AGARI CYBER
INTELLIGENCE DIVISION

REPORT

H2 2020

Email Fraud & Identity Deception Trends

Global Insights from the Agari Identity Graph™

agari
by HelpSystems

Executive Summary

Needless to say, 2020 will rewrite the record books. With successful phishing and business email compromise (BEC) scams growing less reliant on technical acumen than on savvy social engineering, email threat actors rang in the year with every reason to expect outlandish profits ahead. Then came COVID-19. In the blink of an eye, the email attack surface ballooned to include tens of millions of corporate employees working from home. As substantiated in this mid-year analysis from the Agari Cyber Intelligence Division (ACID), the pandemic became the go-to pretext for attackers bent on exploiting a period of unprecedented angst. And it shows: By mid-May, the FBI reported the total volume of phishing and BEC emails exceeded all of 2019. Which means last year's staggering $8.6 billion in potential business losses from advanced email threats may pale in comparison to 2020's final tally.

BEC Themes Evolve, But the Song Remains the Same

COVID-themed attack volume remained relatively steady from mid-March through early June, before trailing off. Yet while the COVID drumbeat has died down, the same BEC riffs play on. With 70% of BEC attacks launched from free webmail accounts, a dramatic increase from 54% during Q4 2019, attackers are putting a premium on speed and flexibility with these temporary, disposable assets. Meanwhile, gift cards continue to be the preferred form of payment in BEC ploys, resulting in the number of payroll diversion attacks decreased to 13% of the total, compared to 25% at the end of last year. SEE MORE ▶

Shell-Shocked Employees Increasingly Report False Positives to SOC Team

Anxious employees armed with tools to report suspect emails walloped Security Operations Centers (SOCs) with more incidents to analyze, triage, and remediate than they could possibly manage. As captured in our H2 2020 ACID Phishing Response Survey of 13 large organizations in a mix of industries, this chronic challenge was further aggravated by a 67% false positive rate. Organizations deploying advanced phishing response workflows to identify the full scope of phishing attacks, however, detected and remediated 90X more verified malicious emails connected or similar to those submitted by employees—a 100% increase from our last report. SEE MORE ▶

DMARC Adoption's Slow Grind Continues; 80% of Fortune 500 Remain Vulnerable

The first half of 2020 saw an additional 25 companies within the Fortune 500 companies adopt Domain-based Message Authentication, Reporting, and Conformance (DMARC)—bringing the total to 20% of all organizations within the index. Yet while salutary, that means 80% of the nation's largest companies remain susceptible to cybercriminals seeking to hijack their domains for use in phishing-based brand impersonation attacks that put their customers at risk of significant financial damage. More encouraging: the 3,800% increase in brands adopting Brand Indicators for Message Identification (BIMI) within just the last six months. SEE MORE ▶

Inside This Report

The intelligence presented in this report reflect data captured via the following sources from January 1 through June 30, 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 **477 million+** domains crawled worldwide
- Incident data from SOC professionals at **13 large companies** spanning multiple industries

ACID is the only counterintelligence research team dedicated to worldwide BEC and spear-phishing investigations and the identity deception tactics, criminal group dynamics, and other relevant trends behind today's most advanced email threats. Created by Agari in 2018, ACID helps to mitigate cybercriminal activity by working with law enforcement and other trusted partners.

Table of Contents

Employee Phishing and Business Email Compromise Trends

KEY FINDINGS

+3,000%
The percentage increase in COVID-themed phishing attacks beginning the week of March 8 and lasting through early June

70%
The increase in BEC scams launched from free webmail accounts, up from just 54% during the fourth quarter of 2019—a 26% jump in just 180 days

2/3
Malicious emails employing identity deception tactics that impersonated well-known brands—most notably the World Health Organization (WHO), the Centers for Disease Control (CDC), and others

Counterfeit Contagion

COVID-19 Becomes the Viral Engine for BEC Attacks in First Half of 2020

Scam artists have always sought to profit when crisis strikes. That includes malicious actors who refine phishing attacks to leverage national or global events–few as consequential to the whole of humanity as the coronavirus pandemic. The gravity of the situation, and the emotional levers it made available to cyber-swindlers, are reflected in data captured during the first half.

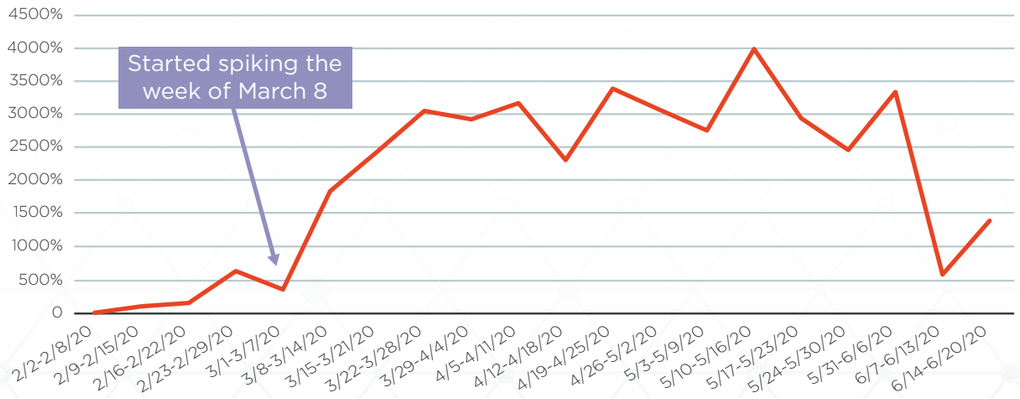
3000%

Rise in COVID-Themed Phishing Attacks Mid-March Through Early June

Starting the week of March 8, the volume of COVID-themed phishing attacks saw explosive growth over levels seen at the beginning of February, as corporate employees grappling with remote working, homebound children, concerns over the virus, and financial uncertainties were targeted in an unprecedented number of socially-engineered attacks. The trajectory of these schemes and its correlation with Google search data related to the outbreak is remarkable and consistent—bringing the symbiosis between events-driven anxieties and actions to exploit them into sharp relief. These coinciding trendlines remained relatively steady from mid-March until early June, before trailing off by quarter's end.

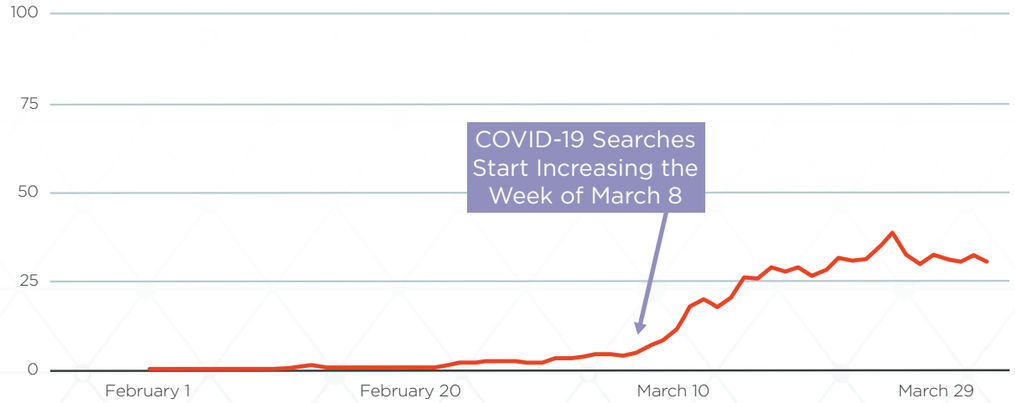
How Bad Has COVID-19 Phishing Gotten?

Cumulative Increase in COVID-19-Themed Email Attacks Since February



Cybercriminals Pay Attention to Global Trends

Source: Google Search Trends



Bait and Phish

Identity Deception Makes the Most of the Lure du Jour

2/3

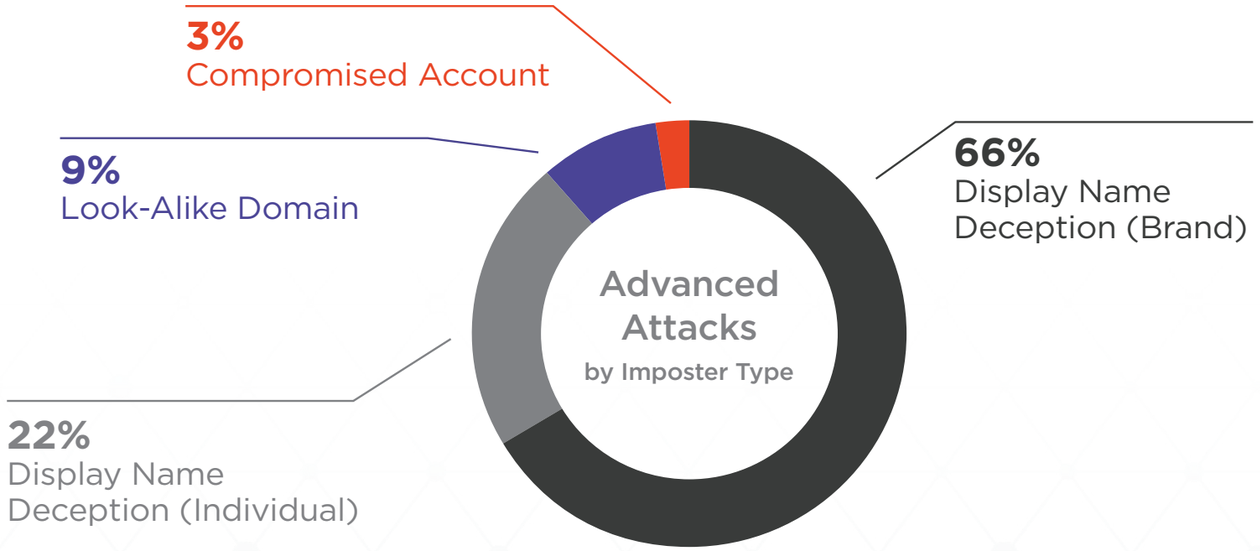
Phishing Emails Employing Identity Deception Impersonating Well-Known Brands

Two-thirds of malicious emails employing identity deception techniques involved display names designed to dupe recipients into believing the messages came from a well-known brand. This includes a significant number of phishing attacks impersonating the World Health Organization (WHO), the Centers for Disease Control (CDC), Microsoft, and others in massive credentials harvesting campaigns launched early in the coronavirus outbreak.

22%

Percentage of Impersonation Attacks Posing as Trusted Individuals

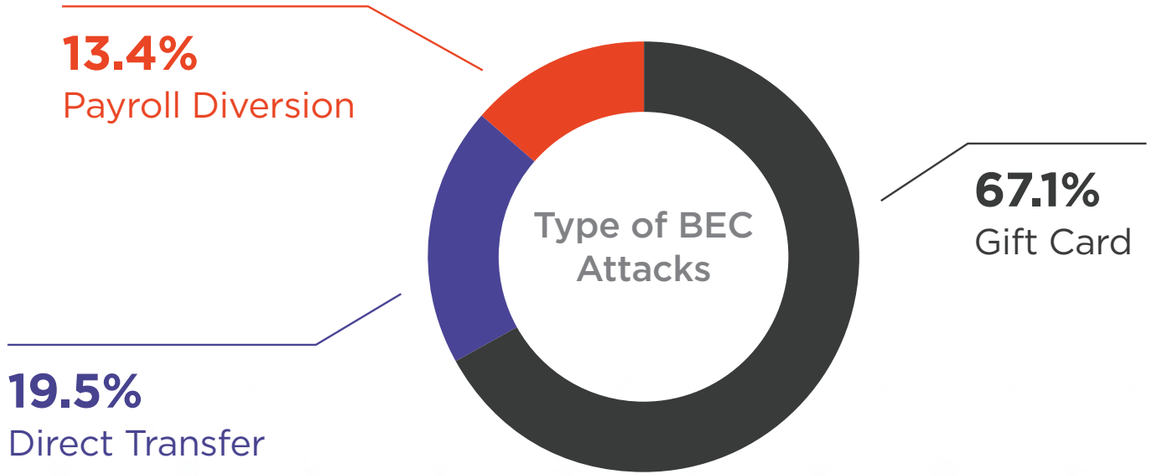
During H1 2020, just under a quarter of all impersonation attacks masqueraded as trusted individuals, usually a senior executive within the recipient's company or an outside vendor. The fraud group we call Ancient Tortoise, for instance, used COVID-19 as the pretext for changes to payment details when targeting companies in aging accounts receivable scams by posing as members of a supplier's accounts receivables team. Another, a criminal organization we call Cosmic Lynx, is the first-reported BEC group operating out of Eastern Europe—suggesting socially-engineered email impersonations are expanding beyond their roots among West African email fraudsters.



BEC Breakout Session

Gift Cards Still King, But Requested Cash-Out Amounts Lose Altitude

Ubiquitous and easy to sell for pennies on the dollar in online cryptocurrency exchanges, gift cards are the preferred payment method in more than 67% of all BEC plays—up from 62% during the fourth quarter of 2019. During the same period, the number of payroll diversion attacks decreasing to 13% of the total, compared to 25% at the end of last year.



Amount Requested Per BEC Attack Type

BEC Attack Type	Average	Median	Minimum	Maximum
Wire Transfer	$66,790	$29,613	$500	$1,555,770
Gift Card	$1,348	$1,000	$80	$15,000

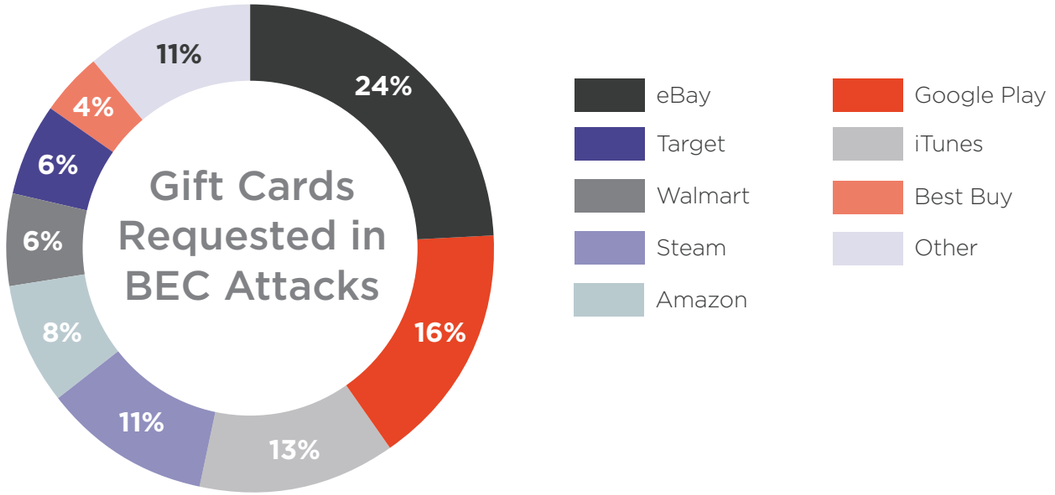
$1,555,770

Maximum Requested in Wire Transfer Ploys During the First Half of 2020

Amounts requested in gift card ruses retreated to $1,348 on average, compared to nearly $1,600 at the end of 2019. Meanwhile, amounts sought in wire transfer schemes rose to an average $66,790, from $55,395 six months earlier. The maximum requested in a wire transfer attack observed by ACID so far this year: $1,555,770—up from $680,456.

Shifts Seen in Gift Cards Requested in BEC Heists During First Half

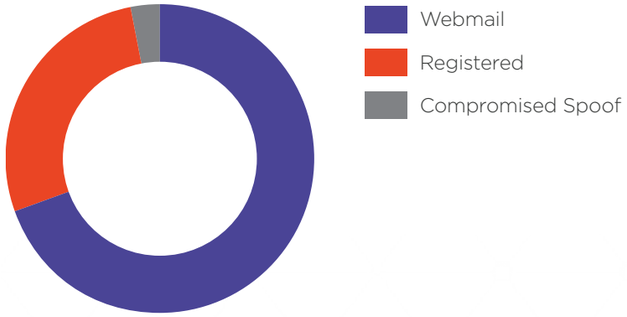
Popular online marketplace eBay has overtaken longtime fraudster favorite Google Play as the top gift card sought in BEC attacks. During the first half of the year, eBay accounted for 23% of all gift cards requested by email scammers—compared to just 5% last June. This change may reflect a glut in Google Play gift cards, or it could mark a shift toward cards for purchasing physical goods for direct use or for resale online.



70%

Percentage of BEC Scams Using Free Webmail—Up More Than 10%

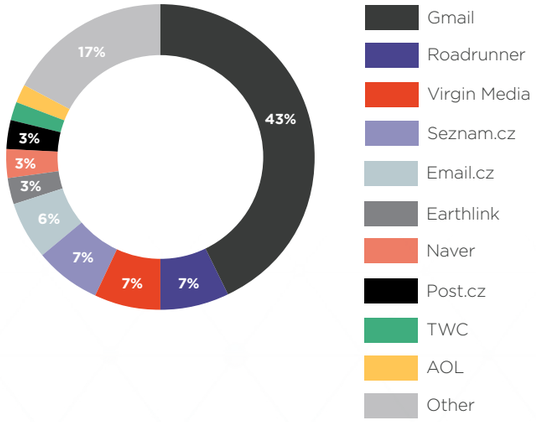
Our data shows that in the first half of 2020, nearly 70% of all BEC emails were sent from a free webmail account—a 10% increase in the last six months.



#1

Gmail Remains The Most Weaponized Email Platform

Gmail accounts were used to launch 43% of all BEC scams, up from 35% since our last report.

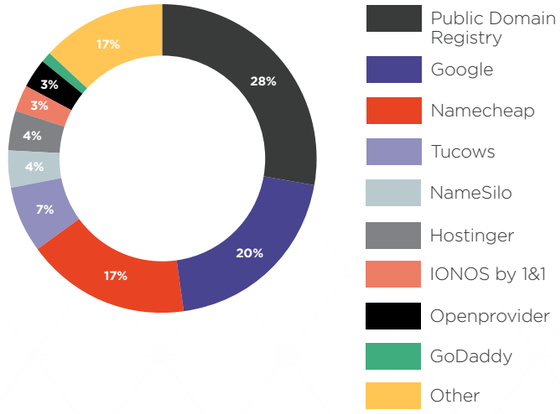


27%

BEC Emails Sent From Registered Lookalike Domains

Nearly 30% of BEC campaigns are launched from a domain registered by the attacker. Nearly two-thirds of these domains are registered with just three domain registrars:

- PublicDomainRegister (28%)
- Google (20%)
- Namecheap (17%)



Phishing Response Trends

KEY FINDINGS

4,521

The total number of potential phishing attacks reported by employees at 13 large organizations participating in our survey during the first half of 2020

67%

Nearly 7 in 10 suspect emails reported by employees are ultimately deemed non-malicious, up from 60% in just six months

90X

Organizations with automated phishing response processes detect 90X the number of similar malicious messages exclusively reported by employees

5,553

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

Phishing Response Challenges Proliferate

Employee-Reported Phishing Attacks Vault Up 65%, Clobbering SOCs

Even before the coronavirus pandemic, phishing was implicated in up to 67% of all corporate data breaches, according to Verizon's 2020 Data Breach Investigations Report (VDBIR). In the first half of 2020, employees empowered to report suspect emails in hopes of foiling new breaches ended up shellacking already overburdened Security Operations Center (SOC) teams with more incidents than they could possibly handle. But organizations employing automated response technologies were able to neutralize unreported threats while accelerating time-to-containment.

Inside the ACID H2 2020 Phishing Incident Response Survey

For this mid-year report, ACID researchers interviewed SOC professionals at 13 large organizations with operations spanning a cross-section of industries—including high-tech, healthcare, agriculture, construction, retail, and energy. 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 January through June, 2020. This section of the H2 2020 Email Fraud and Identity Deception Trends Report features our analysis of these conversations.

67%

The False Positive Rate on Employee-Reported Phishing Incidents

According to a recent study from KnowBe4, one-third of all employees will click on a malicious link or obey a fraudulent email request in phishing simulations. Apparently, these recipients must be sending all of their legitimate email to the SOC team. Joking aside, employee-reported phishing incidents topped 4,521 during the first half of the year, according to 13 large organizations participating in our H2 2020 Phishing Incident Response Survey. Unfortunately, the number of false positives climbed 7% during that same period, to 67% of all reported incidents. Which means SOC analysts are forced to waste valuable time while investigation, remediation, and containment of legitimate breaches grow longer—and more costly.

Breachonomics

Manual Employee Reporting is No Longer Enough

Every minute spent investigating false negatives means actual phishing emails are left undetected, increasing the likelihood of a data breach with each passing moment. Yet today, 25% of all breaches go undetected for a month or more, according to the 2020 Verizon Data Breach Investigations Report. And Ponemon Institute estimates the costs associated with each new breach average $8.9 million. According to the companies included in our mid-year survey, automation is critical to preventing these kinds of incursions from ever happening, and reducing time-to-containment from weeks or months down to mere minutes for those that do. This is in part because on average, automated processes enable them to uncover a far larger number of attacks than those reported by employees.

90X

The Number of Additional Malicious Emails Detected Through Automated Response

The companies in our survey indicate automated phishing response detects 90X more email threats than manual reporting alone. Out of 4,285 verified phishing emails reported during the first half of 2020, organizations with automated phishing response processes identified 643,692 additional email threats that were either similar or directly related to those reported by employees. That's a 100% increase over our last report. Organizations cite automating analysis and triage tasks as key to realizing direct savings and increased efficiency and avoiding breach costs.

4,876

Malicious Phish Reports

9,237,306

All Similar Messages Found

643,692

Similar Messages Confirmed Malicious

90x

Discovery Factor

Continuous Detection and Response

Detecting and Removing Additional, Latent Email Threats

5,553

Additional Email Threats Neutralized Through CDR

Across 145 unique events, organizations employing continuous detection and response (CDR) technologies enhanced with shared threat intelligence identified more than fifty-five hundred malicious messages beyond those detected through automated phishing response alone, according to survey participants. CDR technologies identify latent threats that have evaded detection through dormant payloads, new impersonation techniques, or “time-bombed” URLs that redirect post-delivery. By analyzing company-wide email metadata, these technologies forensically recognize and remove email threats from all inboxes automatically.

36 Minutes

Average Remediation Time on Reported Phishing Attack Using Automation

Participants report that malicious phish reported by end users are remediated within 36 minutes with the aid of automation—specifically automated prioritization of incidents based on potential impact to the organization, and identification of all affected employees. This kind of speed is critical. According to research from Aberdeen, there’s a 30% chance of a first-user click on malicious emails within 60 seconds of delivery, with a median time-to-first-click on malicious emails of just 134 seconds.

Consumer Phishing and DMARC Trends

KEY FINDINGS

80%

Percentage of Fortune 500 companies that continue to leave customers, partners, investors and the general public at risk of phishing-based brand impersonation scams

3.8X

As of June 30, an impressive 5,282 brand domains have BIMI records, up 3.8X in just six months

78%

Percentage of Agari healthcare customers with domains protected by DMARC set to its strictest, enforcement policy to protect against attacks impersonating these brands—a 10% jump in six months

DMARC Adoption Snapshot

The Industry's Largest Ongoing Study of Adoption Trends Worldwide

In a snapshot of more than 477+ million Internet domains, we assess adoption trends for Domain-based Message Authentication, Reporting, and Conformance (DMARC) from January through June 2020.

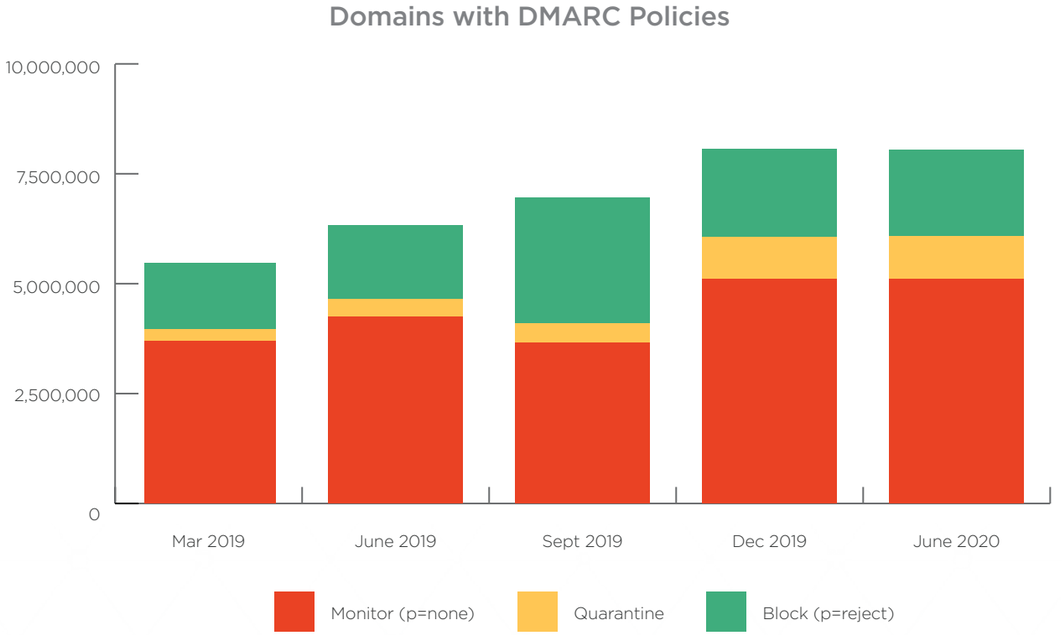
8 Million

At Mid-Year, 8,074,377 Domains Possessed Recognizable DMARC Policies Worldwide

2 Million

Just 2,041,442 Domains Have DMARC Set to Its Highest Enforcement Level

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.



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

DMARC Breakout Session

US Continues to Lead in DMARC Adoption

As part of this mid-year report, ACID examines the state of DMARC adoption by key geographies. Across the board, rising numbers of new domains are causing slippage in the total percentage of domains with DMARC policies, as well as those with DMARC policies at full enforcement.

#1

The Netherlands Tops in DMARC Policies Set to *p=reject*

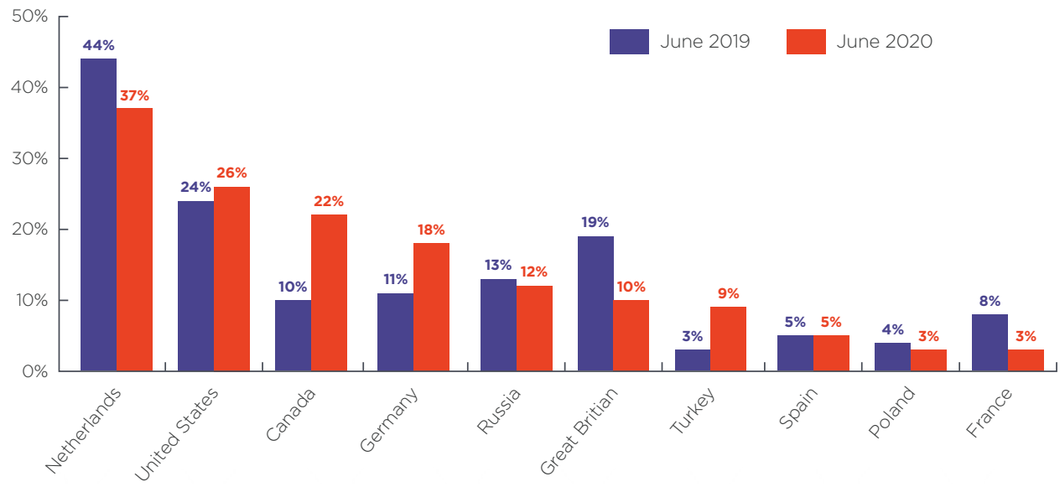
The US continued to dominate in the total number of domains with DMARC policies set to the strictest possible enforcement level. But on a percentage basis, the Netherlands leads the pack, even after seeing a drop year-over-year relative to total domains registered there.

12%

Percentage Increase in Canadian Domains with DMARC policies at Enforcement Jumps 12%

As of June 30, Canada has seen the sharpest rise in domains with DMARC policies set to *p=reject* so far this year, though Germany saw significant gains, as well. Meanwhile, the US saw only tepid increases on a percentage basis.

Top 10 Countries % of Domains with DMARC Enforcement (YoY)



DMARC Adoption Trends Among the World's Largest Companies

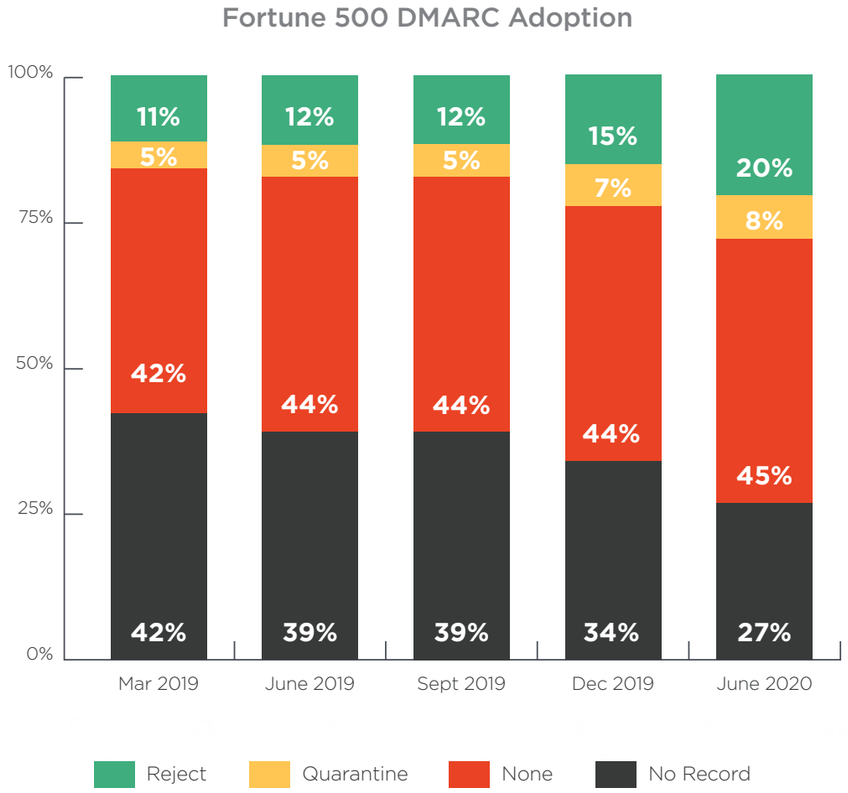
This mid-year report captures DMARC adoption trends among some of the world's most prominent companies. It's important to note that even when organizations have assigned DMARC records to their domains, they are not truly protected unless they are set to a level of enforcement. The sizable proportion of "no record" and "monitor only" policies highlights the fact that these organizations can still be impersonated in phishing campaigns that put their customers, partners, investors, and the general public at risk of serious financial harm.

20%

Fortune 500 Companies with DMARC Records Set at Full Enforcement—Up 66% YoY

80%

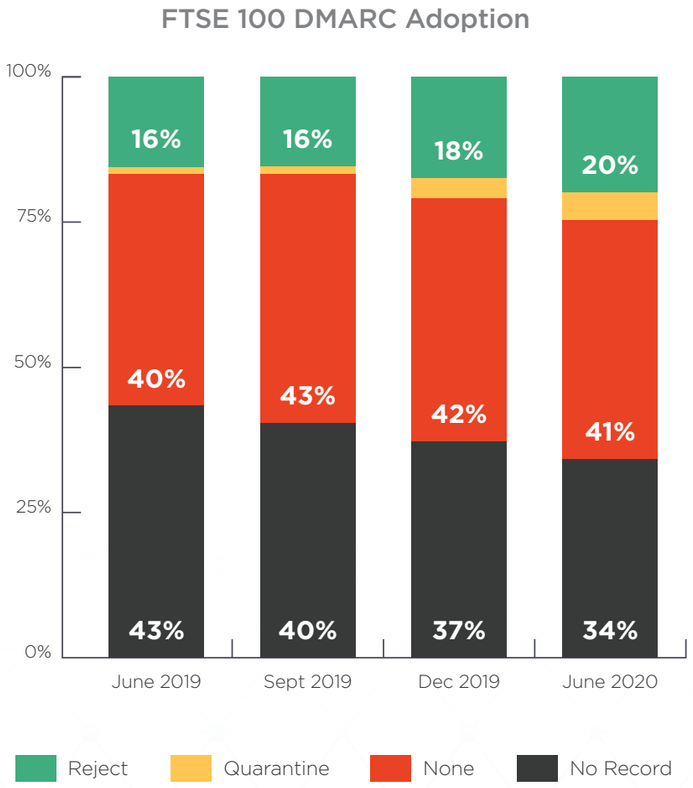
Fortune 500 Companies Remaining at Risk of Being Impersonated in Email Scams Targeting Their Customers, Partners, and More



80%

FTSE 100 Companies That Continue to Put Customers at Risk

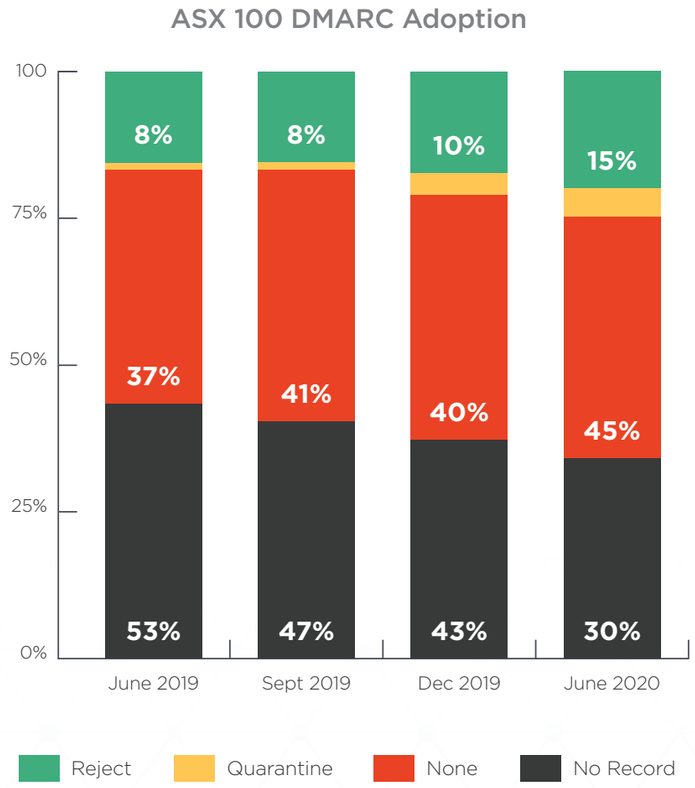
During the first half of 2020, only 20% of the UK's FTSE 100 had domains protected by DMARC set to *p=reject*—up just 2% in the last six months. As of mid-year, 80% of organizations in the FTSE 100 do not yet have protections in place to block fraudsters from impersonating their brands in email attacks.



1 in 10

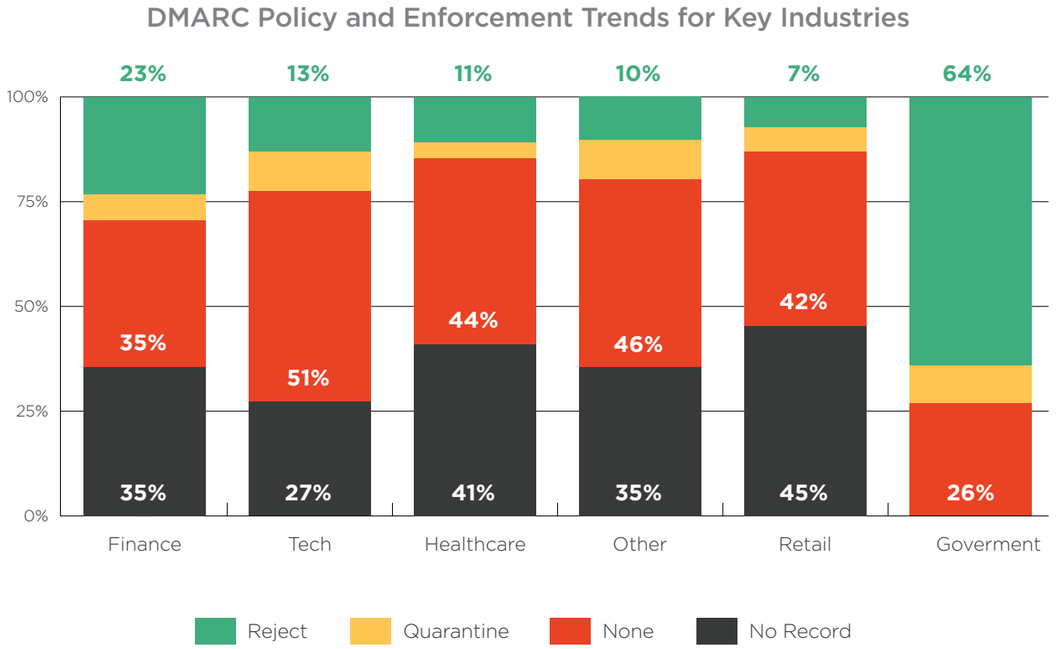
Number of Australia's ASX 100 Companies Now Protected from Brand Impersonation

The number of Australia's ASX 100 companies with DMARC deployed at its top enforcement level grew by 5% over the last six months, and is up 87.5% YoY. But that means 9 in 10 ASX 100 organizations remain defenseless against crime rings seeking to hijack their brands and email domains.



DMARC Adoption by Industry Vertical

Data in our H2 2020 report includes DMARC adoption across key industry verticals is based on public DNS records for primary corporate website domains of large companies with revenues above $1 billion. Every vertical has shown incremental improvements in the percentage of their DMARC-enabled domains at *p=reject* since our last report.



The Agari Advantage
Industry Enforcement Comparison

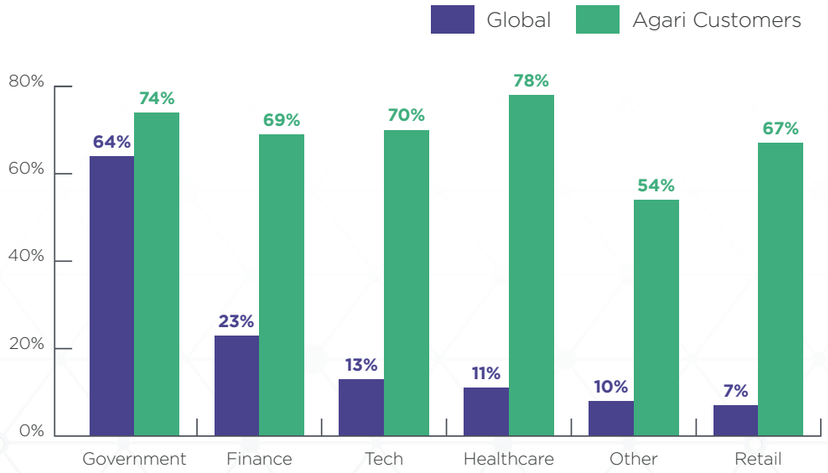
Data in the Agari Email Threat Center enables us to understand how enforcement rates across industries compare with those of Agari customers. Aggregating real-time DMARC statistics from the domains of top banks, social networks, healthcare providers, major government agencies and thousands of other organizations, the Agari Email Threat Center is the largest set of detailed DMARC data in the world both in terms of email volume and domains. To generate real-time threat intelligence, the Agari Email Threat Center analyzed more than 233 billion emails from more than 25,017 domains from January through June 2020.

10%

Increase in Agari Healthcare Industry Customers with Domains at Full Enforcement

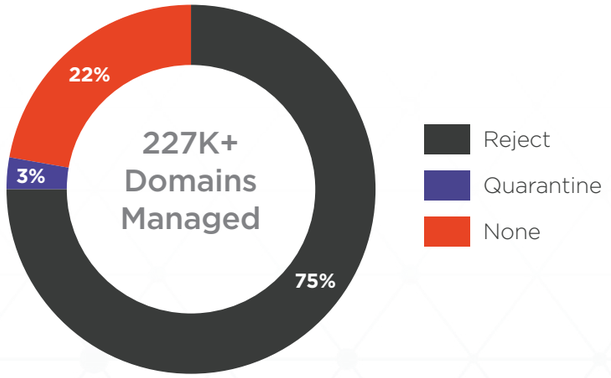
Amid a dramatic surge in phishing campaigns impersonating the Centers for Disease Control (CDC), Vanderbilt University Medical Center, Magellan Health, and other healthcare authorities, Agari customers in the sector redoubled their DMARC implementation efforts, climbing to 78% of domains at *p=reject* enforcement, compared to 68% at the end of 2019—a 10% jump in six months.

Industry Domains at Enforcement



Note: The Agari Email Threat Center tracks authentication statistics across active domains belonging to customers of Agari. Passive or defensive domains that do not process email will not be reflected in the totals.

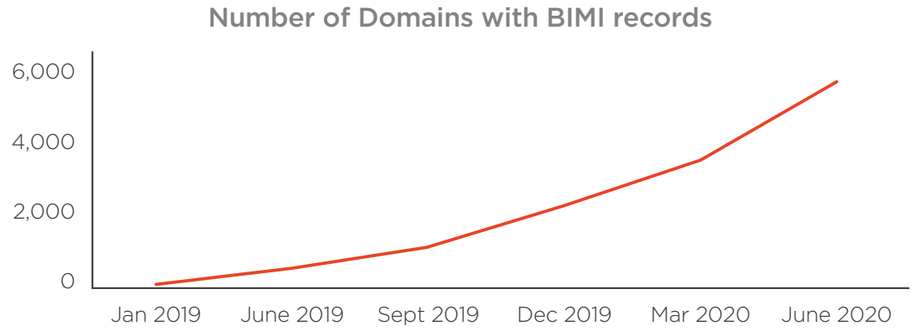
DMARC Enforcement Rate for All Agari Customers



Brand Indicators Adoption

From G Suite, With Love: BIMI Gains Momentum

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 email messages within a recipient ‘s inbox, with built-in protections against brand spoofing.



5,282

The Total Number of Brand Domains with BIMI Records as of June 30

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

3.8X

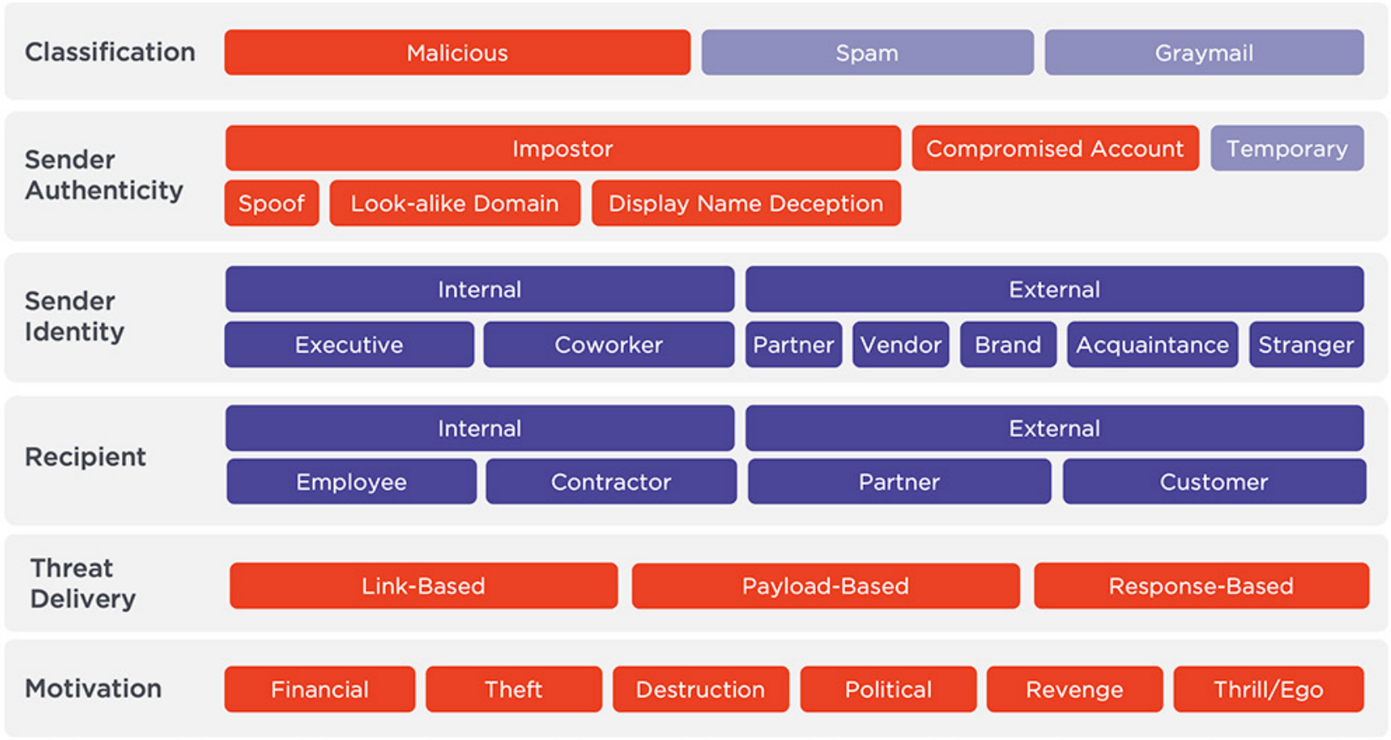
Increase in Brand BIMI Adoption In the Last 90 Days

In July, Google officially launched its BIMI pilot, which allows 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 will start displaying the logo in existing avatar slots in the Gmail interface.

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 six large organizations in a cross-section of industries conducted by Agari in June 2020.

Global DMARC Domain Analysis

For broader insight into DMARC policies beyond what we observed in email traffic targeting the Agari customer base, we analyzed 477 million+ domains, ultimately observing 8,074,377 domains with recognizable DMARC policies attached. This constantly updated list of domains serves as the basis for trend tracking in subsequent reports.

About 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

About Agari by Helpsystems

Agari is the Trusted Email Identity Company™, protecting brands and people from devastating phishing and socially-engineered attacks. Using applied data science and a diverse set of signals, Agari protects the workforce from inbound business email compromise, 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. Agari was acquired by HelpSystems in May 2021.

Learn more at www.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**

agari
by HelpSystems

hds-rp-1021-79d