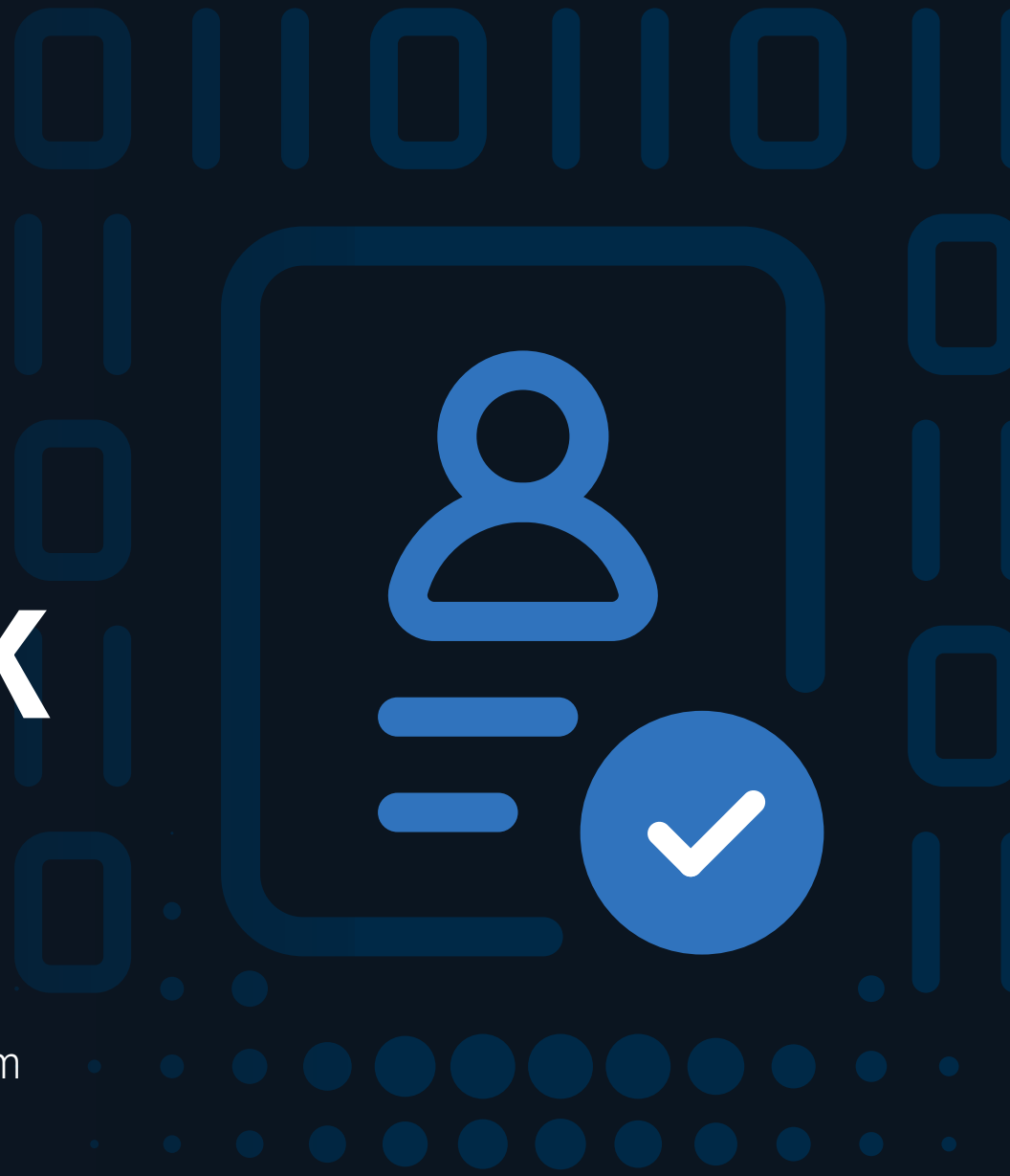
digicert

The 2026 Election Trust Check



Candidates are on the ballot. Impostors could be in your inbox

New DigiCert research finds 82% of U.S. political campaign domains aren't fully protecting voters from fraudulent emails

eBook | 2026

In politics, a familiar name carries weight. When that name appears in an inbox asking someone to donate, sign a petition, volunteer, or click for more information, voters need confidence that the message really came from the campaign it claims to represent. But an email address can be imitated.

That makes protecting a campaign's email domain a fundamental matter of digital trust. Without enforced authentication, fraudulent messages have a greater opportunity to reach voters, creating risk of phishing and financial fraud while potentially damaging the campaign's credibility. DigiCert's research examines a large gap in how campaign domains are not closing that door.

Analysis: Most campaign domains lack strong protection against email impersonation

Political campaigns depend heavily on email. Candidates use it to solicit votes and donations, recruit volunteers, announce events, respond to breaking news, and mobilize supporters before Election Day.

At the center of those communications is the campaign's domain: the core internet identity associated with the campaign, such as candidate.com. It may appear in the campaign's website address and after the "@" in its email. Seeing the same domain in a campaign's website and email can serve as a familiar signal that the message originated from that campaign. Because voters may view that domain as a sign that a message is legitimate, protecting it helps prevent unauthorized senders from stealing the campaign's identity.

To assess how well those identities are protected, DigiCert analyzed the publicly available email-authentication records of 3,756 political campaign domains across all 50 states. Only 18% enforced DMARC, a widely used technology that allows domain owners to block emails pretending to come from their trusted domain.

Put another way, 82% of the campaign domains examined were not using DMARC enforcement to direct email providers to quarantine or reject messages that fail DMARC while appearing to come from their domains as of August 21, 2026. The pattern was consistent across party lines, with Democratic and Republican campaign domains showing similarly low rates of DMARC enforcement.

For campaigns that routinely ask voters to trust a message, click a link and sometimes send money, that lack of protection matters.

When email represents the candidate

Email security is only one part of campaign operations, and this research does not examine whether email configuration affects election outcomes. It addresses a narrower question: How well are campaigns protecting the digital identities they use to communicate with voters?

Campaigns invest significant time and resources in building direct relationships with voters and supporters, with email serving as an important part of that effort. When an unauthorized sender can impersonate a campaign's domain, they can exploit the recognition and credibility the campaign has worked to establish.

And that raises a simple question:

When an email claims to come from a political campaign, how well is the domain behind that identity protected from impersonation?

What we found

DMARC adoption is not all or nothing. Organizations typically begin by publishing DMARC in monitoring mode, using p=none to understand their legitimate email traffic before progressing to an enforcement policy such as p=quarantine or p=reject.

Across the 3,756 campaign domains examined:

- **43.6% had no DMARC record at all, meaning they had not yet begun the adoption process.**
- **38.4% had implemented DMARC but remained at p=none, or monitoring mode.**
- **12.1% used p=quarantine**
- **5.8% used p=reject**

While 56.4% of campaign domains had begun the DMARC adoption process by publishing a "p=" record, only 18% of all domains had progressed to enforcement, meaning just 31.7% of domains with DMARC were actually enforcing it.

Other findings include:

74.5% published SPF

18.7% had neither SPF nor DMARC.

Only 8 domains, approximately 0.2%, published a BIMI record

The findings show that many campaigns have taken an initial step toward email authentication, but far fewer have progressed from monitoring to active DMARC enforcement.

Public cybersecurity priorities are not always reflected in campaign domain protection

DigiCert found campaign domains across both major parties that were not enforcing DMARC, including some associated with candidates who have spoken about cybersecurity, privacy, and election security.

The finding is not intended to question those positions or single out any candidate, campaign or party. Instead, it highlights a practical opportunity for campaigns to apply those same principles to their own digital identity by strengthening email protections and reducing the risk of impersonation.

DMARC adoption varies by office

Enforcement was more common among gubernatorial and U.S. Senate campaign domains, but remained below one-third in every category:

31.6%	30.9%	21.7%	13.3%
Governor	U.S. Senate	U.S. House	State legislature

The research did not examine why adoption rates differed. Across every office, the findings point to an opportunity for campaigns to strengthen protection against email impersonation.

Visual identity stops at the inbox

Political campaigns invest heavily in visual identity. Logos appear across television advertising, websites, social media, fundraising materials, campaign signs, and direct mail.

Very little of that authenticated visual identity has made its way into the inbox.

Only eight campaign domains in the entire nationwide study, approximately 0.2%, published a BIMI record.

BIMI, or Brand Indicators for Message Identification, allows qualifying organizations to display a recognizable logo alongside authenticated email at participating mailbox providers, giving recipients an additional visual cue that the message is associated with the expected sender.

A Mark Certificate adds another layer of trust

Mark Certificates are issued after validation of the organization and its rights to use the logo or mark. When combined with the required email authentication and supported by the recipient's mailbox provider, the certificate helps connect a validated organizational identity and logo with authenticated email.

For a political campaign, the value is straightforward: the same recognizable identity voters see on a campaign website, television advertisement, or yard sign can potentially follow the campaign into the inbox.

That does not mean consumers should automatically trust every message displaying a logo. BIMI is not an alternative to DMARC; it depends on DMARC enforcement. Strong email authentication remains a prerequisite for the broader trust experience. Together, these technologies play complementary roles.

DMARC helps protect the domain behind the message. A Mark Certificate can help make the validated identity behind that authenticated email more visible to the recipient.

With only eight campaign domains publishing BIMI records in this study, authenticated visual identity represents an almost entirely untapped opportunity for political campaigns.

A practical step campaigns can take

DMARC alone cannot provide complete email security, but it is an important defense against domain impersonation. This analysis shines a light on an often-overlooked vulnerability in a critical communication channel for campaigns, which happens to be one they can easily address.

DigiCert offers email-trust resources, including:

Free assisted DMARC enforcement with Valimail, a DigiCert company, to help organizations move toward an appropriate enforcement posture.

Mark Certificates for organizations working toward BIMI readiness and authenticated logo display in participating inboxes.

Campaigns can explore steps to strengthen their email protection here:
https://www.digicert.com

About the research

DigiCert built a nationwide dataset of 5,597 candidate records across all 50 states, using official election authorities and documented secondary sources.

From that dataset, DigiCert identified 3,775 candidate records with campaign websites, representing 3,756 unique campaign domains.

On August 21, 2026, DigiCert checked those domains using publicly observable DNS records for DMARC, SPF and BIMI. Those records help indicate whether a domain has email authentication protections in place. The Cybersecurity and Infrastructure Security Agency, a U.S. federal agency, recommends technologies such as DMARC and SPF to help protect election-related email from spoofing and phishing.

The analysis relied on information visible from the public internet. DigiCert did not access campaign systems, email accounts or sending platforms.

DMARC enforcement was defined as a published policy of p=quarantine or p=reject. Domains using p=none were classified as monitoring rather than enforcing.

The findings represent a point-in-time assessment of publicly published DNS configuration and do not determine whether a campaign has experienced spoofing, whether individual email messages reach the inbox, or whether email authentication has affected an election outcome.

Glossary

Brand Indicators for Message Identification (BIMI)

BIMI is an email specification that allows mailbox providers like Gmail and Apple to display the sender's logo alongside their authenticated message in the recipient's mailbox. An organization uses DNS to publish their BIMI record. The BIMI record includes the URLs of their logo file and mark certificate PEM file.

Sender Policy Framework (SPF)

An organization uses SPF to establish which email servers are authorized to send messages on its domains. For example, DigiCert must publish that the Microsoft 365 email servers are authorized to send messages as digicert.com. Organizations publish the SPF information using DNS.

DomainKeys Identified Mail (DKIM)

DKIM is a mechanism for the sending email server to include a cryptographic signature of the message content that the receiving email server verifies. DKIM uses public key cryptography. Organizations publish the public part of their signing key in their DKIM record so receiving email servers can use it to verify signatures. DKIM is different from S/MIME in that it only authenticates the sending server, not the sending end user.

Domain-based Message Authentication Reporting and Conformance (DMARC)

Senders use DMARC to tell receiving email servers how to handle messages that fail SPF and DKIM: none, quarantine, or reject. Setting DMARC policy to 'quarantine' or 'reject' is called DMARC enforcement.