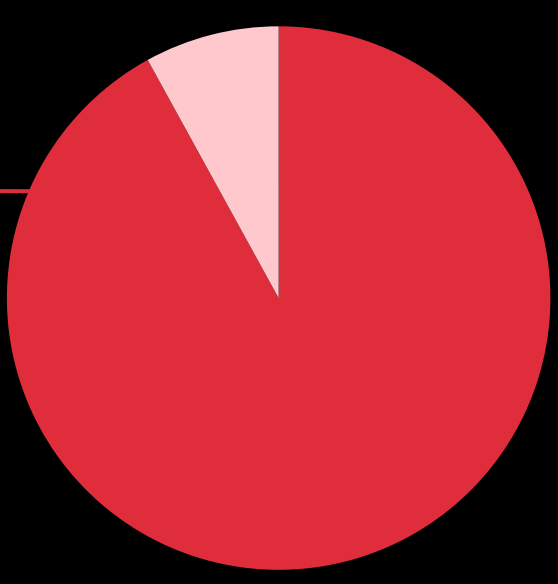
PAUBOX

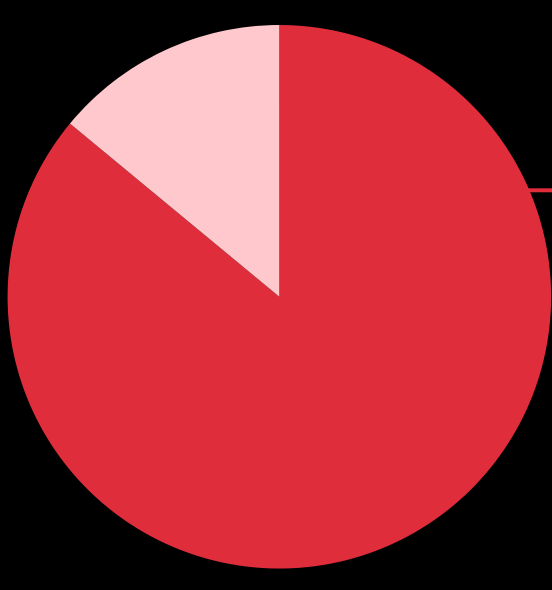
What Healthcare IT leaders get wrong about email security

Why Healthcare IT leaders are overestimating their email security and what the downstream consequences are.



92%

of healthcare IT leaders say they are confident in preventing email breaches



86%

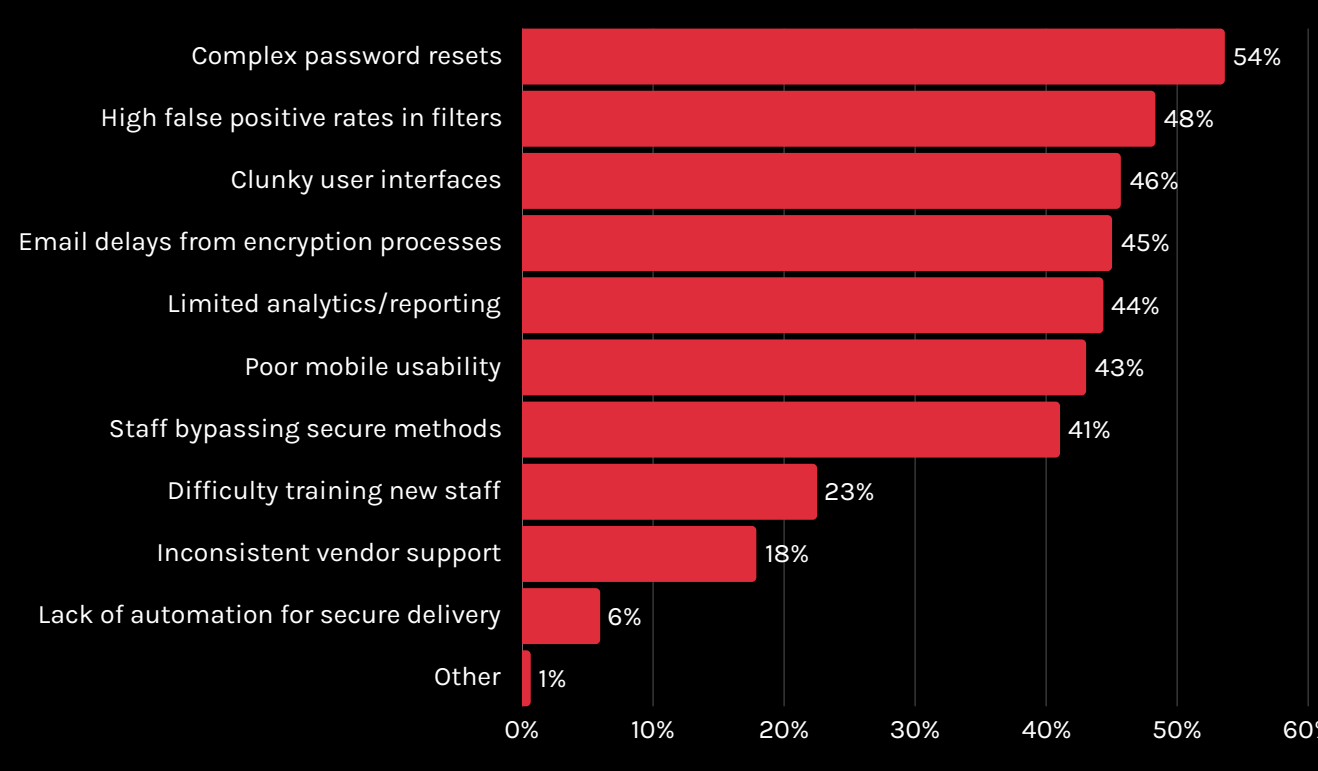
say their current email security tools cause workflow friction

> "In too many assessments, we find email compliance depends on user behavior rather than enforced policy."
>
> - Rick Kuwahara, Paubox Chief Compliance Officer

8 out of 10

admit they worry about their HIPAA compliance status

TOP FRUSTRATIONS WITH EMAIL SECURITY TOOLS



Why it matters

Patient data doesn't just live in EHRs. It flows through inboxes, attachments, referrals, and care coordination chains every single day. If your email system isn't locked down, your HIPAA posture is a house of cards.

ANATOMY OF AN AI-POWERED PHISHING ATTACK

MYTH	FACT
"Portals equal compliance."	Most portals introduce friction—leading to non-compliance workarounds.
"Our staff are well-trained, so we're secure."	Human error is inevitable. You need tools that compensate, not just train.
"Email is just a communication tool."	Email is your most common PHI exposure point—and your biggest risk.
"More training will solve our readiness against phishing attacks."	Training helps, but 95% of phishing still goes unreported. You need better detection.
"Buying a HIPAA compliant platform checks the compliance checkbox."	Configuration gaps are common. Compliance isn't guaranteed without oversight.

PAUBOX

www.paubox.com