AREA 1

RETURN TO SENDER

The Limitations of Email Authentication Against Phishing

Any time email fraud is mentioned, email authentication (specifically, SPF, DKIM and/or DMARC) is almost always brought up as the answer. While email authentication can protect against some forms of fraud and spoofing, it is largely ineffective against the most common and dangerous type of email fraud — phishing. Stopping email fraud and sophisticated phishing attacks, especially those relying on social engineering, require advanced detection techniques.

WHY EMAIL AUTHENTICATION IS INEFFECTIVE AGAINST PHISHING

Email authentication typically refers to any one of three common email authentication standards that verifies the origin of an email and who it claims to be from: SPF, DKIM and DMARC. These standards serve useful security functions such as validating server and tenant origins, protecting message integrity and providing policy enforcement.

All three standards can help with preventing some forms of phishing, but attackers can easily circumvent email authentication. (See our accompanying Email Authentication Cheat Sheet below for specifics on each standard.)

Recent ongoing research has exposed at least 18 techniques to trick email authentication into thinking an email from an attacker's server is verified as coming from a legitimate address.[1] The fact stands that email authentication simply does not protect against certain types of attacks.

Besides specific limitations for each standard, inherent problems with email authentication as a whole prevent it from stopping most phishing attacks from reaching users:

[1] Lemos, Robert. "Email Security Features Fail to Prevent Phishable 'From' Addresses." Dark Reading, 24 July 2020 https://www.darkreading.com/vulnerabilities---threats/email-security-features-fail-to-prevent-phishable-from-addresses/d/d-id/1338448.

- **Anyone can set up emails that pass email authentication**. With the widespread availability of cloud-hosted webmail, anyone, including attackers, can sign up for an inexpensive Google Gmail or Microsoft Office 365 account. Sending email from one of these legitimate email providers results in emails that pass email authentication. To complicate things further, these multi-tenant services mean every user has the same SPF record, making phishing detection that much harder.

- **Email authentication does not inspect content.** Just like sending a letter via registered mail, email authentication only ensures delivery; it does not check whether the contents of the email are benign. Email authentication will not stop a phish or malicious email sent with properly configured SPF, DKIM and/or DMARC. In fact, it just ensures a successful delivery.

  Since content is not inspected, this also means email authentication cannot stop two primary phishing scenarios: embedded URLs and attachments/payloads.

  - While some phishing attacks rely purely on social engineering, others include an embedded link, typically leading to a credential phishing or malicious site.

  - Targeted attacks can use attachments that host malicious payloads that run upon opening. Or, an attachment can include an embedded link to a phishing or malicious site.

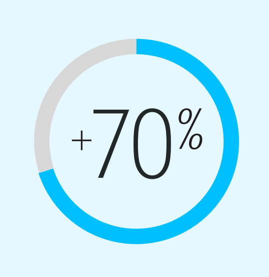
  Email authentication is blind to both of the above-noted threats, as long as the message passes SPF, DKIM and/or DMARC.

- **Email authentication does not protect against look-alike domains.** There is no email authentication standard that can protect against look-alike or cousin domains that were properly created. In other words, email authentication won't alert you that an email was actually sent from name@vend**a**r.com instead of name@vend**o**r.com. And over 70 percent of phishing emails use these one-letter-off domain misspelling attacks that bypass email authentication.

- **Email authentication does not protect against compromised domains**. Email authentication does not protect against legitimate domains that have been compromised. Many phishing attacks come from compromised Office 365 accounts, and compromised tenants can also host phishing sites or malware. This also means email authentication is ineffective against Business Email Compromise (BEC) attacks, particularly Types 3 and 4 BEC attacks, which leverage compromised partners and supply chain vendors to target victims.

- **The vast majority of organizations and domains do not use email authentication**. While email authentication cannot prevent all phishing and targeted attacks, it can still help — if it's been configured. However, not all organizations have set up SPF, DKIM or DMARC, or set them up properly. Some reports suggest that nearly 80% of organizations do not have a DMARC policy in place.[2]

- **Email authentication can be difficult to set up properly.** Email authentication is notoriously difficult to set up and verify it's working as intended. Thus, if email authentication is not set up properly, or DMARC policies aren't configured to reject/quarantine, phishing emails will still get through. In fact, even though more organizations are using DMARC overall, less than 15 percent of those with a DMARC record actually have a "reject" policy to prevent spoofed emails from being delivered.[3]



OVER 70% of PHISHING EMAILS use one-letter-off misspelled domains

[2] "Global DMARC Adoption Report Reveals Nearly 80 Percent of Companies Leave Consumer Data Vulnerable." Business Wire, 16 July 2019, https://www.businesswire.com/news/home/20190716005122/en/%C2%A0Global-DMARC-Adoption-Report-Reveals-Nearly-80-Percent-of-Companies-Leave-Consumer-Data-Vulnerable.

[3] Joss Fong, Cleo Abram. "Why Coronavirus Scammers Can Send Fake Emails from Real Domains." Vox, 2 Apr. 2020, www.vox.com/recode/2020/4/2/21202852/coronavirus-scam-email-who-spoofing-domain-dmarc.

WHAT'S EFFECTIVE AT PROTECTING AGAINST PHISHING ATTACKS?

Stopping phishing attacks from reaching inboxes requires advanced detection techniques.

Area 1 Security's preemptive technology uses ActiveSensors™ for massive-scale web crawling to reveal emergent campaign infrastructure. Our Small Pattern Analytics Engine, SPARSE™, also identifies phishing attack infrastructure, patterns of attack formation and threats within datasets generated by the ActiveSensors™ network. Finally, we employ the six methodologies and techniques below to stop active fraud attempts in progress.

1 CAMPAIGN SOURCE ANALYSIS

Preemptive crawling to discover and track attacker infrastructure

2 MESSAGE SENTIMENT ANALYSIS

Understanding what's being expressed within the message

3 PARTNER SOCIAL GRAPHING

Assessing supply chain partner reputation and vendor account takeover

4 CONVERSATIONAL CONTEXT ANALYSIS

Analyzing variations within an entire message thread for suspected fraud

5 UNIVERSAL MESSAGE CLASSIFICATION

Surfacing Categories of Interest (COIs) for secondary assessments

6 VERDICT ESCALATIONS

Rapid escalations for analyst review and customer SOC confirmation

AREA 1

*To find out how to stop the phish missed by SPF, DKIM, DMARC and other email defenses, **Request a Free Area 1 Trial**.*

AREA 1

Email Authentication Cheat Sheet:

What Is It, and What it Can and Cannot Do

Email authentication typically refers to any one of three common email authentication standards that verifies the origin of an email and who it claims to be from: SPF, DKIM and DMARC. Below is a brief description of what each standard does, what types of threats it can protect against and what types of threats it cannot protect against.

SPF – Sender Policy Framework

PURPOSE	• Validating server origin (i.e., validates where a message originates from) • Defining which email servers and services are allowed to send messages on a domain owner's behalf
BEST FOR	Preventing spoofing of a legitimate email's return address domain, i.e., the "Reply to" email address or return-path domain
LIMITATIONS	• Does not prevent look-alike email, domain or display name spoofing • Does not validate the "From" header; uses envelope "From" to determine sending domain • Validation fails when emails are forwarded or when messages sent to a mailing list is sent to each subscriber • SPF evaluation process is limited to 10 DNS lookups • Does not protect against attacks using "validated" emails with embedded URLs, malicious payloads or attachments

DKIM – Domain Keys Identified Mail

PURPOSE	• Providing tenant origin validation (i.e., checks that an email was sent/authorized by the owner of the domain via a digital signature) • Ensuring email is not altered while transferred from server to server; protecting message integrity
BEST FOR	Preventing spoofing of the "Display From" email address – the address usually shown to the end user when an email is opened
LIMITATIONS	• Does not prevent look-alike email, domain or display name spoofing • Does not protect against replay attacks (DKIM only signs specific parts of a message. Attackers can add other header fields to emails passing DKIM then forward them.) • Does not protect against attacks using "validated" emails with embedded URLs, malicious payloads or attachments

DMARC – Domain-based Message Authentication, Reporting and Conformance

PURPOSE	• Providing policy enforcement and reporting for SPF and DKIM • Stipulating what policy to follow if an email doesn't pass SPF or DKIM authentication (e.g. reject/delete, quarantine, no policy/send) • Reporting function allows domain owners to who is sending email on their behalf
BEST FOR	Protecting against spoofing of your own domain and brand abuse (Does not prevent spoofing of another brand's domain)
LIMITATIONS	• Does not prevent spoofing of another brand's domain • Does not prevent look-alike email, domain or display name spoofing • Domain owners specify what percentage of mail DMARC policies applies to; application percentages of less than 100% are virtually meaningless • Does not protect against attacks using "validated" emails with embedded URLs, malicious payloads or attachments