KnowBe4

Closing the Gap in Email Security: How To Stop The 7 Most Sinister AI-Powered Phishing Threats

WWW.KNOWBE4.COM

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | Email: Sales@KnowBe4.com

From business email compromise (BEC) and spear phishing to credential theft and account takeover, today's phishing threats are more targeted, more convincing and harder to spot. While traditional tools such as secure email gateways (SEGs), filters and authentication protocols provide baseline protection, they fall short against modern threats.

This paper explores the most menacing phishing threats security teams face and explains how combining integrated cloud email security (ICES) with an anti-phishing incident response (IR) product is the only truly effective way to give IT and SecOps the speed, visibility and automation required to stop these attacks in their tracks.

The Threat Landscape

The threat landscape is as diverse as it is sophisticated, with cybercriminals having a digital Pandora's Box to pick attack vectors from. However, certain threats are more dangerous than others. **Here are seven of the most forbidding phishing threats currently targeting your organization.**

Business Email Compromise

BEC is one of the most financially damaging cyber threats, where attackers impersonate trusted individuals, such as executives, vendors or colleagues, to trick employees into transferring funds or sharing sensitive data. These attacks are typically low in volume but high in sophistication. They often bypass traditional security filters due to their lack of malicious links or attachments. Modern BEC campaigns increasingly leverage AI to craft more believable messages and are expanding into variants like vendor email compromise, where attackers hijack legitimate business conversations to redirect payments or steal data. With losses nearing $3 billion annually according to FBI research, BEC remains a top concern for security teams worldwide.

Spear Phishing

Spear phishing is a targeted form of phishing where attackers tailor emails to a specific individual, role or department within an organization. Unlike generic phishing campaigns, spear phishing uses personal or contextual information to appear credible, often referencing real projects, coworkers or internal systems. These emails aim to manipulate victims into clicking malicious links, downloading malware or handing over sensitive credentials. Spear phishing is especially dangerous because it often serves as the entry point for larger attacks, including ransomware or data exfiltration. Its growing success rate has made it a preferred tactic for threat actors pursuing high-value targets.

Payload-less Phishing/Zero Payload Attacks

Payload-less phishing attacks, also known as zero-payload or text-only BEC, involve no malicious links or attachments, just carefully crafted messages designed to manipulate recipients through social engineering alone. These emails often mimic internal communications or urgent requests from executives, asking employees to perform actions like transferring funds, sending sensitive documents or purchasing gift cards. Because there's no detectable payload, these messages often evade SEGs and traditional anti-phishing filters. The reliance on tone, urgency and authority makes payload-less phishing especially effective in exploiting human trust without triggering technical defenses. KnowBe4 Threat Lab research continues to show an increase in such attacks, especially in the context of BEC and executive impersonation.

Credential Phishing

Credential phishing is one of the most widespread and persistent email threats, where attackers lure victims into entering login credentials on fake login pages that mimic trusted services like Microsoft 365 or Google Workspace. These attacks often start with a benign-looking message prompting the user to "verify" or "update" their account. Attackers with harvested credentials are then free to access email systems, file shares and other cloud apps, enabling further compromise. With the rise of multi-factor authentication, attackers are also deploying sophisticated techniques like adversary-in-the-middle phishing kits to bypass security controls.

Account Takeover

Account takeover (ATO) is a critical email-based threat where an attacker gains unauthorized access to a legitimate user's email account, typically through credential phishing, brute-force attacks or session hijacking. Once inside, the attacker exploits the trust and access associated with the compromised account to conduct further malicious activity, such as sending internal phishing emails, initiating BEC scams, exfiltrating sensitive data, or establishing persistence through inbox rules and external forwarding. Because these messages come from trusted, authenticated sources, they often bypass traditional SEGs. ATO is especially dangerous due to its stealth and potential for lateral movement, making it one of the most effective and costly forms of email-based social engineering. Detecting and mitigating ATO requires behavioral analysis, identity monitoring and automated response workflows that can recognize and contain suspicious activity in real time.

Internal Email Threats/Insider Risk

Internal email threats occur when either a compromised internal account or a negligent insider is the source of the threat. These risks can involve anything from an employee mistakenly sending sensitive files to the wrong person, to an attacker using a compromised account to launch phishing attacks within the organization (lateral phishing). Nearly 10% of employees have admitted to sending work emails to their personal accounts — a practice that increases the risk of data leakage, according to KnowBe4 research. Since these threats originate from "trusted" sources, they're harder to detect and often go unnoticed until damage has been done.

Email Spoofing and Lookalike Domains

Email spoofing and the use of lookalike domains are common tactics in social engineering, where attackers mimic legitimate email addresses or register visually similar domains (e.g., substituting "rn" for "m") to deceive recipients. These emails often appear to come from trusted sources, such as business partners or executives, and are used in BEC, phishing and impersonation scams. When organizations lack proper domain protection protocols like SPF, DKIM and DMARC, spoofed emails are more likely to reach inboxes. This method remains a low-effort but high-reward tactic for threat actors seeking to exploit brand trust and user complacency.

Traditional Approaches to Mitigating Phishing

Traditional approaches to mitigating phishing attacks have focused primarily on policy enforcement and technical controls at the email gateway. While these methods remain foundational, nearly all are insufficient against today's sophisticated, payload-less and AI-enhanced attacks. **Here are five of the most common traditional defenses and their limitations.**

1. Secure Email Gateways

- They block known spam, malware and phishing emails using blacklists, signature detection and sandboxing
- However, they struggle with zero-payload BEC, spoofing and language-based attacks that lack malicious links or attachments. Moreover, they're often static or signature-based — easily bypassed by novel or well-crafted threats.

2. Spam Filters and Heuristics

- They can reduce inbox clutter and filter obvious phishing or scam attempts
- However, they are easily bypassed by well-crafted or targeted spear-phishing emails, and false positives can frustrate users

3. Email Authentication Protocols (SPF, DKIM, DMARC)

- They prevent domain spoofing and improve trust and sender reputation scoring
- They also require proper configuration and ongoing maintenance, and can't mitigate display name spoofing, lookalike domains or BEC attacks

4. Email Client Controls and URL Rewriting

- They typically warn users before they click and allow real-time scanning of links at the moment of click
- Users can simply bypass or ignore these warnings, and these tools are easily fooled by more advanced, AI-generated threats

5. Manual Triage and Incident Response

- It requires hands-on investigation and can result in a timely remediation IF the threat is well understood
- This method is time-consuming, unscalable and far too slow to stop attacks in progress, such as credential use, internal spread, etc.

A Better Together Strategy

When deployed together, ICES platforms and anti-phishing IR create a powerful, layered defense that significantly enhances an organization's ability to detect, respond to and mitigate email-based social engineering threats. Here's how they work in tandem to reduce risk.

Integrated Cloud Email Security

ICES, which often integrate directly with products like Microsoft 365, provide real-time protection against advanced threats via:

- AI, machine learning and natural language processing
- Email content and metadata
- Sender behavior and domain reputation
- User context and historical patterns
- Payloads (or lack thereof) including attachments, links or message tone

These platforms are particularly effective at catching zero-payload BEC, spoofing and spear phishing that SEGs typically miss by leveraging AI and natural language processing to detect intent-based threats, like impersonation or urgency cues.

Anti-Phishing Incident Response

Anti-phishing IR enhances incident handling by automating the investigation, enrichment and remediation of suspicious emails. When integrated with an ICES platform, it can:

- Automatically ingest and analyze reported phishing emails
- Enrich alerts with contextual threat intelligence (e.g., IP, domain, known bad URLs)
- Correlate user reports across the environment to identify patterns or broader campaigns
- Quarantine or remove malicious emails from all affected inboxes, often within seconds
- Trigger response procedures for BEC, credential theft or lateral phishing scenarios, speeding response while reducing analyst fatigue

When ICES and IR work together, they deliver a faster, smarter and more scalable defense against email threats. Threats are identified/detected more quickly, frequently before the end-user even interacts with a malicious message. Suspicious emails reported by users are automatically investigated and remediated, eliminating the delays and inefficiencies of manual intervention. These tools also enable organizations to map and neutralize entire phishing campaigns across all users, rather than responding to incidents in isolation. Security teams gain deeper visibility into attack patterns and can continuously refine detection rules and policies based on real-world threat data.

Benefits of an Integrated Approach

Category	Traditional Approach	Integrated Approach (ICES + IR)	Benefit to SecOps/IT
Threat Detection	Relies on signatures, static rules, SEGs	Uses AI/ML, behavior analytics, NLP to detect intent and anomalies	Detects sophisticated attacks like BEC, spear phishing, zero-payload threats
Speed of Response	Manual investigation and remediation	Automated triage, enrichment and quarantine via SOAR playbooks	Reduces mean time to respond (MTTR) from hours/ days to minutes
User Reporting	Phishing reports go to a shared inbox or ticket queue	Automated phishing workflows ingest, analyze and act on reports	Scales user reporting without overloading IT/helpdesk
Visibility and Context	Limited email metadata, fragmented logs	A single pane of glass that provides enriched threat context (user behavior, attack graph)	Enables faster investigation and more informed decisions
Scalability	Heavily reliant on human analysts and predefined filters	Cloud-native, API-driven, scales with organization size and threat volume	Supports growth without requiring linear team expansion
Internal Threat Detection	Often blind to lateral movement or insider misuse	Behavioral baselining detects anomalies in internal communications	Identifies compromised users and insider threats faster
Integration	Siloed tools and manual handoffs	Seamless integration with SIEM, IAM, EDR and ITSM platforms	Improves workflow automation and cross-tool correlation
False Positives	High volume, hard to tune filters	Context-aware detection reduces alert fatigue	Frees up analysts for high-impact work
Compliance and Reporting	Manual report generation, limited detail	Automated reporting, audit logs and policy enforcement tracking	Simplifies compliance and governance documentation

Conclusion

Today's phishing threats are too advanced, too fast-moving and too targeted for traditional defenses to handle alone. That's why it's critical for IT and SecOps teams to adopt a modern, integrated approach that combines the intelligence of an ICES platform with the speed and automation of an IR product. It strengthens protection across the full threat lifecycle while driving faster response, better visibility and stronger overall resilience.

Learn More About KnowBe4's Cloud Email Security and PhishER Plus

Cloud Email Security PhishER

About KnowBe4

As the provider of the world's largest security awareness training and simulated phishing platform, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud, and other social engineering tactics through a new-school approach developed by an internationally recognized cybersecurity specialist.

Join more than 70k international organizations in trusting the KnowBe4 platform to strengthen your security culture and reduce human risk.

For more information, please visit
www.KnowBe4.com

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com