VALIMAIL

DISINFORMATION AND MALICIOUS EMAIL REPORT

WHY DMARC REMAINS PIVOTAL

EXECUTIVE SUMMARY

Artificial intelligence (AI) makes it easier for bad actors to carry out sophisticated spoofing attacks, blurring the lines between legitimate and malicious communications.

This report highlights the critical importance of foundational security practices, particularly Domain-based Message Authentication, Reporting, and Conformance (DMARC), in this challenging landscape. DMARC provides a simple, cost-effective, and highly reliable method to stop the most common spoofing attacks. By authenticating the source of emails, DMARC layers on top of inbound protection and uniquely addresses outbound email impersonation, thereby protecting employees, brands, and prevents disinformation campaigns from leveraging trusted domains.

Our data reveals that while DMARC adoption is growing, only a fraction of domains are fully protected by strong enforcement policies. This leaves many organizations vulnerable to attacks that can damage their reputation, erode customer trust, and compromise sensitive information. As government regulations and email provider requirements increasingly mandate DMARC compliance, it is imperative for businesses to prioritize and fully implement this essential security measure.

This report delves into the current state of DMARC adoption across various industries, analyzes the effectiveness of different DMARC policies, and underscores why DMARC is a non-negotiable component of any comprehensive cybersecurity strategy in the disinformation age.

KEY TAKEAWAYS

- DMARC is essential for protecting brand reputation, customer trust, and sensitive data in the age of disinformation.
- A layered approach consisting of AI-driven security solutions and email authentication is more effective and uniquely addresses both inbound and outbound protection.
- DMARC effectively stops the most common attack vector: sender spoofing, where a bad actor is pretending to be a trusted sender.
- Most domains with DMARC are not fully protected, leaving them vulnerable to exploitation.
- Government regulations and email providers are increasingly mandating DMARC compliance.

INTRODUCTION

DMARC (Domain-based Message Authentication, Reporting, and Conformance) is an email authentication protocol designed to protect domains from unauthorized use in email messages, such as phishing and spoofing.

It works by enhancing existing authentication protocols, SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail), aligning these protocols with the domain in the visible “From” header of email messages. It provides domain owners with reports and monitoring to offer insights into email authentication and usage, enabling better security and deliverability practices.

WHY DMARC MATTERS
More Than Ever

In an era marked by AI-driven attacks and widespread disinformation, trust in digital communications is eroding.

Malicious actors are increasingly exploiting email to impersonate brands, launch phishing campaigns, and spread false information—often using sophisticated methods made simpler by emerging AI technologies. This environment calls for foundational, cost-effective defenses that can curb the majority of these malicious attempts at their source.

In this report, we'll help you understand DMARC and why it's important.

We'll also share data on global and industry-specific adoption rates across a dozen different industries, showing how companies and organizations across a spectrum of focus areas are choosing to protect their domains against phishing and spoofing.

DMARC IS CRITICAL
in the Modern Email Landscape

DMARC is pivotal in securing email communications and protecting against growing threats like phishing, spoofing, and the deliberate spread of disinformation. Here's why it's indispensable:

01

PREVENTS DOMAIN SPOOFING

DMARC ensures that only authorized senders can use your domain to send emails. This protects your brand and customers from phishing attacks that impersonate your organization.

02

STRENGTHENS EMAIL AUTHENTICATION

By aligning with SPF and DKIM, DMARC provides an additional layer of verification, ensuring that email headers are legitimate and match the sender's domain, while allowing domain owners to stand up and say that all mail they send should be properly authenticated.

03

PROVIDES VISIBILITY AND MONITORING

DMARC generates reports that give domain owners insights into who is sending emails on their behalf and how authentication mechanisms are performing. This transparency helps organizations detect unauthorized use and improve email security.

04

ENHANCES TRUST, SECURITY, AND DELIVERABILITY

Implementing DMARC signals to email providers that your domain is secure, improving sender reputation and increasing the likelihood that legitimate emails reach the inbox.

05

PART OF A GROWING MANDATE

Microsoft, Yahoo, and Google require bulk email senders to implement DMARC. The PCI DSS 4.0 standard includes DMARC, noting it as a "good practice," and multiple US government agencies, including the National Institute of Standards and Technology (NIST) and U.S. Department of Homeland Security (DHS) have either recommended or mandated that email senders should implement DMARC. More and more every day, industry oversight groups, standards bodies, and gatekeeping entities are indicating that DMARC is a best practice and should be implemented.

By showcasing how DMARC meets the challenges posed by AI-enabled spoofing and disinformation—and highlighting its growing acceptance as a standard practice—this report aims to underscore why DMARC is an essential line of defense in 2025.

THE OVERALL VIEW

DMARC adoption is strong (and growing) at the larger end of the different industries we've examined. Overall, DMARC adoption is growing monthly and is significant (at the larger end) of each industry. Industry DMARC adoption rates – as measured from the largest companies in each segment – ranged from 74% to 94%, with online retail leading the pack with the highest adoption rate and arts and recreation-related entities lagging significantly, with the lowest adoption rate.

However, DMARC adoption data globally, overall, and at the smaller end of these different industries shows us that more work remains to be done. Many companies do not yet know about or understand how critical DMARC is to protecting their email domains against phishing and spoofing.

And remember that DMARC adoption does not mean DMARC protection.

DMARC policies are another area of concern. In many industries, a significant number of companies have implemented a policy of p=none, likely in response to the Microsoft, Yahoo, and Google email sender requirements (Yahoo/Google announced in 2023, Microsoft in 2025), not realizing that while this "checks the box" for delivering mail to mailbox providers, it does nothing to actually protect email domains against malicious, false use.

So, while DMARC adoption rates might appear high, a significant percentage of tracked domains in each segment are **unprotected.**

Read **What is DMARC: Records, reports, and how it works**

WHY DMARC MATTERS in 2025

In 2024, bad actors executed some very sophisticated attacks utilizing phishing and spoofing. North Korea targeting domains with weak DMARC policies, supply chain attacks on multiple US municipalities, fake bank payment notifications, spear phishing attacks on retailers, and more – attackers are now leveraging advanced techniques to exploit weaknesses in email systems, making DMARC more critical than ever for securing your email domains against misuse.

This includes growing cybersecurity threats like:

ADVANCED PHISHING ATTACKS

Cybercriminals craft highly convincing phishing campaigns that bypass traditional filters.

SUPPLY CHAIN ATTACKS

Spoofed emails targeting business partners or customers undermine trust and can cause significant financial losses.

EMERGING AI TOOLS

Malicious actors are using AI-generated emails to mimic legitimate communications, increasing the success rate of their attacks.

DMARC combats these threats by **preventing the unauthorized use** of a domain and ensuring that **only legitimate emails** are **delivered** to recipients.

Industry, government, and regulatory bodies worldwide are increasingly mandating DMARC compliance for industries handling sensitive data, such as finance and healthcare. Major email providers like Microsoft, Google, and Yahoo require email senders to implement DMARC, improving deliverability and reputation for compliant organizations. Failing to comply with DMARC mandates can result in penalties, reduced deliverability, and reputational damage.

DMARC is a non-negotiable for organizations combating email fraud, phishing, and spoofing. Its ability to adapt to growing threats, meet regulatory demands, and provide visibility into email ecosystems makes it indispensable. By leveraging DMARC's robust authentication and reporting capabilities, businesses can safeguard their brand, build trust, and protect their domains.

DMARC's Multi-Pronged Protection

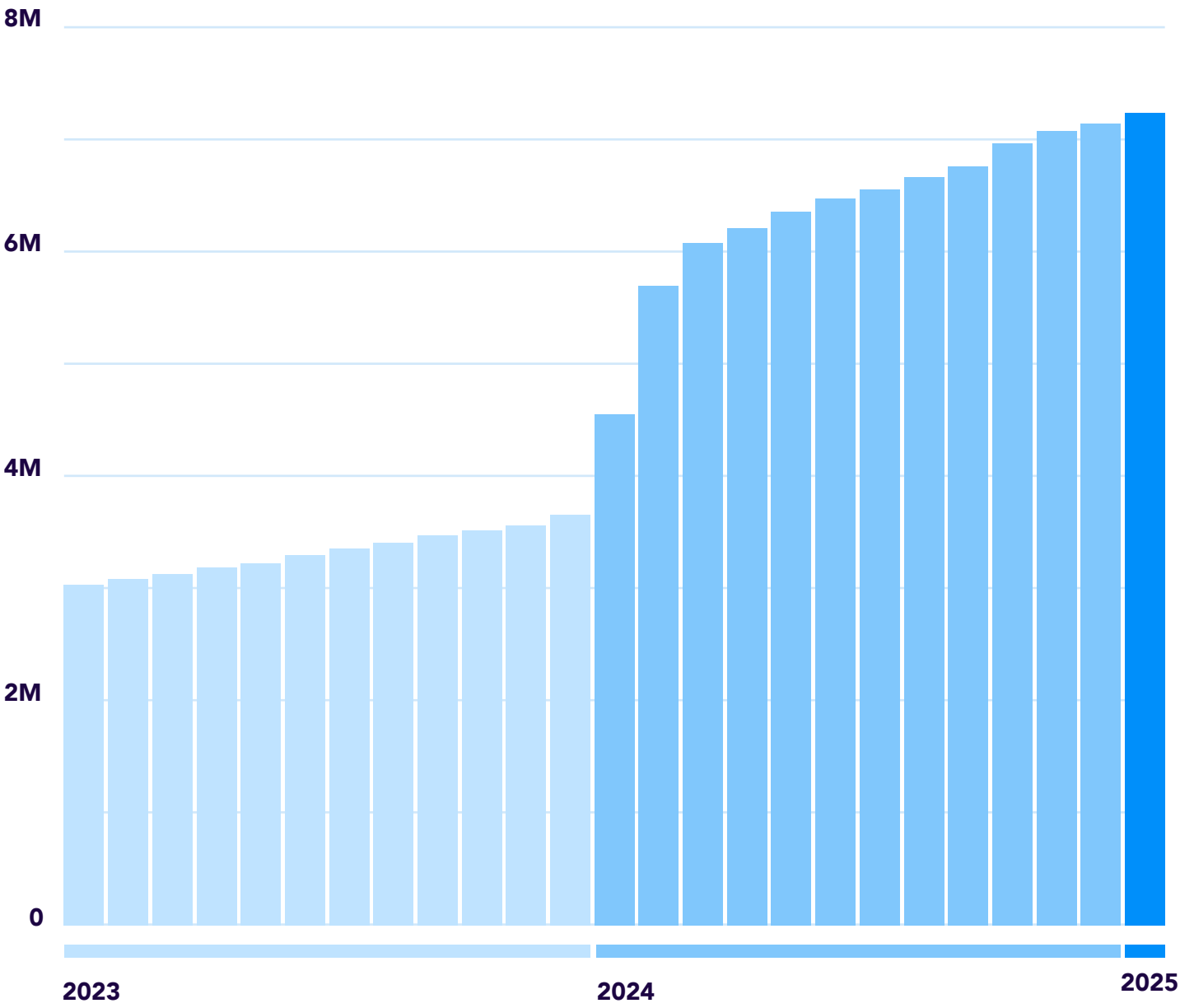
DMARC protects against email threats both internal and external.

Internal threats can include compromised employee accounts, misconfigured internal email systems, or even malicious insiders trying to impersonate other users within the organization. By enforcing DMARC policies and aligning SPF and DKIM authentication for outgoing messages, organizations can ensure that even internally generated emails meet strict identity verification requirements. If an attacker tries to spoof an internal sender or use a compromised system to send fraudulent messages, DMARC can flag or reject these emails before they cause damage.

Externally, DMARC is essential in defending against impersonation attacks such as phishing, business email compromise (BEC), and domain spoofing. Threat actors frequently forge the "From" address in emails to appear as though they're coming from a trusted brand, partner, or vendor. With DMARC in place and set to a policy of "reject," receiving mail servers can block these unauthenticated attempts outright. This helps prevent malicious messages from ever reaching the inbox.

THE CURRENT
DMARC Landscape

Global DMARC Adoption 2023 Through Today



SIGNIFICANT DMARC ADOPTION in 2024

In 2024, DMARC adoption experienced a significant surge. This increase was notably influenced by updated sender requirements from major email providers like Yahoo and Google.

In Q1 alone, over half a million domains within this group had newly published DMARC records, marking a substantial boost in adoption rates. Moving toward the beginning of 2025, we now observe that more than 7.2 million tracked domains have published a DMARC record.

However, challenges remain; **most domains newly implementing DMARC have implemented the technology with a policy of p=none without reporting, meaning their domains are not protected against phishing and spoofing. Not only do they lack protection, but without reporting, they lack visibility into threats and potential threats.** We track nearly 3.4 million domains that fit this criteria today. These domain owners still need to move to a posture of enforcement, ensuring that bad actors are not able to forge email messages purporting to be from their brand or organization.

INDUSTRY-SPECIFIC
DMARC Adoption Rates

For this research, Valimail compiled a list of thousands of domain names, aligned with specific industries and sectors, covering the following:

For each industry investigated, Valimail is providing reports on three different DMARC-related metrics:

DMARC ADOPTION RATE

This is the percentage of domains within an industry that have implemented DMARC, irrespective of DMARC policy and, by extension, protection level.

DMARC POLICIES

The industry percentages with current DMARC policies of p=none, p=quarantine, or p=reject. This is valuable for understanding the number of domains actually configured to protect against phishing and spoofing, which is not doable with a policy of none.

REPORTING

The percentage of domains that have properly designated where aggregate DMARC reports should be sent. Without these RUA reports (and a helpful dashboard like ours to help you visualize that reporting), you're flying blind. Moving to a p=quarantine or p=reject configuration becomes unsafe because legitimate email can be blocked easily and unknowingly.

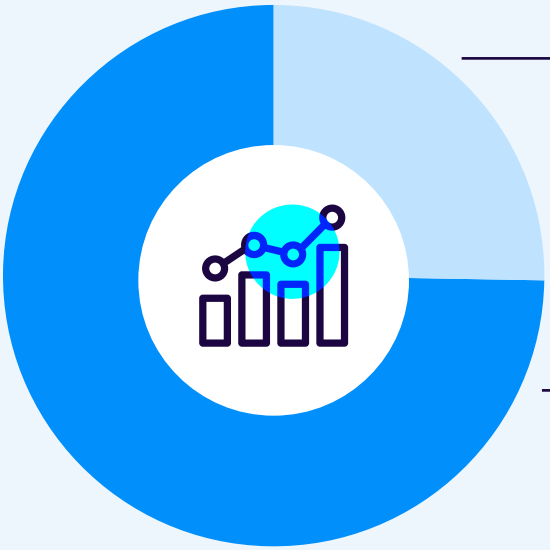
Arts and Recreation

This segment focuses on companies related to performing arts, crafts, recreational facilities, and video/computer gaming.

COMPANIES LISTED INCLUDE:

IGN, BLIZZARD, MICHAELS, THE WASHINGTON BALLET, AND MORE

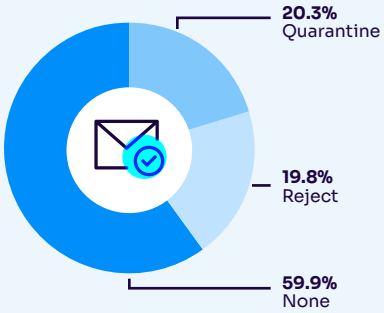
DMARC ADOPTION RATES



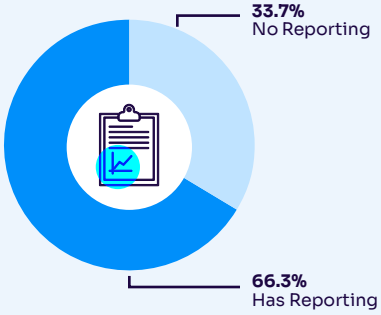
25.4%
No DMARC

74.5%
Has DMARC

DMARC POLICIES



DMARC REPORTING



Nearly **75%** of domains surveyed in the arts and recreation segment have published a DMARC record.

However, of the domains that have implemented DMARC, about 60% have only implemented the bare minimum, non-protective DMARC policy of p=none. This means that only about 40% of the surveyed domains in this space are configured to prevent the use of their domain name in spoofed email messages.

For reporting, we check to see if the domains in this sector with DMARC records have implemented a “RUA” setting, enabling aggregate DMARC feedback to monitor for proper authentication results and to identify potentially fraudulent use of their email domain. Just about a third of arts and recreation segment domains have failed to configure this reporting, meaning that they’re flying blind regarding monitoring for spoofing and phishing.

Securing our email using DMARC/DKIM and then monitoring our secured email flow using Valimail, I've been able to see on a regular basis how much bad-actor email was generated (unbeknownst to us), and we've been able to accurately see how our 3rd-party email partners have been able to securely send email on our behalf. **For a not-for-profit organization to have access to tools like this is really beneficial**.

Brian Parsons
Senior Manager, IT Services, Canadian Stage

LEARN MORE ABOUT EMAIL PHISHING, SPOOFING, AND SECURITY CHALLENGES IN THIS INDUSTRY

- Phishing Attacks in the Recreation Industry
- Leveling Up Security: Understanding Cyber Threats in the Gaming Industry

CURIOUS ABOUT THE CURRENT DMARC STATUS FOR YOUR DOMAIN?

Visit the Valimail DMARC Checker and see your domain's current protection.

WANT TO UPGRADE PROTECTION AGAINST PHISHING OR SPOOFING?

Start by signing up for your free Valimail Monitor account today.

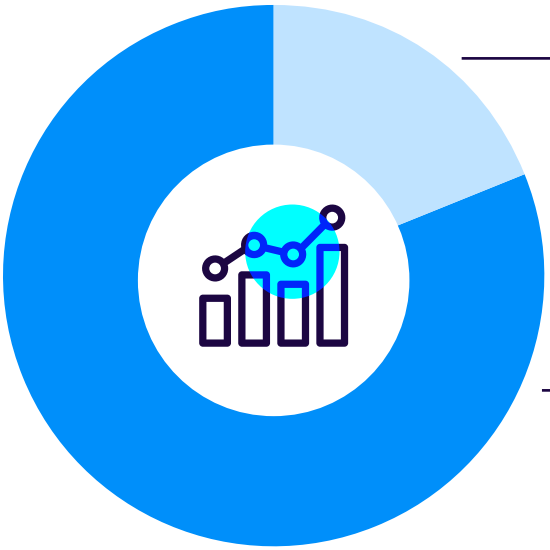
Education and Training

Our education and training segment contains domain names of companies and organizations related to education, training, certification, and distance learning.

COMPANIES LISTED INCLUDE:

CLEVER, BLACKBOARD, PEARSON, MEMBEAN, AND MORE

DMARC ADOPTION RATES

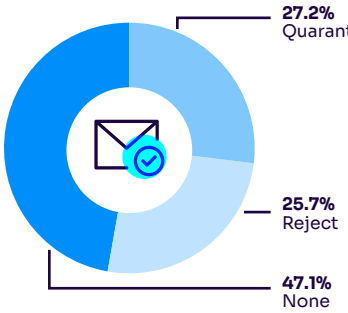


19%
No DMARC

81%
Has DMARC

Just over **80%** of domains surveyed in this sector have published a DMARC record.

DMARC POLICIES

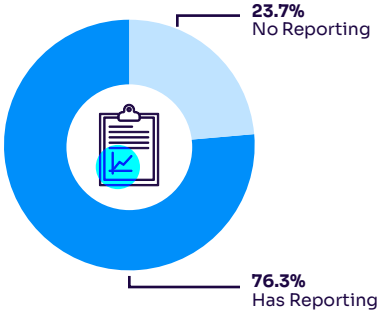


27.2%
Quarantine

25.7%
Reject

47.1%
None

DMARC REPORTING



23.7%
No Reporting

76.3%
Has Reporting

Of the education and training domains surveyed that have implemented DMARC, nearly half have only implemented the bare minimum, non-protective DMARC policy of p=none. This imperfect configuration means that nearly half of the surveyed entities in this space are not able to prevent use of their domain name in spoofed email messages.

For reporting, we check to see if the domains in this sector with DMARC records have implemented a “RUA” setting, enabling aggregate DMARC feedback to monitor for proper authentication results and to identify potentially fraudulent use of their email domain. Nearly a quarter of the domains surveyed in education and training have failed to configure this reporting, meaning that they’re flying blind when it comes to monitoring for spoofing and phishing.

The DMARC analysis performed by **Valimail provides clear visibility** and prevents the headache of having to try to manually review reports.

Lewis Wild
Founder, Wild Computing LTD

LEARN MORE ABOUT EMAIL PHISHING, SPOOFING, AND SECURITY CHALLENGES IN THIS INDUSTRY

- Phishing Tests, the Bane of Work Life, Are Getting Meaner
- Cyberattacks still ravage schools, defying White House efforts launched last year

CURIOUS ABOUT THE CURRENT DMARC STATUS FOR YOUR DOMAIN?

Visit the Valimail DMARC Checker and see your domain's current protection.

WANT TO UPGRADE PROTECTION AGAINST PHISHING OR SPOOFING?

Start by signing up for your free Valimail Monitor account today.

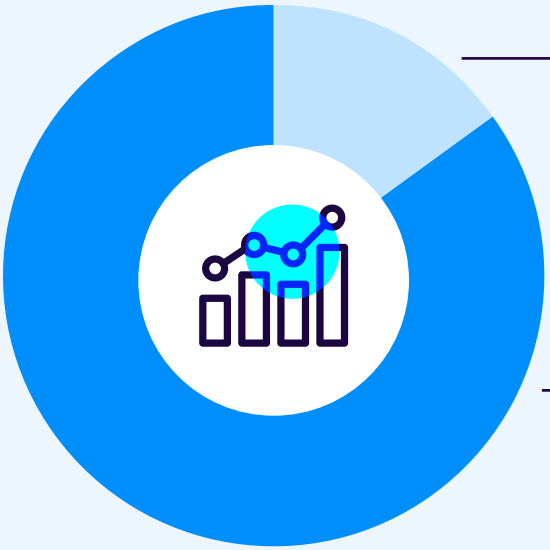
Financial Services

This segment focuses on companies that provide banking services, investment services, insurance services, financial planning, fintech, and related entities.

COMPANIES LISTED INCLUDE:

JP MORGAN CHASE, VISA, SCHWAB, MOODYS, NAVIENT, AND MORE

DMARC ADOPTION RATES

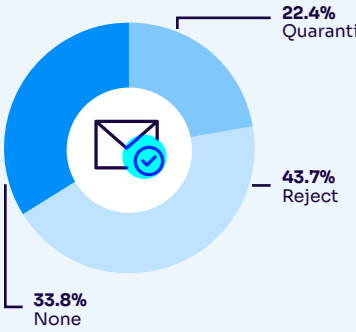


15.2%
No DMARC

84.8%
Has DMARC

Over **80%** of domains surveyed in this sector have published a DMARC record.

DMARC POLICIES

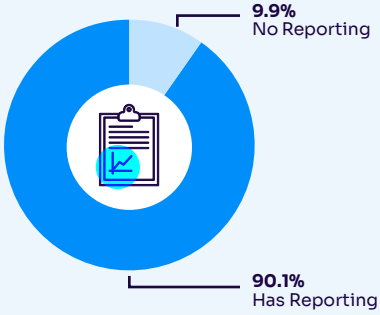


22.4%
Quarantine

43.7%
Reject

33.8%
None

DMARC REPORTING



9.9%
No Reporting

90.1%
Has Reporting

Of the financial services domains surveyed that have implemented DMARC, a third have only implemented the bare minimum, non-protective DMARC policy of p=none. This imperfect configuration means that only about two-thirds of the surveyed entities in this space are able to prevent use of their domain name in spoofed email messages. That 33% gap is especially concerning given that companies in this space are often a prime target for email fraud, phishing and spoofing attacks.

For reporting, we check to see if the domains in this sector with DMARC records have implemented a “RUA” setting, enabling aggregate DMARC feedback to monitor for proper authentication results and to identify potentially fraudulent use of their email domain. Just under 10% of the domains surveyed in financial services have failed to configure this reporting, meaning that they’re flying blind when it comes to monitoring for spoofing and phishing.

Email deliverability is always a concern, and **Valimail ensures our email gets delivered**. We love the simplicity of their interface and working with their super knowledgeable Customer Support team.

Opeyemi A.
Chief Information Security Officer (CISO), Trinity Financial Services

LEARN MORE ABOUT EMAIL PHISHING, SPOOFING, AND SECURITY CHALLENGES IN THIS INDUSTRY

- Cybercriminals attack banking customers in EU with V3B phishing kit
- Phishing victims turn to class- lawsuits against banks
- GenAI Increasingly Powering Scams, Wall Street Watchdog Warns

CURIOUS ABOUT THE CURRENT DMARC STATUS FOR YOUR DOMAIN?

Visit the Valimail DMARC Checker and see your domain's current protection.

WANT TO UPGRADE PROTECTION AGAINST PHISHING OR SPOOFING?

Start by signing up for your free Valimail Monitor account today.

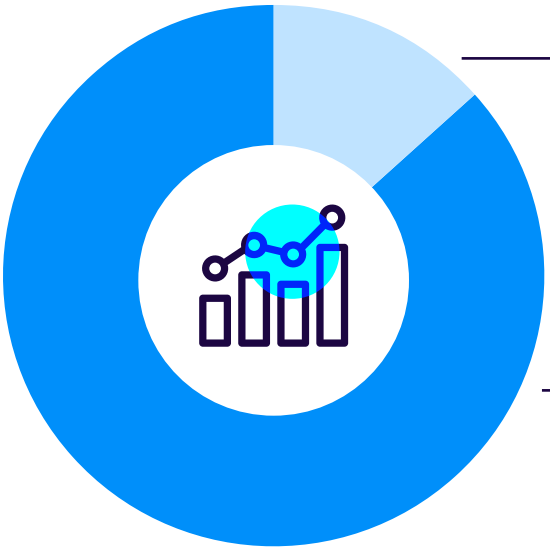
Healthcare

Our healthcare sector includes top companies focused on life sciences, pharmaceuticals, medical devices, health insurance, and care providers.

COMPANIES LISTED INCLUDE:

LILLY, ABBVIE, MEDTRONIC, HCA HEALTHCARE, RESMED, AND MORE

DMARC ADOPTION RATES

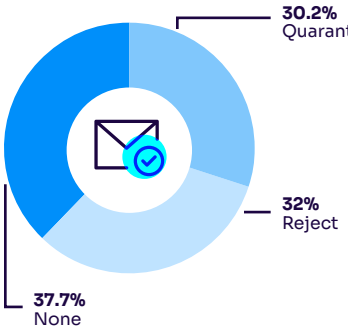


13.4%
No DMARC

86.6%
Has DMARC

Over **80%** of the surveyed domains in this sector have published a DMARC record.

DMARC POLICIES

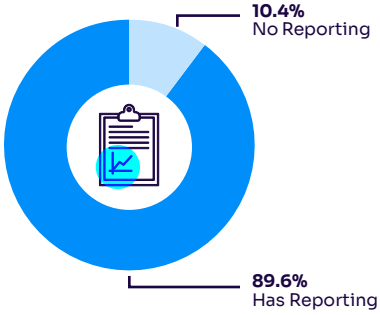


30.2%
Quarantine

32%
Reject

37.7%
None

DMARC REPORTING



10.4%
No Reporting

89.6%
Has Reporting

Of the healthcare domains surveyed that have implemented DMARC, just over a third have only implemented the bare minimum, non-protective DMARC policy of p=none. This imperfect configuration means more than a third of surveyed domains in this space are not able to prevent the use of their domain name in spoofed email messages. This is especially concerning given the highly sensitive patient data, financial records, and prescription information that many healthcare-related companies must protect.

For reporting, we check to see if the domains in this sector with DMARC records have implemented a “RUA” setting, enabling aggregate DMARC feedback to monitor for proper authentication results and to identify potentially fraudulent use of their email domain. Just over 10% of the domains surveyed in healthcare have failed to configure this reporting, meaning that they’re flying blind when it comes to monitoring for spoofing and phishing.

Valimail's solution provides great value! Valimail helps us with the DMARC/DKIM validation and functionality of understanding the DMARC solutions. Their **DMARC reporting and dashboard is highly intuitive and useful**!

Justin Reynolds
IT Administrator, Mercy Healthcare

LEARN MORE ABOUT EMAIL PHISHING, SPOOFING, AND SECURITY CHALLENGES IN THIS INDUSTRY

- Phishing attacks are targeting the health care industry; some tactics to familiarize yourself with to stay safe
- FBI, HHS issue advisory on cyberthreat actors targeting health care to divert payments
- Healthcare Data Breaches Due to Phishing

CURIOUS ABOUT THE CURRENT DMARC STATUS FOR YOUR DOMAIN?

Visit the Valimail DMARC Checker and see your domain's current protection.

WANT TO UPGRADE PROTECTION AGAINST PHISHING OR SPOOFING?

Start by signing up for your free Valimail Monitor account today.

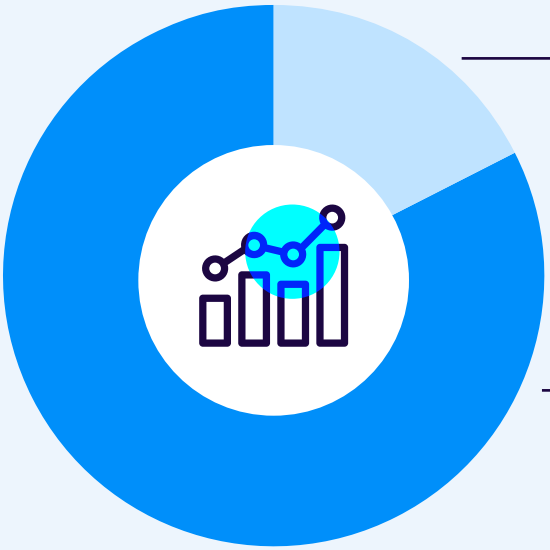
Higher Education

Our focus area for higher education consists of US-based four-year postsecondary educational institutions.

COMPANIES LISTED INCLUDE:

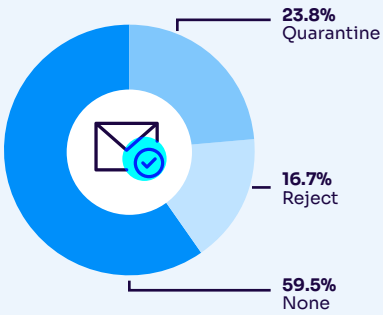
MIT, HARVARD, YALE, CASE WESTERN RESERVE UNIVERSITY, AND MORE

DMARC ADOPTION RATES

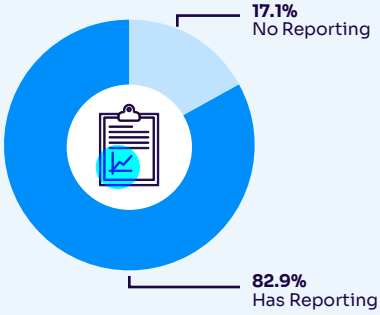


Over **80%** of the surveyed domains in this sector have published a DMARC record.

DMARC POLICIES



DMARC REPORTING



Of the higher education domains surveyed that do have DMARC policies, just under two-thirds have only implemented the bare minimum, non-protective DMARC policy of p=none. This imperfect configuration means that a significant number of domains in this space cannot prevent the use of their domain name in spoofed email messages.

For reporting, we check to see if the domains in this sector with DMARC records have implemented a “RUA” setting, enabling aggregate DMARC feedback to monitor for proper authentication results and to identify potentially fraudulent use of their email domain. Just over 17% of the domains surveyed in higher education have failed to configure this reporting, meaning that they’re flying blind when it comes to monitoring for spoofing and phishing.

Valimail provided us with the tools and information we needed to **drastically improve our DMARC pass rate in a matter of months**, as well as confidently enforce DMARC without impacting email communications.

Daniel McConnell
Senior Security Engineer, University of Pittsburgh

LEARN MORE ABOUT EMAIL PHISHING, SPOOFING, AND SECURITY CHALLENGES IN THIS INDUSTRY

- Office 365 Phishing Campaigns Targeting Universities
- Ransomware Attack on North Carolina A&T State University
- Silent Librarian Spear Phishing Campaigns

CURIOUS ABOUT THE CURRENT DMARC STATUS FOR YOUR DOMAIN?

Visit the Valimail DMARC Checker and see your domain's current protection.

WANT TO UPGRADE PROTECTION AGAINST PHISHING OR SPOOFING?

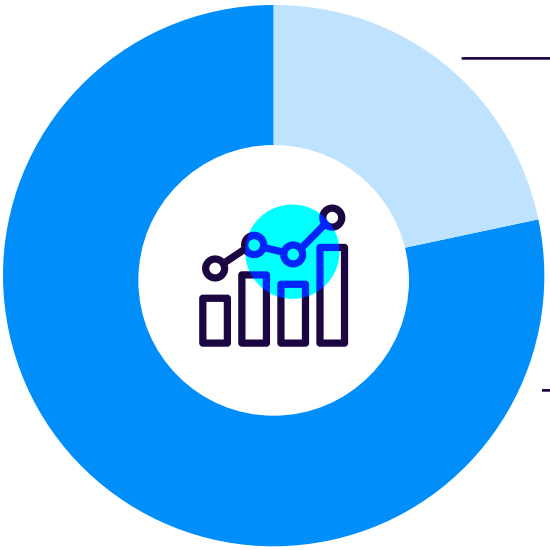
Start by signing up for your free Valimail Monitor account today.

Information Technology

Our IT segment consists primarily of domains of technology, systems, cybersecurity, and electronic infrastructure-related companies.

COMPANIES LISTED INCLUDE:
WORDPRESS, DROPBOX, SLACK, DELL, DOCUSIGN, AND OTHERS

DMARC ADOPTION RATES

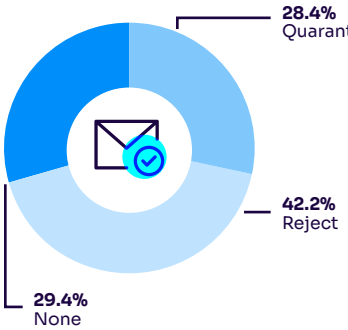


21.8%
No DMARC

78.2%
Has DMARC

Just under **80%** of the surveyed domains in this sector have published a DMARC record.

DMARC POLICIES

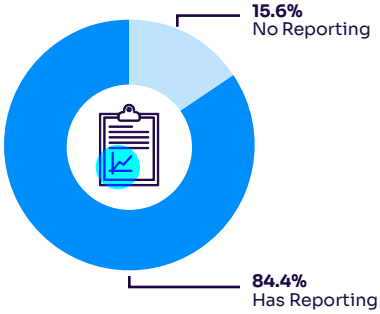


28.4%
Quarantine

42.2%
Reject

29.4%
None

DMARC REPORTING



15.6%
No Reporting

84.4%
Has Reporting

Of the IT domains surveyed that have implemented DMARC, 29% have only implemented the bare minimum, non-protective DMARC policy of p=none. This imperfect configuration means that nearly a third of surveyed domains in this space lack the ability to prevent the use of their domain name in spoofed email messages.

For reporting, we check to see if the domains in this sector with DMARC records have implemented a “RUA” setting, enabling aggregate DMARC feedback to monitor for proper authentication results and to identify potentially fraudulent use of their email domain. Just over 15% of the domains surveyed in IT have failed to configure this reporting, meaning that they’re flying blind when it comes to monitoring for spoofing and phishing.

The whole business of DKIM, SPF, and DMARC is very complicated. Valimail has greatly **simplified the process** and provided me with useful information in managing our email.

Jack Gostl
President, Argos Computer Systems, Inc

LEARN MORE ABOUT EMAIL PHISHING, SPOOFING, AND SECURITY CHALLENGES IN THIS INDUSTRY

- US charges five in 'Scattered Spider' hacking scheme
- Twilio Hackers Hit Over 130 Orgs in Massive Okta Phishing Attack
- Proofpoint Email Routing Flaw Exploited to Send Millions of Spoofed Phishing Emails

CURIOUS ABOUT THE CURRENT DMARC STATUS FOR YOUR DOMAIN?

Visit the Valimail DMARC Checker and see your domain's current protection.

WANT TO UPGRADE PROTECTION AGAINST PHISHING OR SPOOFING?

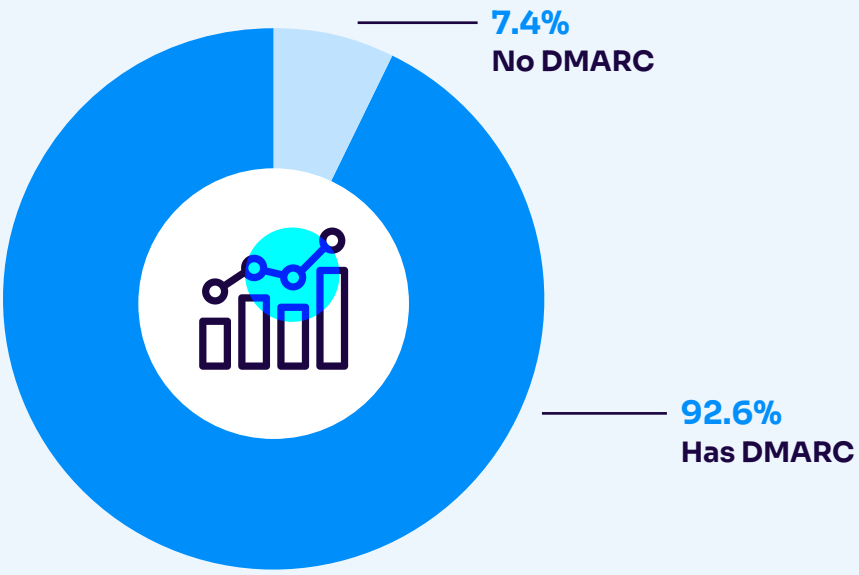
Start by signing up for your free Valimail Monitor account today.

Manufacturing

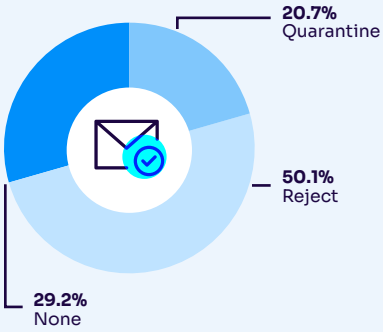
This segment focuses on companies engaged in the mechanical, physical, or chemical transformation of materials, substances, or components into new products.

COMPANIES LISTED INCLUDE:
FORD, GM, WHIRLPOOL, TYSON FOODS, AND MORE

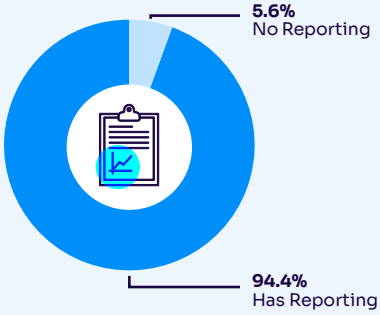
DMARC ADOPTION RATES



DMARC POLICIES



DMARC REPORTING



Over **90%** of the surveyed domains in this sector have published a DMARC record.

Of the manufacturing domains surveyed that have implemented DMARC, just about 29% have only implemented the bare minimum, non-protective DMARC policy of p=none. This imperfect configuration means that a very significant number of the companies surveyed in this space are not able to prevent the use of their domain name in spoofed email messages.

For reporting, we check to see if the domains in this sector with DMARC records have implemented a “RUA” setting, enabling aggregate DMARC feedback to monitor for proper authentication results and to identify potentially fraudulent use of their email domain. Just over 5% of the domains surveyed in manufacturing have failed to configure this reporting, meaning that they’re flying blind when it comes to monitoring for spoofing and phishing.

With Valimail, managing **our authentication mechanisms has become so much easier**. This can be managed, for example, by a person from the marketing department.

Bartosz Czerek
Digital Workplace Engineer, HuberSuhner

LEARN MORE ABOUT EMAIL PHISHING, SPOOFING, AND SECURITY CHALLENGES IN THIS INDUSTRY

- Abnormal Security revealed manufacturing sector under siege, as advanced email attacks surge
- Don't Take the Bait: Ways to address the phishing issue within manufacturing
- 8 biggest cybersecurity threats manufacturers face

CURIOUS ABOUT THE CURRENT DMARC STATUS FOR YOUR DOMAIN?

Visit the Valimail DMARC Checker and see your domain's current protection.

WANT TO UPGRADE PROTECTION AGAINST PHISHING OR SPOOFING?

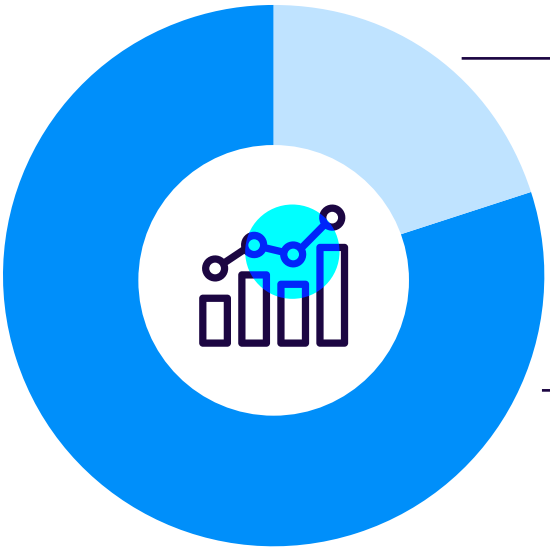
Start by signing up for your free Valimail Monitor account today.

Marketing, Consulting, and Services

This includes accounting, advertising, architecture, auditing, consulting, and marketing.

COMPANIES LISTED INCLUDE:
MAILCHIMP, DELOITTE, XERO, FRESHBOOKS, AND MORE

DMARC ADOPTION RATES

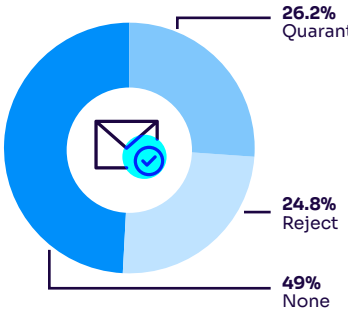


20.2%
No DMARC

79.8%
Has DMARC

Just shy of **80%** of the surveyed domains in this sector have published a DMARC record.

DMARC POLICIES

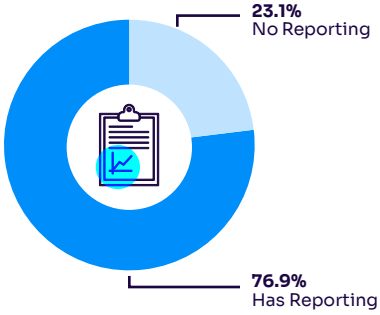


26.2%
Quarantine

24.8%
Reject

49%
None

DMARC REPORTING



23.1%
No Reporting

76.9%
Has Reporting

Of the marketing, consulting, and services domains surveyed that have implemented DMARC, only about half have implemented the bare minimum, non-protective DMARC policy of p=none. This imperfect configuration means that a very significant number of the companies surveyed in this space are not able to prevent the use of their domain name in spoofed email messages.

For reporting, we check to see if the domains in this sector with DMARC records have implemented a “RUA” setting, enabling aggregate DMARC feedback to monitor for proper authentication results and to identify potentially fraudulent use of their email domain. About 23% of the domains surveyed in this sector have failed to configure this reporting, meaning that they’re flying blind when it comes to monitoring for spoofing and phishing.

[Valimail] **setup was also incredibly fast and easy and we deployed this utility in a matter of minutes**, rather than days or weeks. We were really impressed by how simple the entire setup was, including bringing in all of our clients.

Jeff Mankini
Founder & CEO, UpClick Digital

LEARN MORE ABOUT EMAIL PHISHING, SPOOFING, AND SECURITY CHALLENGES IN THIS INDUSTRY

- Fake HMRC scam letters target small business owners in latest attack
- Ransomware attack allegedly strikes accounting firm
- 5 ways to mitigate the risks of business email compromise attacks
- Information about a Recent Mailchimp Security Incident

CURIOUS ABOUT THE CURRENT DMARC STATUS FOR YOUR DOMAIN?

Visit the Valimail DMARC Checker and see your domain's current protection.

WANT TO UPGRADE PROTECTION AGAINST PHISHING OR SPOOFING?

Start by signing up for your free Valimail Monitor account today.

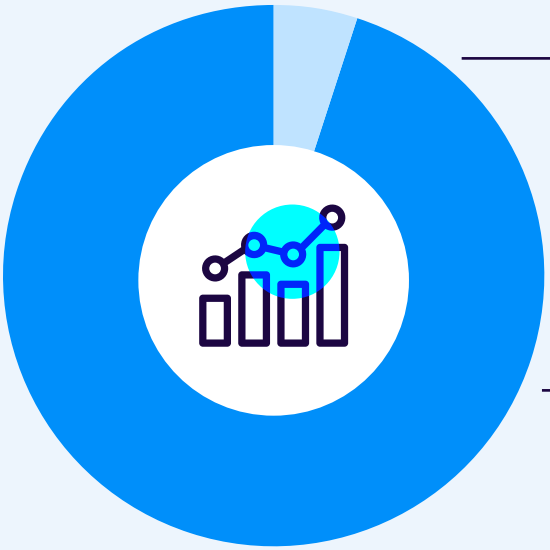
Online Retail

This includes stores selling online as well as “bricks and clicks” retailers selling online, as well as other retailers and marketplaces that sell direct-to-consumer.

COMPANIES LISTED INCLUDE:

IKEA, KOHLS, EBAY, SALLY BEAUTY, CABELAS, AND MORE

DMARC ADOPTION RATES

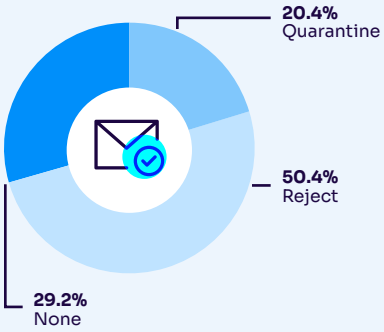


5%
No DMARC

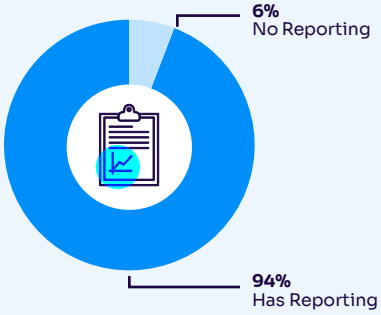
95%
Has DMARC

95% of the surveyed domains in our online retail sector have published a DMARC record.

DMARC POLICIES



DMARC REPORTING



Of these retail-related domains surveyed that have implemented DMARC, just about 29% have only implemented the bare minimum, non-protective DMARC policy of p=none. This imperfect configuration means that a very significant number of the companies surveyed in this space are not able to prevent the use of their domain name in spoofed email messages.

For reporting, we check to see if the domains in this sector with DMARC records have implemented a “RUA” setting, enabling aggregate DMARC feedback to monitor for proper authentication results and to identify potentially fraudulent use of their email domain. About 6% of the domains surveyed in this sector have failed to configure this reporting, meaning that they’re flying blind when it comes to monitoring for spoofing and phishing.

The [Valimail] **user interface is remarkably intuitive** and made the setup process a breeze, even for someone not deeply technical. I was particularly impressed by the **effectiveness of their email authentication system, which significantly reduced phishing attempts and improved our email deliverability**.

Varun Sidhu
Digital Marketing Manager - Ecommerce, Jan&Jul

LEARN MORE ABOUT EMAIL PHISHING, SPOOFING, AND SECURITY CHALLENGES IN THIS INDUSTRY

- Black Friday kicks off surge in phishing attacks on consumers
- Scammers are emailing people with fake subscription renewal notices
- Walmart tops list for phishing scams; Customers should be wary of emails

CURIOUS ABOUT THE CURRENT DMARC STATUS FOR YOUR DOMAIN?

Visit the Valimail DMARC Checker and see your domain's current protection.

WANT TO UPGRADE PROTECTION AGAINST PHISHING OR SPOOFING?

Start by signing up for your free Valimail Monitor account today.

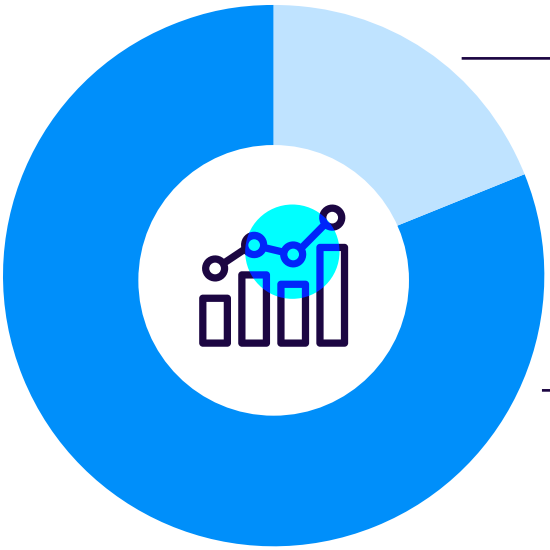
Transportation and Logistics

This includes shipping companies, airlines, transit systems, and other companies focused on the moving of parcels and/or people.

COMPANIES LISTED INCLUDE:

UBER, EXPEDIA, DHL, JETBLUE, FEDEX, AND OTHERS

DMARC ADOPTION RATES

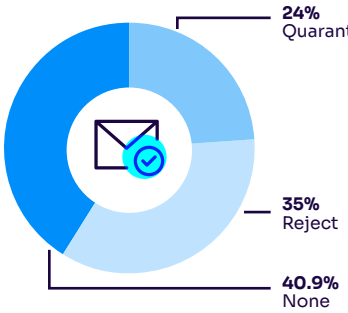


18.9%
No DMARC

81.1%
Has DMARC

Just over **81%** of the surveyed domains in this sector have published a DMARC record.

DMARC POLICIES

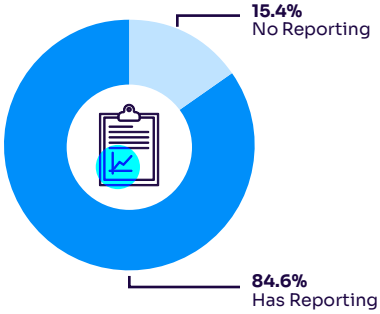


24%
Quarantine

35%
Reject

40.9%
None

DMARC REPORTING



15.4%
No Reporting

84.6%
Has Reporting

Of these transportation and logistics-related domains surveyed that have implemented DMARC, just about 40% have only implemented the bare minimum, non-protective DMARC policy of p=none. This imperfect configuration means that a very significant number of the companies surveyed in this space are not able to prevent the use of their domain name in spoofed email messages.

For reporting, we check to see if the domains in this sector with DMARC records have implemented a “RUA” setting, enabling aggregate DMARC feedback to monitor for proper authentication results and to identify potentially fraudulent use of their email domain. About 15% of the domains surveyed in this sector have failed to configure this reporting, meaning that they’re flying blind when it comes to monitoring for spoofing and phishing.

Valimail has been an absolute game-changer for our email security. Their **set it and forget it approach** means we no longer have to worry about managing DKIM and DMARC manually - **the platform takes care of everything with automated enforcement and real-time monitoring**.

Nick Taylor
System Engineer, Schlumberger

LEARN MORE ABOUT EMAIL PHISHING, SPOOFING, AND SECURITY CHALLENGES IN THIS INDUSTRY

- 10K Targeted in Phishing Attacks Spoofing FedEx, DHL Express
- Transportation Companies Hit by Cyberattacks Using Lumma Stealer and NetSupport Malware

CURIOUS ABOUT THE CURRENT DMARC STATUS FOR YOUR DOMAIN?

Visit the Valimail DMARC Checker and see your domain's current protection.

WANT TO UPGRADE PROTECTION AGAINST PHISHING OR SPOOFING?

Start by signing up for your free Valimail Monitor account today.

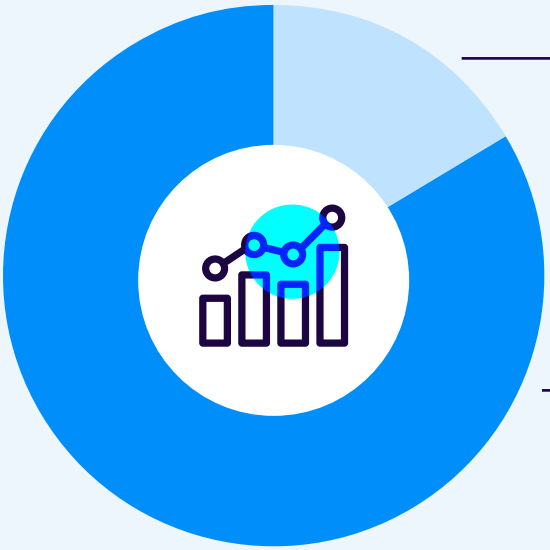
Travel and Hospitality

Our travel and hospitality segment includes top companies for lodging and accommodations, restaurants, and travel.

COMPANIES LISTED INCLUDE:

MARRIOTT, TACO BELL, SPIRIT AIRLINES, CARNIVAL CRUISE LINES, MGM RESORTS, AND MORE

DMARC ADOPTION RATES

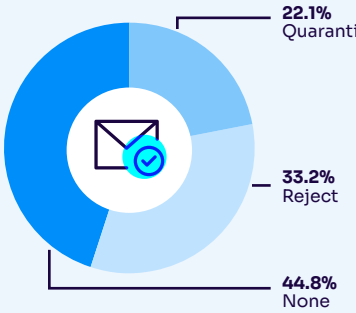


16.5%
No DMARC

83.5%
Has DMARC

Just over **83%** of the surveyed domains in this sector have published a DMARC record.

DMARC POLICIES

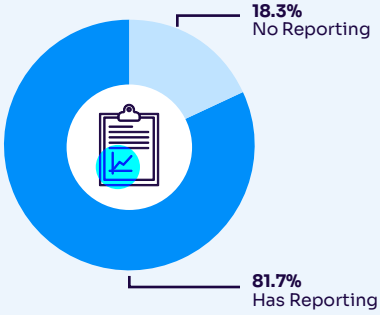


22.1%
Quarantine

33.2%
Reject

44.8%
None

DMARC REPORTING



18.3%
No Reporting

81.7%
Has Reporting

Of the travel and hospitality domains surveyed that have implemented DMARC, just over 44% have only implemented the bare minimum, non-protective DMARC policy of p=none. This imperfect configuration means that a very significant number of the companies surveyed in this space are not able to prevent the use of their domain name in spoofed email messages.

For reporting, we check to see if the domains in this sector with DMARC records have implemented a “RUA” setting, enabling aggregate DMARC feedback to monitor for proper authentication results and to identify potentially fraudulent use of their email domain. About 18% of the domains surveyed in this sector have failed to configure this reporting, meaning that they’re flying blind when it comes to monitoring for spoofing and phishing.

Before Valimail, managing our SPF record was challenging and enforcing DMARC seemed impossible due to the 10-lookup limit. **Valimail made the process seamless.**

Matthew Tyrney
Systems Engineer, Omni Hotels & Resorts

LEARN MORE ABOUT EMAIL PHISHING, SPOOFING, AND SECURITY CHALLENGES IN THIS INDUSTRY

- Hospitality Industry Targeted by Global Fake Login Phishing Attack
- Unmasking a Sophisticated Phishing Campaign That Targets Hotel Guests
- Hackers target hotel and travel companies with fake reservations

CURIOUS ABOUT THE CURRENT DMARC STATUS FOR YOUR DOMAIN?

Visit the Valimail DMARC Checker and see your domain's current protection.

WANT TO UPGRADE PROTECTION AGAINST PHISHING OR SPOOFING?

Start by signing up for your free Valimail Monitor account today.

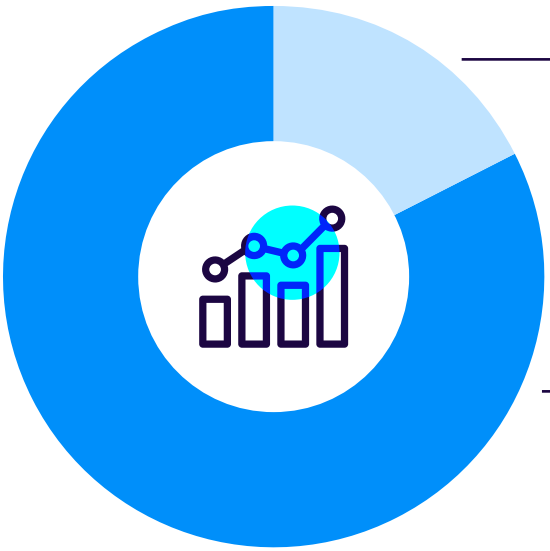
U.S. Government

This segment focuses on domains utilized by various levels of government and government-related entities in the U.S., from local to federal.

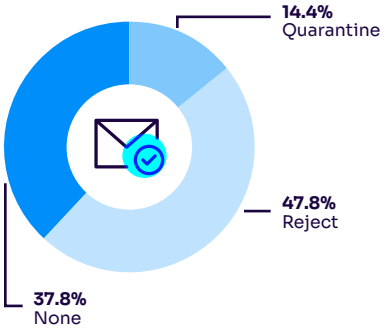
COMPANIES LISTED INCLUDE:

THE UNITED STATES POSTAL SERVICE, THE STATE OF ILLINOIS, THE OHIO LOTTERY, THE SUPER COURT OF CALIFORNIA/LOS ANGELES, AND OTHERS

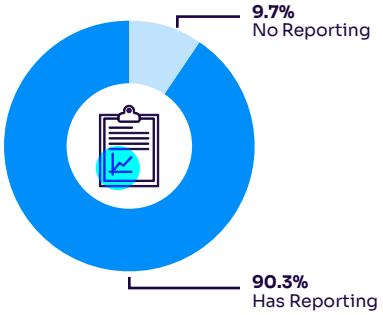
DMARC ADOPTION RATES



DMARC POLICIES



DMARC REPORTING



Just over **82%** of the surveyed domains in our U.S. Government segment have published a DMARC record.

Of the domains surveyed that have implemented DMARC, just over 37% have only implemented the bare minimum, non-protective DMARC policy of p=none. This imperfect configuration means that a very significant number of the companies surveyed in this space are not able to prevent the use of their domain name in spoofed email messages.

For reporting, we check to see if the domains in this sector with DMARC records have implemented a “RUA” setting, enabling aggregate DMARC feedback to monitor for proper authentication results and to identify potentially fraudulent use of their email domain. Just under 10% of the domains surveyed in this sector have failed to configure this reporting, meaning that they’re flying blind when it comes to monitoring for spoofing and phishing.

FedRAMP requires enforceable DMARC policies on all cloud service offerings (CSOs) that send emails on behalf of the Federal Government.

FedRAMP Knowledge Base
Guidance for CSP technical teams, 3PAOs, Agency Reviewers
Published in July 2024

LEARN MORE ABOUT EMAIL PHISHING, SPOOFING, AND SECURITY CHALLENGES IN THIS INDUSTRY

- FBI Warns of Increase in Business Email Compromise Attacks on Local and State Governments
- US warns of North Korean hackers using email security flaws for phishing attacks
- US Government Agencies Impersonated in Aggressive DocuSign Phishing Scams

CURIOUS ABOUT THE CURRENT DMARC STATUS FOR YOUR DOMAIN?

Visit the Valimail DMARC Checker and see your domain's current protection.

WANT TO UPGRADE PROTECTION AGAINST PHISHING OR SPOOFING?

Start by signing up for your free Valimail Monitor account today.

CHALLENGES to DMARC Adoption

DMARC is critical for combating email spoofing and phishing attacks. However, implementing it can feel daunting for many organizations. Let's break down the key challenges to DMARC adoption and how to tackle them.

TACKLING TECHNICAL COMPLEXITY

The technical side of DMARC implementation can seem very scary. To get DMARC up and running, you need to configure SPF and DKIM. Both require editing DNS records—a process that feels like a tightrope. One small error and your legitimate emails might bounce or disappear.

Things get more complicated if your organization uses third-party email services—think marketing platforms, CRMs, or ticketing systems. You need full awareness of all sending services that are meant to be allowed to send email messages on your organization's behalf. Failure to identify and properly configure email authentication for one or more email services while implementing DMARC can impede proper email delivery.

And how permissive are those authentication settings? Things like SPF records with multiple "includes" containing wide swaths of IP addresses can allow for an exceedingly broad authorization to send mail on your behalf can lead you to wonder: Are you really appropriately protected?

FIGHTING THE AWARENESS GAP

A big part of the problem is that many organizations don't know what DMARC is or why it matters. There's a common belief that other security measures like firewalls or antivirus software are enough to stop phishing. Unfortunately, that's just not true. Email is one of the weakest links in most organizations' security.

These challenges are real, but they're manageable with the right approach. Take it one step at a time: understand the technical requirements, educate your team, and work with your third-party senders to ensure everything is in sync. By investing in DMARC, you're investing in the security and reputation of your organization's email communications.

Additional Resources

THE STEP-BY-STEP PATH TO DMARC

Phishing and spoofing attacks are no joke, and DMARC is your best bet to keep your domain safe. To learn how to roll it out correctly, visit the Valimail blog, where we'll guide you through everything you need to consider as you prepare to embark upon your DMARC implementation journey.

Visit the Valimail blog

DON'T FORGET BIMI

Once you've achieved full DMARC protection for your email domain, it's time to take it to the next level, enhancing your brand's email presence with BIMI (Brand Indicators for Message Identification). BIMI allows your brand or company logo to appear alongside authenticated emails in supported inboxes, providing visual trust that helps recipients quickly recognize and trust your messages.

BIMI is a powerful security and marketing tool that reinforces your brand's legitimacy while showing that your domain is protected against spoofing and phishing attacks.

BIMI logos are supported by Gmail, Yahoo Mail, Apple's iCloud, and other mailbox providers. Want to learn more about BIMI? Reach out to us to request a demo of Valimail Amplify today.

SECURE YOUR DOMAIN

Use this data to help inform the process as you move to implement DMARC fully and properly. Many companies have implemented DMARC to date, knowing that no matter what industry you're in, **email security isn't optional; it's essential**.

Phishing and email spoofing aren't just problems for big tech companies or financial institutions; they affect **every** organization that uses email. Attackers are constantly looking for weak spots, and if your domain isn't protected with DMARC, you're giving them an open invitation to impersonate your brand and trick your customers, partners, and employees.

Implementing DMARC, along with SPF and DKIM, helps ensure that only authorized senders can use your domain, stopping impersonation attacks before they reach inboxes. Cybersecurity isn't just about firewalls and endpoint protection—**email authentication is a critical layer of defense**. If you haven't deployed DMARC yet, now is the time.

PROTECT YOUR DOMAIN, YOUR REPUTATION, AND THE PEOPLE WHO RELY ON YOUR EMAIL.

Schedule your demo with Valimail today!

NOTES ON METHODOLOGY

- Rankings for determining the top companies or organizations in various industries are based on a multitude of factors, including web traffic, ARR (annual rate of revenue), market capitalization, number of customers, and other data. Not all industries can be ranked in the same fashion.
- DMARC policies were queried at each domain's top ("org") level.
- DMARC data for this report was most recently queried in February 2025.

ABOUT THE AUTHOR

Al Iverson has been helping email senders and IT administrators properly implement email authentication, DMARC, and other best practices for a very long time. As a long-time deliverability expert with deep experience related to email technology and email marketing best practices, Al has published the email deliverability-focused blog Spam Resource since 2001 and managed all things deliverability for a well-known Marketing Cloud platform for fifteen years.

As Valimail's Industry Research and Community Engagement Lead, he monitors email authentication trends, analyzes evolving email deliverability and protection requirements, advocates for best practices, and connects and builds relationships and communities online and in person to educate businesses, IT professionals, and marketers on why email authentication and domain protection are so important.

In the preparation of this report, Al was gratefully assisted by Alyssa Harmon, Angela Noh, Katie Knowlton, Warren Duff, Mary Lawler, and the entire Valimail marketing team.

Valimail is the global leader in DMARC-as-a-service, and the inventor of hosted DMARC.