# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>03</td>
</tr>
<tr>
<td>Research Overview</td>
<td>04</td>
</tr>
<tr>
<td>Top US Colleges and Universities</td>
<td>05</td>
</tr>
<tr>
<td>Takeaways</td>
<td>06</td>
</tr>
<tr>
<td>Top 6 Recommendations</td>
<td>07</td>
</tr>
<tr>
<td>About</td>
<td>09</td>
</tr>
</tbody>
</table>
INTRODUCTION

250ok, a leader in advanced email analytics for DMARC, deliverability, design and engagement, recently developed a series of DMARC adoption reports for a variety of global industries.

Domain-based Message Authentication, Reporting & Conformance (DMARC) is a sender-published policy for messages that fail authentication. By deploying and monitoring DMARC, institutions lower the likelihood their domains are spoofed and used for phishing attacks on students, parents, and employees, among other recipients.

Implementing protections across institutions’ domains provides a critical first-step in deterring malicious emails. As data protection, online security, and brand trust become more important discussions for the general public, 250ok determined a need to identify which industries and institutions are doing the most, or least, to protect their stakeholders.

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

On February 12, 2018, 250ok conducted an analysis of 3,614 top-level domains controlled by accredited US colleges and universities. The scope of this study focused on the adoption of DMARC, an email authentication, policy, and reporting protocol that helps businesses prevent spoofing of their domains (e.g., www.college.edu).

It is worth noting a meaningful number of institutions likely use a subdomain for some of their messaging (e.g., “college.edu” is a root domain; “mail.college.edu” 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 subdomain as they will automatically inherit the DMARC policy of the root domain.
TOP US COLLEGES AND UNIVERSITIES

DMARC Adoption

Almost 90% (3,211) of top-level .edu domains lack the most basic DMARC policy, which leaves students, parents, alumni, and employees at risk of phishing attacks.

11.2% (403) of all .edu domains reviewed had a DMARC policy in place.

Only .4% (14) of the .edu domains reviewed were at a reject policy, the gold standard for DMARC.
TAKEAWAYS

- The analysis revealed domains controlled by US higher education institutions indexed lower in their adoption of a DMARC policy (11.2%) when compared to top US and EU retailers (15.8%) and significantly lower than technology companies listed in the SaaS 1000 (35%).

- Less than 1% of all US institutions had the gold standard DMARC policy in place.

- Almost 90% of colleges and universities in the US have zero DMARC protection in place.
TOP 6 RECOMMENDATIONS FOR PROTECTING .EDU EMAIL PROGRAMS

Properly setting up email authentication and deploying a DMARC policy on all actively operated domains are mandatory tasks for colleges and universities wanting to protect their brand, customers, and employees from phishing attacks.

Recommendations:

1. Implement both SPF and DKIM for all domains; however, if DKIM is further out on your road map, SPF is an ideal place to begin. For SPF we recommend -all or ~all, and strongly advise against the use of +all.

2. Publish a DMARC record for all domains, whether you send mail from them or not. Deploying a DMARC none policy (p=none) is a perfectly fine starting point. It's a great step to get used to the DMARC data and begin the process of evaluating the length and complexity of your DMARC journey.

3. Find a DMARC software solution that will help you quickly interpret the large amounts of DMARC data you will receive and guide you through the process of getting to a reject policy for your domains responsibly.
TOP 6 RECOMMENDATIONS FOR PROTECTING .EDU EMAIL PROGRAMS

4 If you do not have email authentication expertise or resources that can manage the process of getting to reject for your domains, engage with a consultant who can guide you through the process and expedite your timeline to achieving a reject policy for your domains.

5 For domains non-sending and defensively registered domains, publish a DMARC with reject policy. It is a quick win to start protecting your brand by locking down these assets that should never be sending mail.

6 Now that you are seeing reporting on all of your domains and you have expertise overseeing the project, build your DMARC plan. Responsibly move to a quarantine policy (p=quarantine) and, eventually, a reject policy (p=reject). The key here is “responsibly.” Different businesses will have different journeys. In many cases, top-level (root) domains have a complex ecosystem of internal systems and third parties that use the domain, which impacts the timeline for deploying a DMARC reject policy responsibly.

For more information on how 250ok DMARC software and services can help you responsibly deploy DMARC on your domains, contact us.
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, and maintaining his celebrated blog, EmailKarma.net. 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 focuses on advanced email analytics, insight and deliverability technology to power a large and growing number of enterprise email programs ranging from clients like Adobe, Marketo, 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.