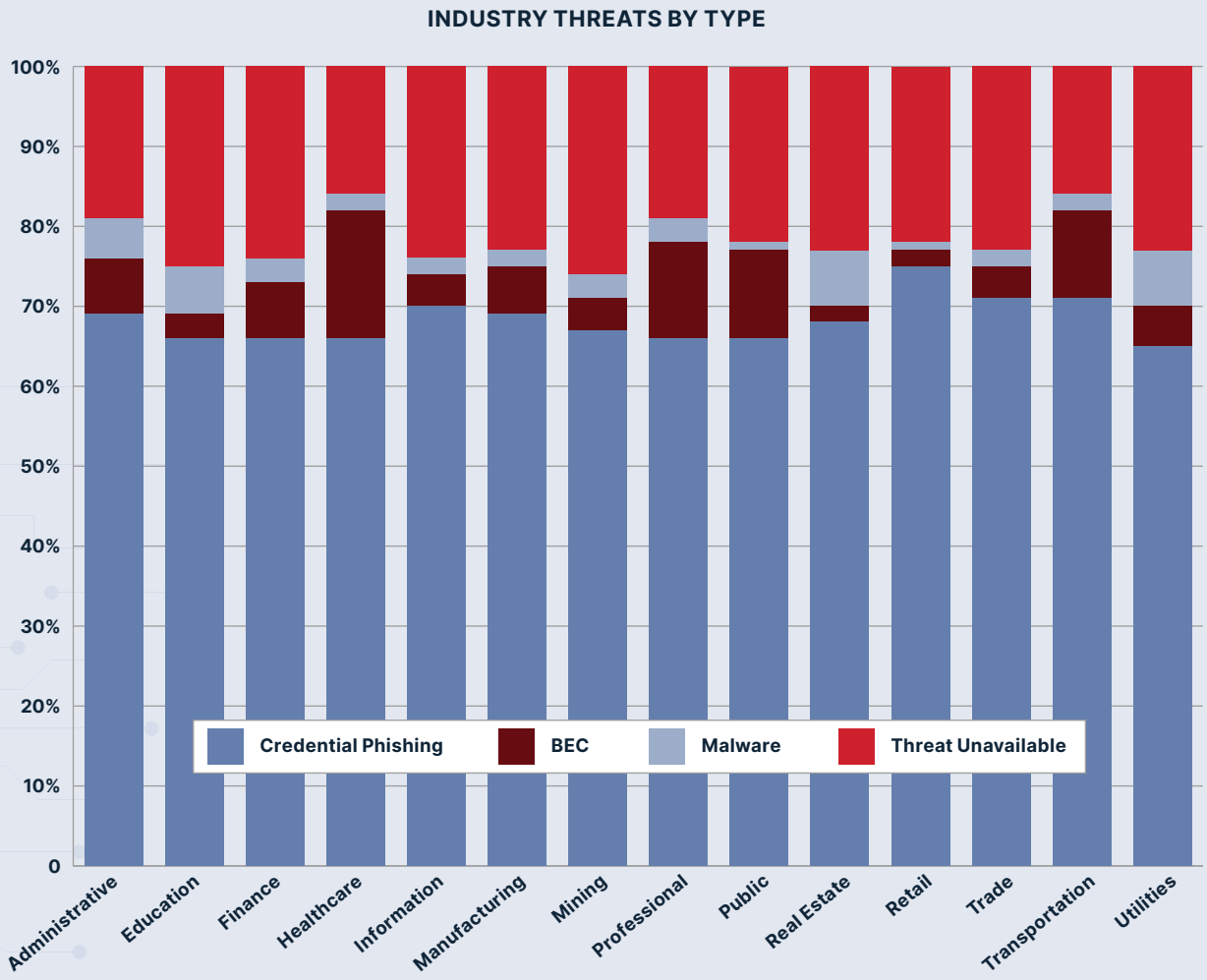
# Threat Actors, See You in the Cloud!

As organizations continue to move services to the cloud, including messaging, it's not surprising credential phishing remains the top category hitting our customers with **67%** of phish identified as malicious—10% higher than what we observed the previous year. Threat actors target credentials to ease their way into your network.

The second leading threat category we observed this year is Business Email Compromise (BEC) at **7%**. To dig deeper into these types of threats, we dedicated a section of this report to focus on the details of the tactics we observed.

While our analysts respond to reported emails in less than 60 minutes, the malicious category of "Threat Unavailable" ranks just under credentials at 23%, as actors quickly remove threats to minimize detection.

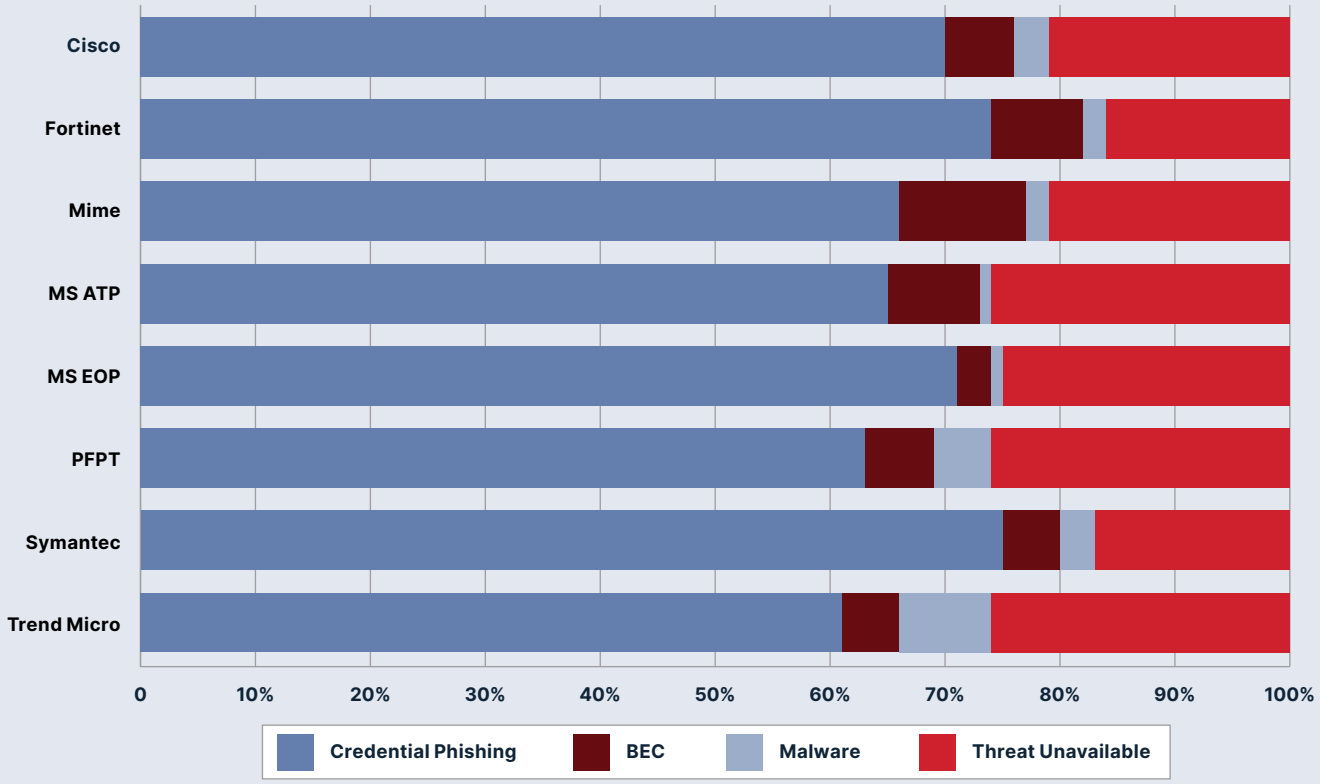
**No industry has cracked the code on evading hackers. The trends are consistent across industries.**



# Secure Email Gateways Don't Stop Advanced Phishing Attacks

When deciding between a variety of email security solutions available, many organizations opt for a Secure Email Gateway (SEG). One of the popular SEG features organizations can enable is URL detection control. URL detection control essentially re-writes the URL, adding codes or characters that are unique to the SEG making it impossible for the user to quickly determine if they should interact with the link. Those same solutions also include features to block BEC. Threat actors figured this out and updated their tactics to use multiple stages in their delivery of either malware or a credential stealing page. They've adjusted the language used to get users to engage in a conversation that leads to various types of financial loss.

**SEG – ATTACK TYPES OF CONFIRMED MALICIOUS PHISH FOUND IN ENVIRONMENTS PROTECTED BY RESPECTIVE SECURITY VENDORS**




## EMPOWER EMPLOYEES TO REPORT PHISHING THREATS

*"We need employees to report suspected phishing threats so we can find malicious emails in our environment. We outsource our reported email analysis to the Cofense Phishing Defense Center (PDC) through our Managed Phishing Detection and Response service, so we don't have to worry about any SOC team resource constraints nor lag in responses.*

*Cofense PDC's email analysis is fast, accurate, and puts us in a proactive and efficient state. We reported over 18k emails last month, and Cofense Managed PDR service's average processing time was around 13 mins – that is so valuable and impressive."*

Vice President, Financial Services

# Hand Over Your Credentials!

**As organizations continue to adopt a "Cloud First" strategy, which includes migrating to Microsoft 365™**, it's not surprising to see a 10-percentage point increase in credential phishing attacks – now making up 67% of all phishing emails observed.

Last year we added a new member to the Cofense family of solutions – Cofense Protect. Cofense Protect utilizes computer vision to analyze emails the way a human would, looking for any anomalies in email content and corresponding landing pages that may indicate a phish. Albeit a smaller volume of emails than what the PDC investigates, of the emails analyzed by Protect, we identified a growing trend of phishing campaigns containing HTML attachments. Last year, we recognized a 150% growth rate in HTML attachments found in phishing attacks. This represents about 30% of all credential phishing attacks detected by Protect.

What's the reason for the increase? Threat actors are aware that many solutions, including anti-virus and SEGs, can detect most malicious file attachments, so they focus instead on HTML attachments.

Why HTML? This file type is difficult to block as some business applications send this file type for legitimate purposes. Often, when the user opens the HTML file, it opens a login page they are familiar with using providing a false sense of security.


**RECOMMENDATION:**

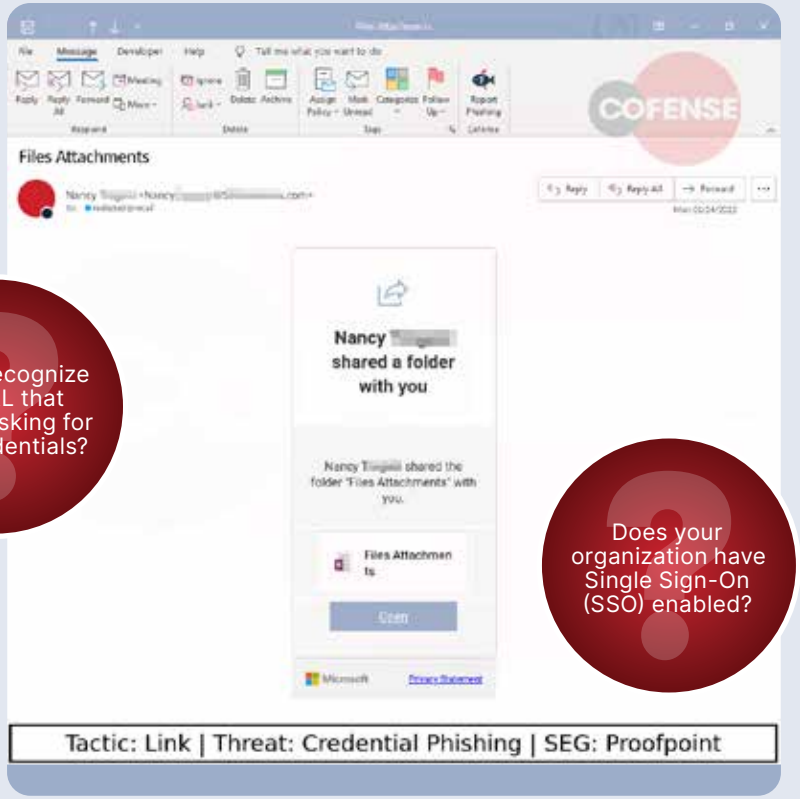
*Restrict usage of this file type to only users in your organization that have a legitimate business purpose. Find the business/application owner that is sending these file attachments and find alternate ways to interact with the intended audience. Then block these file types from all inbound external messages. While this may seem overwhelming and time-consuming, it will greatly reduce your risk of credential theft.*

# Credential Theft – What Can We Do About It?

According to a February 2022 Microsoft report, Multifactor Authentication enterprise adoption is slow at 22%. With this slow adoption and the volume of credential phish remaining high, we need to shift in how we train our workforce to recognize credential phishing to make them part of the solution. This is critical because as seen below, it is becoming increasingly difficult to identify a legitimate alert from cloud services.

It was refreshing to see increased use of credential phishing simulations this past year, but there are additional steps you can take to help your users defend against threats. As we dig into these attacks, we recognize it can be difficult to easily detect these are bad. As you interact with the email, clicking on the link or HTML attachment, the login page opens – one that we're all familiar with – and prompts us to enter our credentials. This is where we need to shift our training efforts.

**CLONED MICROSOFT EMAIL**

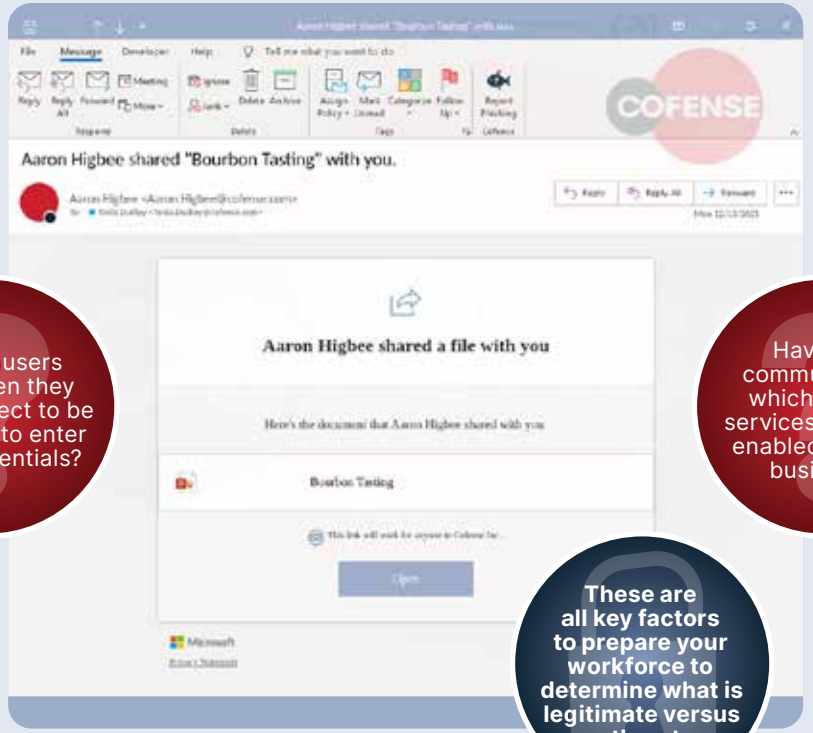



Do you recognize the URL that opened asking for your credentials?

Does your organization have Single Sign-On (SSO) enabled?

VS

**AUTHENTIC MICROSOFT EMAIL**




Do your users know when they should expect to be prompted to enter their credentials?

Have you communicated which trusted services you have enabled for your business?

**These are all key factors to prepare your workforce to determine what is legitimate versus a threat.**

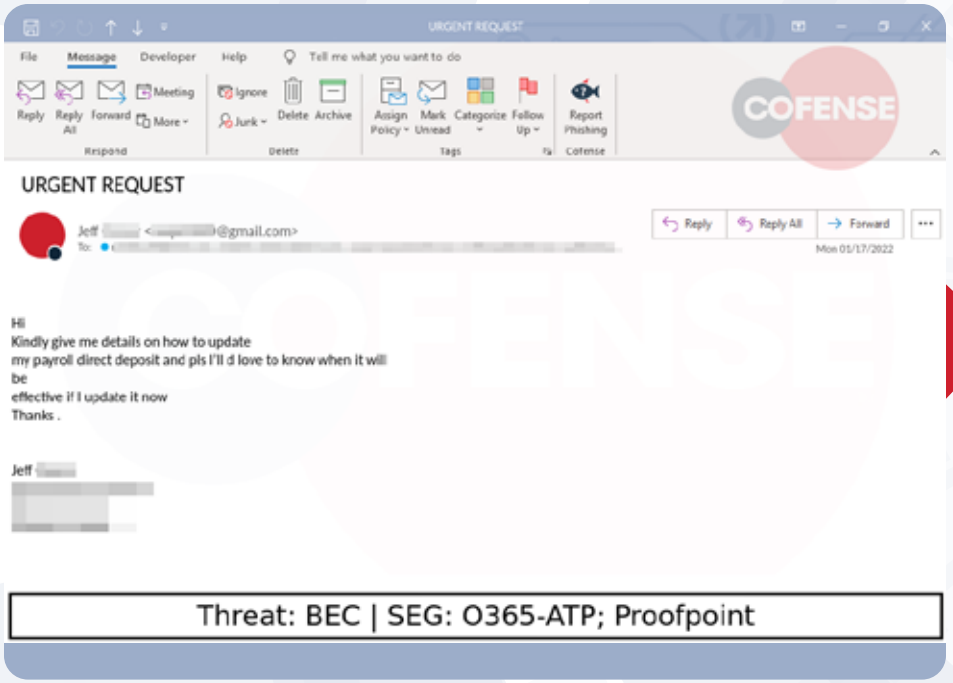
*actual phishing email from January 24, 2022

# Business Email Compromise: Did You Get Trapped in That Conversation?

**Business Email Compromise (BEC) is responsible for billions of monetary losses across the globe.** While there are multiple "flavors" of conversational-based phishing attacks, the trends observed by Cofense include direct deposit scams, gift card fraud, and invoice scams. In 100% of these attacks, no malware, exploits, or malicious payloads are installed onto end-user computers – they rely solely on human interaction.

BEC Phishing Attacks Rely Solely on **Human Interaction**

## Business Email Compromise: Direct Deposit Scam




Threat: BEC | SEG: O365-ATP; Proofpoint

*actual direct deposit scam email from January 17, 2022

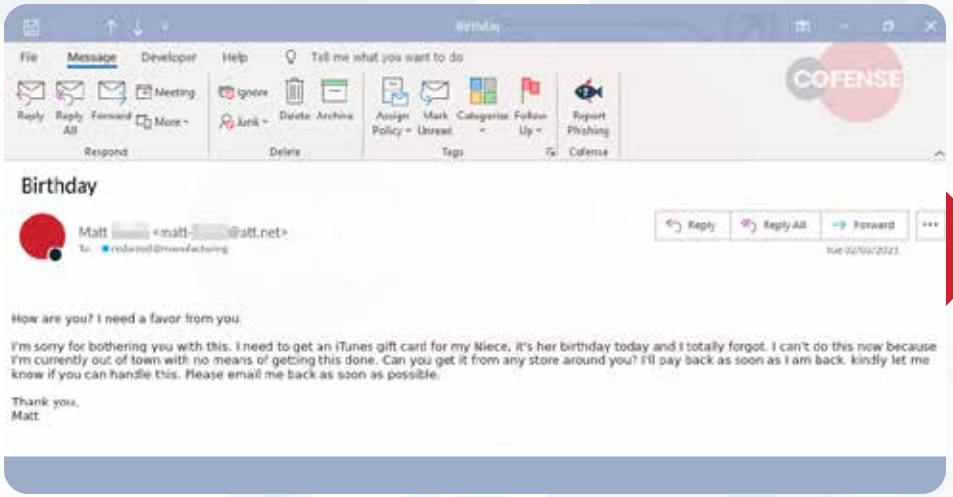
**Direct Deposit Scam:**

One of the more difficult-to-catch BEC attacks is direct deposit scams, also tracked as payroll diversion. To carry out these attacks, actors socially engineer those in payroll or human resources positions with requests to update employee direct deposit information to accounts under their control.

To limit their chances of exposure, actors use disposable prepaid cards instead of traditional bank accounts to avoid detection and limit the impact of takedown. To add an extra layer of obfuscation, actors recruit money mules to purchase the prepaid cards on their behalf, making it even harder to detect who is behind the scam.

To carry out these attacks, actors create email accounts looking like the victim they are going to re-route payroll for and routinely ask what information is needed to change payroll. Once a conversation has started, actors may provide completed I9 forms or voided checks to raise the authenticity of the attack. Once successful, it can take weeks before these attacks are noticed, causing unnecessary stress to both the victim and the organization.


## Business Email Compromise: Gift Card Fraud



Birthday

Matt <matt@att.net>

How are you? I need a favor from you.

I'm sorry for bothering you with this. I need to get an iTunes gift card for my Niece, it's her birthday today and I totally forgot. I can't do this now because I'm currently out of town with no means of getting this done. Can you get it from any store around you? I'll pay back as soon as I am back. kindly let me know if you can handle this. Please email me back as soon as possible.

Thank you.
Matt

*actual gift card fraud email from February 2, 2021

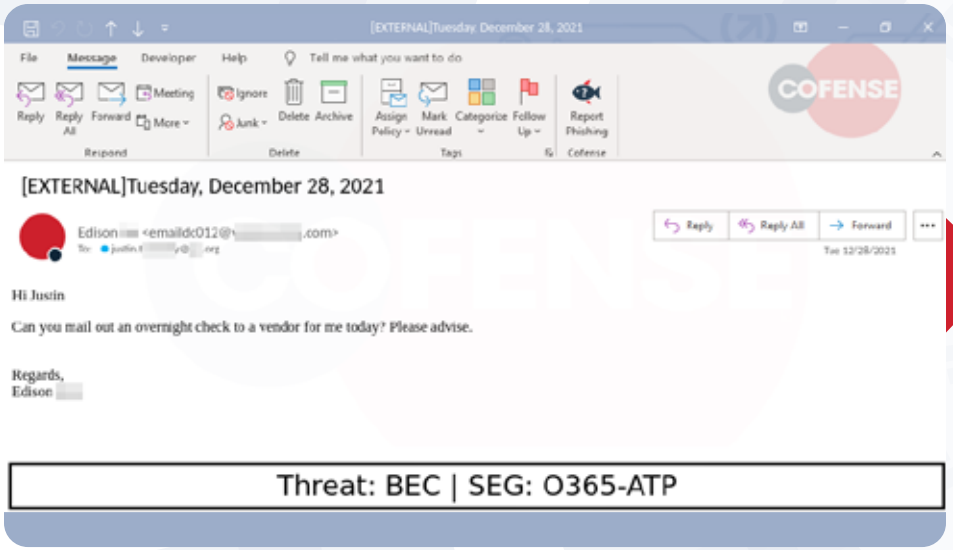
**Gift Card Fraud:**

This is how gift card BEC works. Actors pretend to be the CEO or someone in authority while requesting the employee to run a "task" or "errand" on their behalf. In many cases, scammers request the cell phone number of employees to move the conversation out of the email chain and over to something that isn't routinely tracked: SMS. Not only is it more difficult to track but having a phone number makes the attack seem more trustworthy, raising the likelihood that yes, the potential victim is speaking to someone in authority.

While traditional BEC attacks routinely use the bank accounts of romance victims, it is becoming much more difficult for scammers to fully cash-out their ill-gotten gains. In addition, a small percentage is taken from the total amount at each hop, drastically diminishing the returns from the scammers. With gift card scams on the other hand, actors make use of gift card-to-crypto exchanges to convert their stolen gift cards directly to cryptocurrencies, such as Bitcoin, within minutes. While the initial benefits and losses may seem small, actors are able to fly under the radar of federal, state, and local authorities due to the complexity of the scams. In addition, regulators do little to track gift cards which have been stolen, almost making this the perfect BEC crime.

**Attackers will go to the extent of emulating original fonts, signatures, and grammar to help raise the chances of success of an invoice scam.**

## Business Email Compromise: Invoice Scam




*actual invoice scam email from December 28, 2021

**Invoice Scam:**

The first step of invoice scams can start weeks before the financial attack takes place, with most actors not knowing who their final victim will be. For the attack to be successful, an actor must first compromise an email account, through credential phishing or purchasing account credentials on the dark web, to gain access to the email account. Once compromised, actors set up email forward rules in the compromised inbox to lie, watch, and wait for the discussion of invoices or purchase orders. Once a potential attack vector has been identified, the actors will quickly create email infrastructure, forge invoices, and hijack threads to impersonate the legitimate invoice. To the end user, there are very few things they can detect as malicious in these attacks.

This is an especially heinous attack vector for many reasons. First, the attacker can lie in wait in an inbox for months before carrying out an attack. Second, since attackers use email forward rules to create persistence in the user's inbox, the industry standard of resetting a password after a breach will not help with the attack, as email forward rules still exist on the account. Third, by hijacking a known and trusted email thread, the attack is timely and typically known to the potential victim. Attackers will go to the extent of emulating original fonts, signatures, and grammar to help raise the chances of success.

# The Year of Ransomware

**While there were significant security incidents in the last year that leveraged major software vulnerabilities**, we can't overlook the impact ransomware had on organizations. We observed nearly 100 malware families; however, the number of emails delivering malware was significantly lower than the previous year. It was also apparent that threat actors realized to make it to the inbox, they had to either use odd file types not detected by the SEG or deliver their malware through other tactics (hint: the cloud).

## Get Upstream: Tackle the Phishing Problem Early Before Ransomware Takes Its Toll

Ransomware has captured headlines for years, due to its sensationally disruptive nature. **Phishing is now one of the primary entry points for ransomware operations** targeting entire organizations and it is more important than ever to catch a ransomware operation at the phishing stage, before it is even identifiable as a ransomware attack.

Once inside, a threat actor can use any of a large variety of custom and commodity tools to move laterally, escalate privileges, establish persistence, and deliver the final ransomware payload. **Considering this, an excessive focus on signatures of the ransomware itself (often driven by media attention) is counterproductive. By the time an actual ransomware binary is detectable within a targeted organization's network, it may be too late to mitigate the impact.** To enable the necessary advanced protection, Cofense Intelligence has identified phishing payloads that are known to be precursors of ransomware and we continue to collect and publish signatures for these payloads, as part of associated phishing campaigns.

### IT'S ALWAYS A PHISH

**Phishing is oftentimes a preliminary part of a multi-step ransomware operation process rather than the direct delivery mechanism itself. We see it in the tactics used to distribute one of the more well-known ransomware variants – Conti ransomware. Conti ransomware operators are some of the most notable culprits when it comes to obtaining initial access to an organization or individual with a phish. Using this methodology, we saw many successful ransomware attacks over the last year, including the disruption of Ireland's public healthcare system and halting business for a major Scandinavian hotel chain.[1]**

1 https://www.wsj.com/articles/inside-a-ransomware-hit-at-nordic-choice-hotels-11641983406

# Breaking Down a Ransomware Attack

While we don't see "the ransomware" delivered in an email, it does start with a phish by first delivering tools to deploy their entry point to begin their mission. We're going to dig into the following malware sample to shed light on how a threat actor would lay the groundwork to launch the attack.

**STEP 1**

Looking at the phishing email to the right, we see an interesting file type use to deliver the malware - AsyncRAT, a remote access tool. While this file type does not appear common to the general email user, the native Windows operating system has no problem executing this file.

**STEP 2**

Once the phishing threat is delivered and a user opens the attachment, the AsyncRAT is installed and provides the threat actors access to a menu of options to execute their attack plan.

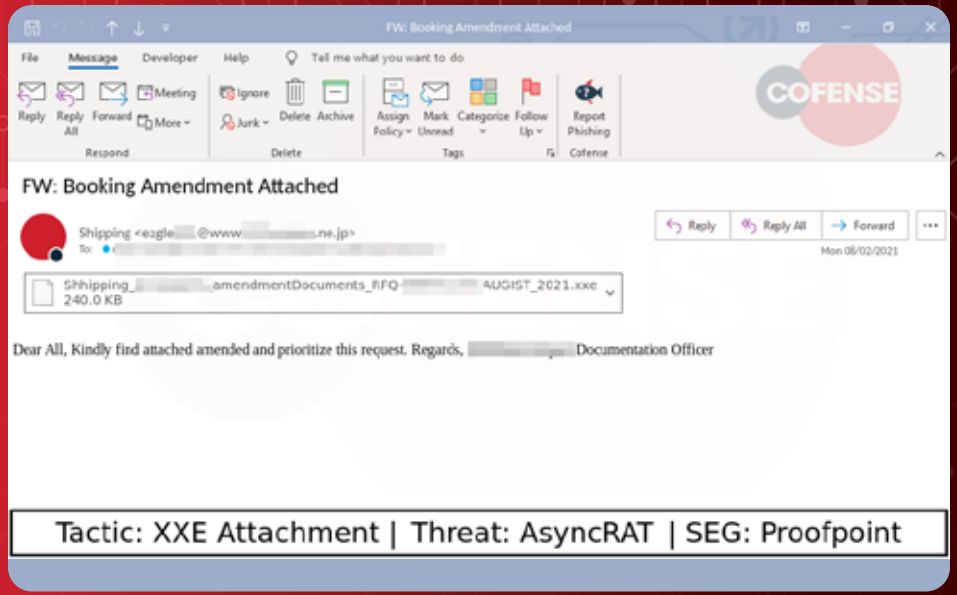
**STEP 3**

Once inside the network, a threat actor can install a keylogger to gain access to credentials, do further reconnaissance of the organization, locate sensitive information and securely exfiltrate the data.

**STEP 4**

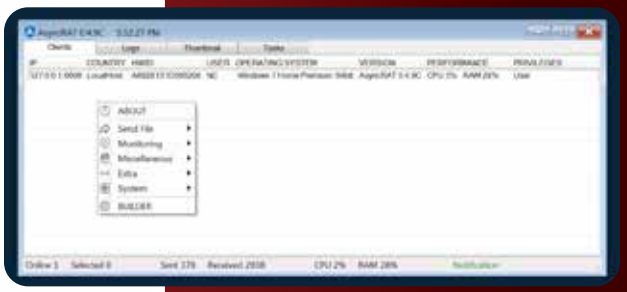
Once the threat actor has gained access and exfiltrated sensitive data, a ransom note is delivered to an organization. This has been a growing trend over the last couple of years to guarantee payment by threatening to leak the stolen data.

**RANSOMWARE PRECURSOR**




*actual ransomware email from August 2, 2021


**AsyncRAT OPTIONS MENU**



# Phishing Prevention Starts With Human Conditioning

**There is one element of phishing prevention and detection that will always remain critical – humans.** Humans will always be able to detect something about an email that is just not right. Continuous conditioning is critical to keep employees aware of the latest threats, the ones that are likely to end up in their inboxes.

## Model Simulation Scenarios After Threats That Matter

Over the past few years, we've encouraged and recommended aligning your simulation program to what is landing in your user's inbox when it comes to real phish. A bright spot we found was in the type of simulation campaigns sent. It's exciting to see a 7-percentage point increase in the number of campaigns that were simulating credential phish. Our customers are aligning their conditioning program with real threats landing in inboxes.

**SCENARIO TYPE**

| | 2021 | | | | 2020 | | | |
|---|---|---|---|---|---|---|---|---|
| | Susceptibility | Report % | Resiliency | % Scenario | Susceptibility | Report % | Resiliency | % Scenario |
| **Attachments** | 13% | 26% | 2 | 10% | 13% | 25% | 2 | 12% |
| **Credentials** | 2% | 24% | 10 | 36% | 14% | 24% | 2 | 29% |
| **URL** | 7% | 29% | 4 | 54% | 8% | 25% | 3 | 59% |
| | **6%** | **27%** | **5** | | **10%** | **25%** | **3** | |

### SUSCEPTIBILITY VS RESILIENCY

**Susceptibility Rate:** This rate shows how many users were susceptible to the scenario versus the total number of emails delivered.

**Resiliency Rate:** This is the percentage of users who reported the email, without falling victim to it, compared to the percentage of users who fell susceptible.

# Timing Is Everything When Conducting Simulation Training

Not only does tuning your templates to the threat landscape help drive improved human conditioning, but so does timing. We recently published a Cofense Intelligence Strategic Analysis Report that examined the timing of the delivery of real phishing campaigns. By following their patterns, as seen in the chart to the right, it's best to launch your simulation campaign on Tuesday or Wednesday.

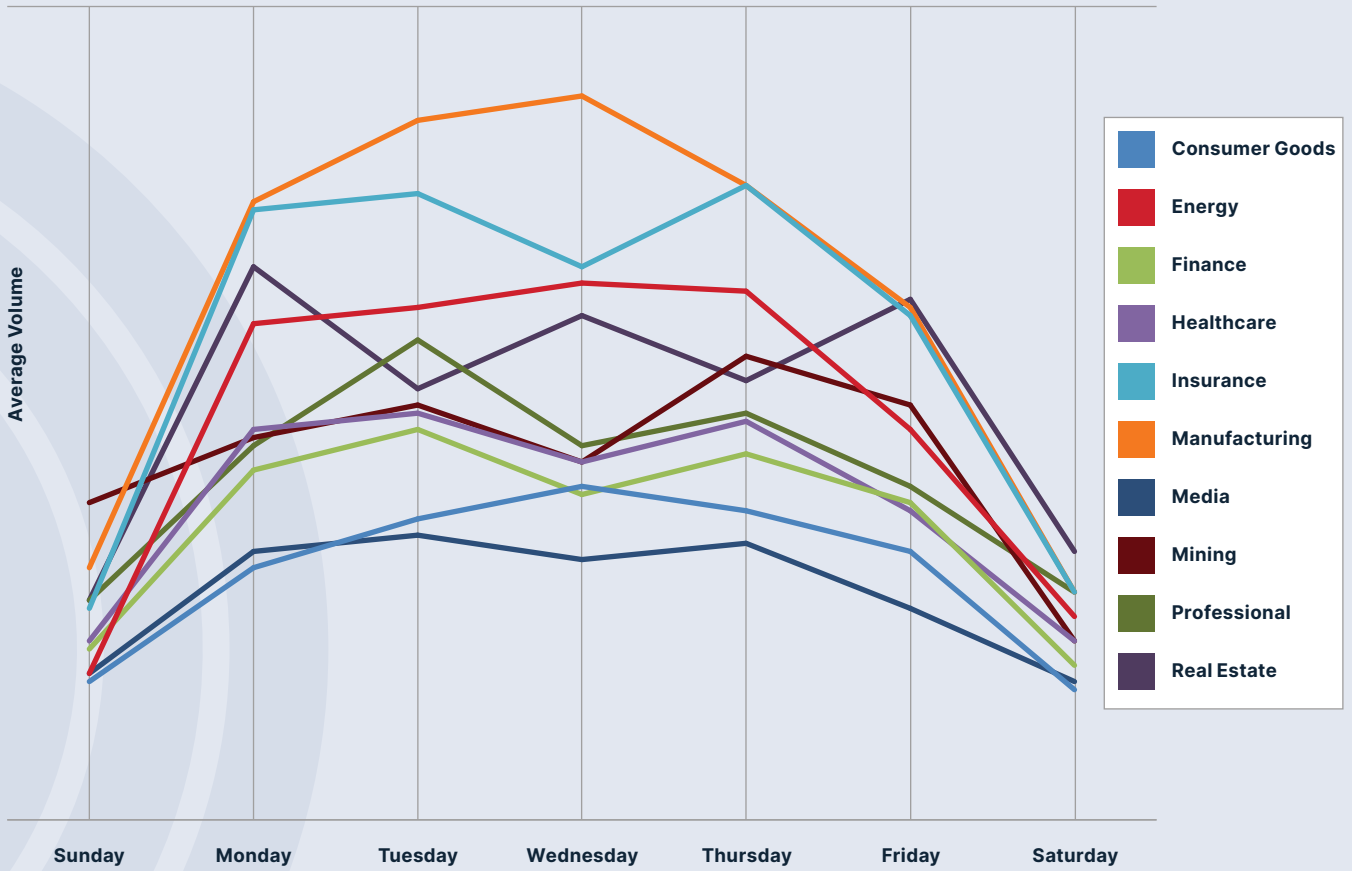
**SUSCEPTIBILITY PLUMMETS WITH COFENSE AWARENESS TRAINING**

IT Ops Manager, Higher Education

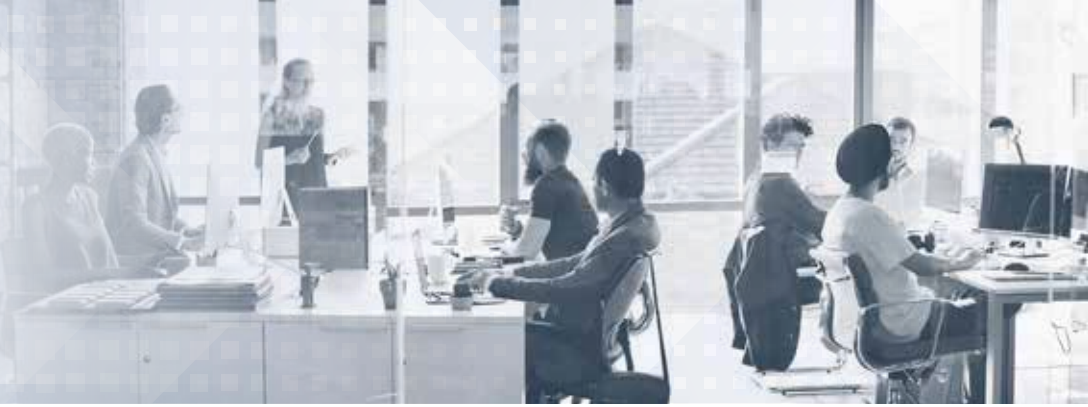
Hi, **Robert**. We've been using **COFENSE** for a few years now and can absolutely vouch that it's raised awareness among our staff about their part in the security. We've seen the susceptibility to phishing attacks plummet and user engagement and reporting of suspicious emails to IT become a normal thing.

Like Comment Share

**AVERAGE PHISHING EMAIL VOLUME RECEIVED PER DAY OF THE WEEK**



# Oops! I Did It Again: Addressing Repeat Clickers



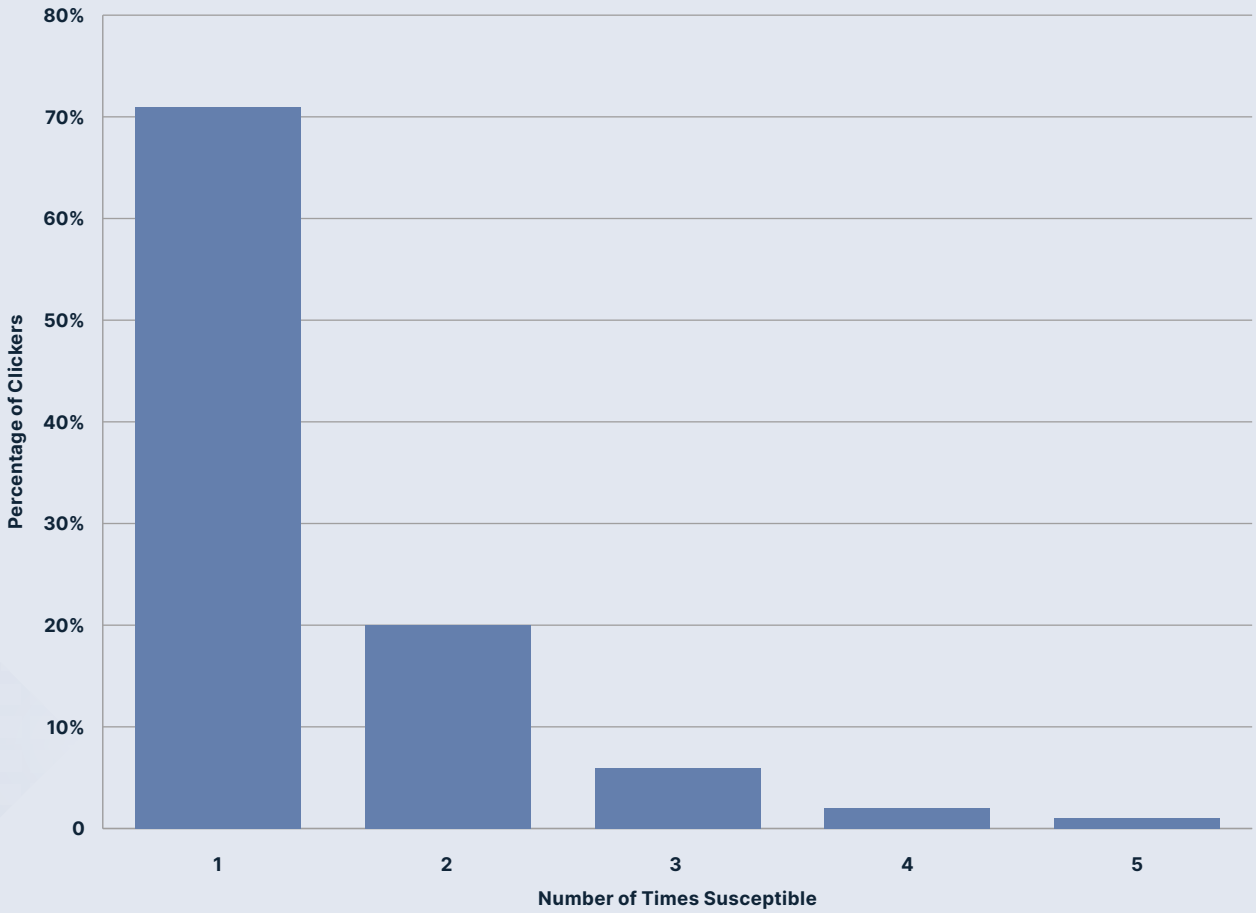
When it comes to identifying the riskiest corporate citizen, addressing your repeat clickers is certainly one way to reduce the risk to your organization. And while you may be tempted to rush to this step to fast track your program, it can take up to FOUR scenarios before they "get it." One method we often recommend is to run a follow-up scenario to only those who interacted with the scenario. However, it's still recommended to filter this on your users who interacted with multiple scenarios.

While reducing the interaction (click) is often the focus with repeats, don't forget to incorporate positive reinforcement to influence your report rate. Sending out a "Thank You for Reporting" follow-up can go a long way to drive the desired behavior.

**What is a "Repeat Clicker?"**

**Individuals within an organization who repeatedly fall victim to phishing emails**

**REPEAT CLICKERS – NUMBER OF SCENARIOS TO REDUCE SUSCEPTIBILITY**



# Phishing Simulation Training – No Manual Required

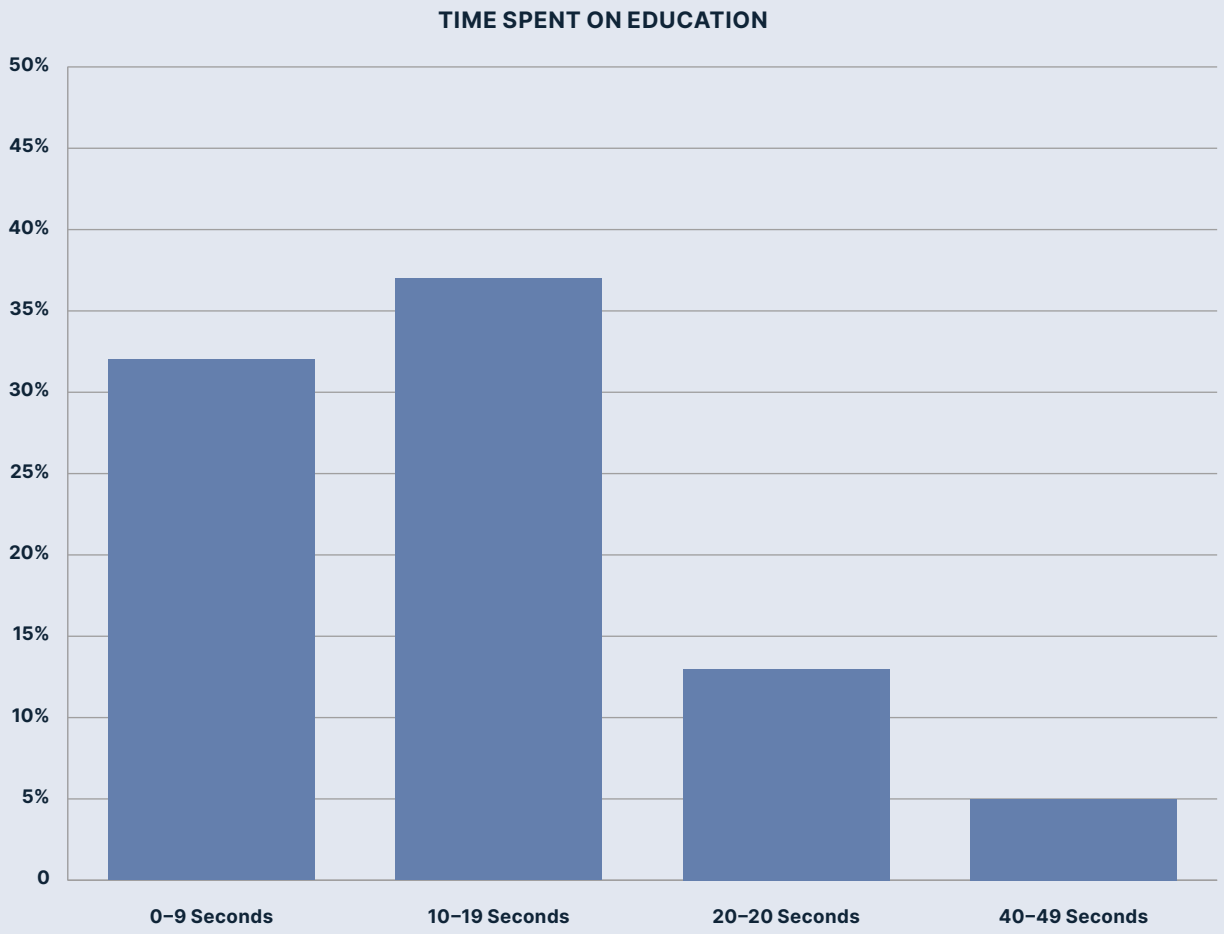
When we pioneered the phishing simulation market, we knew it may be tough for organizations to accept that running a simulation campaign is a teachable moment – not a "gotcha" exercise. To help demonstrate the effectiveness of this methodology, we wanted to highlight how long susceptible users are staying on the education page by providing this metric in the scenario campaign results.

It didn't surprise us that the time spent on simulation training aligned with what we knew to be true – users are decreasing their susceptibility while spending little time on the education landing page.

We have aggregated the data across all campaigns for the year and found that 70% of users who click the link directing them to the education page fall into our first two-time spent buckets (0-9 and 10-19 seconds). Many customers add their branding and logos to the landing page, giving the user a quick indication they just interacted with a simulation.

*It didn't surprise us that this metric aligned with what we knew to be true – users are decreasing their susceptibility while spending little time on the education landing page.*

When you combine this metric with our Repeat Clicker chart on the previous page, it's clear that recipients are learning based on the dramatic decline in susceptibility.



# Measuring Up to Your Peers: Industry Results

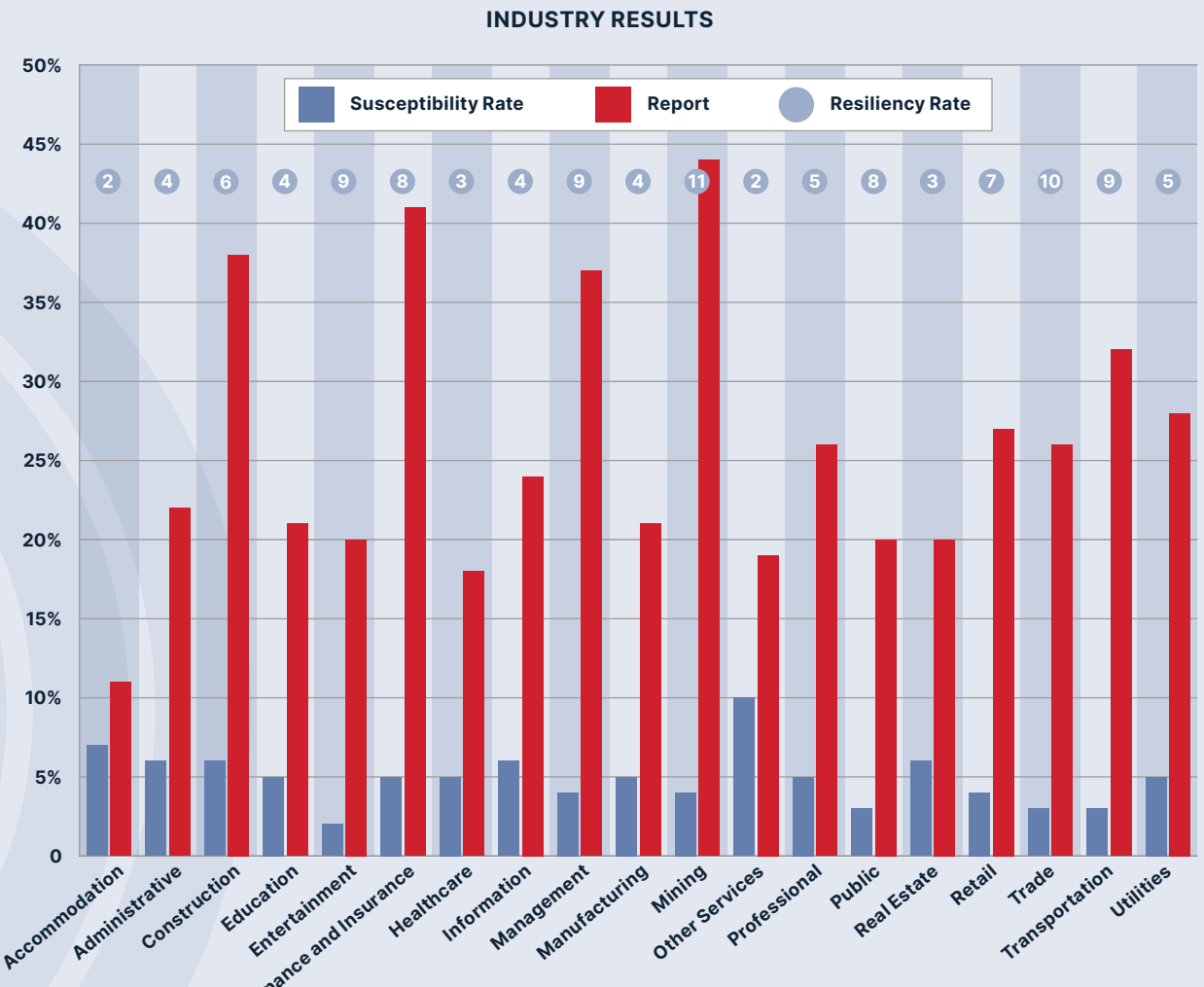
**Keep Your Organization Safe**

**Enable Multi-Factor Authentication (MFA)**

It wouldn't be a complete report without highlighting the susceptibility, reporting and resiliency results by industry, as we know your industry and sector networks are important to see how you align.

As you might have guessed, industries with more regulation continue to show a higher resilience. We also recognize that organizations that run more frequent campaigns narrow their learning time. As you continue to mature your program, we recommend maintaining a higher frequency of simulations with more targeted business functions, such as finance or human resources.

**As you might have guessed, industries with more regulation continue to show a higher resilience.**



# Catching Up With Cofense

www.cofense.com

## What's New? A Lot.

Early on in our journey as a company, we grew our focus from solely security awareness simulation training to more broadly addressing the real phishing threats facing organizations. When it comes to solving these problems, there are two common ways you can enhance a product line: acquisition or innovation. We opted for the one-two-punch, both acquisition and continuous innovation – taking our multi-layered email security architecture to a whole new level.

Last year we welcomed the people and technology of Cyberfish into the Cofense family, bringing computer vision and artificial intelligence to our portfolio and stopping phishing emails in real time before they have been reported or added to block lists. Now known as Cofense Protect, hundreds of organizations are already using this innovative technology for real-time protection against unknown threats by scanning emails and landing pages as a human would – noting discrepancies in images, language, and behavior to catch attacks that evade more traditional email security solutions.

We have also introduced Cofense Validator, the only product available that uses real, active phishing threats to test the efficacy of secure email gateways (SEGs), giving organizations a clear and objective understanding of how their SEG is performing against live phishing threats.

We also celebrated five years without phishing related breaches for any of our managed service customers. That means since its inception in 2016, we have seen nothing but success when it comes to the service performed for our customers. The combination of human expertise, the power of always evolving Cofense solutions, and strong partnerships with each organization is the perfect recipe for success when it comes to defending against phishing attacks.

**The continuous evolution and demonstrable results of our solutions show that the mission remains clear for Cofense: We stop phish.**

### COFENSE MANAGED PHISHING DETECTION AND RESPONSE SERVICES CAN HELP YOU AVOID A BREACH.

*"This product has provided staff augmentation to both a lean Information Security team as well as lean support teams that do not have the bandwidth to field reports from ~5k users. With this, it is "set it and forget it." Our users are able to report, get back accurate information, and if an email is found to be malicious, the appropriate teams receive email alerts to take necessary remediation efforts."*

Trust Radius review

*"The Cofense Phishing Defense Center is really helping our organization to analyze threats and block the malicious ones before reporting. Its threat hunting capability through intelligent scanning and monitoring of the global networks is really impressive and trustworthy. Before, there was a lot of risk in manual hunting and reporting at the same time. Now, with the arrival of Cofense PDC, that pressure has been relieved because of the automation, and the IT and SecOps team has been relieved."*

Trust Radius review