PAUBOX RESEARCH

PAUBOX

BEC turns trusted identities into healthcare email breaches

Impersonation appears inside the most damaging 2025 email breaches. Identity abuse is harder to spot than a malicious attachment.

What we found

Impersonation appears inside the most damaging email breaches of 2025.

Business email compromise begins with a message that appears to come from an executive, a vendor, or internal staff. Because the sender looks legitimate, recipients follow through and disclose PHI. Recent attacks abuse trusted messaging and cloud infrastructure, so the messages look legitimate by default and scale easily.

What it means for buyers

Display-name spoofing goes unflagged
Impersonation succeeds because identity abuse is harder to spot than malicious content.

Lookalike domains blend in
Spoofed names and near-identical domains pass as legitimate senders.

High-risk roles go unprotected
Executives and vendors are impersonated, yet rarely given targeted protection.

WHY PAUBOX

#1

on G2 for email encryption in healthcare, rated by verified users.

Inbound Email Security
Detects spoofed sender identities and lookalike domains in inbound email.

ExecProtect+ guards key roles
Targeted protection for executives and other frequently impersonated identities.

HITRUST certified
Annual third-party audit of every control.

Sources: Paubox 2026 research, Top 3 Healthcare Attacks in 2025 | Microsoft Digital Defense Report 2025 | U.S. HHS Office for Civil Rights breach portal (January to December 2025).