THE CHAIN REACTION OF TRUST:

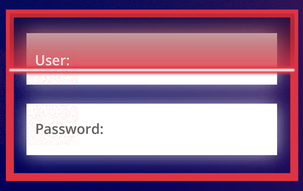
How Account Takeover (ATO) fuels Business Email Compromise (BEC)

How one stolen login can turn trust into opportunity for attackers, and how Mimecast breaks the chain.

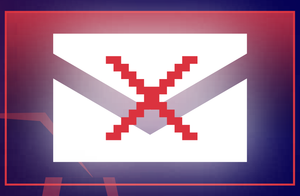
1 ACCOUNT COMPROMISED

Stolen or reused credentials

- Gain access and remain undetected
- Steal credentials via phishing or social engineering
- Establish a foothold for further attacks



50% of all email attacks aim to steal credentials



2 TRUST EXPLOITED

Attackers act as trusted users

- Send internal phishing or fake invoices
- Change mailbox rules
- Move laterally toward leadership

Mihra AI **Where AI fuels the threat, Mimecast uses AI to fight back**

Mihra™ AI detects patterns in AI-generated phishing, learning from 1.8-billion emails a day to outpace attackers at their own game.

3 BEC ATTACK LAUNCHED

The pivot to fraud and impersonation

- Launch payment or wire fraud attempts
- Impersonate executives or vendors
- Trick finance teams into transferring funds

BREAK THE CHAIN BEFORE TRUST IS BROKEN

Mimecast Account Takeover Protection connects the dots between ATO and BEC. We empower security teams to detect, respond, and prevent attacks before they spread.

mimecast

Discover how Mimecast's AI-powered protection keeps your organization safe from attacks that hide in plain sight.

READ THE ATO USE CASE