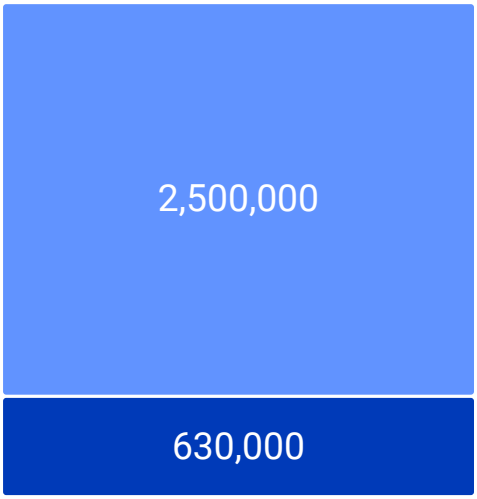
Attack 1. Phishing and credential compromise leading to mailbox takeover



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

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

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.

PAUBOX

Stop email phishing attacks with AI security

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

Talk to an expert