Email Is Still the #1 Breach Vector *and AI Is Changing the Threat Model*

CISO Chicago | April 2026

Shelby Kiger

Who Am I

- Cybersecurity Engineer/Architect at McDonald's Corporate
- Primary Focus:
  - Identity security and authentication flows
  - Enterprise email security architecture
  - Endpoint and OS hardening at scale
- Professional Background:
  - Contributing author to multiple CIS Benchmarks
  - Incident response and digital forensics
  - Business Email Compromise investigations
  - Large-scale threat hunting and email security assessments

I have built - and broken - email security from consulting, forensics, and enterprise engineering angles

The Paradox Most CISOs Are Living

- **We've hardened everything…except the entry point**
  - MFA deployed broadly
  - Endpoint detection and response on laptops and servers
  - Cloud posture and configuration management
  - Mature security awareness and phishing training
- Yet initial access is still dominated by:
  - Phishing
  - Credential theft
  - Business email compromises

Why Email Still Works

- Email sits at the intersection of
  - Business trust
  - Identity and authentication workflows
  - Finance, HR, IT, and vendor relationships
  - High-urgency, exception-based processes
- Attackers don’t need to break email security - they only need **one message that fits normal work**

A Simple Question

IT Help Desk support@company.com

URGENT: ACCOUNT VERIFICATION

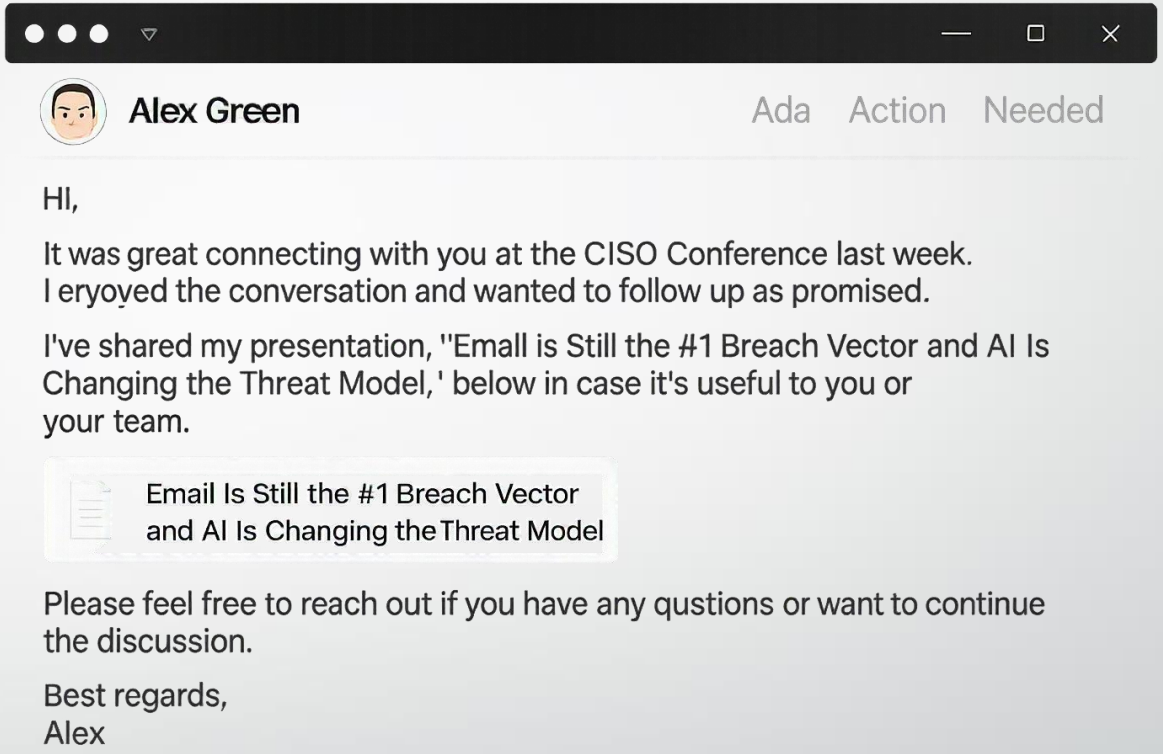
Dear user,

We have detected unusal activity on your account and it is necessury to corifirm your identity in order to maintain access.

VERIFY YOUR ACCOUNT

Please complete the verifcition process as soon to aviod any disruptions.

Sinecerely,
IT Help Desk



The Historical Phishing Landscape

Historically, phishing campaigns were:

- Template-driven
- Reused across many targets
- Easy to recognize once "seen before"
- Heavily dependent on obvious factors

As a result:

- Attacks have repeated themselves
- Indicators were observable and reusable
- Grammar, tone, and urgency errors were common

The Historical Defense Model

- Traditional email security largely:
  - **Relied on rules and deny lists**, forcing defenders to constantly play catch-up
  - **Failed to reliably detect novel or low-volume attacks**, especially sophisticated variants
  - **Required a "first victim"** before defenders could extract indicators of compromise (IoCs)
  - Depended on **post-incident analysis** to build signatures and rules for future detection
- AI breaks this assumption completely

Operational Limitations of the Historical Model

As phishing volume increased and attacks diversified:

- False positives overwhelmed security teams
- Legitimate business email was disrupted
- Rules required constant tuning to stay effective

Many organizations duplicated controls already present in native email platforms

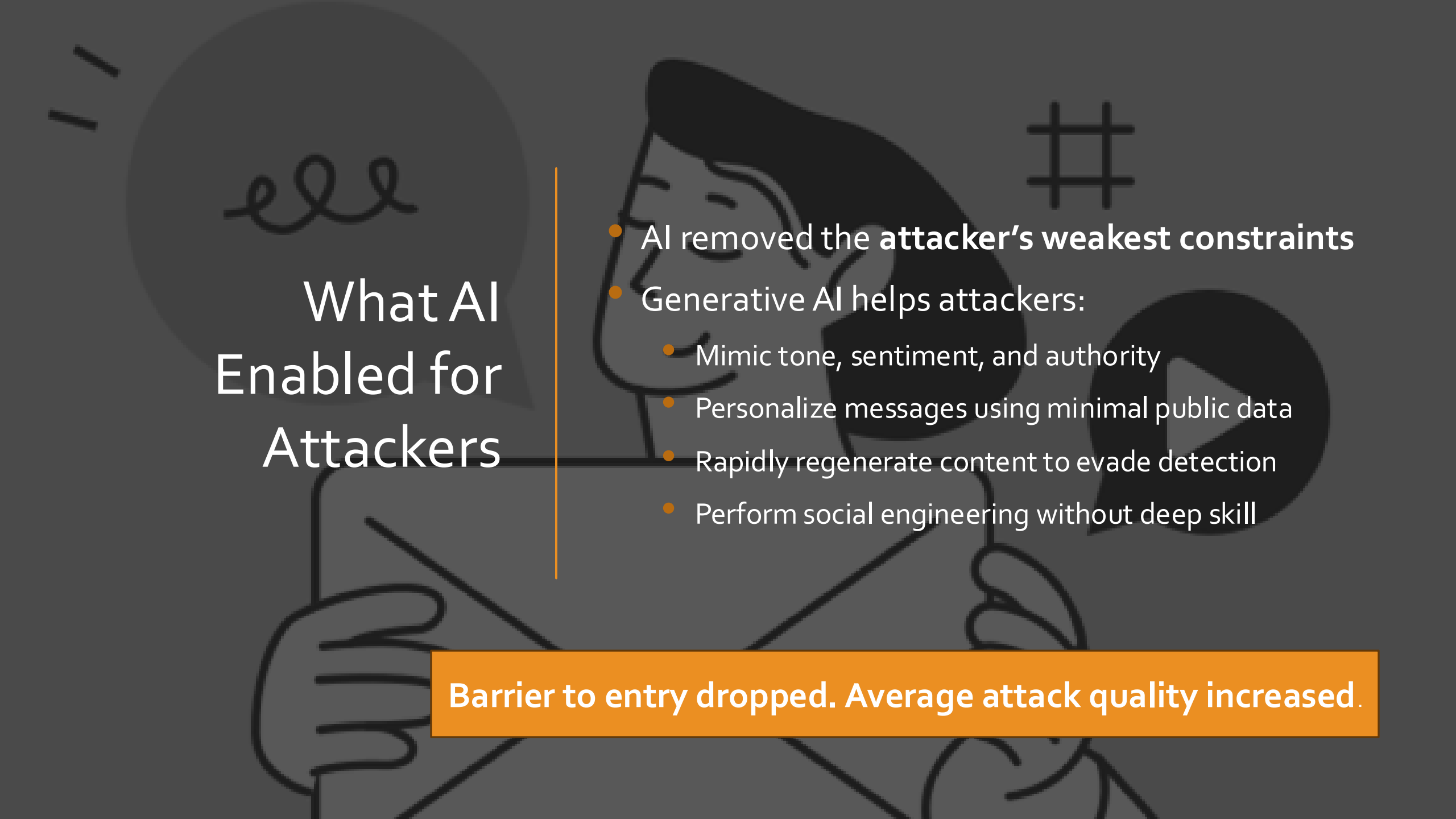
The gap between attacker capability and defender sustainability kept growing

Why This Model Used to Work

- The historical model worked because:
  - Phishing required skill and effort
  - Attacks naturally produced patterns
  - Indicators could be reused
  - Users could be trained to recognize common traits
- These assumptions were reasonable at the time. They are no longer true.

What Phishing Looks Like Now

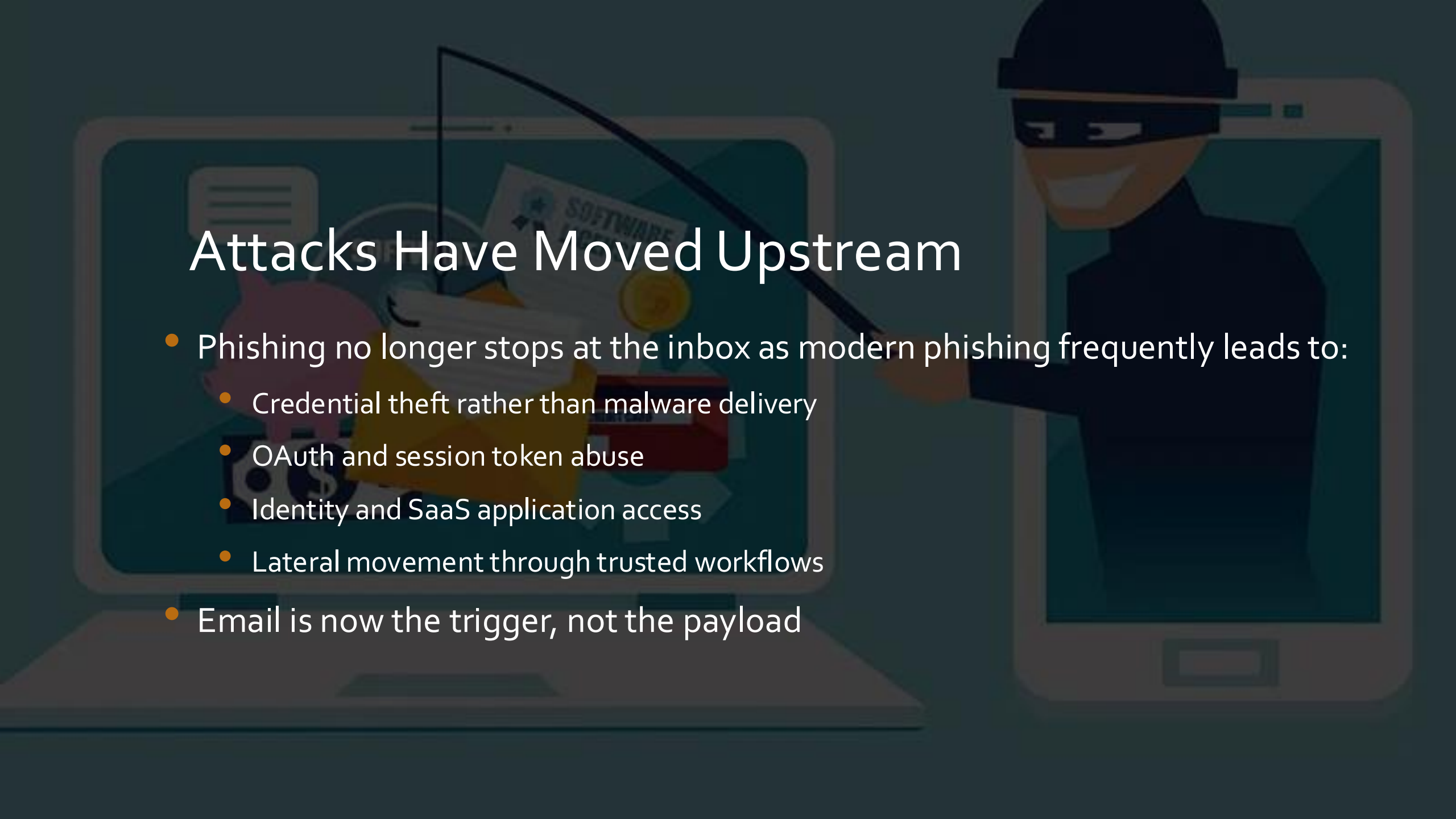
- Modern Phishing is **high-quality by default**
- AI-assisted phishing campaigns are:
  - Grammatically correct
  - Context-aware
  - Culturally fluent
  - Personalized at scale
  - Cheap to generate and iterate
- Messages no longer need to repeat to succeed



What AI Enabled for Attackers

- AI removed the **attacker's weakest constraints**
- Generative AI helps attackers:
  - Mimic tone, sentiment, and authority
  - Personalize messages using minimal public data
  - Rapidly regenerate content to evade detection
  - Perform social engineering without deep skill

Barrier to entry dropped. Average attack quality increased.

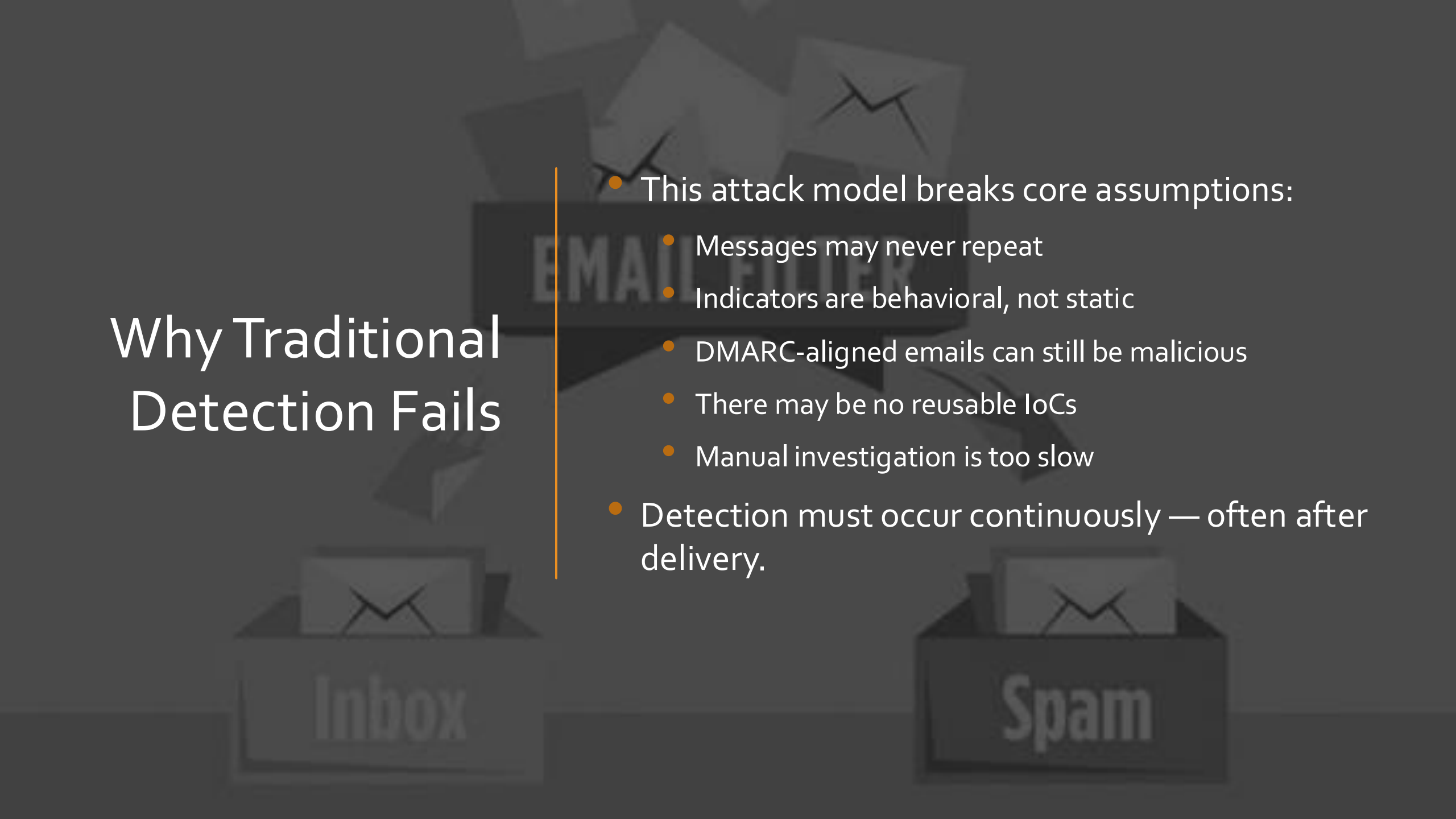


Attacks Have Moved Upstream

- Phishing no longer stops at the inbox as modern phishing frequently leads to:
  - Credential theft rather than malware delivery
  - OAuth and session token abuse
  - Identity and SaaS application access
  - Lateral movement through trusted workflows
- Email is now the trigger, not the payload

Why Traditional Detection Fails

- This attack model breaks core assumptions:
  - Messages may never repeat
  - Indicators are behavioral, not static
  - DMARC-aligned emails can still be malicious
  - There may be no reusable IoCs
  - Manual investigation is too slow
- Detection must occur continuously — often after delivery.



This is Not an Email Protocol Problem

- **Nothing** fundamentally changed about SMTP
- What changed:
  - Attacker economics
  - Speed of iteration
  - Ability to convincingly impersonate normal work
  - Use of identity and SaaS as the attack surface
- This is a **threat model** shift, not a tooling failure

What Defense Must Focus on Now

- Defenses must now focus on:
  - **Behavioral deviations**, not just content
  - **Context**, relationships, and communication history
  - **How users normally interact**, not just what they receive
  - **Post-delivery signals**, not only gateway blocking

Identity Is the Real Control Plane

- If attackers log in:
  - MFA posture matters more than spam filters
  - Session and token lifecycle matters more than DMARC
  - Identity telemetry matters more than headers
- Email security without identity awareness is blind.

Practical Defensive Priorities

- This requires:
  - DMARC at enforcement (p=reject) as table stakes
  - Treating phishing as an identity compromise problem
  - Instrumenting identity and SaaS telemetry aggressively
  - Detecting abnormal account behavior early
  - Reducing dwell time after credential misuse
- **Email and identity security must operate together**

Measuring the Right Outcomes

Stop measuring success by:

- Emails blocked
- DMARC pass rates alone
- Phishing report volume

Start measuring:

- Time to detect credential misuse
- Time to revoke sessions and tokens
- Time to contain abnormal account behavior

Speed is the differentiator.

Which one would most likely succeed in your environment today?

IT Help Desk support@company.com

URGENT: ACCOUNT VERIFICATION

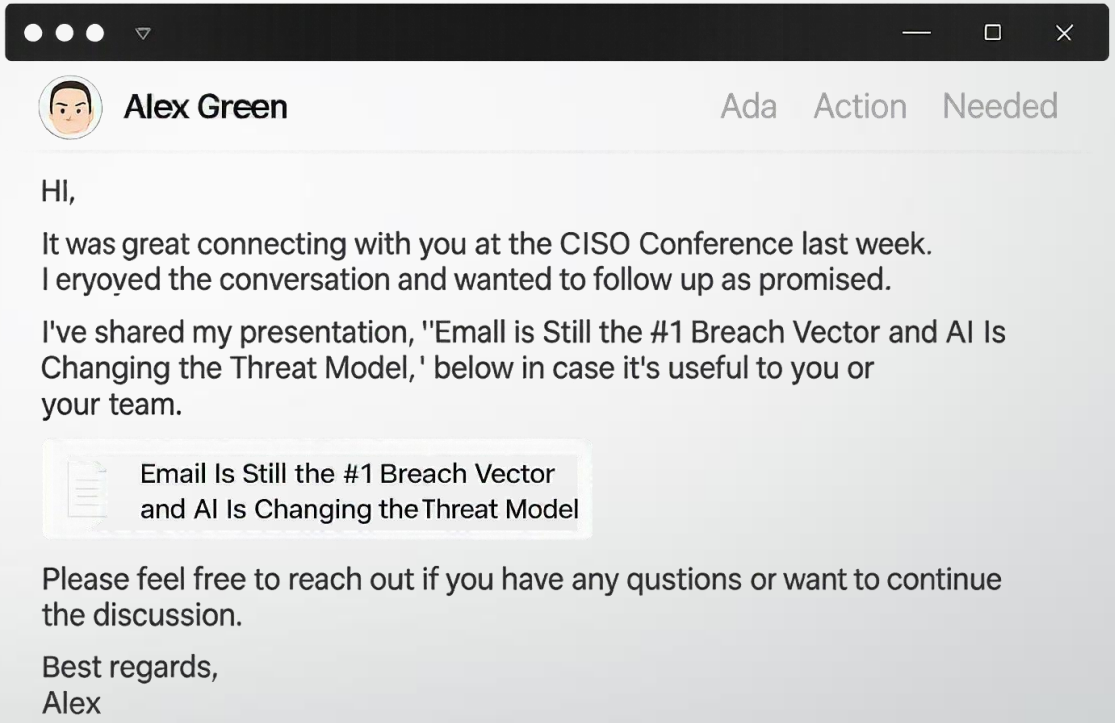
Dear user,

We have detected unusal activity on your account and it is necessury to corifirm your identity in order to maintain access.

VERIFY YOUR ACCOUNT

Please complete the verifcition process as soon to aviod any disruptions.

Sinecerely,
IT Help Desk



Key Takeaways

Email may be the door, but identity is the real breach vector

DMARC is necessary — but not sufficient

AI did not invent phishing — it removed friction

Attackers exploit trust and identity

Signature-based defenses cannot scale to uniqueness

Identity-centric detection is now mandatory

Thank you!

Questions?