AGARI CYBER
INTELLIGENCE DIVISION

REPORT

H1 2021

Email Fraud & Identity Deception Trends

Global Insights from the Agari Identity Graph™

Executive Summary

Call it a case of locking the back window while leaving the front door wide open. A year into the pandemic and amid successful attacks on GoDaddy[1], Magellan Health[2], and a continuous stream of revelations about the SolarWinds "hack of the decade," cyber-attackers are proving all too successful at circumventing the elaborate defenses erected against them[3]. But despite billions spent on perimeter and endpoint security, phishing and business email compromise (BEC) scams continue to be the primary attack vectors into organizations, often giving threat actors the toehold they need to wreak havoc. In addition to nearly $7.5 billion in direct losses each year, advanced email threats like the kind implicated in the SolarWinds case[4] suggest the price tag could be much higher. As corroborated in this analysis from the Agari Cyber Intelligence Division (ACID), the success of these attacks is growing far less reliant on complex technology than on savvy social engineering ploys that easily evade most of the email defenses in use today.

Sophisticated New BEC Actors Signal Serious Consequences

Credential phishing accounted for 63% of all phishing attacks during the second half of 2020 as schemes related to COVID-19 gave way to a sharp rise in payroll diversion scams, as well as fraudulent Zoom, Microsoft and Amazon alerts targeting millions of corporate employees working from home. Meanwhile, the state-sponsored operatives behind the SolarWinds hack were just a few of the more sophisticated threat actors moving into vendor email compromise (VEC) and other forms of BEC. Emerging "capital call" payment scams, for instance, have targeted more than $800,000 in wire transfers—seven times the average $72,000 sought in most BEC attacks. SEE MORE ▶

Employees Walloping SOCs with False Positives as True Threats Go Unnoticed

Amid the pandemic, a blistering threat landscape extending to each remote worker has Security Operations Centers (SOCs) buried under more employee-reported phishing emails than they can possibly handle. As our H1 2021 ACID Phishing Response Survey of aggregated client data reveals, the time-intensive tasks required to analyze, triage, and remediate these incidents are exacerbated by a staggering 61% false positive rate—even as more legitimate threats hit home. A welcome bright spot: Organizations leveraging advanced phishing response workflows report detecting and remediating 88X more verified malicious emails similar or connected to those submitted to employees. SEE MORE ▶

5.8B Malicious Emails Spoofed Domains in H2; 76% of Fortune 500 Still at Risk

Global adoption of Domain-based Message Authentication, Reporting, and Conformance (DMARC) leapt 32% during the second half of 2020. But during a six-month period that saw 5.8 billion malicious emails spoof corporate domains, the number of Fortune 500 companies to deploy DMARC rose only modestly—including a 4% increase in domains with DMARC set at its most aggressive level of enforcement. While any rise in that number is encouraging, it means 76% of the nation's most prominent companies remain at risk of impersonation in phishing attacks targeting their customers and the general public. Far more promising: The 82% rise in the number of brands adopting Brand Indicators for Message Identification (BIMI) at a time when the email channel is more crucial than ever. SEE MORE ▶

Inside This Report

The intelligence presented in this report reflect data captured via the following sources from July through December 2020:

Active defense engagements with **cyber threat actors** to gather intel about emerging BEC tactics and targets

Data extracted from **trillions of emails** analyzed and applied by Agari Identity Graph™

DMARC-carrying domains identified among **426 million** domains crawled worldwide

Incident data from SOC professionals in a **survey of large enterprises** averaging 21,000 employees and spanning multiple industries

Agari Cyber Intelligence Division (ACID) is the world's only counterintelligence research group dedicated to business email compromise (BEC) investigation and cybercrime abatement. Since May 2019, ACID has conducted more than 12,000 active defense engagements with threat actors. ACID works closely with CISOs at global enterprises, law enforcement, and other trusted partners to stop identity-based phishing and socially-engineered cybercrimes.

Table of Contents

Employee Phishing and Business Email Compromise Trends

KEY FINDINGS

$809,000
The average amount targeted in “capital call” scams—an emerging form of BEC in which fraud rings request funds from investors who’ve committed money toward a specific investment

7X
The difference in average amounts sought in capital call payment scams and the $72,000 average targeted in wire payment fraud schemes in the second half of 2020

333%
The percentage increase in the number of payroll diversion scams since July 2020

Bigger Phish Making a Splash in BEC

Sophisticated New Threat Actors Signal Dire Consequences Ahead

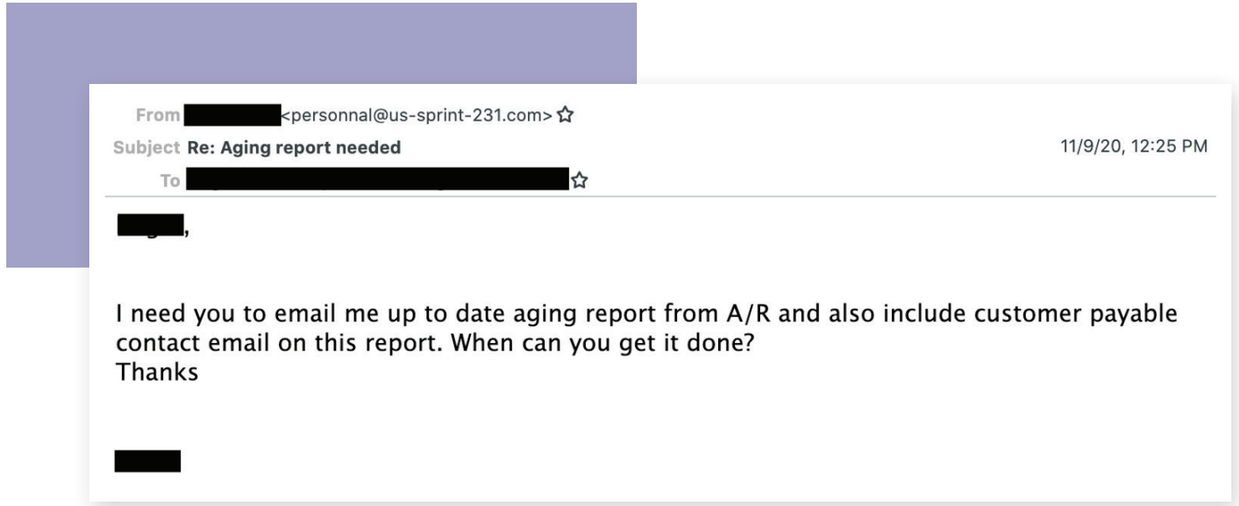
SolarWinds was just a warm-up act. According to industry studies, 80% of firms[5] report a sharp rise in cyberattacks during 2020—the vast majority of them phishing attacks and other advanced email threats. Business email compromise (BEC) alone has led to nearly $30 billion[5] in direct financial losses since 2016, and it's getting worse. During the second half of 2020, ACID researchers uncovered a troubling rise in well-funded eastern European crime syndicates piloting new forms of BEC. With 57% of US employees still working from home and hamstrung by housebound children, frustrating vaccine rollouts, and an endless number of other distractions, threat actors appear to be finding plentiful targets for a new wave of socially-engineered email threats that could cost companies plenty.

Big Spike in Average Amount Targeted in BEC, Driven by 2 Big Trends

In November, a dramatic increase in the average amount of money targeted in BEC attacks was tracked back to two primary causes. The first was the resurgence of the BEC threat group we've dubbed Cosmic Lynx[5], which switched up its pandemic-related tactics to include references to COVID-19 vaccines. More worrisome: The group has also started requesting recipients' phone numbers in its emails to redirect the conversation to phone communications. The second driver behind the surge in the amounts sought in BEC scams is a potent new pretext used by threat actors—capital call investment payments. Generally speaking, capital calls are transactions that occur when an investment or insurance firm seeks a portion of money promised by an investor for a specific investment vehicle. In emails to targets, BEC actors masquerade as a firm requesting funds to be transferred in accordance to an investment commitment. Because of the nature of such transactions, the payments requested are significantly higher than these sought in most wire transfer scams. The average payout targeted in capital call schemes: $809,000.

Accounts Deceivable: Aging Report Schemes Gain Traction

During this same period, our researchers also noted a significant increase in the number of BEC attacks requesting aging accounts receivable reports from targeted employees. While this particular form of BEC has been around for more than a year, it has represented a mere fraction of the total. In November, however, nearly 1 in 12 (7%) of all BEC scams our researchers observed requested an aging report. More disconcerting: While a large percentage of this increase can be attributed to the BEC group we call Ancient Tortoise[5], we identified a growing number of other email campaigns coming from actors employing markedly different tactics—suggesting the exploitation of aging financial reports is being more widely adopted within the BEC ecosystem.



Example BEC Email Requesting an Aging Report

Like Vendor Email Compromise (VEC), aging reports scams use compromised information from one organization in order to defraud another. Unlike VEC, however, they do not require the actual infiltration of an employee's email account. Instead, the attacker impersonates a senior executive in emails requesting a copy of a recent aging accounts receivable report, which typically contains a list of all unpaid invoices and the names and email addresses of associated customer contacts. With this information in hand, attackers will then target the victim's customers with requests for payment on overdue invoices to a new bank account.

Taken together, renewed activity from these two organizations is an ominous sign that highly-sophisticated threat actors are moving into an arena once dominated by loosely affiliated West African email crime rings. All while BEC groups of every stripe continue to establish new beachheads[5] worldwide.

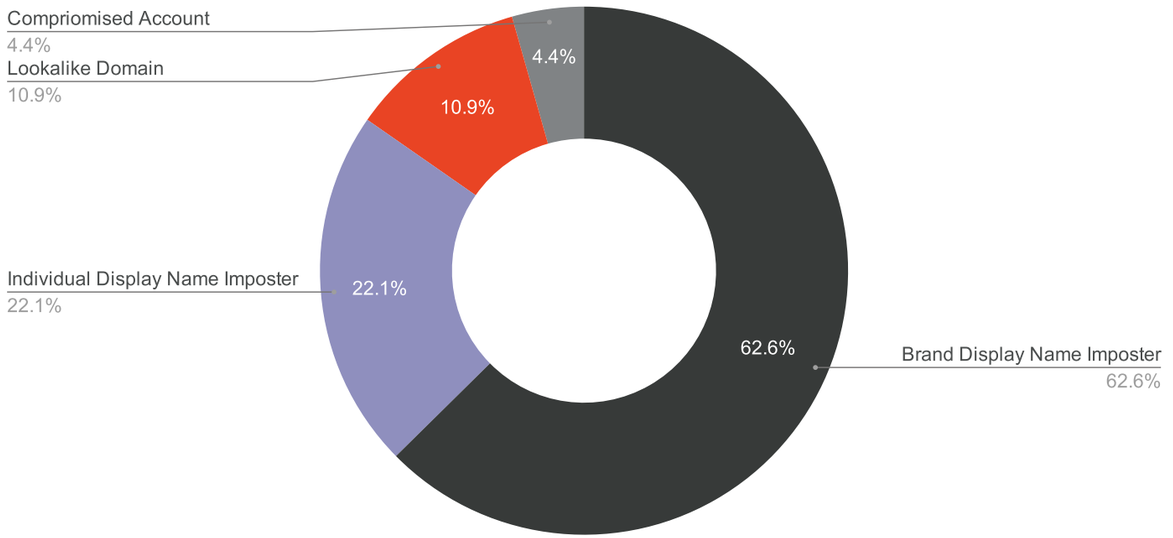
Hit Charade

Go-to Identity Deception Tactics Continue to Deliver for Email Crime Rings

63%

Percentage of Phishing Emails Impersonating Trusted Brands

More than 6 in 10 malicious emails (62.6%) employing identity deception techniques involved display names designed to impersonate a well-known brand during the second half of 2020. This includes a significant number of phishing attacks impersonating Microsoft[10], Amazon, Google, Facebook and others. In the majority of cases, these were coordinated campaigns designed to harvest login credentials from their targets.



Advanced Phishing Attacks by Imposter Type

1 in 5

Impersonation Attacks Pose as Specific Individuals

Just under a quarter (22%) of all impersonation attacks pose as a trusted individual, usually a senior executive within the recipient's company or an outside vendor. As mentioned, a cunning new impersonation tactic involves posing as specific individuals conducting "capital calls" in emails requesting payment from recipients on funds committed toward an investment vehicle. In the case of the group we call Ancient Tortoise, ACID researchers have confirmed the threat actors are acquiring aging accounts receivable reports in order to target companies with requests for payment on legitimate overdue invoices.

BEC Breakout Session

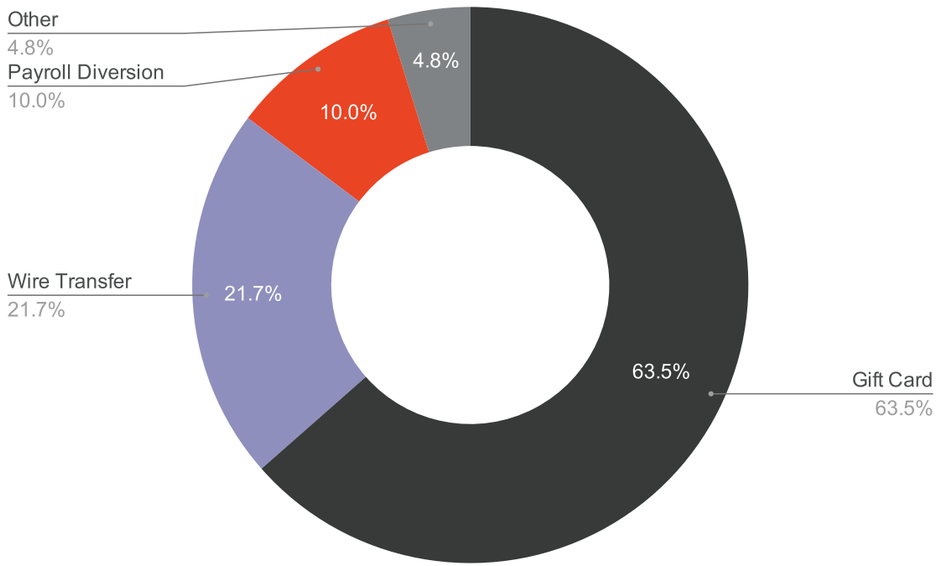
Gift Cards Down But Still Dominant; Payroll Diversions Gain Traction

Potential Losses Grow as BEC Actors Seek Bigger Bounties

Gift cards continue to rank as the #1 choice for cash-outs in BEC scams, though they lost some altitude during the second half of 2020. In Q3, gift cards were requested in 71% of all BEC attacks. But in Q4, that figure dropped to 60%. Meanwhile, wire transfers continue to appeal to BEC actors, accounting for 22% of BEC schemes in H2 2020. The average amount sought in these attacks rose 8%—boosted by those six-figure capital call scams, as well as a minimum request amount of $2,600.

Amount Requested Per BEC Attack Type

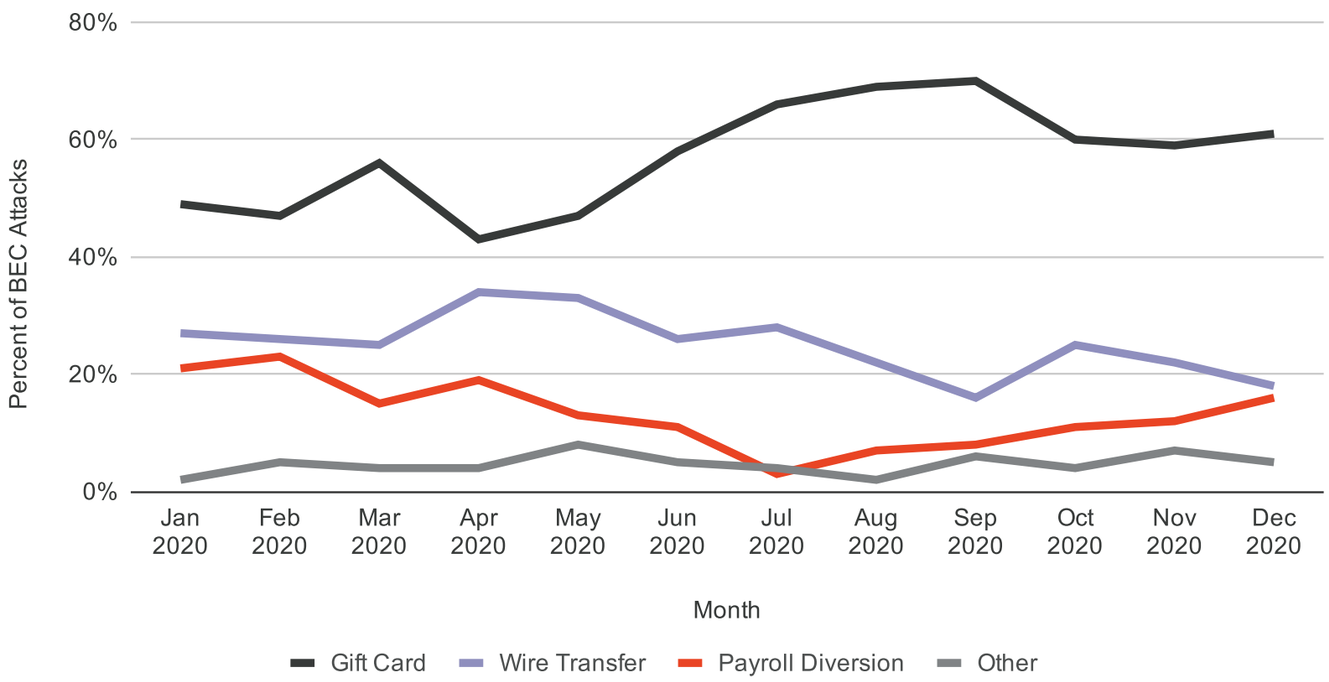
BEC Attack Type	Average	Median	Minimum	Maximum
Wire Transfer	$72,044	$35,200	$2,600	$999,600
Gift Card	$1,270	$1,000	$100	$8,000



Cash-Out Method for BEC Attacks

Payroll Diversion Scams on the Rise for Six Straight Months

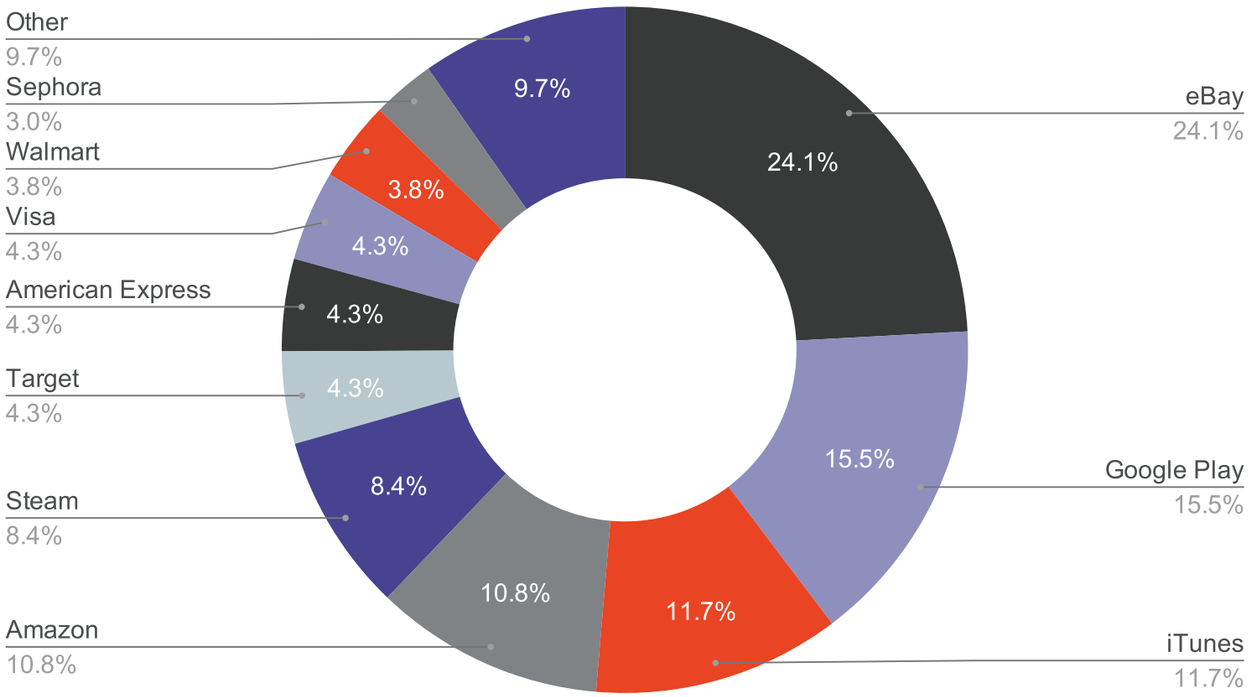
While payroll diversion ruses made up just 10% of all BEC scams throughout the last half of 2020, we saw some notable upward movement in these attacks throughout this six month period. In fact, the number of fraudulent requests to change the employee bank accounts used for direct deposit has increased for six straight months. With 7 in 10 corporate employees working remotely—including more than 15 million[11] who have moved across town, to nearby cities, or to far-flung Zoom towns during the first six months of the pandemic—may have given this pretext added believability. The steady increase in incidents suggests it's working.



Trends in BEC Cash-Out Methods

eBay Still #1 in Gift Card Scams, But Shifts May Be Underway

Maybe we should blame it on Pokémon[12]. Online marketplace eBay continues to be the most favored gift card sought in BEC attacks. During the second half of 2020, eBay accounted for nearly 1 in 4 (24.1%) gift cards requested by email scammers, followed most closely by Google Play (15.5%), iTunes (11.7%), and Amazon (10.8%). But during the fourth quarter, ACID researchers saw a significant increase in the number of scams seeking American Express, Visa, and OneVanilla gift cards. Generally BEC actors have traditionally requested brand-specific gift cards with an eye toward the online cryptocurrency exchange market, where the cards can be sold at some portion of their face value. This new shift may suggest cybercriminals are gravitating toward cash equivalents that can be used to place purchases of virtually any kind, online and off, at full face value.

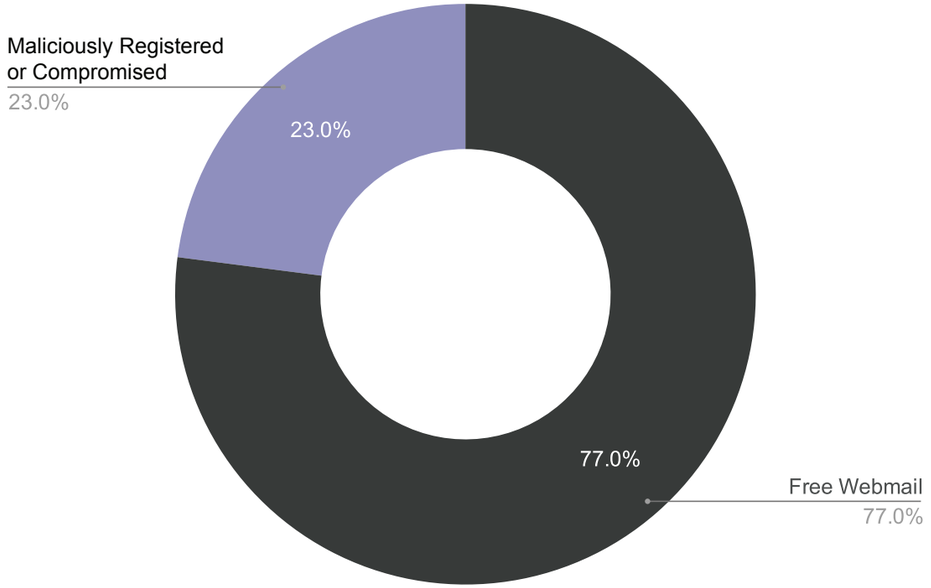


Gift Cards Requested in BEC Attacks

77%

Percentage of BEC Scams Using Free Webmail Accounts

During the second half of 2020, more than three-quarters (77%) of all BEC attacks were sent from a free webmail account—up 17% from January 2020.

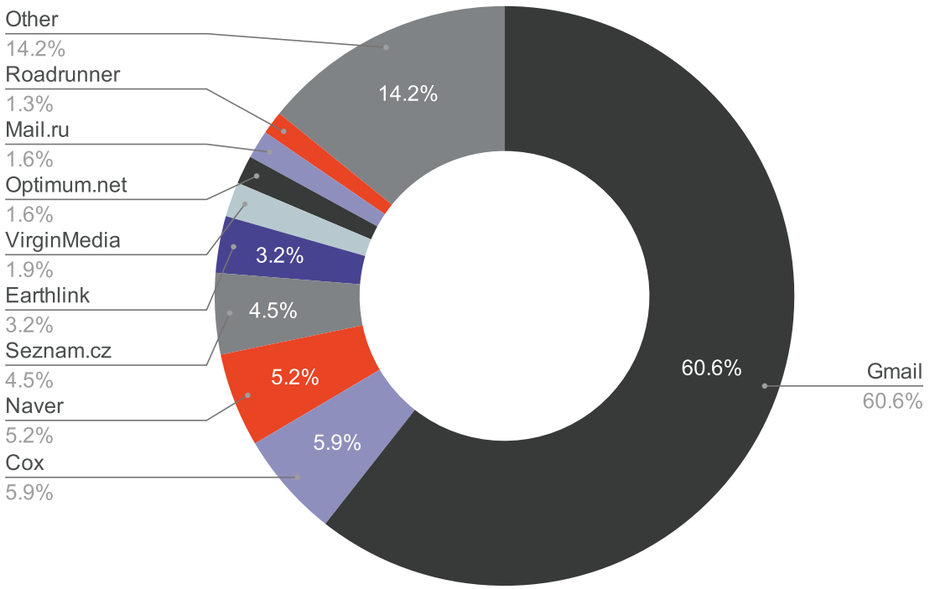


Email Account Type Used in BEC Attacks

#1

Gmail Continues to Be Top Platform for BEC Attackers

Google's Gmail remains the most weaponized email platform, accounting for 61% of BEC emails sent via free webmail accounts. That's up from 43% in June 2020, nearly double the number seen last January (35%).



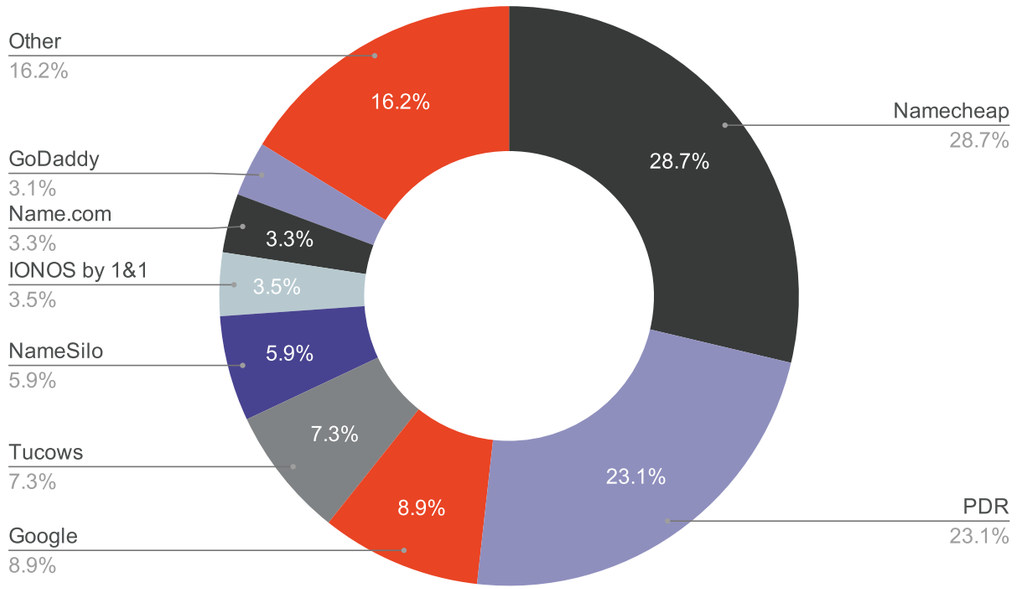
Email Service Providers Used in BEC Attacks

1 in 4

BEC Attacks Leverage Lookalike Domains

Meanwhile, 23%, or nearly 1 in 4, BEC attacks are sent from a domain registered by the attackers. Nearly two-thirds of these domains are registered with just three public domain registrars:

- Namecheap (29%)
- PDR (20%)
- Google (9%)



Registrars Used for Look-Alike Domain Attacks

Phishing Response Trends

KEY FINDINGS

65,898

The total number of potential phishing attacks reported by employees at large organizations participating in our survey during the second half of 2020

61%

More than 6 in 10 suspect emails reported by employees are ultimately deemed non-malicious

88X

Organizations with automated phishing response processes detect 88X the number of similar malicious messages exclusively reported by employees

21,712

The number of latent email threats detected and removed via continuous detection and response (CDR) capabilities that would have otherwise gone undetected post-delivery

Phishing Response Pressures Escalate

Employee-Reported Phishing Attacks Battering Overburdened SOCs

Evidence is mounting that Security Operations Center (SOC) teams may be buckling under an avalanche of phishing attacks both real and imagined. Even before work-from-home mandates, phishing was implicated in as much as 67% of all corporate data breaches, according to Verizon's 2020 Data Breach Investigations Report (VDBIR). And while Ponemon Institute's 2020 Total Cost of a Data Breach Report estimates an average $8.6 million[13] in costs per incident for US-based companies, the organization finished collecting data in April[14]. It warns remote working amid the pandemic is likely to increase that amount by another $137,000 per breach[15]. It didn't help that during the second half of 2020, anxious employees swamped already resource-constrained SOC teams with a title wave of suspected phishing incidents—most of which were ultimately deemed false positives. But organizations employing automated response technologies report were able to neutralize unreported threats while accelerating time-to-containment.

Inside the ACID H1 2021 Phishing Incident Response Survey

For this report, ACID researchers analyzed data from large organizations with an average of 21,000 employees in industries such as high-tech, healthcare, agriculture, construction, retail, energy, and more. The objective is to gain insights on reported incident volumes, false positive rates, and the impact of automation on the investigation and remediation of email threats from July through December 2020. This section of the H1 2021 Email Fraud and Identity Deception Trends Report features our analysis of these conversations.

61%

The False Positive Rate on Employee-Reported Phishing Incidents

Our mass experiment in working remotely via home Internet connections and personal computers has provided email threat actors with whole new avenues to potentially infiltrate corporate networks. It doesn't help that one-in-five employees fall for malicious emails and two-thirds[16] of them will go on to provide credentials to the fraudsters, according to a report from Microsoft. The really weird aspect about this: When they aren't clicking on actual phishing attacks, they're forwarding legitimate emails—a lot of them—to the SOC team for fear they're fraudulent. According to large client organizations participating in our H1 2021 Phishing Incident Response Survey, employee-reported phishing incidents topped 65,898 during the second half of the year. Unfortunately, 61% of them were ultimately found to be false positives. Which means SOC analysts were forced to spend valuable time investigating and resolving them—even as time-to-containment of true breaches and attacks grows longer and more costly.

Breachonomics

Manual Employee Incident Reporting: Too Much & Never Enough

Each minute wasted chasing down false positives means another minute a legitimate phishing email remains an active threat, increasing the chances it will lead to a data breach. According to Ponemon Institute, the average time to containment was already 280 days before the pandemic. And 76% of companies say remote working is likely to make that worse. But according to the organizations in our survey, automation is proving critical to preventing these kinds of infiltrations from ever happening—and collapsing time-to-containment from weeks or months down to just minutes for those that do. This is in part because on average, automated processes enable them to uncover far more attacks than those reported by employees.

88X

The Number of Additional Malicious Emails Detected Through Automated Response

Organizations in our survey report automated phishing response detects 88X more email threats than manual processes alone. Out of 13,986 verified phishing emails reported during the second half of 2020, companies with automated phishing response processes successfully identified 972,347 additional email threats that were similar, or directly related, to those reported by employees. Automating tasks associated with analysis and triage are credited as being central to achieving increased efficiencies and savings while avoiding breach costs.

13,989

Malicious Phish Reports

19,239,914

All Similar Messages Found

972,347

Similar Messages Confirmed Malicious

88x

Discovery Factor

Continuous Detection and Response

Detecting and Removing Additional, Latent Email Threats

21,712

Additional Email Threats Neutralized Through CDR—a 4X Increase Over June 2020

Organizations in our survey report that continuous detection and response (CDR) technologies leveraging shared threat intelligence identified more than 21,712 malicious messages beyond those detected through automated phishing response alone. That's a 4X increase over the previous six month period. Additionally, 724 unique events identified solely through these technologies. At their most essential, CDR technologies identify latent threats that have evaded detection through new identity deception techniques, dormant payloads, or "time-bombed" URLs that redirect only after they've been delivered to the target's inbox. By analyzing company-wide email metadata, these technologies forensically recognize and remove email threats from all inboxes automatically.

38 Minutes

Average Remediation Time on Reported Phishing Attack Using Automation

According to survey participants, legitimate phishing attacks reported by end users are remediated within 38 minutes with the aid of automated response technologies that prioritize incidents based on potential impact to the organization and the identification of all affected employees. To put the importance of this kind of capability into perspective, studies from Aberdeen show there's a 30% chance of a first-user click on a malicious email within 60 seconds of delivery, with a median time-to-first-click on malicious emails of just 134 seconds.

Customer Phishing and DMARC Trends

KEY FINDINGS

5.85 Billion

Malicious emails spoofing corporate and government email domains from July through December 2020, with those in Healthcare, Technology and Government impersonated most in phishing scams

32%

The percentage increase in global domains with an identifiable DMARC policy during the second half of 2020, a number that reached 10.7 million domains worldwide—up from 8.1 million during H1

3 in 4

Today, 76% of Fortune 500 companies remain vulnerable to getting impersonated in phishing scams targeting their customers, partners, investors, and the general public

82%

The increase in brand domains that have BIMI records, which reached 9,079 in the fourth quarter of 2020—up from just 4,983 in Q1 2020

DMARC Adoption Snapshot

The Industry's Largest Ongoing Study of Adoption Trends Worldwide

In a snapshot of more than 426 million+ Internet domains, we analyze adoption trends for Domain-based Message Authentication, Reporting, and Conformance (DMARC) from July through December 2020.

10.7 Million

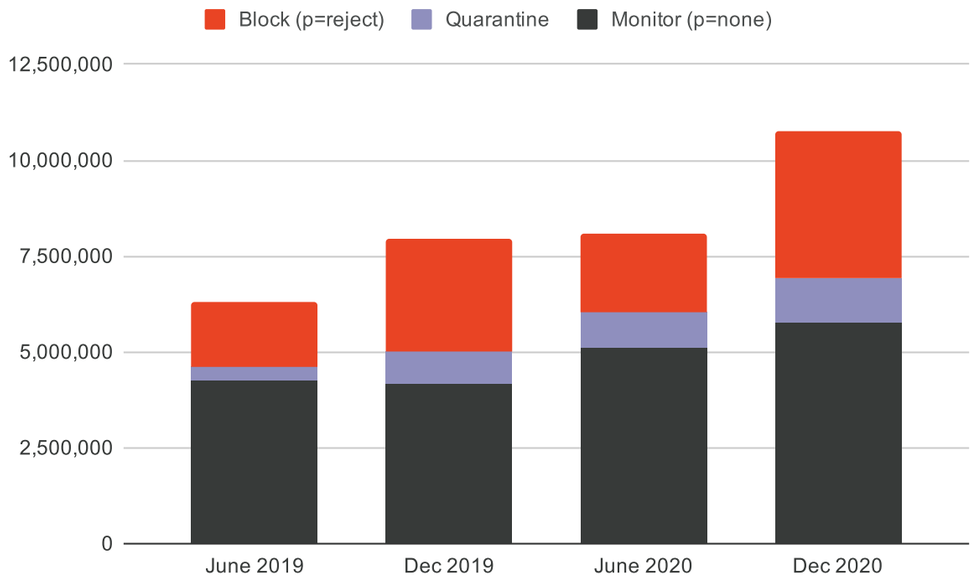
The Number of Domains With Recognizable DMARC Policies Worldwide—up 32% in Just Six Months

But don't break out the champagne just yet. While this notable increase in the number of domains with an identifiable DMARC policy is encouraging, it still represents just a tiny fraction of the half-billion domains our researchers scanned worldwide.

3.8 Million

3,826,830 Domains Have DMARC Set to Its Highest Enforcement Level—an 87% Increase from H1 2020, But Woefully Low in Absolute Numbers

Failure to implement DMARC with the p=reject enforcement leaves organizations at risk from cybercriminals seeking to pirate their brand and domains to target phishing attacks at their customers and other consumers and businesses. These domains may also be blacklisted by receiver systems, or experience reduced deliverability rates for the brand's legitimate email messages, resulting in costly disruptions to their email-based marketing and revenue streams. But when implemented properly, DMARC has been shown to reduce domain spoofing to near zero while boosting email conversion rates as much as 10%, according to Forrester Research.



Growth in Number of Domains with DMARC Policies, 2019–2020

For more information on DMARC adoption and its benefits, visit **www.agari.com/dmarc-guide**

DMARC Breakout Session

Germany Vaults Ahead in DMARC Set at Reject

As part of this report, ACID examines the state of DMARC adoption by key geographies during the second half of 2020. In any given period, a rising number of new domains can cause changes to the total percentage of domains with DMARC policies, as well as those with DMARC policies at full enforcement.

#1

Germany Leapfrogs US & The Netherlands with DMARC Policies at Full Enforcement

Among the ten largest country-code domains, the United States racked up a 21% increase in the percentage of domains with DMARC policies set to the strictest possible enforcement level in just six months, helping it to outpace The Netherlands. But during the same period, Germany achieved a remarkable 38% increase in DMARC policies at full enforcement, the level needed to prevent domains from being used to send phishing attacks.

3

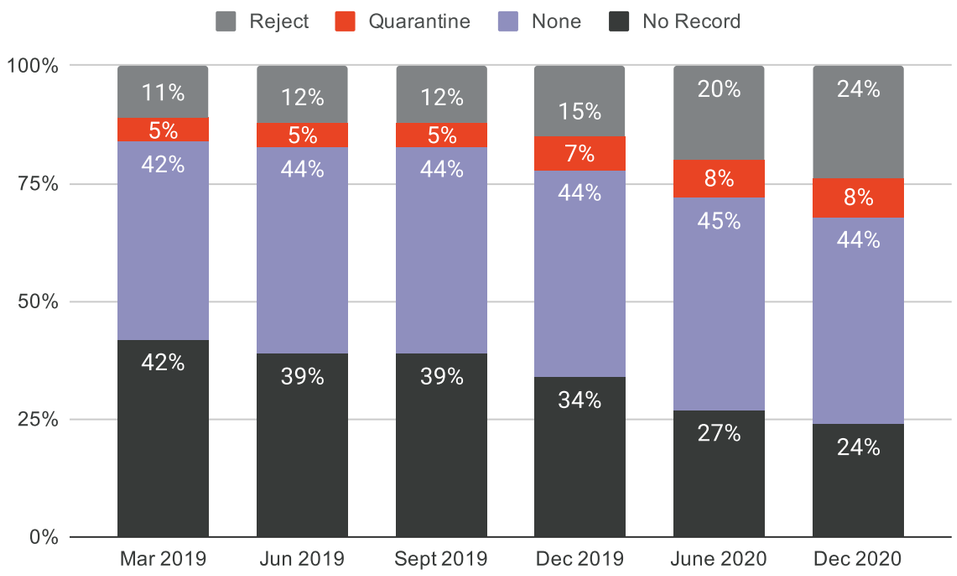
The Total Number of Countries with at Least 50% of Domains with DMARC Policies Set to Reject

Among all countries, just three have at least 50% of domains with DMARC policies set to their strictest enforcement level—Germany, Colombia, and the British Virgin Islands.

10 Largest Country-Code Domains, Ranked by DMARC Enforcement Rate

DMARC Adoption Trends Among the World's Largest Companies

This report captures DMARC adoption trends among some of the world's most prominent companies through the second half of 2020—including Germany's HDAX, which joins the Fortune 500, FTSE 100 and the ASX 100 in our index for the first time. It's important to note that even when organizations have assigned DMARC records to their domains, they are not truly protected unless they are set to a level of enforcement. The sizable proportion of "no record" and "monitor only" policies highlights the fact that these organizations can still be impersonated in phishing campaigns that put their customers and other consumers and businesses at risk of serious financial harm.



DMARC Adoption by Large Public Companies: Fortune 500 (United States)

5.85 Billion

The Number of Malicious Emails Spoofing Domains During H2 2020

From July through December 2020, the number of malicious emails spoofing corporate or government domains topped 5.8 billion (or 2.28% of all email). That's 32 million fraudulent emails impersonating the domains of well-known brands every day of the week, at a rate of 1.3 million per minute.

24%

Fortune 500 Companies with DMARC Set at Full Enforcement to Prevent Domain Spoofing

That's an increase of 20% from June 2020. Together with the 8% of DMARC-assigned domains with a p=quarantine policy, 32% of Fortune 500 domains with DMARC policies set with at least some level of protection rose 10% during the same period.

3/4

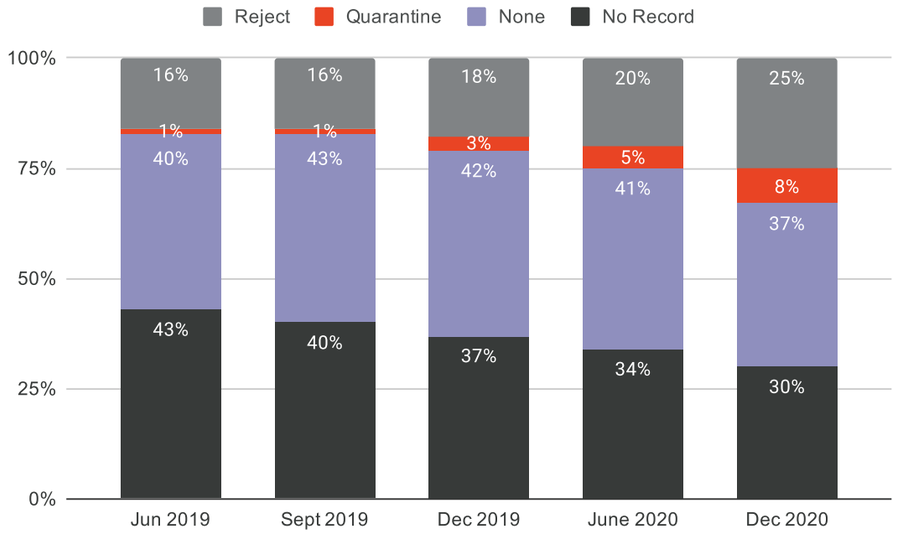
Fortune 500 Companies Remaining at Risk of Being Impersonated in Email Scams Targeting Customers, Partners & More

Maybe it got put on the back-burner because of everything else 2020 threw their way. Whatever the case, 76% of Fortune 500 companies lack the protection needed to prevent email threat actors from hijacking their domains and impersonating their brands in phishing attacks. Which may help explain why Gartner ranks DMARC implementation[17] as a top priority for every organization in 2021.

1 in 4

FTSE 100 Companies Protect Against Brand Impersonation—a 25% Increase

The number of companies on the UK's FTSE 100 with domains protected by DMARC set to p=reject grew to 25 during the second half of 2020—up from 20 at mid-year. While commendable, it still means that 75% of the FTSE 100 does not yet have protections in place to prevent threat actors from impersonating their brands in email attacks targeting customers, investors, and the general public.

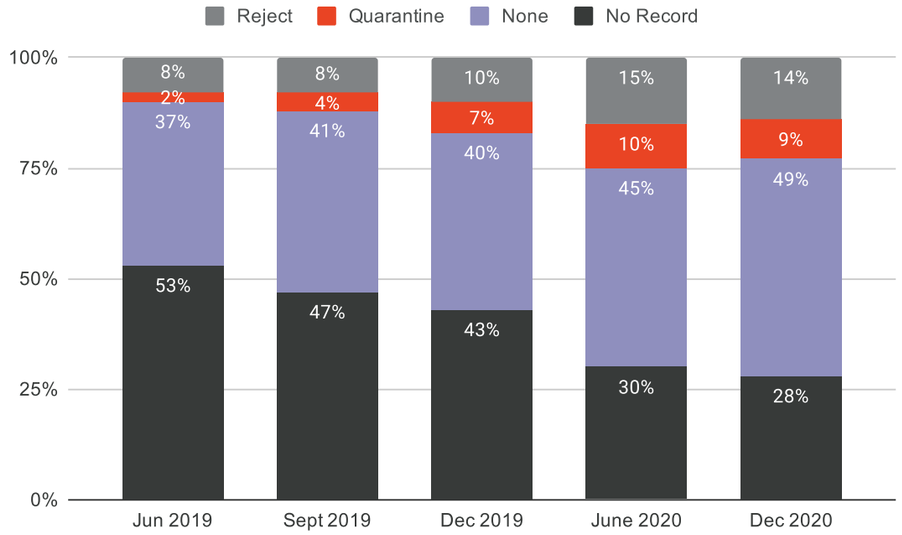


DMARC Adoption by Large Public Companies: FTSE 100 (United Kingdom)

86%

Number of Australia's ASX 100 Companies That Continue to Put Customers at Risk

Amid a push to increase the number of Australian government domains protected by DMARC[18], the private sector is still struggling with deployment, even as the total number of domains in use continues to rise. Today, just 14% of ASX 100 companies have DMARC policies set to full enforcement—leaving 85% at risk of email threat actors pirating their domains for use in phishing attacks.

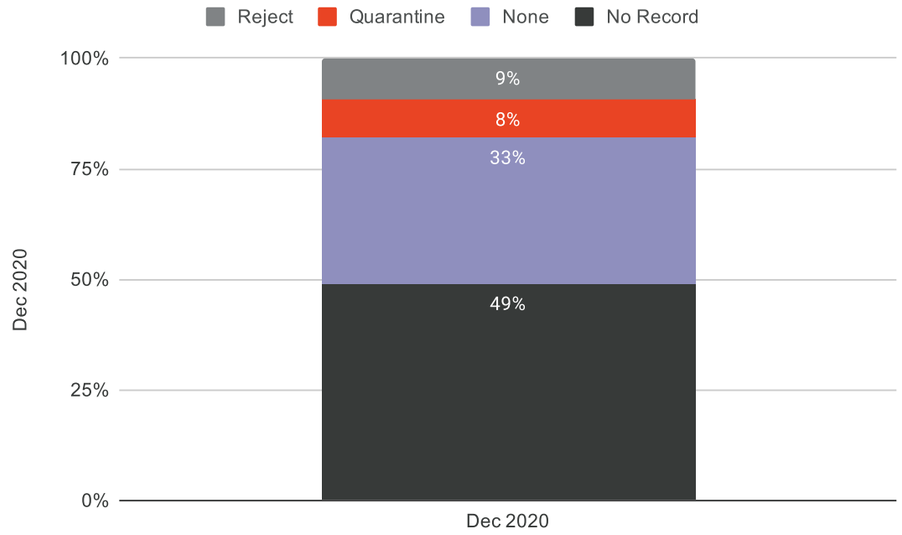


DMARC Adoption by Large Public Companies: ASX 100 (Australia)

9%

HDAX Companies With DMARC Policies Set to Full Enforcement

A sustained onslaught of BEC and phishing campaigns were implicated in attacks that have cost the German government[19] and businesses[20] tens of millions of euros in 2020—and even led to loss of life[21]. These dramatic wake-up calls were likely a factor in that country's spike in domains with DMARC policies set at reject, noted earlier. But for the large companies within the HDAX stock index, deployment across a very large number of domains can be costly and time consuming. As a result, just 9% of the 110 companies in the index have domains with DMARC policies at full enforcement, and another 8% at quarantine. That leaves 91% of HDAX companies with domains at risk of abuse by fraudsters.



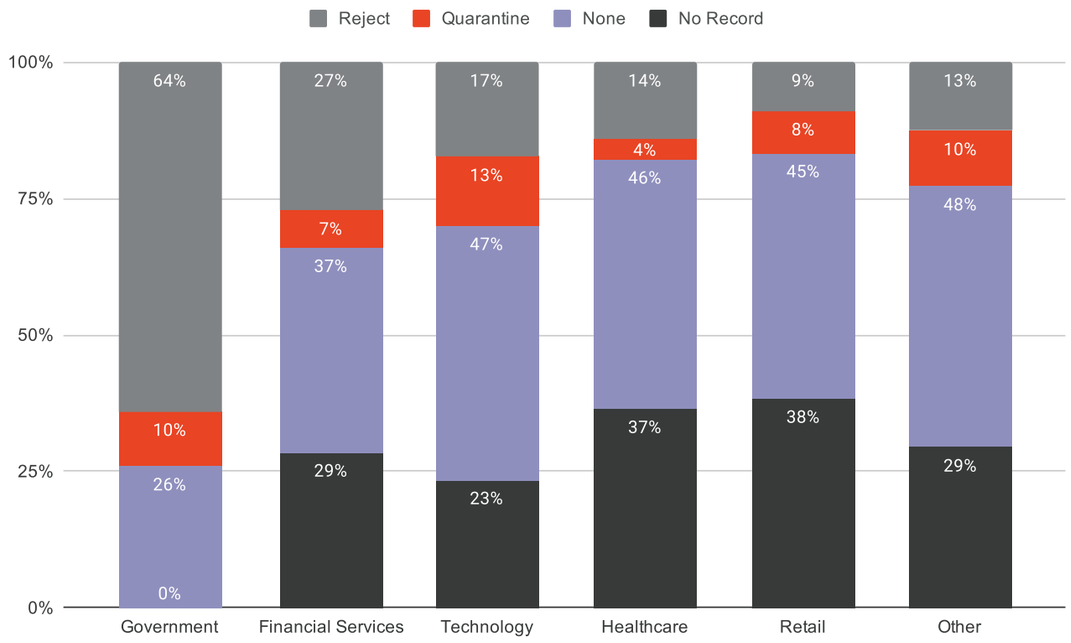
DMARC Adoption by Large Public Companies:
HDAX (Germany)

DMARC Adoption by Industry Vertical

Data in our H1 2021 report includes DMARC adoption across key industry verticals and is based on public DNS records for primary corporate website domains of large companies with revenues above $1 billion USD. Every vertical has shown incremental improvements in the percentage of their DMARC-enabled domains at p=reject since our last report.

Tech, Healthcare & Government Most Impersonated in Phishing Attacks

Putting a fine point on the need for DMARC protection: During the second half of 2020, organizations in technology, healthcare, and government were impersonated most in phishing attacks leveraging unprotected email domains. None of which is surprising, given the ongoing COVID-19 pandemic and the resulting 57% of corporate employees working from home. Ever the opportunists, fraudsters also sought to exploit unprotected domains for attacks related to US political crises—leading to a noticeable spike in spoofed domains leading up to the November presidential elections through the first several days of 2021.



DMARC Enforcement Rates for Key Industry Sectors

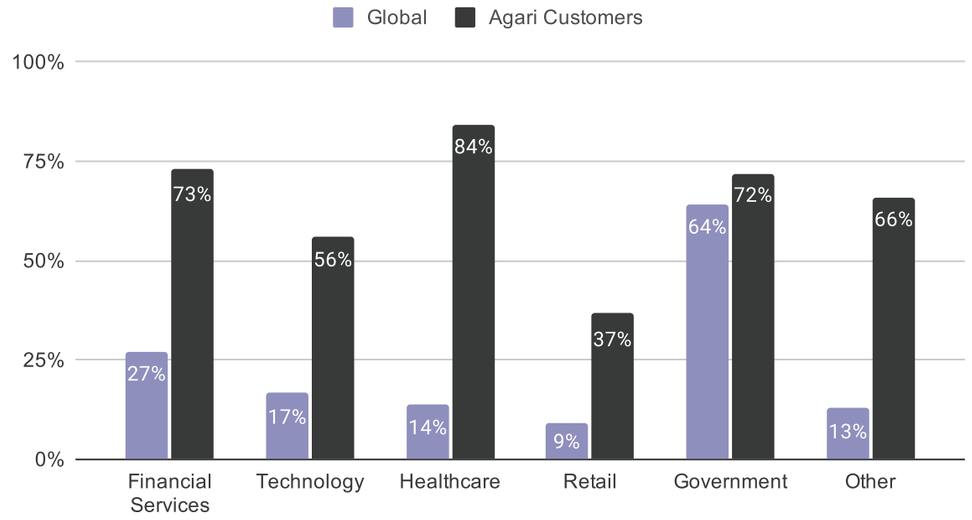
The Agari Advantage
Industry Enforcement Comparison

With real-time statistics from the domains of top banks, social networks, healthcare providers, major government agencies and thousands of other organizations, the Agari Email Threat Center is the largest set of detailed DMARC data in the world both in terms of email volume and domains. This data enables us to understand how enforcement rates across industries compare with those of Agari customers. To generate real-time threat intelligence, the Agari Email Threat Center analyzed more than 257.9 billion emails from more than 20,727 domains from July through December 2020.

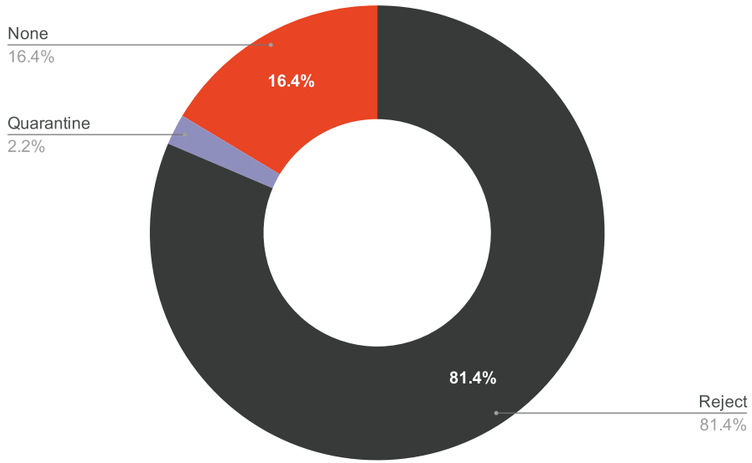
6X

Agari Healthcare Industry Customers with Domains at Full DMARC Enforcement vs. the Industry Average

Take the worst pandemic in modern history. Add fear, confusion, and unprotected email domains and mix. From phishing campaigns impersonating Vanderbilt University Medical Center to the Centers for Disease Control (CDC) to Health and Human Services (HHS) and other healthcare authorities, Agari customers in the sector had ample reason to beef up DMARC implementation efforts. As of December 2020, 84% of Agari healthcare customers' domains are set at a p=reject enforcement level. That's 6X the industry average of only 14% of domains protected with DMARC at its highest enforcement level.



Share of Industry Domains at Strong DMARC Enforcement, December 2020

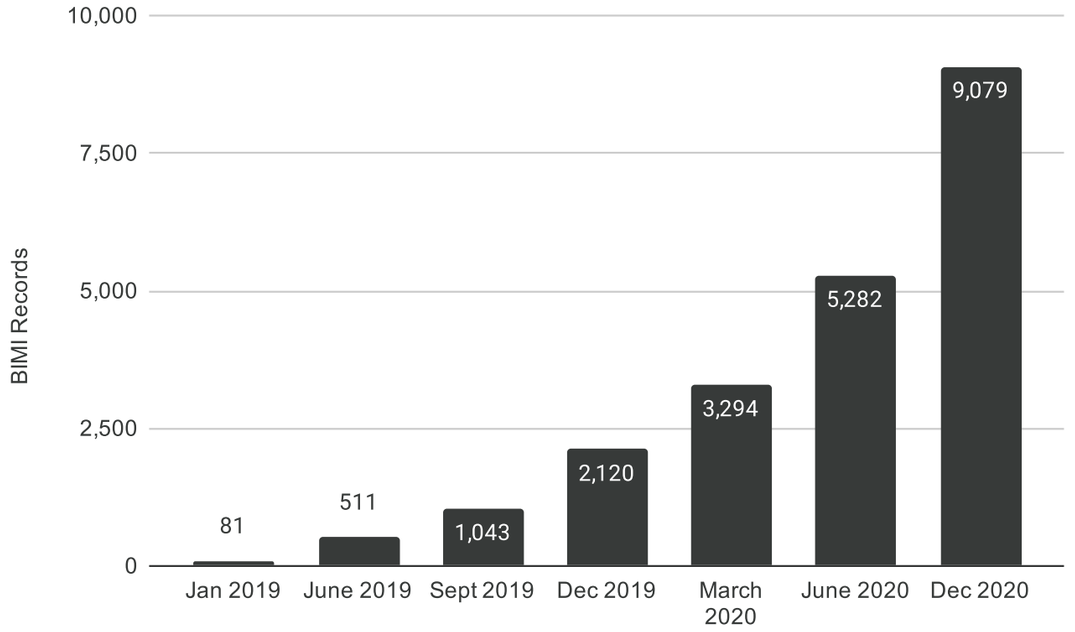


DMARC Enforcement Rate for All Agari Customers

Brand Indicators Adoption

BIMI is Officially Trending as Adoption Skyrockets

Brand Indicators for Message Identification (BIMI) benefits the entire email ecosystem by providing businesses with a standardized method for publishing their brand logos next to their email messages within a recipient ‘s inbox, with built-in protections against brand spoofing. At a time when email’s role as the indispensable digital channel has never been more critical to marketers, the launch of Google’s high-profile BIMI pilot provided additional rocket fuel for this rapidly-growing standard.



Growth in Number of Domains with BIMI Record, 2019–2020

9,079

The Total Number of Brand Domains with BIMI Records as of December 31, 2020

BIMI only works with email that has been authenticated through the DMARC standard for which the domain owner has specified a DMARC policy enforcement, so only authenticated email messages can be delivered.

DMARC has been shown to boost deliverability rates. BIMI adds a verified logo indicating the email is legitimate and comes from an authentic domain from the brand. Though it will take time for BIMI to gain additional mindshare and trust, early tests show it has already been shown to boost open rates by as much as 10%[22].

72%

Increase in Brand BIMI Adoption in Just 6 Months

During the second half of 2020, BIMI adoption grew 72% from just 5,282 in H1. One significant contributing factor: the July launch of Google's BIMI pilot, which allowed a select group of organizations who authenticate their emails using DMARC to validate ownership of their corporate logos and securely use them in email messages. Once these authenticated emails pass Google's anti-abuse checks, Gmail displays the logo in existing avatar slots within the Gmail interface. Google and other inbox providers are expected to expand their BIMI pilots to more brands in 2021.

Protecting Against Advanced Email Threats Through the Power of Trusted Email Identity™

As the financial and reputational damage from phishing, BEC, and other advanced email threats continue to mount, Agari has become the market leader in protecting brands and people from devastating phishing and socially-engineered attacks through solutions that include:

Agari Phishing Defense™ prevents email threats from reaching employee inboxes by scoring every message flowing into and within the organization to defend against low-volume, highly-targeted identity deception-based attacks.

Agari Brand Protection™ protects your customers from costly phishing attacks by automating and simplifying DMARC email authentication and enforcement, preserving brand identity, and boosting digital engagement.

Agari Phishing Response™ prioritizes reported incidents, automating investigative analysis and triage, to elevate the most suspicious emails to the top of the list. Then, it reduces manual efforts with remediation workflows to accelerate time-to-containment.

Agari Active Defense™ BEC Threat Intelligence Service uses automated active engagement to uncover criminals' tactics and techniques and deliver highly-focused, actionable intel about specific phishing and BEC threats targeting your organization.

Leveraging applied data science and a diverse set of signals, Agari protects the workforce from inbound BEC scams, supply chain fraud, spear-phishing, and account-takeover-based attacks—reducing business risk and restoring trust to the inbox. Agari also prevents spoofing of outbound email from the enterprise to customers, increasing deliverability and preserving brand integrity and reputation. Learn more at www.agari.com.

About This Report

Taxonomy of Advanced Email Threats

ACID has established a classification system for cyber threats—a threat taxonomy—that breaks down common email-based attacks in terms of how they are carried out and what the perpetrators aim to achieve. This taxonomy helps readers understand the terms used in this report and what they mean to email security.

The metrics and data analyzed in this report are collected from the sources indicated below.

Aggregate Advanced Email Attack Data

For inbound threat protection, Agari uses machine learning—combined with knowledge of an organization's email environment—to model good, legitimate traffic. Each message received by Agari is scored and plotted in terms of email senders' and recipients' identity characteristics, expected behavior, and personal, organizational, and industry-level relationships. For the attack categorization analysis, we leveraged anonymous aggregate scoring data that automatically breaks out identity deception-based attacks that bypass upstream Secure Email Gateways (SEGs) into distinct threat categories, such as display name deception, compromised accounts, and more. See section on "Taxonomy of Advanced Email Attacks" on the preceding page.

Phishing Incident Response Trends

This report presents results from a survey of large organizations in a cross-section of industries conducted by Agari in December 2020.

Global DMARC Domain Analysis

For broader insight into DMARC policies beyond what we observed in email traffic targeting Agari's customer base, we analyzed **426 million** domains, ultimately observing 10,744,092 domains with recognizable DMARC policies attached. This constantly updated list of domains serves as the basis for trend tracking in subsequent reports.

End Notes

[1] Mike Moore, “GoDaddy suffers embarrassing phishing attack,” TechRadar, April 3, 2020

[2] Dmitry Dontov, “What Businesses Are The Most Vulnerable To Cyberattacks,” Forbes, January 19, 2021

[3] Colin Bastable, “Why the $26 billion in BEC scams are worse than you think,” SC Magazine, September 23, 2020

[4] Michael Novinson, “SolarWinds CEO Confirms Office 365 Email ‘Compromise’ Played Role In Broad-Based Attack,” CRN, February 4, 2021

[5] Adam Rowe, “What Do the Worst Security Threats of the Year Tell Us About 2021,” Tech. co, December 24, 2020

[6] Colin Bastable, “Why the $26 billion in BEC scams are worse than you think,” SC Magazine, September 23, 2020

[7] Crane Hassold, “Cusmic Lynx Returns in 2021 with Updated Tricks,” Agari Email Security Blog, February 11, 2021

[8] Crane Hassold, “Ancient Tortoise: A Deeper Look at the Aging Report BEC Attack Chain,” Agari Email Security Blog, January 14, 2020

[9] Agari, “Threat Intelligence Brief: The Geography of BEC,” White Paper, August 2020

[10] Lindsey O’Donnell, “How Email Attacks are Evolving in 2021,” ThreatPost, February 11, 2021

[11] Cynthia Paez Bowman, “Coronavirus Moving Study: People Left Big Cities, Temporary Moves Spiked In First 6 Months of COVID-19 Pandemic,” MyMove, February 17, 2021

[12] Ambrose Leung, “eBay’s Trading Card Report Shows a 574% Increase in Pokémon Card Sales in 2020,” Hyperbeast, February 11, 2021

[13] IBM, Ponemon Institute, “Cost of a Data Breach Report, 2020

[14] Dice Staff, “Data Breach Costs: Calculating the Losses for Security and IT Pros, February 22, 2021

[15] IBM, Ponemon Institute, “Cost of a Data Breach Report, 2020

[16] “Why are we still falling for phishing attacks,” T_HQ, December 18, 2020

[17] Kasey Panetta, “Gartner Top 10 Security Projects for 2020-2021,” Gartner, September 15, 2020

[18] Chris Duckett, “DMARC inching its way onto Australian government domains,” ZDNet, December 7, 2020

[19] Sabina Weston, “German government loses ‘tens of millions’ in COVID-19 phishing attack,” ITPro, April 20, 2020

[20] Tara Seals, “Steganography Anchors Pinpoint Attacks on Industrial Targets,” ThreatPost, May 29, 2020

[21] Heather Landi, “Could patients be at risk during a hospital cyberattack? It depends on how far hackers are willing to go,” Fierce Healthcare, Nov 23, 2020

[22] Jennifer Cannon, “Everything marketers need to know about BIMI: The latest email standard,” Marketing Land, March 9, 2020

About Fortra's Agari Cyber Intelligence Division

Agari Cyber Intelligence Division (ACID) is the world's only counterintelligence research group dedicated to business email compromise (BEC) investigation and cybercrime abatement. ACID has conducted more than 12,000 active defense engagements with threat actors since May 2019. ACID works closely with CISOs at global enterprises, law enforcement, and other trusted partners to stop identity-based phishing and socially-engineered cybercrimes.

Learn more at acid.agari.com

AGARI CYBER
INTELLIGENCE DIVISION

Discover How Agari Can Improve Your Current Email Security Infrastructure

As your last line of defense against advanced email attacks, Agari stops attacks that bypass other technologies—protecting employees and customers, while also enabling incident response teams to quickly analyze and respond to targeted attacks.

Get Free Trial www.agari.com/trial

Visit the Agari Threat Center

To see up-to-date global and sector-based DMARC trends across the Agari customer base, visit: **www.agari.com/threatcenter**

Calculate the ROI of Implementing Agari

To discover how much money you can save by adding Agari to your email security environment, visit: **www.agari.com/roi**

hds-rp-0922-79d