POLYMORPHIC PHISHING ATTACKS: 5 INSIGHTS TO STOP THEM

Discover why AI + human oversight is the key to defend against these dynamic threats.

Polymorphic phishing threats apply changes rapidly — as frequently as every 15-20 seconds!

What exactly makes a phishing attack polymorphic? In these campaigns, attackers make slight changes to the same email—to the subject line or sender name, for instance—as they probe security systems to see what might get through.

Polymorphic attacks normally begin with a targeted campaign, designed to grab user credentials. When the first few users take the bait, the attacker uses their credentials to target other users. Again, the dynamic change in the attack prevents automated controls from screening out the messages.

Why are polymorphic attacks so successful? Because a campaign that lacks uniformity doesn't look like a campaign and makes it difficult for security teams to keep rules up to date. For many cybersecurity teams who lack bandwidth, finding the full scope of a polymorphic attack to quarantine is challenging and time-consuming.

Even worse, polymorphic attacks are not only effective, they are very easy to launch thanks to automated and inexpensive kits sold on the black market.

This is why human reporting, plus AI and threat intelligence are all needed for a comprehensive phishing defense strategy.

Did You Know?

- **Over 76% of phishing attacks** now use **polymorphic elements**—changing sender names, URLs, or subject lines to evade detection filters.[1]
- **Over 80% of modern phishing toolkits** now include **AI or automation features** to dynamically alter content, making each email appear unique.[2]
- **Phishing-as-a-Service platforms** automate the creation of **brand-specific, polymorphic campaigns**, fueling a surge in large-scale, tailored attacks.[3]
- Government agencies warn that these adaptive campaigns are **eroding traditional email defenses**, requiring human intelligence and advanced detection to stay ahead.[4]

Sources:

[1] SecurityMEA, *"AI-Powered Polymorphic Phishing Campaigns on the Rise,"* 2025.

[2] AI Tech Park, *"Phishing Threat Trends Report,"* October 2024.

[3] Europol, *Internet Organised Crime Threat Assessment (IOCTA 2024).*

[4] FBI IC3, *2024 Internet Crime Report.*

PHISHME COFENSE

The Stakes Are High Around the Globe

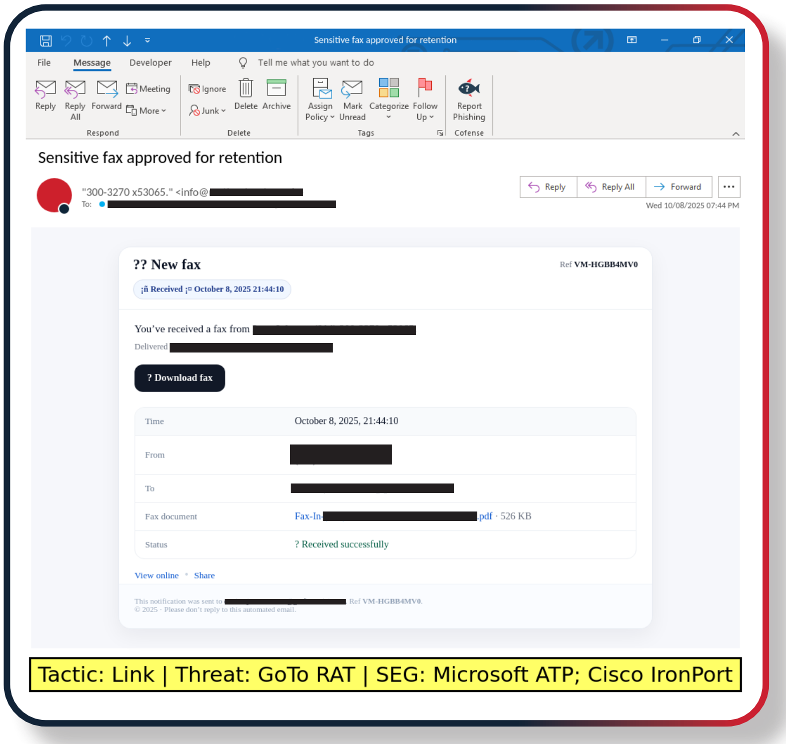
Real-world polymorphism

“Polymorphism is easy to achieve via simple programmatic logic in phishing kits. By using templates and wordlists, actors are able to quickly generate similar, but slightly different emails en masse. The predominant advanced actors in the phishing landscape, however, have figured out an even better method for creating unique emails.

“Emotet, QakBot, and others have been using stolen emails at a massive scale for some time now. Beyond having unique subjects, their typical phishing emails will have unique bodies constantly changing payload hashes, and payload URLs.

“Without diligent tracking of all attributes of these botnets, identifying which emails are part of a campaign is difficult at best.”

- Jason Meurer, Senior Technical Product Manager



Sensitive fax approved for retention

"300-3270 x53065." <info@[redacted]

To: [redacted]

Wed 10/08/2025 07:44 PM

?? New fax

Ref **VM-HGBB4MV0**

¡ñ Received ¡¤ October 8, 2025 21:44:10

You’ve received a fax from [redacted]

Delivered [redacted]

Time	October 8, 2025, 21:44:10
From	[redacted]
To	[redacted]
Fax document	Fax-In[redacted].pdf · 526 KB
Status	? Received successfully

This notification was sent to [redacted]. Ref VM-HGBB4MV0.
© 2025 · Please don’t reply to this automated email.

Tactic: Link | Threat: GoTo RAT | SEG: Microsoft ATP; Cisco IronPort

This email delivers content that is customized to the recipient including the recipient’s email address. What makes it polymorphic is that the embedded URL is unique to each email and is generated for each recipient meaning that a static signature to block one of the URLs would have no impact on the rest of the campaign.

Top 5 Insights to Help You Level Up Your Phishing Defense Against Polymorphic Attacks

1. Technology Controls Are Not Foolproof

Even the most advanced security technologies cannot stop every phishing email. Polymorphic attacks are engineered specifically to bypass these controls by constantly changing their characteristics, such as URLs, sender information, and email content. This allows them to slip through automated defenses and spread rapidly across an organization once a single user is compromised.

- **Designed for Evasion:** Polymorphic attacks use automation to create unique variants that do not match known threat signatures, rendering many traditional security tools ineffective.
- **Rapid Metastasis:** A single polymorphic phish that bypasses controls can quickly lead to a widespread incident as it is forwarded or used to compromise additional accounts.
- **The Inevitable Gap:** No matter how sophisticated, technology controls will always have a gap that determined attackers can exploit. A comprehensive defense acknowledges this and plans for it.

2. Human Intuition Is a Critical Detection Layer

While machines excel at identifying known patterns, they lack the contextual understanding and intuition that humans possess. An employee might recognize that a request is unusual for a specific colleague or notice subtle cues in language that an automated system would miss. This human element is an invaluable asset in spotting the sophisticated, socially engineered phish that are designed to look legitimate to technology.

- **Context Is Key:** People can evaluate a message based on their knowledge of internal processes, team dynamics, and normal communication styles—factors a machine cannot easily assess.
- **Detecting the Unseen:** Human intuition can flag a message that feels “off,” even when all technical indicators appear normal. This is crucial for identifying novel or highly targeted attacks.
- **The Last Line of Defense:** When a polymorphic phish bypasses all technical filters, an alert employee becomes the last and most important line of defense against a breach.

Phishing & The Human Element

Why are humans a critical layer in your phishing defense strategy?

Consider this:

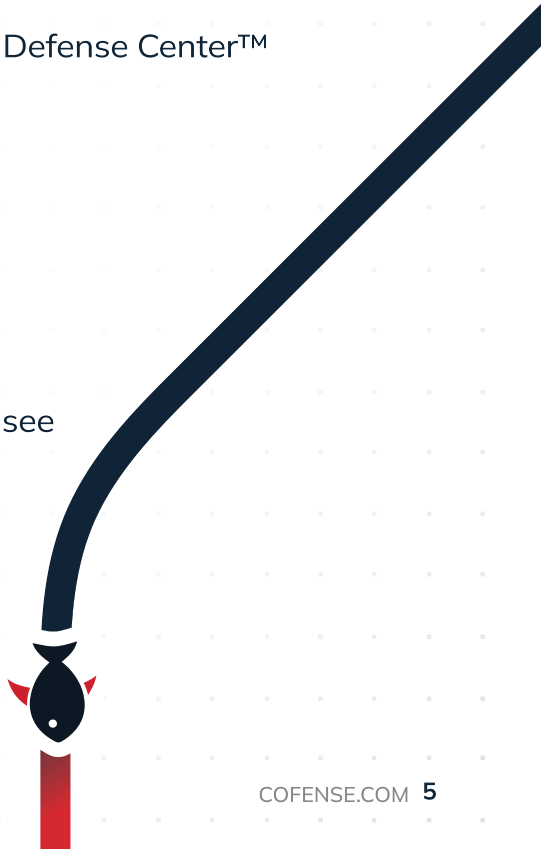
100%

of threats seen by the Cofense Phishing Defense Center™ are identified and reported by users.

0%

are stopped by perimeter controls.

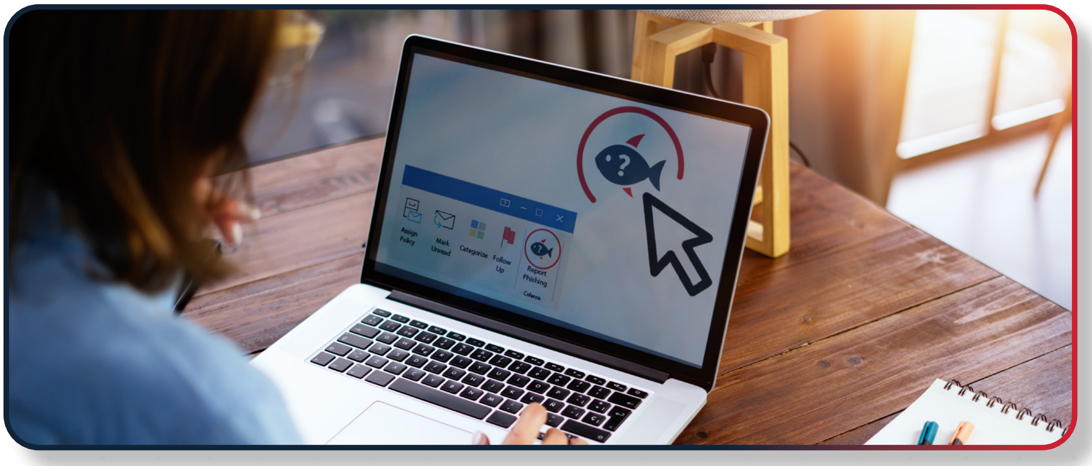
Ordinary employees, trained to say something when they see something, alert our phishing experts to investigate possible threats. This is exactly where timely insights help you stay left of breach, in particular when facing attacks that morph in the blink of an eye.



3. Awareness Training Must Be Relevant and Targeted

Generic security awareness training is not enough to combat specific and evolving threats like polymorphic phishing. To be effective, training must focus on the actual threats that are bypassing your perimeter defense and reaching employee inboxes. Using real-world examples of phishing campaigns that have targeted your organization makes the training relevant and actionable.

- **Focus on Real Threats:** Base training scenarios on the polymorphic phishing attempts that your organization is currently facing, not on generic templates.
- **Actionable Intelligence:** Teach employees to recognize the specific tactics, lures, and social engineering techniques used in recent campaigns that have hit your environment.
- **Beyond Theory:** Practical, relevant training moves awareness from a theoretical concept to a practical skill, empowering employees to become an effective part of your security posture.



TIP: Cofense strongly suggests you avoid randomized phishing training, where each employee receives a different phishing scenario. The intent of randomization is to prevent users from tipping each other off: *"Hey, I just got this training scenario. Don't click!"* But isn't that what you want to happen when real threats arrive—people sounding the alarm about something risky?

4. Reporting Is the Gateway to Visibility

Your security team cannot fight threats they cannot see. When employees fail to report suspicious emails, your organization loses critical visibility into the threats that have successfully bypassed your technological defenses. A strong reporting culture turns your entire workforce into a human threat-detection network, providing the security team with the real-time intelligence needed to respond.

- **Closing the Visibility Gap:** Employee reporting is the only way to gain insight into the malicious emails that have reached the inbox, which is the most critical stage of an attack.
- **From Individual to Organization:** A single reported phish can alert the security team to a widespread campaign, allowing them to protect the entire organization before further damage occurs.
- **Data for Proactive Defense:** The data gathered from reported phish provides valuable intelligence that can be used to strengthen security controls and refine future training efforts.

> *“Building a culture where users can report phishing attempts gives you vital information about what types of phishing attacks are being used.”*
>
> **- UK National Cyber Security Centre**

5. Augment Human Detection with Automated Response

Human detection is critical, but manual response is too slow to effectively contain a fast-moving phishing attack. Once an employee reports a threat, purpose-built automation should take over. This ensures a rapid and consistent response, allowing security teams to analyze, contain, and remediate the threat across the entire organization in minutes, not hours.

- **Speed and Scale:** Automation allows security teams to instantly find and remove every instance of a reported phish from all user inboxes, dramatically reducing the risk of further compromise.
- **Protecting the Bottom Line:** A swift, automated response minimizes the potential impact of a breach, protecting sensitive data, financial resources, and brand reputation.
- **Freeing Up Security Teams:** By automating the repetitive tasks of incident response, security analysts can focus their expertise on more complex threat analysis and strategic defense improvements.

At a Glance

1. Technology controls won't stop every phishing attack. Polymorphic attacks are designed to fool controls and quickly metastasize.
2. Humans have what machines lack—the intuition to detect phish that evade technology.
3. Awareness training should focus on the most relevant threats, such as polymorphic campaigns that hit your email gateway.
4. If your people don't report phishing, your security teams can't see the threats that make it to the inbox.
5. Once humans have detected a threat, purpose-built automation will speed response and remediation to protect your bottom line.

Conclusion

In an era where phishing attacks are increasingly polymorphic and adaptive, true resilience comes from the balance of **human expertise and advanced technology**. By uniting AI-driven detection with human insight, organizations can not only identify and stop evolving threats in real time but also safeguard sensitive data with confidence. **Cofense** leads this charge, combining human-supervised AI, real-time intelligence from over **35 million trained users**, and continuous employee education to help organizations stay ahead of attackers. Together, we build a smarter, stronger, and more adaptive defense against the next generation of phishing.

Contact us today to learn how Cofense can help protect your organization.

Cofense is the only cybersecurity company leveraging expert-supervised AI for phishing detection and response—delivering human-vetted intelligence and real-world training to help enterprises stay ahead of modern threats. Built to augment existing email defenses, Cofense identifies attacks that bypass perimeter filters, remediates them in minutes, and continuously strengthens the human layer through simulations modeled on active phishing campaigns. Informed by insights from over 35 million trained users, Cofense enables faster containment of threats and measurable reductions in risk. Organizations like Mastercard and Blue Cross Blue Shield rely on Cofense to reduce exposure, meet regulatory demands, and build lasting resilience against the most persistent cyber threat: phishing.

Smarter phishing defense. Stronger human security.

Scan the QR code or visit cofense.com to learn how to catch more phish with Cofense.