zimbra
A SYNACOR PRODUCT



A GROWING CYBERSECURITY RISK

Unsupported email systems and legacy platforms lack modern security protocols. These vulnerabilities make them easy targets for cybercriminals. Without updates or support, your organization is exposed to serious threats.

ZOOM IN

To The Rise of Brute Force Email Attacks: the methods hackers use to rapidly test countless username and password combinations, to gain unauthorized access to systems or accounts

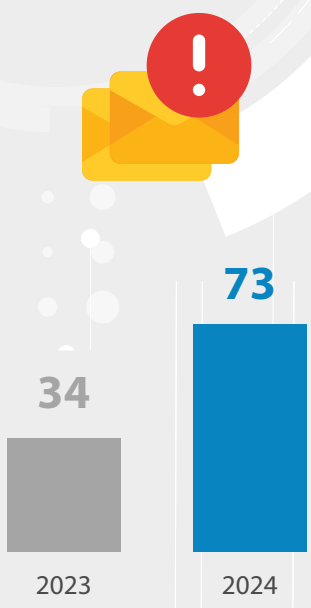
1. Email account takeover attacks surged by 1,760% since 2022*
2. Attackers now use AI tools for sophisticated credential-stuffing and phishing attacks
3. Old systems can't detect AI-generated threats because they rely on rules based on known attack patterns

THE COST

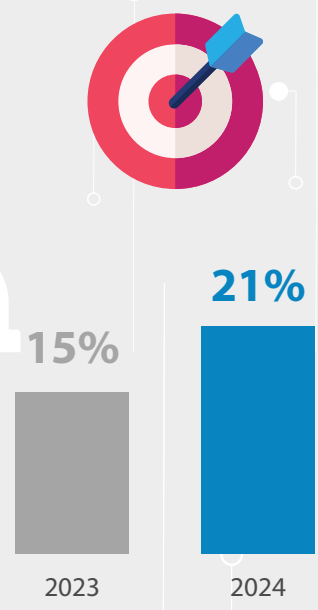
of successful brute force attacks can quickly lead to Business Email Compromise (BEC)—scams where hackers hijack real email accounts to fool employees into wiring money or leaking data.



AVERAGE BEC SCAMS LOSSES



% OF REPORTED CYBER ATTACKS



HIGH-LEVEL BEC TARGETS

Source: Cloud Security Alliance

BUSINESS EMAIL

COMPROMISE

scams amassed <$55B in losses the past decade*

ONE OF THE MOST

financially damaging forms of cyber crime

EMAIL ACCOUNT

TAKEOVER

attacks have surged by 1,760% from 2022*

LARGELY DUE TO THE

Widespread adoption of generative AI tools

BEC ATTACKS NOW INVOLVES AI

Challenges Of Detecting Ai-Powered Attack



Key challenge comes from the fact that rules based on known attacks have no basis to deny new threats.



Some email vendors use AI defensively toimprove the flawed way of only looking for exact matches.

THE REALITY

How To Protect Against Cyber Exploits?

Deploy authentication protocols to validate authenticity and prevent domain spoofing.

In 2025, Domain-based Message Authentication, Reporting & Conformance has moved from best practice to mandatory requirement in many industries, with adoption rising from 43% to 54% of senders in 2024.*



PROTECT

Against Cyber Exploits By Taking Action Today: Request a Product Demo to learn how a supported Zimbra solution help reduce your risk, secure your data, and stay compliant.

1. Prevent spoofing and implement DMARC authentication
2. Conduct vendor assessments to maintain strong data governance
3. Secure data with encryption, access controls, and disaster recovery plans
4. Ensure compliance with data sovereignty regulations (e.g.,GDPR, HIPAA, PDPA)

SPEAK TO OUR ZIMBRA EXPERTS

Source:
https://perception-point.io/blog/key-takeaways-from-perception-points-2024-annual-report/
https://www.blackfog.com/brute-force-attacks-in-2025-how-they-work-whats-changed-and-how-to-stop-them/
https://cloudsecurityalliance.org/blog/2024/11/08/threat-report-bec-and-vec-attacks-continue-to-surge-outpacing-legacysolutions
https://www.rsm.global/australia/insights/business-email-compromise-fraud-how-businesses-can-protect-themselves
https://www.scworld.com/news/most-cyber-insurance-claims-stem-from-bec-fraud-report-says
https://www.thesslstore.com/blog/business-email-compromise-statistics/