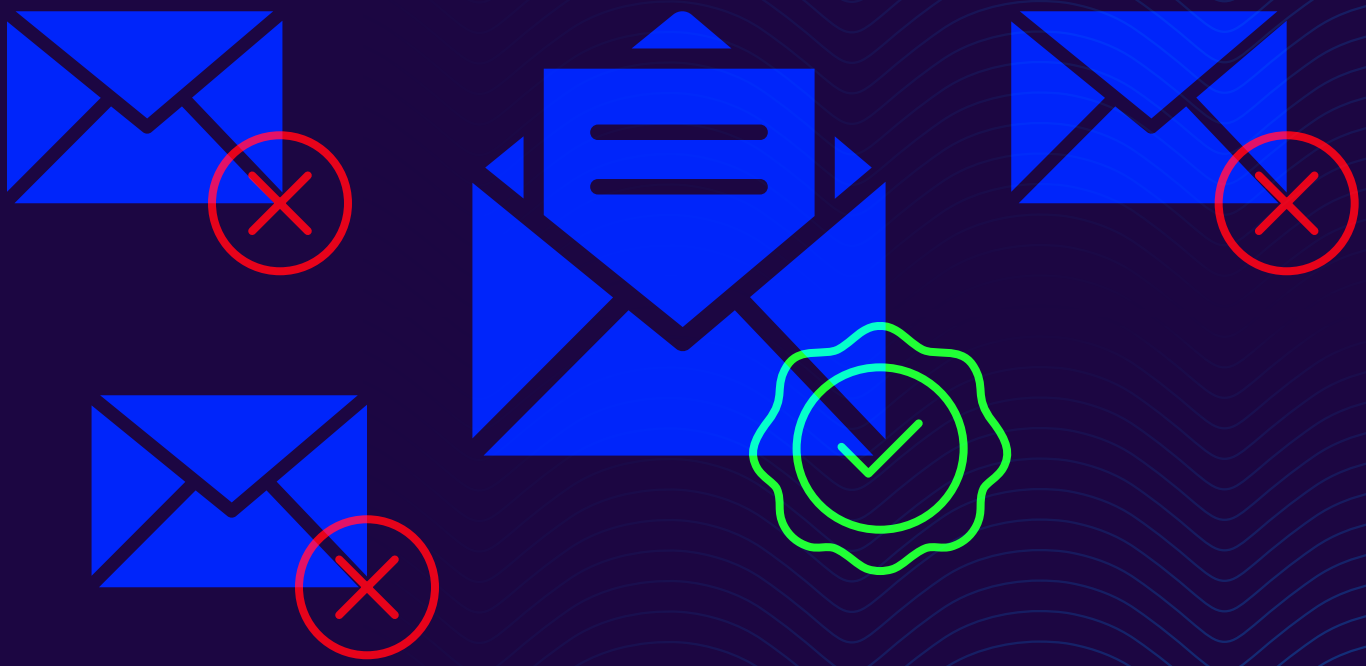
VALIMAIL
TRUST YOUR EMAIL

AN EXECUTIVE'S FAQ ABOUT

Email Authentication



This FAQ will help you understand how email authentication helps your organization protect itself from phishing. Email authentication takes a radically different approach from other security solutions you've already invested in — including secure email gateways, user security training, and Identity and Access Management (IAM).

What is email authentication?

Email authentication provides a means for you as a domain owner to ensure the integrity of your email domain name, and thus helps you protect your users against impersonation attacks undetected by secure email gateways (SEG). Email authentication protects the organization's name, brand, reputation, and improves overall security. When properly implemented, email authentication blocks spammers, phishers, and "shadow email" senders from hijacking your domain name to send email. Email authentication is commonly implemented using Domain-based Message Authentication, Reporting and Conformance (DMARC), the widely-accepted open technical protocol. DMARC is described in more detail below.

Why would I need email authentication?

Email headers are remarkably easy to fake, because when email protocols were first designed decades ago they didn't build in a mechanism to verify the sender's identity. Attackers have taken advantage of this loophole on a staggering scale, piggybacking off of the legitimacy of real domains and company brands to make their spam and phishing messages look wholesome, authentic, and clickable.

These days, over 90% of corporate cyberattacks start as phishing attacks.[1] Chances are, if your brand is recognizable and unprotected, at least some of those attacks have used your domain against internal employees and external customers. For example, attackers are likely to target your internal users by impersonating an internal employee in a spear phishing attempt — using your trusted domain against employees who wouldn't suspect an attack to come from an internal email address. Attackers may also target your customers by abusing your domain to send specially crafted spear phishing attacks meant to look like they're coming from you. Email authentication eradicates the most pernicious version of these types of attacks — what's known as same-domain or exact-domain spoofing.

Does email authentication have something to do with login and passwords? Do I need it if I've already invested a lot in identity and access management (IAM) systems?

Email authentication is not an IAM solution. It has nothing to do with the email sign-in process. The authentication occurring is not authentication of whether users checking their email are allowed to access data within the email system. Instead, email authentication is checking whether the sender of an email is legitimate and authorized to use your email domain.

[1] Source: *Mimecast State of Email Security Report 2019*, May 2019

How does email authentication help protect my brand value?

Your customers are less likely to interact with your brand after being phished with a message that leverages your company identity. An email fraudster is like a brand vampire, leaching off the legitimacy of your company's trustworthiness. The more fraudsters take advantage of your brand name, the more they weaken its reliability.

Email authentication keeps your brand reputation intact by preventing phishers from using your domain in any capacity, and typically increases deliverability rates for your legitimate marketing email by 10%.[2]

How can email authentication keep my fellow executives and employees from getting spear phished?

Email authentication protects your brand from being spoofed — ensuring that no matter who receives a message sent with an address using your domain, it's a legitimate email sent by an authorized user. It also protects recipients inside your organization who may be targeted by attackers pretending to be their colleagues or supervisors. A growing contingent of attackers have learned to take advantage of the implicit trust an email recipient has for an email that appears to be sent from an address containing their employer's internal domain.

Email authentication can help prevent spear phishing attacks against executives or other employees where the attacker pretends to be someone who supposedly works for the organization.

We already train our employees to delete phishing email messages. Why should I add email authentication?

Most organizations are responding to the phishing threat with training and simulations, and 57% say they've been able to quantify a reduction in susceptibility as a result. Yet 11% of end users will still click on links, and 4% will ultimately submit data requested in a phishing test.[3]

Humans are error prone. Social engineering plays on empathy and sympathy, and humans' tendency to act and react. We may not see an obvious phish every time. Our minds are used to interpreting meaning from patterns or typographical errors. Exact-domain impersonation is the most common phishing attack, and is nearly impossible to detect on email clients.

If I use email authentication, can I get rid of my employee anti-phishing training program?

Email authentication works to eradicate phishing attacks generated using your domains. But until everyone else uses it you'll still need to worry about inbound phishing attempts made using other domains and other techniques. So, no, don't stop training employees on anti-phishing and other security best practices.

I already have a secure email gateway, why would I need email authentication?

Secure email gateways (SEGs) filter questionable content coming into the inboxes of your organization's users. The gateway's primary function is to reduce the amount of inbound spam and malicious mail, but this is based on content filtering technology that looks for things like keywords, links, attachments, and behaviors, while also employing techniques including blocklisting and IP reputation scoring. SEGs can't stop modern phishing attacks that trick end-users using highly-crafted social engineering techniques and sender identity impersonation.

[2] Source: Valimail customers

[3] Source: *Proofpoint State of the Phish Report* (January 2019)

While most secure email gateways do have some email authentication functionality, they remain stunted as data reporting add-ons, and are not designed to get your domain to DMARC enforcement. DMARC enforcement protects employees and executives against phishing attacks and protects your brand on outbound email to customers and partners.

Whether it's bulk mail systems, transactional email, content management systems, or hosted ecommerce or accounting systems, there are dozens of third-party apps that send email using the company's domain. All of these outbound email systems can potentially be abused by email fraudster's intent on leveraging your name, and none of that outbound mail is inspected by your company's secure email gateways.

Email authentication fills this protection gap. Email authentication occurs at the domain name system (DNS) level, so the verification, blocking, and tracking of email happens no matter what system sends or receives a message with your domain in the "From" field.

What is DMARC?

Domain-based Message Authentication, Reporting and Conformance (DMARC) is the widely-accepted open technical protocol used for email authentication. DMARC is supported by all the major email providers (Google, Microsoft, Yahoo, etc.). DMARC makes it possible to authenticate the sender of an email, but most companies find it very difficult to implement. Approximately 80% of companies that attempt to implement email authentication fail to get to enforcement of DMARC policy, which is the ultimate and most critical aspect of DMARC necessary to ensure protection.[4]

What is the big deal about email authentication enforcement?

To get the most out of DMARC, organizations must set their policies to reject or quarantine unauthenticated messages. Unfortunately, the bulk of organizations simply leave their domain's DMARC policy at p=none, which means "do nothing and send a report."

According to a recent study, less than 17% of the 850,000 domains with published DMARC records are currently at enforcement due to overly permissive policies or outright misconfigurations in their DMARC records.[5]

My IT department says it has already adopted SPF and/or DKIM for email authentication, so we're OK with authentication now, right?

Individually, SPF and DKIM do not block unauthenticated mail. When brought together through DMARC to ensure alignment between the visible <From:> address and either SPF or DKIM, the recipient can be assured of the senders' authenticity.

Can my in-house IT staffers deploy email authentication themselves?

One of the hardest parts of email authentication is both establishing and maintaining DMARC enforcement. While your in-house IT staff can make attempts to accomplish this, keep in mind that it is rare. Most DIY in-house projects fail to reach enforcement — recent figures show that less than 20% of in-house projects successfully enforce DMARC.

[4] Valimail, https://www.valimail.com/blog/what-is-dmarc-enforcement-and-why-is-it-so-important/

[5] ibid.

Staff will be in an ongoing process of manual DNS updates and configurations, trying to overcome standards limitations, mapping IP addresses to sending services/platforms with limited visibility, managing changes, and so on. Each step comes with its own set of complexities, making the process error-prone and time/resource-intensive. Without automation, the cycle of tedium repeats and organizations often fail to reach enforcement due to the risk of blocking good email.

Managing DMARC manually is a hefty responsibility that is fraught with risk. Any potential change in DNS could interrupt the flow of critical business communication. Because manual DMARC configurations are made in a TXT file stored in the DNS record for your domain, a single typographical error could bring costly repercussions.

I see a number of DMARC reporting vendors out there that can help us. Why not work with them?

Non-automated solutions offer a combination of reporting and consulting, but leave the onus on the customer to perform the actual work.

While they may pose as automated solutions, their business models depend on selling consulting services to set up and maintain DMARC configurations. The question is whether you're willing to maintain ongoing overhead to configure SPF, DKIM, and DMARC, update DNS as services are added or IP addresses change, etc. Even at enforcement, email authentication requires monitoring and constant updates. If a consultant comes in to take care of manual configuration, you should expect to continue paying those fees in perpetuity.

Valimail fully automates service identification and management of authentication controls to get organizations to DMARC enforcement in a shorter time frame, with considerably fewer staff resources, and with less risk of blocking good email than any other solution. After pointing a DMARC record to the Valimail cloud, customers never touch DNS again. All controls are managed in a single, intuitive, one-click dashboard.

What does the FTC say about email authentication?

In a recent Federal Trade Commission (FTC) Bureau of Consumer Protection Staff Perspective report, FTC experts explain that "the best way to prevent people from falling for phishing messages may be to keep these scam email messages from ever showing up in their inboxes."

According to the FTC, fully implementing DMARC is the best way to accomplish this feat today. FTC research shows that the market still has a long way to go with DMARC adoption.

When examining the top 500+ domains in Alexa.com rankings, the FTC found that while 86% of top businesses had implemented SPF authentication, just 36% had adopted DMARC. The FTC urges businesses to fully implement DMARC in order to protect their brands and the consumers who trust those brands.

"With DMARC, a business can protect its domains from being used by phishers and other scammers by instructing receiving domains to automatically reject unauthenticated messages that claim to be from the business's domains," the FTC writes. "This powerful tool could be an effective means of combating phishing scams."

[6] Source: Public DNS records

[7] Federal Trade Commission, *"Businesses Can Help Stop Phishing and Protect their Brands Using Email Authentication,"* March 2017. https://www.ftc.gov/system/files/documents/reports/businesses-can-help-stop-phishing-protect-their-brands-using-email-authentication-ftc-staff/email_authentication_staff_perspective.pdf

[8] ibid.

How can Valimail help?

The Valimail platform automates email authentication and ecosystem control for enterprises wanting to enforce trusted email communications. The system's patented technology provides enterprises unparalleled control over who is permitted to send in their name, preventing unauthorized senders and brand impersonators in real time. Valimail's anti-phishing impersonation platform is fully automated and operates in the cloud, requiring no software, training, or ongoing work for clients. The results? Secure, trusted email that protects employees, partners, and customers, and improves email deliverability and marketing program revenue for your company.

What kind of companies use Valimail?

Companies of all sizes and across industries use Valimail. Any company that relies on email to conduct business can benefit. Valimail provides the first and only truly automated email authentication solution for brand protection and anti-fraud defense. Valimail's patented, standards-compliant technology provides an unrivaled one-click solution for DMARC enforcement to stop phishing attacks, increase deliverability, and protect organizations' reputations.

Who are some of your customers?

Valimail authenticates billions of email messages every month for many forward-looking, global brands including American Cancer Society, Fannie Mae, Federal Aviation Administration (FAA), Fenwick & West, Manulife, Mercedes-Benz, Nextdoor, Splunk, Square, Uber, Wix, and many more.

Schedule a free demo at www.valimail.com/demo/

TRUST YOUR EMAIL

Valimail is the global leader in DMARC-as-a-service, and the inventor of hosted DMARC. The company's cloud-native products stop impersonation attacks and protect brands by authenticating sender identity. With patented industry-leading technology, Valimail unlocks DMARC enforcement for businesses of every kind and every size – increasing enforcement success rates from less than 25% to over 95%. As the only FedRAMP-certified platform and the vetted DMARC partner for Microsoft 365 environments and Twilio SendGrid, Valimail also holds leadership positions on every key email authentication standards body, championing increased trust and safety in the email ecosystem. For more information, visit www.valimail.com.