Attack 2. BEC and impersonation

What the 2025 HHS data shows

While HHS breach data does not isolate impersonation as a standalone category, impersonation appears repeatedly inside the most damaging email breaches in 2025, often acting as the trigger that turns access into disclosure.

These incidents appear under both “Hacking/IT incident” and “Unauthorized access/disclosure.” In many cases, recipients voluntarily disclosed sensitive information because the sender appeared legitimate.

How this attack works

Business email compromise (BEC) begins with impersonation.

An attacker sends an email that appears to come from:

- An executive or department leader
- A known vendor or business associate
- Internal IT, billing, or administrative staff

The email requests information, prompts a reply, or initiates a side conversation. Because the sender looks legitimate, the recipient follows through.

Recent attacks have demonstrated how impersonation is evolving beyond traditional phishing emails. In 2025, attackers began abusing trusted messaging and cloud infrastructure, including healthcare Direct secure messaging systems and Google-hosted services, to deliver messages that appeared legitimate by default.[2,3]

These attacks did not rely on malware. They relied on inherited trust. When messages arrive through channels and platforms recipients already trust, identity abuse becomes harder to detect and easier to scale.

> “Attackers increasingly exploit trust in **familiar identities**, such as executives and vendors, rather than relying on **malicious attachments or links**.”
>
> Microsoft

Where defenses fail

Impersonation attacks succeed because identity abuse is harder to spot than malicious content.

Common breakdowns:

- Display name spoofing not flagged
- Lookalike domains blend in with legitimate senders
- Lack of protection for high-risk identities like executives
- Overreliance on recipients to question trusted-looking requests

Healthcare workflows amplify the risk. Urgent requests and vendor communication are routine.

How Paubox reduces risk

Paubox reduces impersonation risk by blocking these attacks from reaching users in the first place.

Paubox Inbound Email Security:

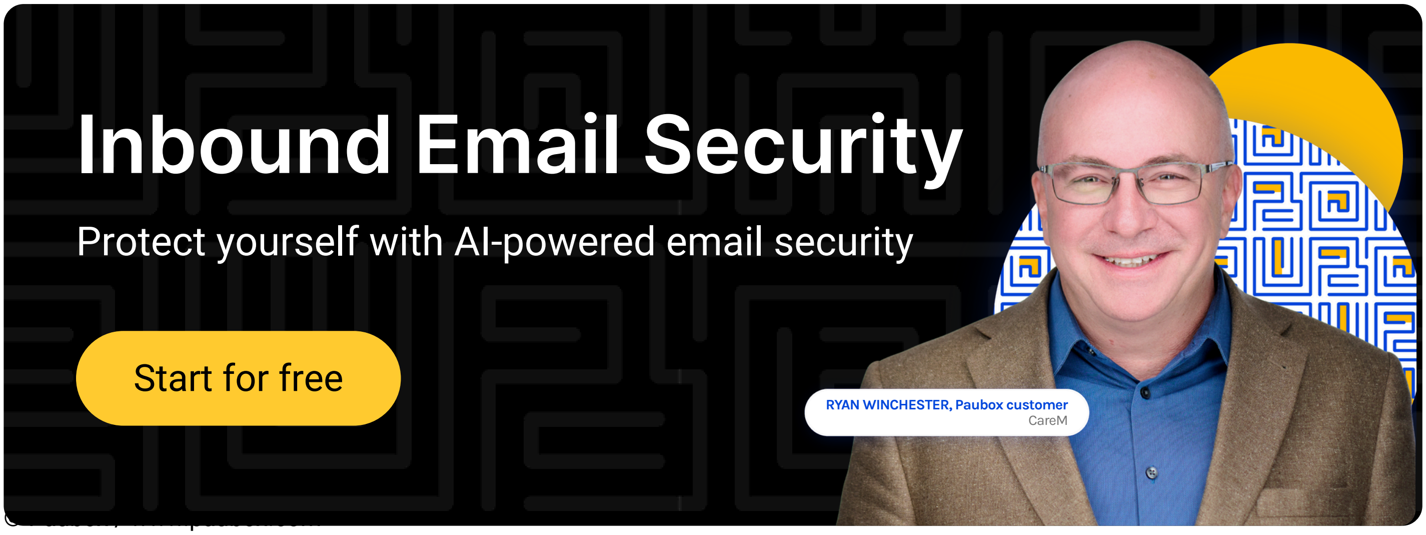
- Detects spoofed sender identities and lookalike domains
- Flags messages that abuse trusted names or brands
- Reduces reliance on users to identify subtle impersonation

Paubox ExecProtect+ adds targeted protection for executives and other frequently impersonated roles.

Why this attack persists

Impersonation persists because email still treats identity as trustworthy by default. Microsoft's Digital Defense Report states, "Attackers increasingly exploit trust in familiar identities, such as executives and vendors, rather than relying on malicious attachments or links."[5]

The 2025 HHS data shows that when attackers can convincingly mimic a trusted sender, email becomes a liability. As long as identity abuse reaches inboxes, BEC will remain a leading cause of healthcare email breaches.


Inbound Email Security
Protect yourself with AI-powered email security
Start for free
RYAN WINCHESTER, Paubox customer
CareM

PAUBOX

Stop email phishing attacks with AI security

Surface hidden threats with generative AI email security that learns and evolves.

Talk to an expert