Executive summary

60% of healthcare IT leaders reported breaches or security incidents involving email last year—and 73% expect breaches to continue in 2025. Why? This isn't about one hospital or one breach—this is about a broken infrastructure used across the country, exposing millions of patients to preventable risks.

Modern healthcare relies heavily on email for patient care communication, administrative processes, and sensitive information sharing. However, this crucial channel has become dangerously vulnerable. Our research reveals the reality: email security in healthcare is at a critical breaking point.

Based on new data from 150 healthcare IT leaders, this report pulls back the curtain on an overlooked risk in healthcare technology—legacy email systems. These systems are quietly undermining HIPAA compliance, straining operational efficiency, and exposing protected health information to cybercriminals.

Healthcare organizations currently allocate only 11–20% of their IT budgets to email security, despite email being

Key insights

60%

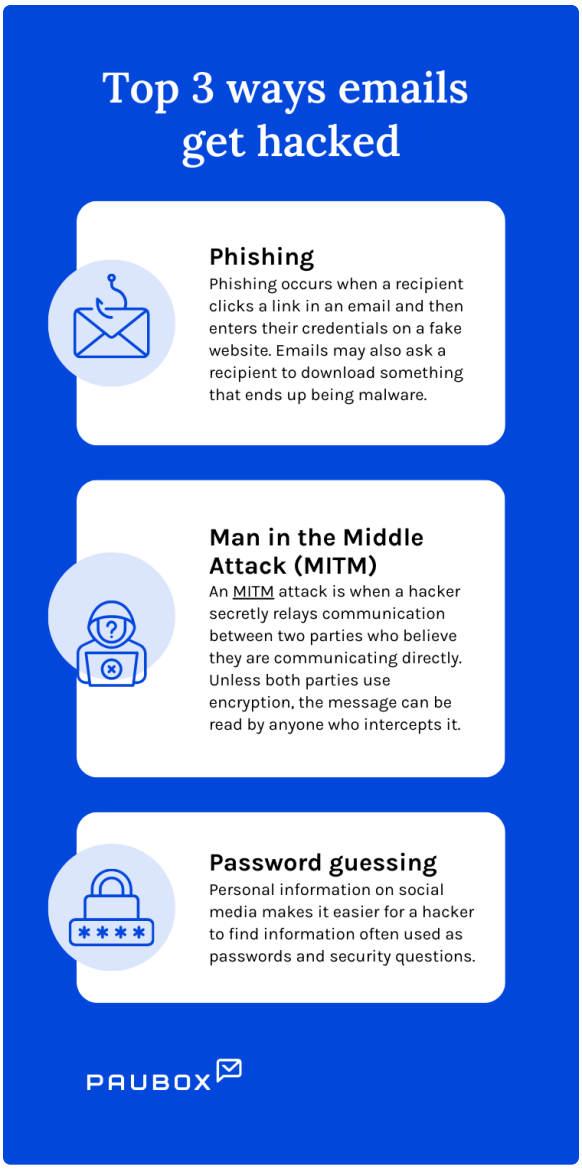
of healthcare organizations experienced email-related security incidents

73%

anticipate increased security challenges in the coming year

their top cybersecurity vulnerability. In comparison, the financial services sector dedicates approximately 6–14% of overall IT budgets[1] specifically to cybersecurity, reflecting a proactive stance toward protecting sensitive financial data. Yet, despite healthcare's comparable or even slightly higher proportional spending, 74% of healthcare IT leaders still report dissatisfaction with their current email security solutions. This gap results in overworked security teams, ineffective protections, and substantial financial and operational risk, highlighting an urgent need to reassess and enhance healthcare email security investments.

> Despite rising cybersecurity budgets, only 11–20% of IT spending is directed toward email security



[1] " The cyber clock is ticking: Derisking emerging technologies in financial services ", www.mckinsey.com