Introduction

More than four years after its launch, Domain-based Message Authentication, Reporting, and Conformance (DMARC) remains the most powerful weapon to date in the fight against phishing and spoofing. This email authentication protocol has revolutionized the email fraud landscape, disrupted longstanding phishing tactics, and protecting more brands, consumers, and employees than ever before. DMARC has the potential to abolish an entire class of fraud, but its success relies on its adoption.

In this annual report, we track DMARC’s progress. We analyze some of the world’s largest brands to look at DMARC adoption rates by region and industry sector, as well as by implementation stage. We also leverage Return Path’s Data Cloud to consider adoption among mailbox providers, enterprises, and email message gateways whose enforcement of DMARC policies is critical.

As a proud founding member of DMARC, we were heartened to see that DMARC adoption rates around the world and across industries are rising. However, adoption rates in some areas are not increasing as quickly as we expected. We hope these key DMARC stats, success stories, and common industry roadblocks will help spark progress among email experts everywhere. DMARC helps companies better defend their customers, brands, and bottom line from email fraud, and we will continue to track and support DMARC adoption worldwide.

Robert Holmes
General Manager, Email Fraud Protection
DMARC Sender Adoption Growth Worldwide

Last year, Return Path analyzed more than 1,000 global brands across 33 countries and found that, globally, only 22 percent of the companies surveyed were publishing a DMARC record—and therefore taking proactive steps toward better email fraud protection.

One year later, we looked at those same companies and found that 29 percent are now publishing a DMARC record, representing a 24 percent increase in adoption year over year.

While EMEA (Europe, the Middle East, and Africa) and Australia and New Zealand are still lagging behind other regions in terms of overall adoption—with 16 percent and 18 percent respectively—their year-over-year increases are higher than in North America. Latin America made the most progress since last year, with a whopping 47 percent increase year over year.

North America remains at the top of the leaderboard in overall DMARC usage, with an adoption rate of 42 percent.

<table>
<thead>
<tr>
<th>Region</th>
<th>Sample size</th>
<th>No DMARC Record</th>
<th>Policy in place</th>
<th>YOY Increase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia &amp; NZ</td>
<td>74</td>
<td>82%</td>
<td>18%</td>
<td>33%</td>
</tr>
<tr>
<td>EMEA</td>
<td>395</td>
<td>84%</td>
<td>16%</td>
<td>25%</td>
</tr>
<tr>
<td>Latin America</td>
<td>79</td>
<td>72%</td>
<td>28%</td>
<td>47%</td>
</tr>
<tr>
<td>US &amp; Canada</td>
<td>501</td>
<td>58%</td>
<td>42%</td>
<td>20%</td>
</tr>
<tr>
<td>Grand Total</td>
<td>1049</td>
<td>71%</td>
<td>29%</td>
<td>24%</td>
</tr>
</tbody>
</table>
DMARC by the Numbers

2.5 billion
Mailboxes worldwide are protected by DMARC

70%
Of global consumer mailboxes are currently DMARC-enabled

122%
Increase in users that sent 100 or more DMARC reports

24%
Year-over-year increase in DMARC adoption across 1,000 top global brands

145%
Year-over-year increase in the number of domains that had a reject policy in place in 2015

Source: Return Path
DMARC adoption varies widely when we break out our data by vertical. While the biggest and most progressive brands within key verticals were the first to embrace DMARC, some industries have been notably slower to take action against email fraud. The majority are below the global average adoption rate of 29 percent.

Some verticals, like technology and payment services, have expanded their DMARC coverage significantly since last year, while others—social media and logistics, for example—have plateaued.

### DMARC Sender Adoption Rate by Vertical

<table>
<thead>
<tr>
<th>Vertical</th>
<th>Sample Size</th>
<th>DMARC Adoption</th>
<th>YoY Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social media</td>
<td>59</td>
<td>59%</td>
<td>+8</td>
</tr>
<tr>
<td>Technology</td>
<td>61</td>
<td>51%</td>
<td>+16</td>
</tr>
<tr>
<td>Logistics</td>
<td>22</td>
<td>41%</td>
<td>0</td>
</tr>
<tr>
<td>Payment Services</td>
<td>87</td>
<td>32%</td>
<td>+10</td>
</tr>
<tr>
<td>Travel</td>
<td>110</td>
<td>31%</td>
<td>+5</td>
</tr>
<tr>
<td>Banking</td>
<td>275</td>
<td>27%</td>
<td>+8</td>
</tr>
<tr>
<td>Retail/Gaming/eCommerce</td>
<td>267</td>
<td>25%</td>
<td>+4</td>
</tr>
<tr>
<td>Public sector</td>
<td>16</td>
<td>25%</td>
<td>+6</td>
</tr>
<tr>
<td>ISP/Telco</td>
<td>77</td>
<td>21%</td>
<td>+5</td>
</tr>
<tr>
<td>Healthcare</td>
<td>75</td>
<td>16%</td>
<td>+5</td>
</tr>
<tr>
<td>Total</td>
<td>1049</td>
<td>29%</td>
<td>+6</td>
</tr>
</tbody>
</table>
Leading the Way

Social Media

Like last year, social media—one of the most targeted industries—is leading the way in the fight against inbound and outbound phishing, with a DMARC adoption rate of 59 percent, compared to 51 percent in 2015. Social media networks are big, their technology is new, and their need for information security is high.

Trust is at the core of the social media business model, and brands send large volumes of messages to billions of users every day. When user accounts are compromised and personal information exposed, the consequences can be disastrous, eroding trust and compromising business at lightning speed.

Technology

The technology sector is perhaps the biggest DMARC success story of 2016. These companies not only had the second-highest DMARC adoption rate overall, but they also increased adoption by 16 percentage points since last year—the highest increase of any other industry.

Like social media, we suspect that this progress is due to a combination of need and receptivity. Technology companies know that protecting their customers and employees from email fraud is paramount, and these companies are nimble enough to support the DNS and mail server updates required for DMARC implementation.

Travel

The growing popularity of online travel is making it an increasingly vulnerable security target: in 2015, more than 20 travel-related websites experienced data breaches. With online travel sales expected to grow to $523 billion in 2016, the travel industry knows that email is a critical channel to protect. At 31 percent, it is just above the cross-industry DMARC adoption average. While these companies are making good progress, they still have a ways to go.

For more information, download our Travel Guide to Email Fraud.
Lagging Behind

$ Banking

The vast majority of banks included in this analysis are not using the DMARC standard. With an adoption rate of 27 percent, banking has increased its DMARC profile by only eight percentage points since last year.

Legacy IT infrastructure, convoluted email ecosystems, and risk-aversion all stand in the way of system-wide technological changes that make innovative anti-phishing solutions like DMARC possible. However, the launch of dot bank domain names is extremely encouraging, and could represent a secure and preferred path to DMARC adoption.

Retail

The retail industry is arguably the hottest new cybercrime target. In 2010, fewer than 10 percent of businesses in the S&P 100 Index identified cybersecurity as a risk. Today, Bloomberg found that more than 75 percent of them do.

Unfortunately, retailers are not making enough progress in protecting their customers and employees from email fraud. Combined with gaming and eCommerce, retail's DMARC adoption rate is at 25 percent, which is only four percentage points up from last year.

For more information, download our Retail Guide to Email Fraud.

Healthcare

The healthcare industry's DMARC adoption rate continues to seriously lag—it is the lowest of all sectors for two years in a row, at 16 percent. Medical data is worth ten times more than a credit card number on the black market, and is highly coveted by cybercriminals.

Healthcare providers are seeing an exponential increase in security incidents each year. It is time for this industry to start being proactive in the fight against phishing and spoofing.

For more information, download our Healthcare Guide to Email Fraud.
Next, let’s look at DMARC implementation by breaking it down into the types of policies that brands have adopted.

A large percentage of senders implemented a “none” policy, signifying that they adopted the DMARC standard but did not commit to the stringent email operations required to fully block malicious emails.

Three industry sectors—payment services (29 percent), social media (34 percent), and logistics (56 percent)—show the highest implementation of the DMARC “reject” policy, which instructs mailbox providers to block suspected fraudulent messages.

---

None: The entire email authentication ecosystem is monitored to map out legitimate traffic.

Quarantine: Messages that fail DMARC move to the spam folder.

Reject: Messages that fail DMARC do not get delivered at all.
Prioritizing yet another implementation can be difficult to make a case for internally. So we thought we would share some real-life success stories from early adopters to help you get the resources you need to start your DMARC journey.

<table>
<thead>
<tr>
<th>Company</th>
<th>Success Story</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Financial Services Company</td>
<td>After implementing Return Path’s recommendations for a DMARC reject policy, the percent of suspicious messages that this company blocked grew from 13 percent to 96 percent—a 600 percent increase.</td>
</tr>
<tr>
<td>Global Leader in Shipping and Logistics</td>
<td>In a 30-day period, more than 12 million messages from 49 domains were blocked thanks to DMARC.</td>
</tr>
<tr>
<td>US Retail Giant</td>
<td>In addition to a 92.8 percent reduction in suspicious emails after implementing DMARC, this brand experienced a 73 percent drop in authentication failures of legitimate mail across all domains, giving their marketing, transactional, and customer-support emails the best possible chance of being delivered.</td>
</tr>
<tr>
<td>Blocket, Sweden’s Largest Online Marketplace</td>
<td>Implementing DMARC meant a 99 percent reduction in suspicious messages in just three months, as well as a 70 percent drop in customer service tickets relating to phishing.</td>
</tr>
<tr>
<td>HM Revenue &amp; Customs</td>
<td>SPF and DMARC resulted in the elimination of 94 to 100 percent of fraudulent emails.</td>
</tr>
</tbody>
</table>
DMARC Adoption Among Mailbox Providers

Mailbox providers are serious about proactively protecting their users from phishing and spoofing—that's why their DMARC adoption rate has risen dramatically over the past two years. Today, it is estimated that 70% of the world’s consumer inboxes are protected by DMARC.

“ Overnight, the bad guys who have used email spoofing to forge emails and launch phishing attempts pretending to come from a Yahoo! Mail account were nearly stopped in their tracks.”

Jeff Bonforte, SVP of Communications Products, Yahoo!
Regional Coverage

The more that mailbox providers incorporate DMARC into their email filtering decisions, the greater the impact. While the overall adoption rate among mailbox providers is growing, when we look at the percentage of consumer inboxes protected by DMARC, we see that some countries are well ahead of others.

Canada leads the world in DMARC inbox protection with 90 percent coverage, followed by the United States, Brazil, and Spain at 85 percent. Both the United Kingdom and Australia are showing good adoption with 75 percent and 72 percent respectively.

Spain has made the most progress since last year, increasing its inbox protection by 25 percentage points.

At 30 percent, Germany has the lowest percentage of inboxes protected. Even worse, they have made no increase in inbox protection since last year.

Source: Return Path
DMARC has proven to be an effective defender of domain-based email threats in the consumer space. This growth of awareness and adoption is slowly permeating into the enterprise. Targeted email attacks, such as employee spear-phishing or executive whaling do not always include a payload, URL, or attachment, making it very difficult for traditional messaging gateways to detect and filter out these threats. A growing number of these attacks spoof the company’s own domains to deceive targeted employees.

In 2015, an increasing number of enterprise-messaging gateways enabled DMARC on their devices in order to detect and block spear-phishing emails that spoof corporate domains (see figure to the right). As more of these gateways enable DMARC, we will see more organizations leveraging DMARC to reject emails that spoof their domains from IP addresses not owned by the business.

However, it is important to note that enterprise-messaging gateways are in the early stages of rolling out DMARC, and reporting capabilities are still a big hurdle. 2016 will see an increased focus on providing enhanced reporting capabilities that threat intelligence platforms can leverage to identify malicious activity faster.
The Future of DMARC

ARC will drive greater DMARC adoption

In October 2015, Google announced plans to join both Yahoo! and AOL to become the third major mailbox provider to expand their use of DMARC. From June 2016, any email from a @gmail.com address, that does not come from Google’s infrastructure, will get rejected by mailbox providers and secure enterprise gateways that check DMARC.

Not all mail passes directly from sender to recipient. Some services like mailing lists or account forwarding receive a legitimate message and might make changes to it before sending it on, potentially resulting in SPF, DKIM, and/or DMARC alignment failure.

Authenticated Received Chain (ARC) aims to solve this problem by preserving the email authentication results of the original message thereby eliminating the risk of blocking legitimately forwarded messages. Once ARC becomes a IETF standard, we will see more companies following Yahoo!, AOL and Google’s lead to implement DMARC fully.

Building consumer awareness around trusted email

In February 2016, Google announced that it will provide a visual indication of whether a sender’s identity can be trusted in its Gmail interface. DMARC.org intends to take this a step further by collaborating with mailbox providers to develop a standardized indicator that visually flags messages failing authentication to consumers. This will remove the guesswork and deliver a safer, more transparent email experience for end users by making them aware of good versus bad email in their inbox.

This has implications for marketers and will drive brands to implement the latest authentication protocols more broadly in order to maintain positive subscriber engagement across their email marketing programs.

“We’re rapidly moving toward a world where all email is authenticated. Implementing a DMARC policy ensures that a sender’s reputation doesn’t drop due to the actions of spammers. If your domain doesn’t protect itself with DMARC, you will be increasingly likely to see your messages sent directly to a spam folder or even rejected.”

John Rae-Grant, Google Product Manager
Ready to Implement DMARC?

Start protecting your customers and employees today. Download our guide, Getting Started with DMARC, to learn how.

Find out more about Return Path Email Fraud Protection at: returnpath.com/stopemailfraud and @stopemailfraud

Methodology

Return Path conducted this study using a representative sample of more than 1,049 global companies across 33 countries from the following indices: Fortune 500, Inc. 5000 DJIA, NASDAQ, S&P, FTSE, and Forbes’ 2015 “Top 100 Most Recognizable Brands.”

DMARC adoption data was pulled in January 2016. Percentages may not add up to 100 due to rounding.

Contact Us

USA (Corporate Headquarters)
rpinfo@returnpath.com

Australia
rpinfo-australia@returnpath.com

Brazil
rpinfo-brazil@returnpath.com

Canada
rpinfo-canada@returnpath.com

France
rpinfo-france@returnpath.com

Germany
rpinfo-germany@returnpath.com

United Kingdom
rpinfo-uk@returnpath.com

returnpath.com