POLYMORPHIC PHISHING:

How AI Is Redefining the Modern Email Threat

COFENSE

The Strategic Shift Security Leaders Cannot Ignore

Phishing has crossed a structural threshold.

Artificial intelligence has moved from experimentation to full-scale deployment in modern phishing operations. It's now embedded across the complete phishing lifecycle, from content creation and infrastructure management to malware delivery and evasion techniques. The result is polymorphic phishing, a form of email attack in which each message is automatically altered to appear unique, even though the underlying goal, payload, or infrastructure remains the same.

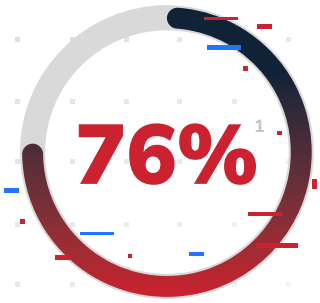
This is not a tactical evolution. It is a strategic one.

The End of Repetition

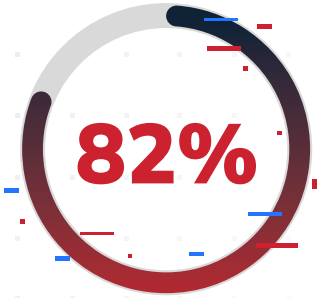
Security programs have historically relied on repetition. Reused domains, recycled file hashes, and recurring templates enabled detection systems to identify patterns and block known indicators.

With the advancement of AI, that assumption is breaking down.

According to data from the Cofense Phishing Defense Center:



of initial infection URLs identified in phishing attacks were unique and not seen across other customer environments.



of malicious files had unique hashes, even when delivering the same payloads, yet 94 percent of those URLs reused previously observed IP infrastructure.

This demonstrates the core principle of polymorphism: **surface-level uniqueness built on shared infrastructure.**

Each attack looks new, but the backend remains consistent.

1. All statistics cited in this eBook are derived from 2025 data published in Cofense report: The New Era of Phishing: Threats Built in the Age of AI (2026).

AI Has Industrialized Variability

Generative AI has eliminated the cost of variation. Threat actors can now:

- Produce thousands of email variations in minutes
- Personalize language to roles, industries, and current events
- Rotate domains and file variants at scale
- Adapt phishing pages based on device, browser, or geography

Polymorphism extends beyond email content. It includes delivery mechanisms, payload selection, and landing page behavior. The Cofense Intelligence team observed credential phishing pages increasingly adjusting based on browser or operating system, and customization techniques nearly doubled between the first and second halves of the year.

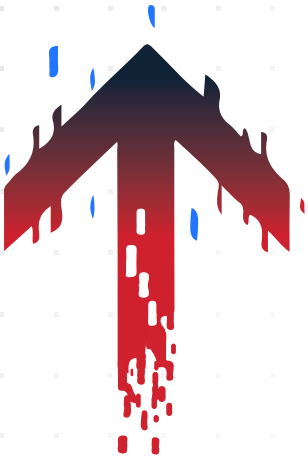
Attackers are engineering campaigns specifically to evade automated analysis and static detection.

This is systematic, not experimental.

Conversational Polymorphism and AI-Driven BEC

Not all polymorphic phishing relies on links or attachments.

of malicious emails identified by Cofense were **conversational attacks** relying solely on plain text interaction, **making them the second-most-common threat vector.**



BEC emails have risen in prominence due to generative AI dramatically improving business email compromise campaigns.

Messages are grammatically precise, contextually relevant, and aligned with internal communication styles. These attacks are often generated using polymorphic techniques to apply small modifications to each email, making them unique for each individual and organization.

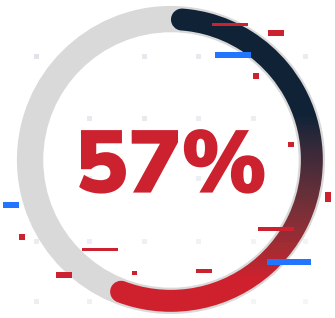
There are no malicious URLs to detonate. No attachments to sandbox. **The payload is persuasion.**

Detection strategies anchored only in link and file analysis are no longer sufficient.

Legitimate Tools as Delivery Mechanisms

Polymorphism is even more dangerous when threats are reinforced with the abuse of legitimate infrastructure to help bypass security filters looking

In 2025, we observed a:



Increase in use of **legitimate remote access tools**

106% increase
in total **remote access trojans reported**

Files are often signed, hosted on trusted cloud platforms, and indistinguishable from sanctioned IT tools.

The technical indicators may appear benign, but the malicious context is not.

The critical question is no longer whether a file is legitimate. It is whether its presence and behavior make sense within the organization's environment.

The Strategic Implications for Organizations

Polymorphic phishing erodes the predictive value of static indicators. If most URLs and file hashes are unique, prior knowledge becomes less actionable.

The shift is clear:

~~Pre-delivery filtering~~ → **Post-delivery visibility**

~~Static indicators~~ → **Behavioral context**

~~Automation alone~~ → **AI augmented by human validation**

The Cofense Phishing Defense Center observed, on average, one malicious email every 19 seconds over the past year. At that scale, detection cannot depend on manual analysis alone. Nor can it rely solely on perimeter blocking.

Organizations must assume that phishing will reach inboxes. The differentiator becomes how quickly threats are identified, contextualized, and remediated after delivery.

Leading in the Age of Polymorphism

Polymorphic phishing is not a temporary surge driven by AI hype. It represents the default operating model of modern phishing campaigns.

Organizations that measure success primarily by block rates at the email gateway risk blind spots. When nearly every attack appears unique, the most valuable signals often come from what gets through.

The mandate for leaders is clear:

- Build visibility into threats that reach employees' inboxes
- Treat user reporting as a critical detection layer
- Correlate unique artifacts back to shared infrastructure and campaign behavior
- Combine AI scale with expert oversight

Attackers have optimized for variation. Defenders must optimize for context.

Polymorphic phishing is not simply another threat trend. It is now the norm in the modern threat landscape. Organizations that recognize this shift early

For a deeper analysis of how AI is reshaping phishing campaigns and accelerating polymorphic attacks, read our full report, The New Era of Phishing: Threats Built in the Age of AI.

Cofense is the leader in post-perimeter phishing defense. Built for the reality that phishing gets through, Cofense helps enterprises identify threats in employee inboxes, remediate active attacks fast, and reduce future risk. Human-supervised intelligence improves accuracy, accelerates response, and strengthens organizational resilience against phishing threats across modern enterprise email environments.