GLOBAL DMARC ADOPTION 2019

Featuring **Matthew Vernhout** (CIPP/C)
Director of Privacy, 250ok

250ok

TABLE OF CONTENTS

INTRODUCTION

250ok, a leader in advanced email analytics for Domain-based Message Authentication, Reporting & Conformance (DMARC), deliverability, design and engagement, recently analyzed several industries' adoption of the strictest email authentication standard. DMARC is a sender-published policy for email messages that fail authentication. **By deploying and monitoring DMARC, brands lower the likelihood their domains are spoofed and used for phishing attacks on recipients, including customers, clients, and employees, amongst others.**

DMARC policies are designed to be an incremental process, from a simple reporting-only system to a strict policy where messages failing authentication are rejected without being delivered or seen by the intended recipient.

What are the policies and what exactly do they mean?

P=NONE (GOOD)

This policy setting is the starting point for all DMARC implementations, and is the least restrictive policy. By setting your policy to p=none, you're asking the receiving domains to handle mail as they normally would and to not take any additional action on mail that could fail authentication. At p=none you will begin to receive daily aggregate reporting from participating ISPs detailing a number of items, such as the number of messages they've seen using your domain name, how many messages passed or failed authentication, and authentication results of the mail.

P=QUARANTINE (BETTER)

Once a domain has received a number of reports at a none stage, and evaluated and corrected any potential authentication issues, it is time to step up to a p=quarantine policy. This policy is a request from a domain to have any mail failing authentication be routed to the spam/bulk/junk folder. This is to limit the impact of potentially legitimate emails not identified in the p=none stage.

P=REJECT (BEST)

For the most secure set-up under DMARC, you can choose to use a reject policy, the strictest policy level. This policy is used to stop mail that fails authentication from even being accepted by the receiving mail systems. A failure of both DKIM and SPF with a reject policy is also a DMARC failure and will cause mail to be rejected.

A 2018 study from the Anti-Phishing Working Group reported a decline in reported phishing attacks during Q4 2018. However, this is not due to less attacks, but instead, phishing is simply getting harder to detect, thanks to new tactics like multiple redirects and valid security certificates. In fact, there was a 29.8% increase in phishing scams targeting SaaS companies in an attempt to get data and credentials.

RESEARCH OVERVIEW

250ok conducted an analysis of 25,700 domains controlled across the following sectors: education, e-commerce, Fortune 500, US government (Executive, Legislative and Judicial), the China Hot 100, the top 100 law firms, international nonprofits, the SaaS 1000, financial services, and travel.

It is worth noting a meaningful number of firms likely use a subdomain for some of their messaging (e.g., “company.com” is a parent or organization domain; “mail.company.com” is a subdomain). However, leaving the parent domain unauthenticated is an open invitation for spoofing, phishing, and mail forgery. A published record at the parent domain will protect the entirety of the domain, including any potential subdomain, as they will automatically inherit the DMARC policy of the parent domain.

Assumptions are made about the presence and validity of SPF and DKIM records if a domain is using DMARC with any type of enforcement, and thus were left out of this report. Also, identifying the presence of a DKIM record requires knowledge of the domain’s selector, which was not available for all company domains at the time of writing this report.

We included several new categories to our analysis, rendering a direct year-over-year aggregate comparison not feasible, but where we reviewed last year's numbers, we indicate changes in adoption.

GLOBAL ADOPTION

When reviewing all the domains in our data set, on average, we see a significant portion of those studied not publishing any type of DMARC record. While this looks bleak, many of the individual industry groups monitored performed significantly better than the overall averages suggest.

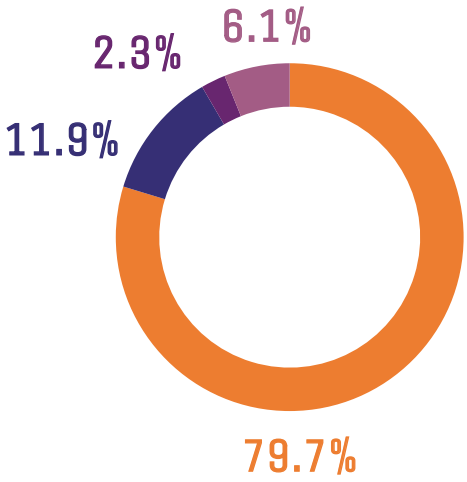
FIGURE 1.1

Global DMARC Adoption 2019

LEGEND

n=21,075 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy



- 20.3% of domains are publishing some level of DMARC policy and 6.1% have a reject policy in place.
- Publishing any DMARC record is an improvement over most domains studied.

POSTSECONDARY EDUCATION

While universities and colleges are full of information about students, parents, and staff, they also contain research and detailed information about their current research efforts. This was most recently highlighted by email phishing and hacking efforts on universities researching military technologies across the United States. Universities in Canada and Southeast Asia have also been targeted for sensitive data and research. According to Campus Safety Magazine, "They believe hackers used phishing tactics, often posing as other institutions, to access the university's network."

This DMARC adoption acts like a vaccine; increased support by the community builds herd immunity to impersonation and fraudulent messages designed to trick recipients into installing malware or providing information via a fake landing page.

250ok conducted an analysis of 6,188 parent domains controlled by accredited colleges and universities in the United States, Canada, and the European Union.

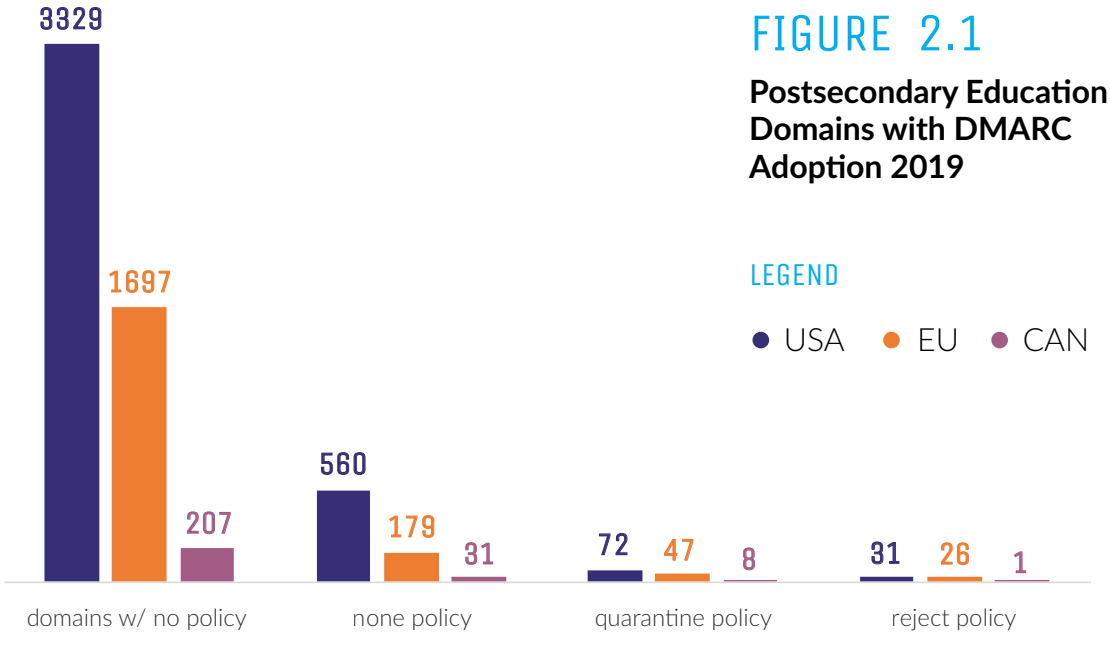


FIGURE 2.1

Postsecondary Education Domains with DMARC Adoption 2019

LEGEND

USA EU CAN

- Postsecondary institutions around the world are trending about the same for adoption of DMARC, with the United States slightly further ahead on moving to a reject policy.

UNITED STATES

250ok conducted an analysis of 3,992 parent domains controlled by accredited colleges and universities in the United States.

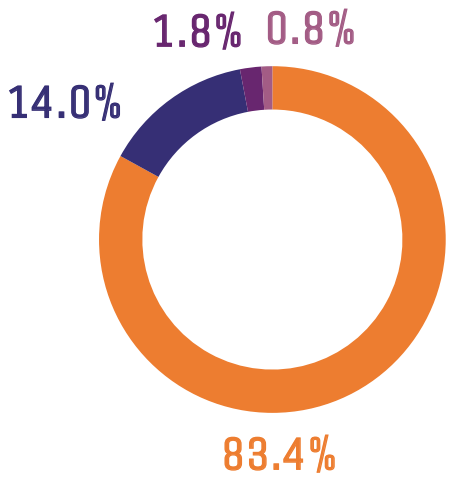
FIGURE 2.2

United States Postsecondary Education DMARC Adoption 2019

LEGEND

n=3,992 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy



Adoption when compared to 2018:

↑ 5.4% *Overall adoption increased from 88.8%*

↑ 4.2% *None policy adoption up from 9.8%*

↑ 0.8% *Quarantine policy adoption up from 1.0%*

↑ 0.4% *Reject policy adoption up from 0.4%*

CANADA

250ok conducted an analysis of 247 parent domains controlled by accredited colleges and universities in Canada.

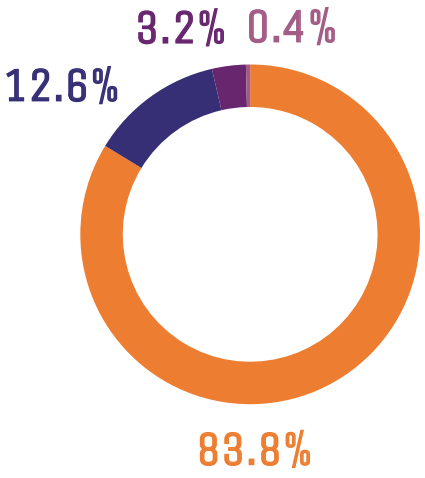
FIGURE 2.3

Canadian Postsecondary Education DMARC Adoption 2019

LEGEND

n=3,992 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy



Adoption when compared to 2018:

↑ 6.5% *Overall adoption increased from 90.3%*

↑ 4.9% *None policy adoption up from 7.7%*

↑ 1.6% *Quarantine policy adoption up from 1.6%*

– 0.0% *Reject policy adoption had no change*

EUROPEAN UNION

250ok conducted an analysis of 1,949 parent domains controlled by accredited colleges and universities in the European Union.

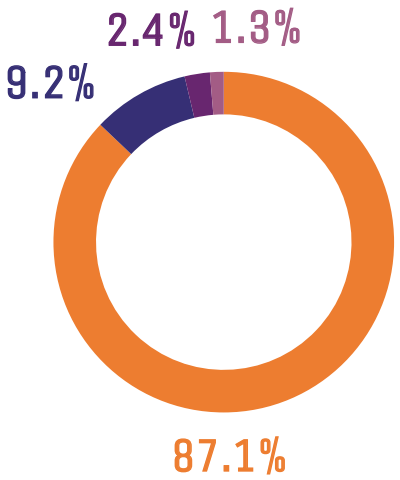
FIGURE 2.4

European Union Postsecondary Education DMARC Adoption 2019

LEGEND

n=3,992 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy



Adoption when compared to 2018:

- ↑ 4.3% *Overall adoption increased from 91.4%*
- ↑ 2.9% *None policy adoption up from 6.3%*
- ↑ 0.9% *Quarantine policy adoption up from 1.5%*
- ↑ 0.5% *Reject policy adoption up from 1.8%*

INTERNET RETAILERS

Internet retailers are increasing adoption of DMARC on their parent domains alongside their commercial mailing domains. This coincides with a general push for DMARC support from their ESPs and continued encouragement for subdomain adoption on their platforms.

Support for DMARC is also a mandatory qualification for participation in the Brand Indicators for Message Identification (BIMI) program, which requires a domain to apply some level of enforcement policy (p=quarantine or p=reject).

In our experience, as the awareness of BIMI and the desire by brands to have their logos populated in an email client grows, the desire to apply DMARC is growing in kind. At the Certified Senders Alliance in Cologne, Germany in April 2019, the Authindicators Working Group announced more than 100 brands were participating in the Verizon BIMI beta, and that Google officially joined the working group with plans to eventually support the standard in their various user interfaces, both mobile and desktop.

However, when you do compare both years' lists, the 2019 ranked brands have a significant improvement over the 2018 group (29% with a record vs. 16%, respectively).

Overall, internet retailers are performing better on DMARC adoption for their corporate or brand domains when compared to global averages we studied this year. However, they are significantly over indexing on p=none (22.3% versus global index of 11.9%) and p=quarantine (4.6% versus global index of 2.3%), and performing about half as well on a full p=reject policy (3.1% versus global index of 6.1%).

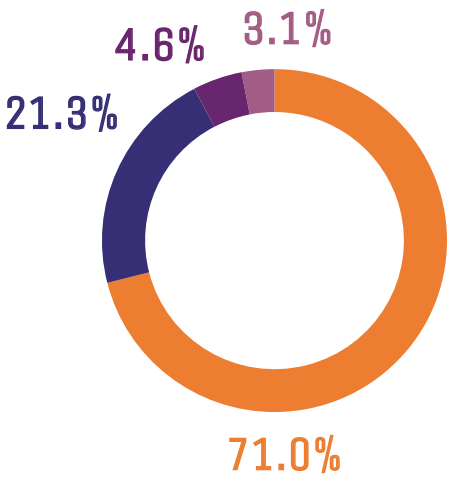
FIGURE 3.1

Global Internet Retailers DMARC Adoption 2019

LEGEND

n=3,033 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy



EUROPEAN UNION

250ok performed an analysis of 1,016 parent domains actively operated by the top 500 EU online retailers by revenue for any indicator of DMARC authentication.

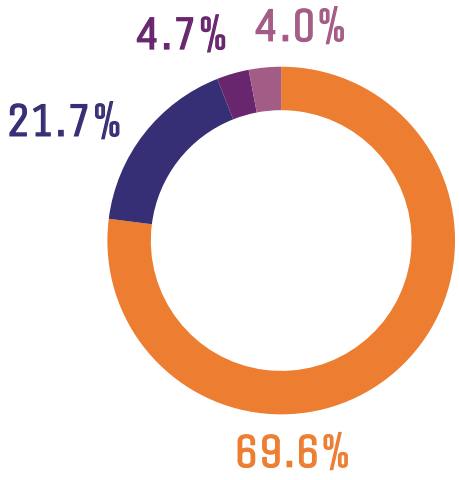
FIGURE 3.2

Top 500 European Union Internet Retailer DMARC Adoption 2019

LEGEND

n=1,016 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy



Adoption when compared to 2018:

- ↑ 14.8% *Overall adoption increased from 84.4%*
- ↑ 10.2% *None policy adoption up from 11.5%*
- ↑ 2.2% *Quarantine policy adoption up from 2.5%*
- ↑ 2.4% *Reject policy adoption up from 1.6%*

UNITED STATES

250ok performed an analysis of 2,017 parent domains actively operated by the top 1000 US online retailers by revenue for any indicator of DMARC authentication.

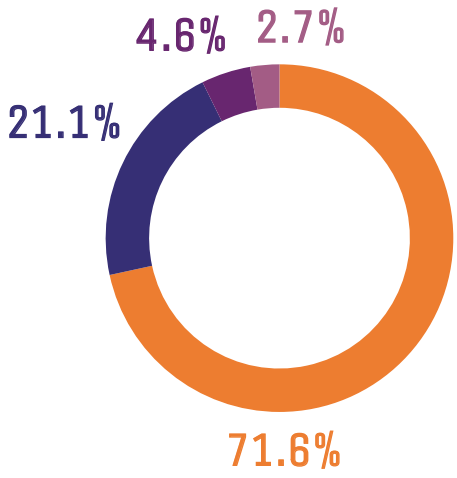
FIGURE 3.3

Top 1000 United States Internet Retailer DMARC Adoption 2019

LEGEND

n=2,017 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy



Adoption when compared to 2018:

- ↑ 12.5% *Overall adoption increased from 84.1%*
- ↑ 8.7% *None policy adoption up from 12.4%*
- ↑ 2.3% *Quarantine policy adoption up from 2.3%*
- ↑ 1.5% *Reject policy adoption up from 1.2%*

FORTUNE 500

(NEW FOR 2019)

250ok performed an analysis of 1,780 parent domains actively operated by the Fortune 500 for any indicator of DMARC authentication.

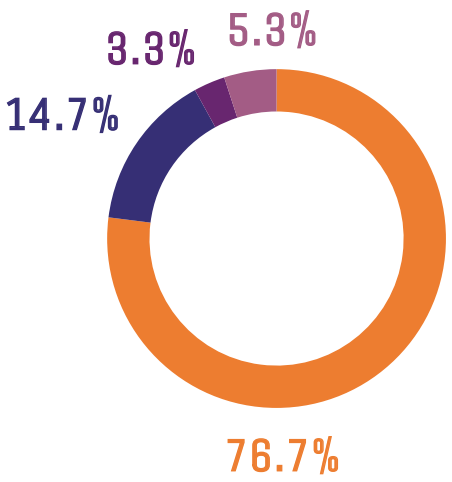
FIGURE 4.1

Fortune 500 DMARC Adoption 2019

LEGEND

n=1,780 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy



CHINA HOT 100

250ok performed an analysis of 307 parent domains owned by the top 100 most valuable Chinese brands, or the China Hot 100, looking exclusively for published DMARC records.

Comparing the numbers to last year, we still see a general lack of DMARC adoption in China's largest companies. This is the second year in a row we've surveyed this same group of companies and found zero domains using a p=reject, though we do note a slight increase in support for p=none and p=quarantine.

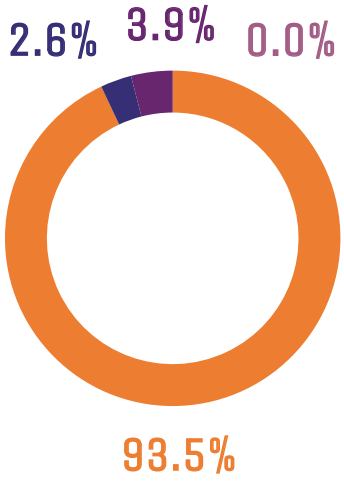
FIGURE 5.1

China Hot 100 DMARC Adoption 2019

LEGEND

n=307 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy



- 93.5% of top-level domains studied lack the most basic DMARC policy, leaving Chinese brands at risk of phishing attacks.
- 6.5% of all domains reviewed had a DMARC policy in place.

Adoption when compared to 2018:

↑ 1.9% *Overall adoption increased from 95.4%*

↑ 0.6% *None policy adoption up from 2.0%*

↑ 0.9% *Quarantine policy adoption up from 1.3%*

– 0.0% *Reject policy adoption had no change*

LAW FIRMS

250ok conducted an analysis of 100 parent domains controlled by the top 100 accredited law firms around the globe, as determined by revenue.

Spear phishing and impersonation continue into 2019 as a serious threat for law firms around the world, and in response, the top 100 firms significantly increased adoption of DMARC. While the sample size is small, the adoption for these institutions is significant.

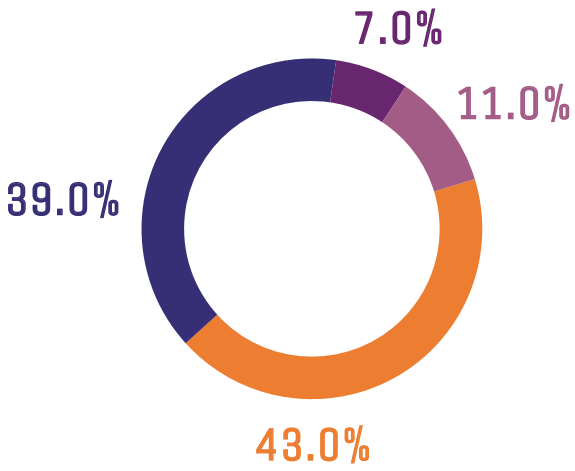
FIGURE 6.1

Top 100 Law Firms
DMARC Adoption 2019

LEGEND

n=100 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy



Adoption when compared to 2018:

↑ 19.0% *Overall adoption increased from 62%*
↑ 6.0% *None policy adoption up from 33%*
↑ 5.0% *Quarantine policy adoption up from 2%*
↑ 8.0% *Reject policy adoption up from 3%*

NONPROFIT ORGANIZATIONS (NPO)

250ok conducted an analysis of 7,300 parent domains controlled by NPOs with at least 25 employees.

This segment of the market is largely failing to adopt DMARC while they continue to hold a significant amount of personal data about their donors and partners. At smaller organizations with budgetary constraints, implementation of wide-scale DMARC support when balanced against their other efforts is a secondary priority. The complexity of managing DMARC, the urgency to adopt a new standard, and being budget-friendly all play a role in low adoption rates.

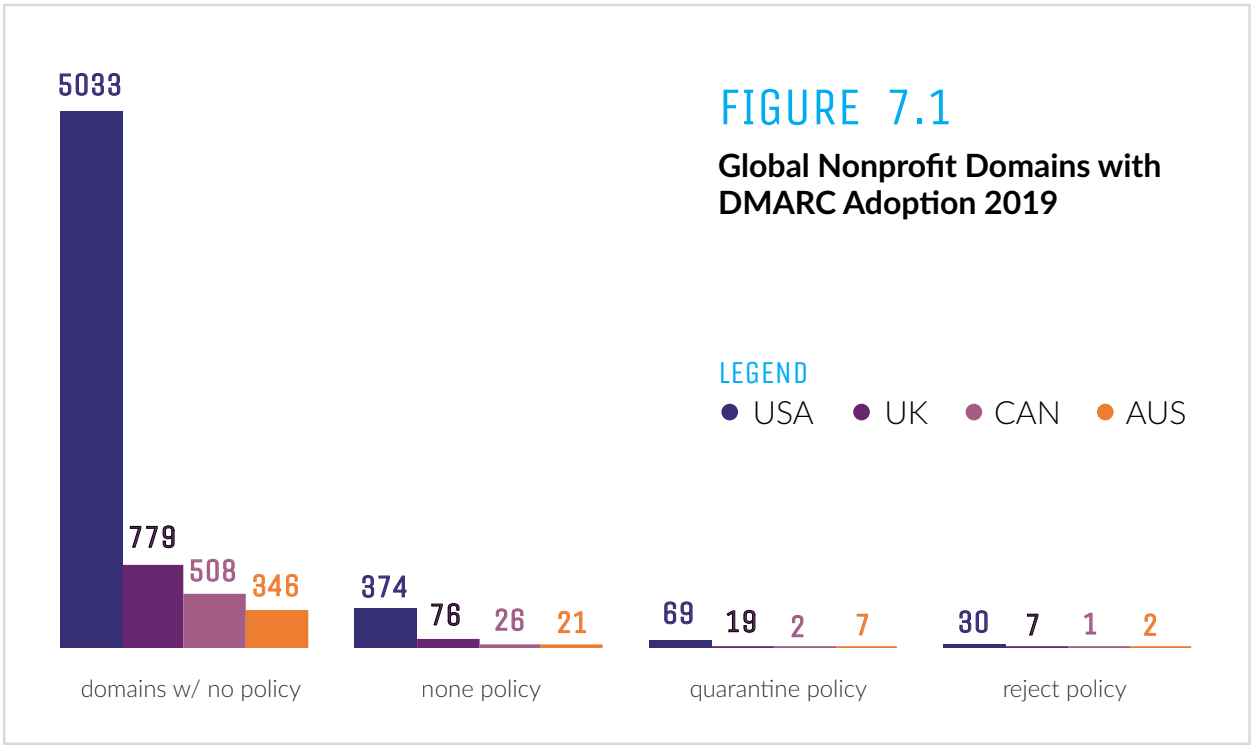


FIGURE 7.1

Global Nonprofit Domains with DMARC Adoption 2019

UNITED STATES

250ok analyzed 5,506 parent domains for NPOs operating within the United States.

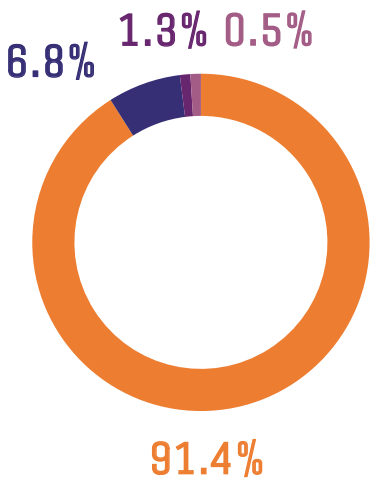
FIGURE 7.2

United States Nonprofits DMARC Adoption 2019

LEGEND

n=5,506 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy



Adoption when compared to 2018:

- ↑ 2.8% *Overall adoption increased from 94.2%*
- ↑ 2.1% *None policy adoption up from 4.7%*
- ↑ 0.5% *Quarantine policy adoption up from 0.8%*
- ↑ 0.2% *Reject policy adoption up from 0.3%*

UNITED KINGDOM

250ok analyzed 5,506 parent domains for NPOs operating with the United Kingdom.

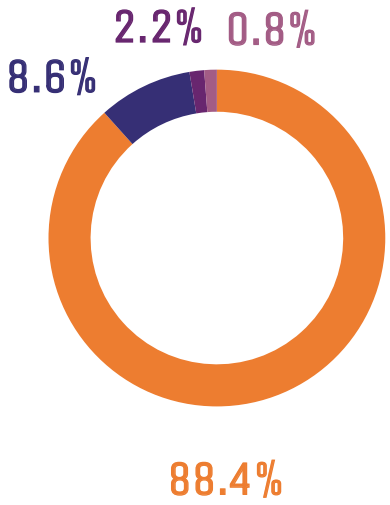
FIGURE 7.3

United Kingdom Nonprofits DMARC Adoption 2019

LEGEND

n=881 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy



Adoption when compared to 2018:

↑ 4.3% *Overall adoption increased from 92.7%*

↑ 2.8% *None policy adoption up from 5.8%*

↑ 1.5% *Quarantine policy adoption up from 0.7%*

– 0.0% *Reject policy adoption had no change*

CANADA & AUSTRALIA

New in 2019, the Canadian NPO category includes 537 parent domains, and the Australian NPO group contains 376 parent domains. Adoption of DMARC for both groups follows closely with the global average and other international organizations.

FIGURE 7.4

Canadian Nonprofits DMARC Adoption 2019

LEGEND

n=537 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy

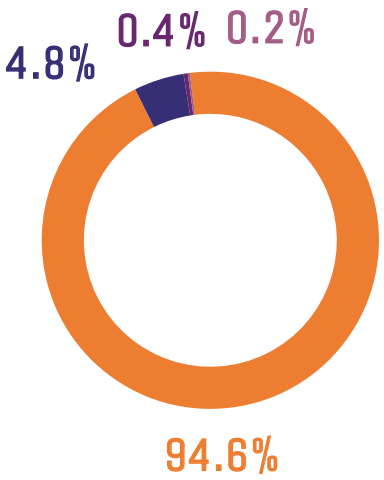


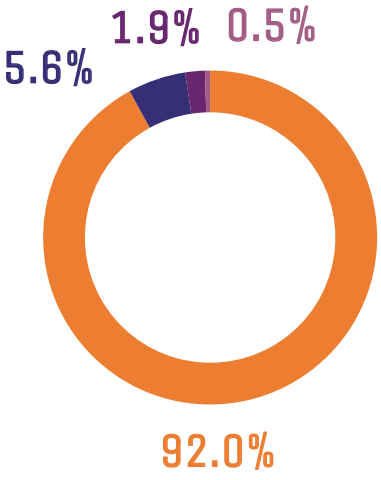
FIGURE 7.5

Australian Nonprofits DMARC Adoption 2019

LEGEND

n=376 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy



SAAS 1000

250ok performed an analysis of the 1,000 parent domains owned by the top 1,000 SaaS businesses, looking exclusively for published DMARC records.

As the SaaS 1000 list changes from year to year, we recognize this is not a direct comparison of the same organizations, as some may have been added or removed, but the change is small enough that we decided it was not significant enough to impact a comparison of the 2018 and 2019 data sets.

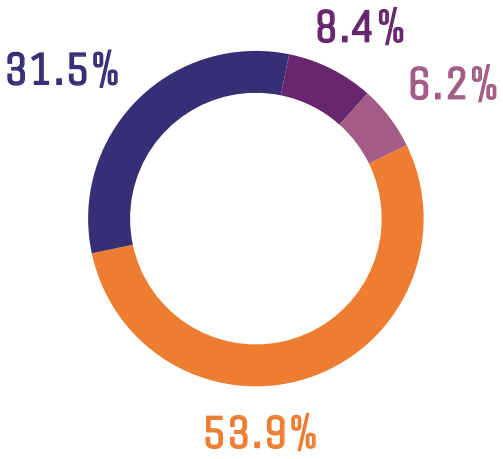
FIGURE 8.1

SaaS 1000 DMARC Adoption 2019

LEGEND

n=1,000 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy



Adoption when compared to 2018:

↑ 11.1% *Overall adoption increased from 65.0%*

↑ 6.5% *None policy adoption up from 25.0%*

↑ 3.2% *Quarantine policy adoption up from 5.2%*

↑ 1.4% *Reject policy adoption up from 4.8%*

FINANCIAL SERVICES

(NEW FOR 2019)

250ok performed an analysis of 2,186 parent domains owned by the top financial services businesses in the United States, looking exclusively for published DMARC records.

This is a new vertical for our reports, but when compared against the global benchmark, financial services trends higher in all categories of DMARC enforcement except for p=reject.

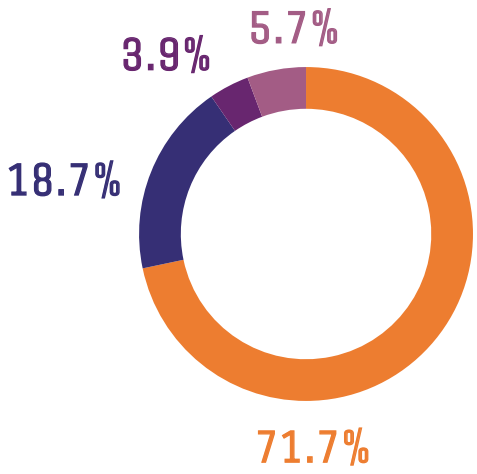
FIGURE 9.1

Financial Services DMARC Adoption 2019

LEGEND

n=2,186 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy



TRAVEL INDUSTRY

(NEW FOR 2019)

250ok performed an analysis of 1,285 parent domains owned by the top travel-related businesses in the United States, looking exclusively for published DMARC records.

This is a new vertical for our reports, and when compared against the global benchmark, the travel industry trends significantly behind in all categories of DMARC enforcement. This is highly concerning as several airlines, hotels, and travel-based organizations experienced large-scale data breaches in 2018.

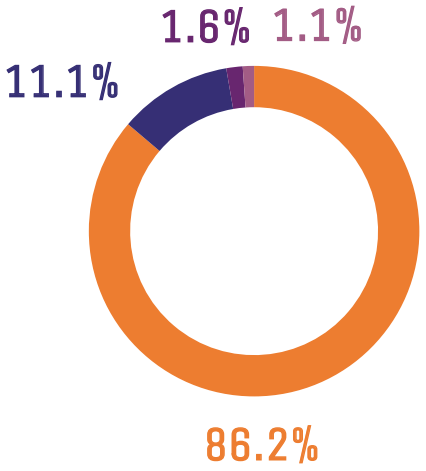
FIGURE 10.1

Travel Industry DMARC Adoption 2019

LEGEND

n=1,285 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy



UNITED STATES .GOV

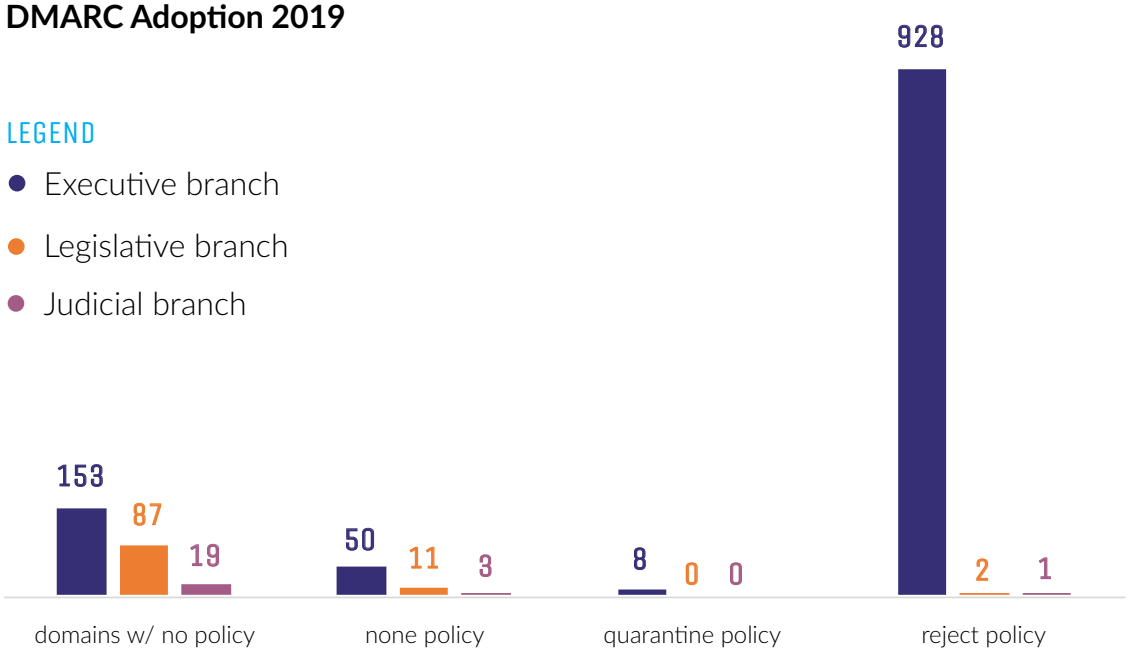
(NEW FOR 2019)

250ok performed an analysis of 1,262 parent domains managed by the three branches of the United States government, looking exclusively for published DMARC records.

In October 2017, the Department of Homeland Security's (DHS) binding operational order 18-01 required the Executive branch of the government move to a reject policy. It was quite successful in motivating their adoption of DMARC.

FIGURE 11.1

United States .gov Domains with DMARC Adoption 2019



EXECUTIVE, LEGISLATIVE & JUDICIAL BRANCH

Overall, the .gov space is the best supporting segment we reviewed, with the Executive branch trailblazing with 81.5% of domains surveyed at a p=reject policy, 0.7% at a p=quarantine, and 4.4% at a p=none, leaving 13.4% of domains without any type of DMARC record.

The smallest of the government branches, Judicial, is way behind in adoption with only 17.3% of domains with any type of policy.

Finally, the Legislative branch pulls up the rear with 13.0% of domains applying a DMARC policy.

FIGURE 11.2

United States Executive .gov DMARC Adoption 2019

LEGEND

n=1,139 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy

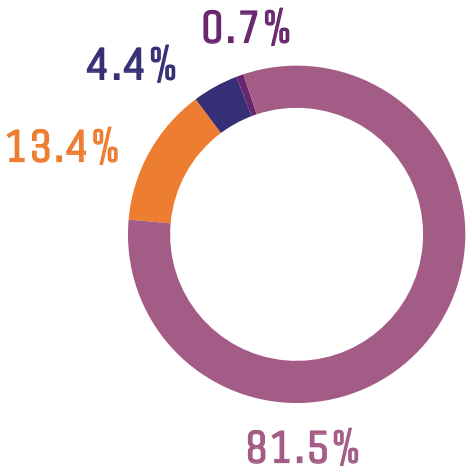


FIGURE 11.3

United States Legislative .gov DMARC Adoption 2019

LEGEND

n=100 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy

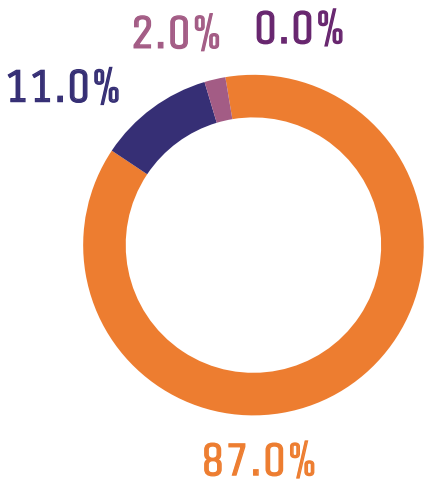


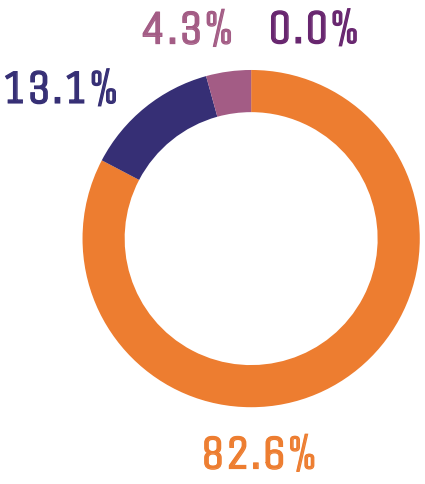
FIGURE 11.4

United States Judicial .gov DMARC Adoption 2019

LEGEND

n=23 domains

- domains w/ no policy
- none policy
- quarantine policy
- reject policy



CONCLUSIONS

After reviewing more than 25,000 domains, DMARC adoption overall trends upward, with nearly 25% of all domains reviewed showing some level of DMARC adoption, proving the standard is slowly maturing.

With the Binding Order from DHS pushing the United States Executive branch to lead the way with a strong enforcement policy, we still see the not-for-profit sector worldwide failing to embrace DMARC, and the China Hot 100 continuing for a second year to be the least likely to adopt DMARC.

This upward progress shows a general maturity to the DMARC standard and a growing understanding of how important authentication is for protecting a brand, their consumers, and their employees.

KEY TAKEAWAYS

1. Adoption is progressing, but has a long way to go.
2. Phishing is still the leading cause of data breaches, and more data was compromised in 2018 than ever before, even though there were fewer major breaches than in 2017.
3. More education and better tools to manage authentication are necessary as many records are improperly formatted, incomplete, or not actually enforcing a policy.

WILL BIMI BE ENOUGH TO DRIVE ADOPTION OF DMARC?

BIMI is the proverbial carrot for brands to drive adoption for DMARC and create a more secure email community. By supporting a DMARC record with an enforcement policy, meaning properly authenticated mail is necessary to implement BIMI, organizations can benefit from BIMI's support of a brand logo in desktop and mobile email clients.

WHY IS ADOPTION SO POOR IN CHINA?

This is likely the result of China's reliance on social platforms and SMS rather than email. Quartz.com reported while China's residents tend to have email addresses, they prefer communication over one of their local social channels such as WeChat or SMS. This would also support the idea that email is simply not a priority for businesses or consumers in the region, and better illuminates the general lack of adoption of email authentication. Yet this raises new questions for marketers outside of China: Should you be concerned your emails are not being read or delivered to China, and are you missing out on a large population by avoiding their preferred communication?

ABOUT

Matthew Vernhout (CIPP/C)

Director of Privacy, 250ok

Matthew Vernhout is a digital messaging industry veteran and Certified International Privacy Professional (Canada) (CIPP/C) with nearly two decades of experience in email marketing. Matthew is 250ok's Director of Privacy, the Vice Chair of the Email Experience Council (eec), director at large with the Coalition Against Unsolicited Commercial Email (CAUCE) and the founder of the Canadian Email Summit. He is a trusted industry expert, recognized as the 2019 eec thought-leader of the year, speaking frequently at email marketing and technology conferences around the globe, and maintaining his celebrated blog, EmailKarma.net.

250ok

250ok is a SaaS platform bringing marketers advanced insights into email deliverability, design, sender reputation, fraud protection, and consumer engagement—the ultimate intelligence add-on to any ESP. Headquartered in Indianapolis, Indiana, 250ok's platform provides data and insights for a large and growing number of businesses in categories ranging from travel, publishing, tech, and retail—including three of the top six US retail e-commerce companies by sales share in 2018.

For more information, visit 250ok.com.