Security

The top 3 healthcare email attacks in 2025 and how to defend against them

A look into how these attacks work, where defenses fail, and which email controls reduce risk.

PAUBOX

Table of contents

Executive summary

In 2025, the United States Department of Health and Human Services (HHS) recorded 170 email-related healthcare breaches, affecting more than 2.5 million individuals.[1]

A review of HHS breach data from January through December 2025 shows that nearly every email-related breach falls into one of three attack patterns:

Mailbox takeover after credential theft
Stolen usernames and passwords allow attackers to log into employee inboxes and access PHI as legitimate users. Credential-based mailbox takeovers accounted for the largest share of exposed patient data.

Executive and vendor impersonation
Attackers pose as trusted individuals, executives, vendors, or internal staff, to trick recipients into sharing sensitive information.

Third-party and business associate email exposure
PHI is exposed through compromised or insecure email communication with vendors and partners. Nearly one in three breaches in 2025 involved a business associate.

This report isolates how these three attacks work, where defenses fail, and which email controls reduce risk. The focus is practical. What to fix first. What to stop relying on. What prevents the next breach.

These attacks rely on fast-moving healthcare workflows and email systems that still assume people will catch mistakes before damage occurs. Each of these attack types triggered reportable breaches in 2025. Many remain under investigation. All represent ongoing compliance and operational risk.

BY THE NUMBERS

170
email-related breaches occurred in 2025

28%
of breaches reported last year were from vendor and business associate email exposure

630,000
individuals were exposed in 2025 by phishing-driven mailbox takeovers

2.5 million
individuals were affected by all email-related breaches in 2025

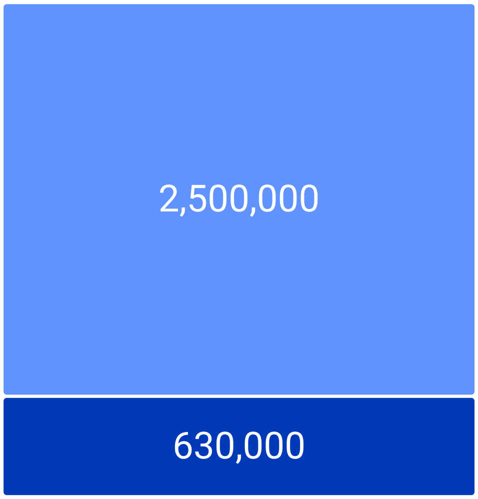
Attack 1. Phishing and credential compromise leading to mailbox takeover

What the 2025 HHS data shows

In 2025, phishing-driven mailbox takeovers accounted for approximately 17% of email breaches, but exposed more than 630,000 individuals, making this the most damaging email attack type by impact.

These incidents are typically classified as "Hacking/IT incident," with email listed as the location of breached information. Once attackers gain valid credentials, they access inboxes as legitimate users and remain undetected for extended periods.

> "**Process failures** and **human error** continue to be a persistent cause of data exposure, particularly when security controls rely on user judgment."
>
> Forrester



630,000 individuals were exposed in 2025 by phishing-driven mailbox takeovers.

Phishing is the most common breach entry point globally, and healthcare breaches continue to carry the highest average cost at $7.4 million, according to IBM.[4]

How this attack works

Phishing is the attack point. Inbox access is the objective.

An employee receives an email that appears to come from IT, HR, a colleague, or a trusted platform. The message prompts them to login, review a document, or reset a password. The landing page looks legitimate, but credentials are captured.

With valid credentials, attackers no longer need to bypass security controls. They log in normally. From there, they typically:

- Review historical email for PHI and attachments
- Search for billing, referrals, or lab-related keywords
- Create inbox rules to forward or hide messages
- Use the compromised account to target others internally or externally

When activity looks legitimate, detection is often delayed.

Where defenses fail

These breaches succeed because email security assumes users will recognize deception.

Common breakdowns:

- Phishing emails reaching inboxes unchecked
- Overreliance on user awareness and training
- Limited monitoring for abnormal mailbox behavior
- MFA is treated as a backstop rather than a preventive control

Once credentials are compromised, downstream controls often fail to recognize the account as compromised.

How Paubox reduces risk

Paubox reduces the likelihood of mailbox takeover by stopping phishing emails from reaching users.

Paubox Inbound Email Security:

- Detects impersonation attempts
- Blocks phishing messages before they reach inboxes
- Reduces reliance on users to identify malicious emails

Paubox ExecProtect+ adds targeted protection for executives and administrators, who are frequently targeted with BEC attacks.

Stopping phishing upstream reduces the likelihood of mailbox takeover downstream.

Why this attack persists

“Process failures and human error continue to be a persistent cause of data exposure, particularly when security controls rely on user judgment”, according to Forrester.[7] As long as phishing reaches inboxes, mailbox takeover will continue. Email-layer prevention is foundational, not optional.

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:

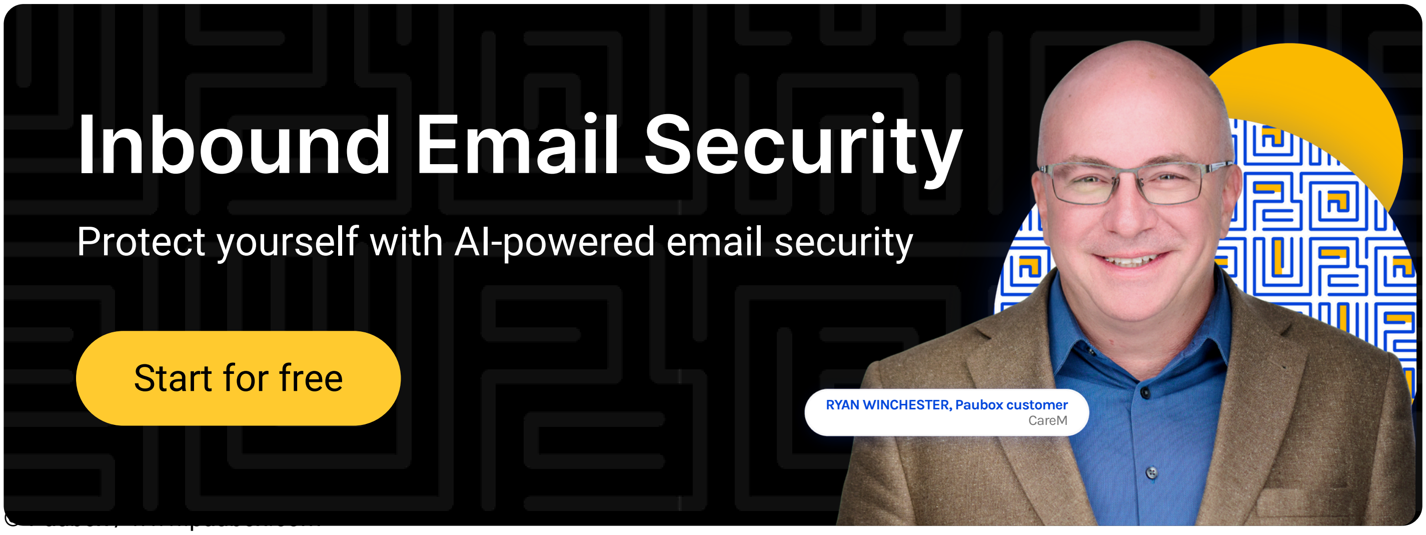
- Detects spoofed sender identities and lookalike domains
- Flags messages that abuse trusted names or brands
- Reduces reliance on users to identify subtle impersonation

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

Attack 3. Vendor and business associate email exposure

What the 2025 HHS data shows

Vendor and business associate email exposure was the most common email breach pattern in 2025, responsible for 28% of all email incidents reported to HHS. Breaches involving third-party vendors are also among the most expensive, with an average cost of $4.9 million per incident, according to IBM.[2]

In these incidents, the covered entity did not always experience a direct technical failure. PHI was exposed through email communication with a vendor or partner. When business associates are involved, breach sizes are typically larger and impact multiple organizations at once.

How this attack works

Vendor-related email exposure follows two paths:

- A vendor's email account is compromised, exposing PHI from multiple covered entities
- PHI is sent to a vendor using email that is assumed to be secure but is not protected

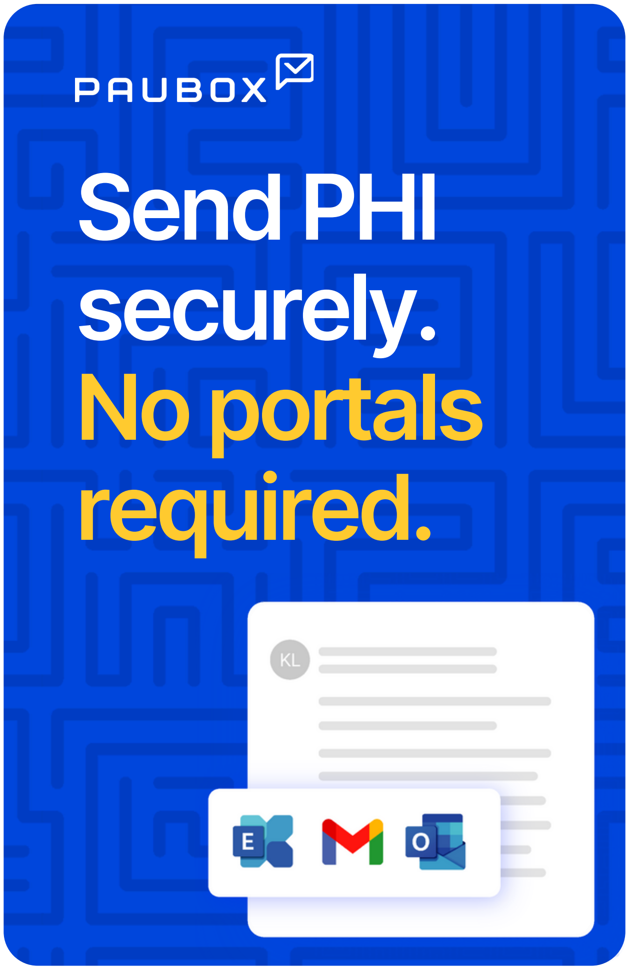
In both cases, the covered entity remains accountable for protecting PHI during transmission.

Where defenses fail

These breaches persist because email security expectations vary across organizations.

Common breakdowns:

- Relying on business associate agreements instead of technical safeguards
- Inconsistent encryption practices across organizations and vendors
- Limited visibility into how PHI is handled after delivery



How Paubox reduces risk

Paubox reduces vendor-related email risk by enforcing protection at the point of sending.

With Paubox:

- All email is encrypted automatically
- Protection does not depend on the vendor's email configuration

This ensures PHI is safeguarded in transit, which is the covered entity's responsibility.

> "Healthcare organizations report limited visibility into **third-party cybersecurity controls**, despite increasing reliance on vendors for core operations."
>
> EY

Why this attack persists

"Healthcare organizations report limited visibility into third-party cybersecurity controls, despite increasing reliance on vendors for core operations", according to EY.[6]

The 2025 HHS data shows that when email protection varies across organizations, exposure scales quickly. Reducing that risk requires enforcing protection before PHI leaves the sender's control.

HIPAA BREACHES ARE ON THE RISE

Cybercriminals are targeting healthcare

Stop attacks with generative AI that detects subtle anomalies in language, behavior, and context that traditional filters overlook.

Explore Paubox Email Suite Plus

Sources

1. U.S. Department of Health and Human Services (HHS). Office for Civil Rights. Breach portal: Notice to the Secretary of HHS breach of unsecured protected health information.January–December 2025. Analysis includes archived and under-investigation breaches where email was listed as the location of breached information.
2. Paubox. Phishing campaign exploits Google Cloud email infrastructure. Paubox blog, 2025.
3. Paubox. Healthcare Direct secure messaging abuse highlights impersonation risk. Paubox blog, 2025.
4. IBM. Cost of a data breach report 2025. IBM Security and Ponemon Institute, 2025.
5. Microsoft. Microsoft digital defense report 2025. Microsoft, 2025.
6. EY. U.S. healthcare cyber resilience survey. Ernst & Young LLP, 2025.
7. Forrester. The state of threat intelligence 2025. Forrester Research, 2025.

PAUBOX

Stop email phishing attacks with AI security

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

Talk to an expert