PAUBOX RESEARCH

PAUBOX

Phishing defense beyond DMARC for healthcare IT directors

Only 18% of healthcare IT and security leaders report using link rewriting and sandboxing, as phishing arrives from Microsoft's own addresses.

What we found

Since mid-October 2026, phishing has arrived from Microsoft's own notification addresses and passed SPF and DMARC.

Passing DMARC confirms the sending domain, so the open question is what checks the link. Healthcare IT and security leaders selected link rewriting and sandboxing (18%) less often than six other inbound measures.

What it means for IT directors

Microsoft's own addresses send phishing

Lures from these addresses reached 27% of one security firm's monitored organizations between October 13 and 21, 2026.

Links carry most phishing payloads

Links carried 66.2% of phishing payloads, so a message that passes authentication still needs its links checked.

Bring one question to the renewal

Among IT directors, 15% report using link rewriting and sandboxing. Ask what checks a link after authentication passes.

WHY PAUBOX

#1

in 10 of 21 G2 Cloud Email Security reports for Fall 2026, including Best Usability and Best Results.

AI reads message intent

Generative AI analyzes tone, sender behavior, and message intent to surface hidden threats.

Compromised accounts stopped automatically

Blocks attacks from compromised accounts and lookalike domains that impersonate colleagues.

HITRUST certified

Independently certified against the HITRUST framework.

Paubox survey of 170 healthcare IT and security leaders, March 2026 | KnowBe4 Phishing Threat Trends Report Vol. 8 (October 2026) | Recon InfoSec, "Catch Phishing That Passes DMARC From Microsoft's Own Address" (November 10, 2026).