250ok

# MULTI-INDUSTRY DMARC ADOPTION 2018

Featuring **Matthew Vernhout** (CIPP/C)

*Director of Privacy, 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.

Across the board, DMARC adoption is at a troublingly low rate. Although the US federal government mandated the strictest DMARC policy (p=reject) for all government-owned domains, other industries lag behind in protecting their email and their consumers from phishing, spoofing, and other trust-damaging attacks.

A 2017 study from the Anti-Phishing Working Group reported an average of 443 brands per month were targeted for phishing attacks in the first half of 2017, up from 413 per month during the same period in the previous year. These attacks are a threat to brand trust, as 91% of all cyber attacks begin with a phishing email. Although most of today's consumers are aware of phishing attacks, two in five US consumers fell victim to an online phishing attack, according to a 2017 Cyber Monday phishing survey by DomainTools.

# RESEARCH OVERVIEW

250ok looked at several industries' adoption of DMARC by reviewing a specific set of domains. Each industry's report follows, with more specific indicators for what was reviewed and when.

When we decided to review the domains in this report, we opted to use information already publicly available. When publishing email authentication records, there are several DNS records created; mainly the TXT records for SPF, DKIM and DMARC. Two of these records are available without any additional knowledge beyond the domain you want to review: SPF and DMARC, as they are published in a consistent format for each of the domain or subdomain record you want to evaluate.

DKIM records require a little more knowledge to evaluate. We did not review each DKIM record as part of this process, since not all of the selectors were available to us.

It is also worth noting a meaningful number of institutions likely use a subdomain for some of their messaging (e.g., "nonprofit.org" is a root domain; "mail.nonprofit.org" is a subdomain). However, leaving the root domain unauthenticated is an open invitation for spoofing, phishing, and mail forgery. A published record at the root domain will protect the entirety of the domain, including any potential subdomains, as they automatically inherit the DMARC policy of the root domain; however, subdomains can have their own DMARC policy.

# INDUSTRY FINDINGS

e-Retailers

Colleges and Universities

SaaS 1000

Chinese Brands

Law Firms

Nonprofit Organizations

# e-Retailers — EU

250ok performed an analysis of top level (root) domains actively operated by the top 500 EU online retailers by revenue for any indicator of DMARC authentication.

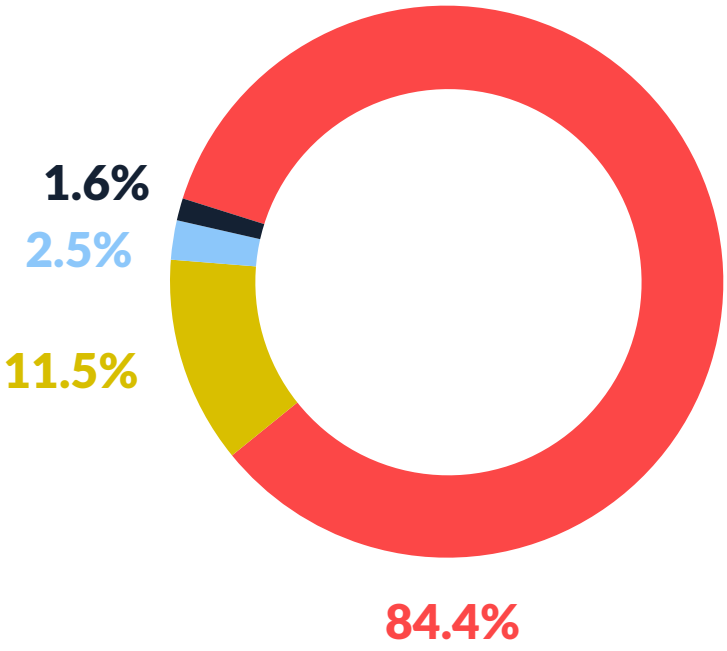



**FIGURE 1.1**

**DMARC Adoption Among Top EU e-Retailers**

**Legend**

n=1,016 domains

- Domains w/ no DMARC
- None policy - *good*
- Quarantine policy - *better*
- Reject policy - *best*

- 84.4% of top-level domains studied lack the most basic DMARC policy, which leaves some of the largest e-Retailers at risk of phishing attacks.
- 15.6% of all domains reviewed had a DMARC policy in place.

# e-Retailers — US

250ok performed an analysis of top level (root) domains actively operated by the top 1,000 US online retailers by revenue for any indicator of DMARC authentication.

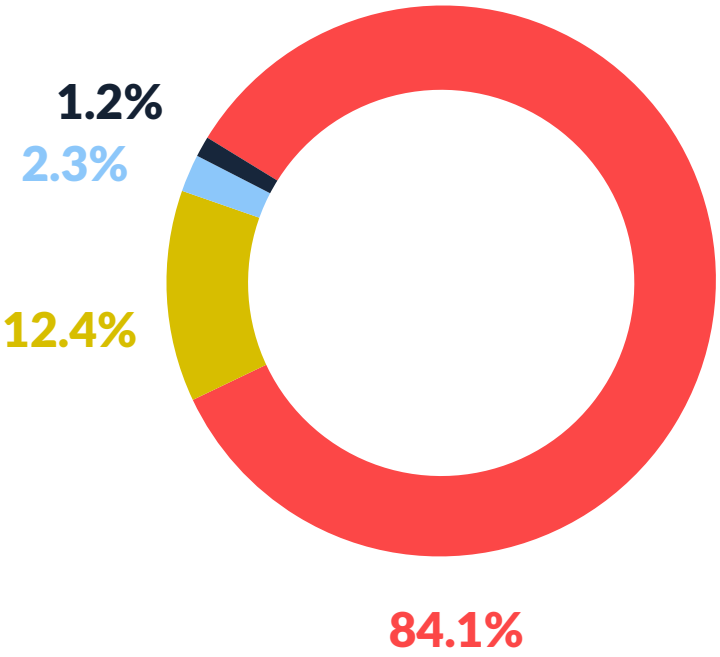



**FIGURE 1.2**

**DMARC Adoption Among Top US e-Retailers**

**Legend**

n=2,017 domains

- Domains w/ no DMARC
- None policy - *good*
- Quarantine policy - *better*
- Reject policy - *best*

- 84.1% of top-level domains studied lack the most basic DMARC policy, which leaves some of the largest e-Retailers at risk of phishing attacks.
- 15.9% of all domains reviewed had a DMARC policy in place.

# Colleges and Universities — Canada

250ok conducted an analysis of 247 top-level domains controlled by accredited Canadian colleges and universities.

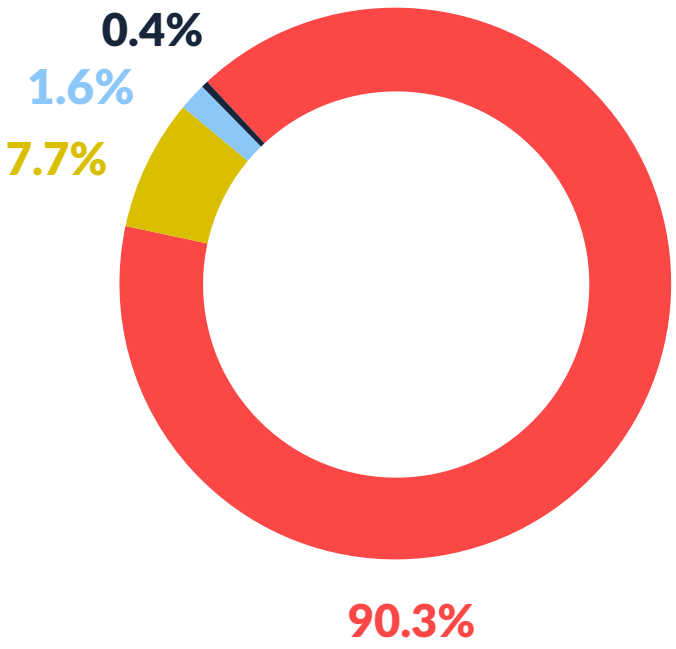



**FIGURE 2.1**

**DMARC Adoption Among Top Canadian Colleges and Universities**

**Legend**

n=247 domains

- Domains w/ no DMARC
- None Policy - *good*
- Quarantine Policy - *better*
- Reject Policy - *best*

---

- 90.3% of top-level domains studied lack the most basic DMARC policy, which leaves students, parents, alumni, and employees at risk of phishing attacks.
- 9.7% of all domains reviewed had a DMARC policy in place.

# Colleges and Universities — EU

250ok conducted an analysis of 2,117 top-level domains controlled by accredited EU colleges and universities.

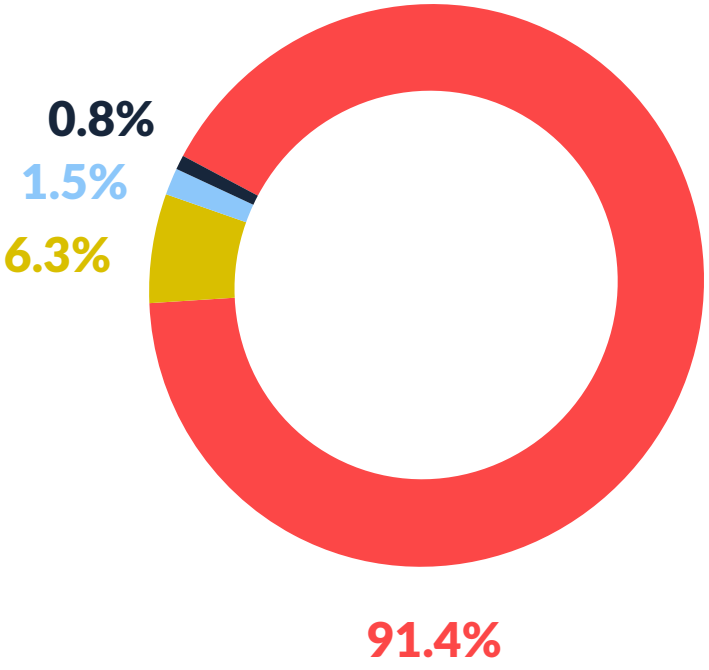



**FIGURE 2.2**

**DMARC Adoption Among Top EU Colleges and Universities**

**Legend**

n=2,117 domains

- Domains w/ no DMARC
- None Policy - *good*
- Quarantine Policy - *better*
- Reject Policy - *best*

- 91.4% of top-level domains lack the most basic DMARC policy, which leaves students, parents, alumni, and employees at risk of phishing attacks.
- 8.6% of all domains reviewed had a DMARC policy in place.

# Colleges and Universities — US

250ok conducted an analysis of 3,614 top-level domains controlled by accredited US colleges and universities.

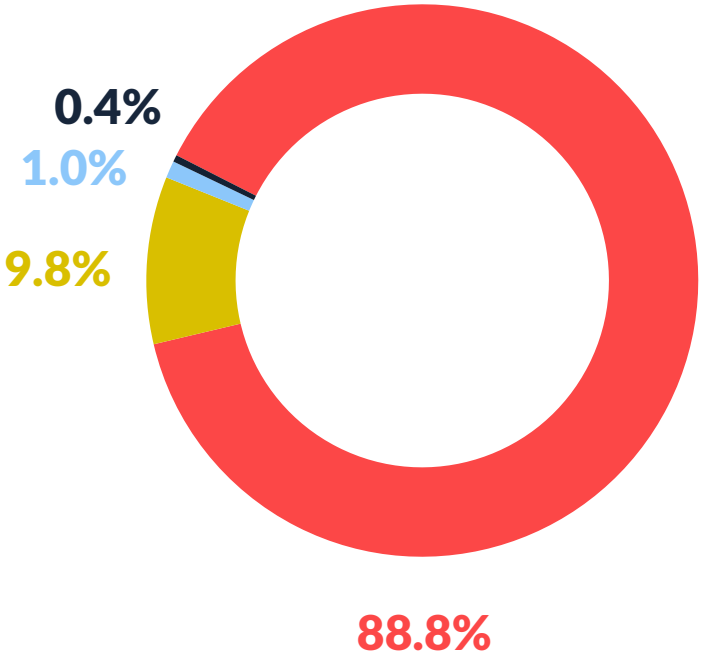



**FIGURE 2.3**

**DMARC Adoption Among Top US Colleges and Universities**

**Legend**

n=3,614 domains

- Domains w/ no DMARC
- None Policy - *good*
- Quarantine Policy - *better*
- Reject Policy - *best*

---

- 88.8% of top-level domains lack the most basic DMARC policy, which leaves students, parents, alumni, and employees at risk of phishing attacks.
- 11.2% of all .edu domains reviewed had a DMARC policy in place.

# SaaS 1000

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

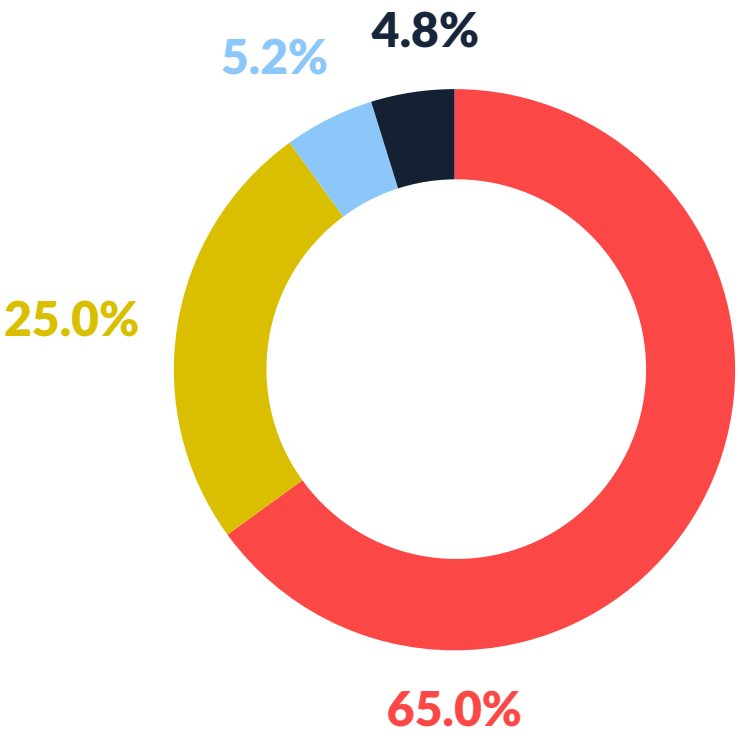



**FIGURE 3**

**DMARC Adoption Among SaaS 1000**

**Legend**

n=1,000 domains

- Domains w/ no DMARC
- None policy - *good*
- Quarantine policy - *better*
- Reject policy - *best*

---

- 65% of top-level domains studied lack the most basic DMARC policy.
- 35% of SaaS companies reviewed had a DMARC policy in place.

# Chinese Brands

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

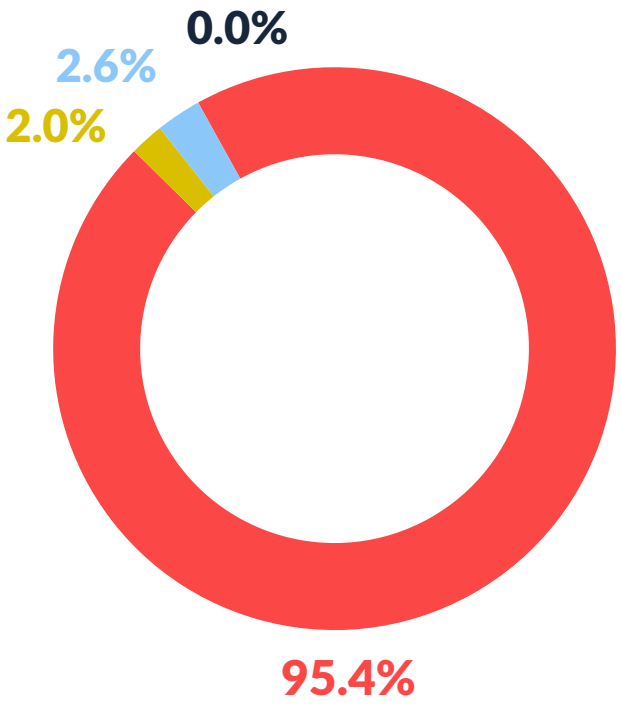



**FIGURE 4**

**DMARC Adoption Among Top 100 Chinese Brands**

**Legend**

n=307 domains

- Domains w/ no DMARC
- None policy - *good*
- Quarantine policy - *better*
- Reject policy - *best*

---

- 95.4% of top-level domains studied lack the most basic DMARC policy, which leaves Chinese brands at risk of phishing attacks.
- 4.6% of all domains reviewed had a DMARC policy in place.

# Law Firms

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

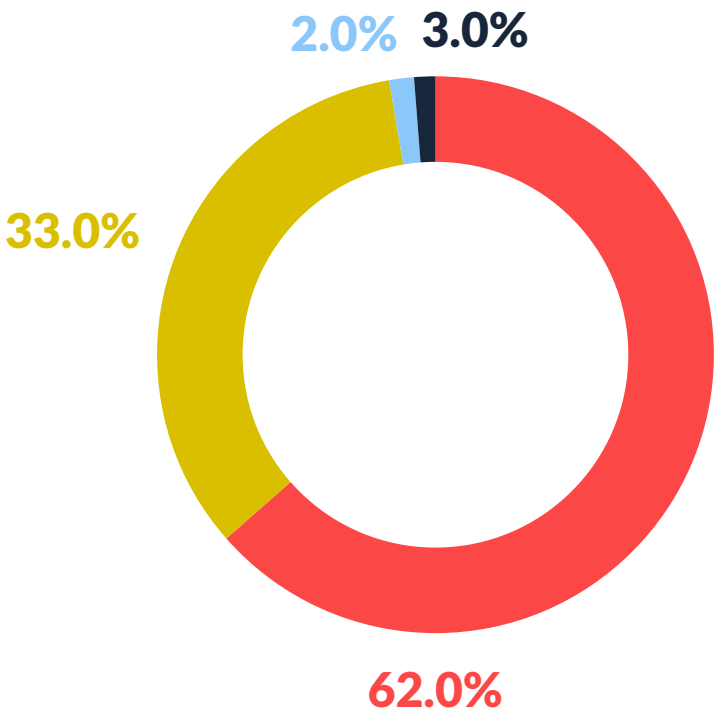



**FIGURE 5**

**DMARC Adoption Among Top 100 Law Firms**

**Legend**

n=100 domains

- Domains w/ no DMARC
- None policy - *good*
- Quarantine policy - *better*
- Reject policy - *best*

---

- Highest category of adoption in our series of DMARC reports, with 38% of domains reviewed using at least a none policy.
- Currently, only 3% of the top 100 law firm domains world wide have a reject policy.

# Nonprofts Organizations — UK

250ok conducted an analysis of 881 top-level domains controlled by UK-based NPOs with at least 25 employees.

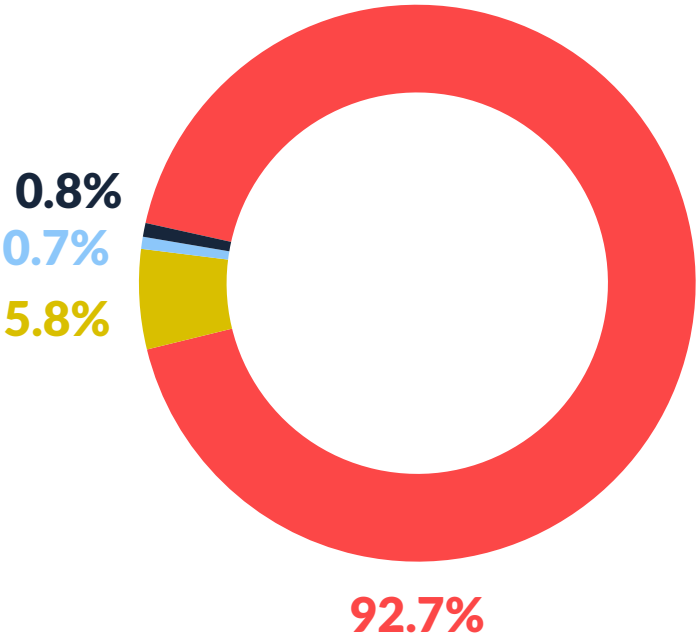



**FIGURE 6.1**

**DMARC Adoption Among UK Nonprofit Organizations**

**Legend**

n=881 domains

- Domains w/ no DMARC
- None policy - *good*
- Quarantine policy - *better*
- Reject policy - *best*

- 92.7% of top-level domains studied lack the most basic DMARC policy, which leaves donors, volunteers, staff, and more at risk of phishing attacks.
- 7.3% of all domains reviewed had a DMARC policy in place.

# Nonprofts Organizations — US

250ok conducted an analysis of 5,506 top-level domains controlled by US-based NPOs with at least 25 employees.

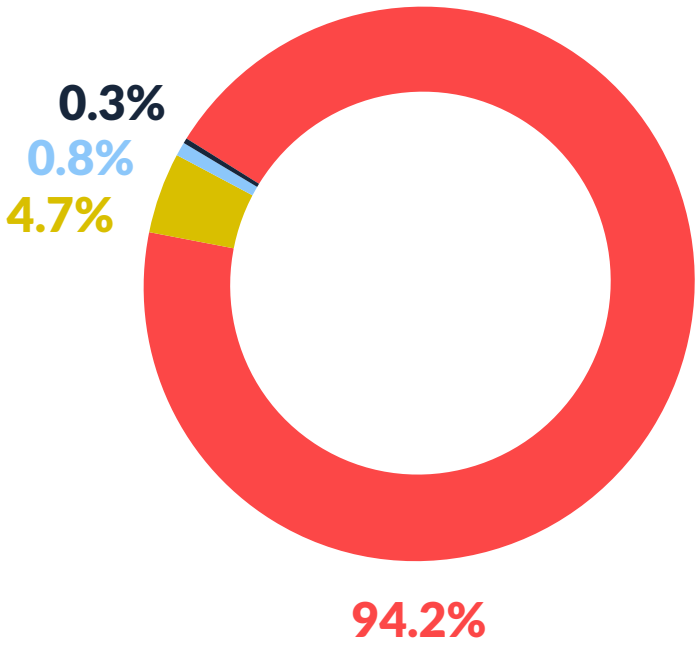



**FIGURE 6.2**

**DMARC Adoption Among US Nonprofit Organizations**

**Legend**

n=5,506 domains

- Domains w/ no DMARC
- None policy - *good*
- Quarantine policy - *better*
- Reject policy - *best*

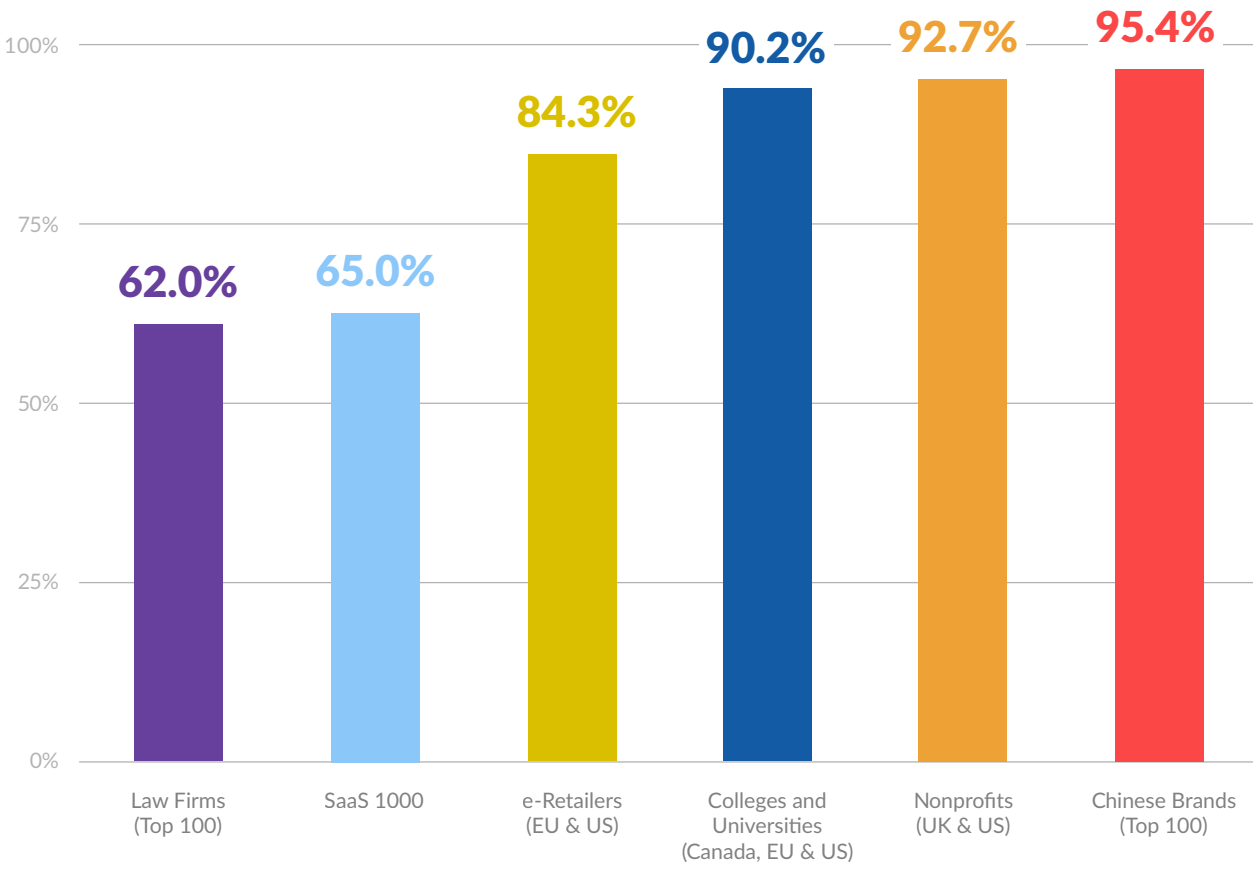
---

- 94.2% of top-level domains studied lack the most basic DMARC policy, which leaves donors, volunteers, staff, and more at risk of phishing attacks.
- 5.8% of all domains reviewed had a DMARC policy in place.

# MULTI-INDUSTRY OVERVIEW

**FIGURE 7**

**Domains with No DMARC Adoption**




- SaaS 1000 and the top 100 law firms have the best DMARC performance.
- Chinese brands and nonprofits have the worst DMARC performance.

# TAKEAWAYS

After reviewing almost 17,000 domains and multiple industry verticals, it is obvious there is a worldwide lack of DMARC adoption. Managers of email programs within any industry need to understand the following:

1. The benefits of DMARC.
2. The risks associated with ignoring DMARC.
3. The need to protect even small domains and domains that do not send emails.

These data points show a significant number of businesses and nonprofits are missing out on an opportunity to protect their brands and their consumers. Implementing a DMARC policy, even at a p=none, allows for a domain owner to understand where their legitimate email messages are originating from and be aware in the the case of spoofing or phishing of their brands. The information an organization can learn about their domain, the assistance it can provide to the brand's reputation, and the ability to proactively be aware of potential threats against their brands make deploying DMARC quite simply a must.

Emails without authentication are already starting to be impacted with slower delivery and rate limiting, and new visual indicators (both positive and negative) are coming to mailbox providers. With the ever-evolving nature of email, those who choose to not get caught in the past should start with DMARC.

# ABOUT

## Matthew Vernhout (CIPP/C)

*Director of Privacy, 250ok*

Matthew Vernhout is the Director of Privacy at 250ok and is a Certified International Privacy Professional (Canada) with nearly two decades of experience in email marketing. He actively shares his expertise on industry trends, serving as director at large of the Coalition Against Unsolicited Commercial Email (CAUCE), chair of the Email Experience Council's (EEC) Advocacy Subcommittee, and senior administrator of the Email Marketing Gurus group. He is a trusted industry thought-leader, speaking frequently at email marketing and technology conferences around the globe. Matthew has contributed to several benchmark publications during his career including *DMARC Adoptions Among e-Retailers*, *The EEC's Global Email Marketing Compliance Guide*, *The Impact of CASL on Email Marketing*, and more.

250ok

250ok focuses on advanced email analytics, insight and deliverability technology to power a large and growing number of enterprise email programs ranging from clients like eHarmony, Pinterest, and Furniture Row who depend on 250ok to cut through big data noise and provide actionable, real-time analytics to maximize email performance.

For more information, visit 250ok.com.