Five Essential Strategies to Combat Phishing Threats

Phishing accounts for over 34% of breaches and costs organizations an average of $4.76M per incident. Nearly 1 in 3 employees still click on phishing simulations.

Phishing remains one of the most common and effective attack methods. Research shows it contributes to over 34% of confirmed breaches. The financial impact is significant as well, with credential-related breaches averaging $4.76 million per incident. And despite years of security awareness training, nearly a third of employees still click on simulated phishing emails.

Why does phishing work so well? Attackers exploit gaps in visibility, speed, and user behavior. While no single strategy eliminates the risk, layering defenses and improving detection and response can dramatically reduce exposure. Here are five essential strategies every organization should consider.

1. Correlate Events Across Multiple Sources

Phishing is rarely a single action. It usually unfolds across multiple systems: a suspicious email, a malicious link, and a login attempt from an unusual location. Looking at these signals in isolation makes them easy to miss. Correlating data from email gateways, authentication systems, firewalls, and endpoints helps connect the dots and surface the bigger picture.

2. Monitor Email Authentication in Real Time

Controls like SPF, DKIM, and DMARC help block spoofed messages, but they are only effective if you can measure their effectiveness. Real-time monitoring of authentication outcomes can quickly highlight gaps, anomalies, or spoofing attempts that bypass filters. Treating email authentication as live telemetry rather than a "set and forget" control strengthens the first line of defense against phishing.

3. Detect Anomalous User Behavior

Credential theft is often the end goal of phishing. Once inside, attackers rely on stolen accounts to move quietly through systems. This makes behavioral analytics critical. By establishing baselines for normal user activity, security teams can detect anomalies like unexpected logins, large data transfers, or access from new geographies. These subtle shifts can serve as early indicators of compromise, helping stop attackers before they escalate.

4. Automate Response Workflows

When phishing succeeds, speed of response can mean the difference between containment and compromise. Manual investigation and remediation often take too long. Automating common workflows, such as disabling accounts, isolating devices, or triggering resets, reduces dwell time and limits attacker movement. Even partial automation can significantly improve response outcomes.

5. Measure and Improve Security Awareness

Phishing is not just a technical challenge. Human behavior remains a key factor. Nearly 29% of employees still click on phishing simulations. Measuring awareness programs through metrics like reporting rates, simulation outcomes, and incident correlations provides better insight than completion statistics alone. This allows organizations to refine training and track how awareness translates into real resilience.

Staying Ahead of Phishing Threats

Phishing thrives on fragmented signals, delayed responses, and human error. Building a layered defense that combines event correlation, authentication monitoring, behavioral analytics, automated response, and measurable awareness training strengthens your ability to detect and contain threats before they spread.

Read our guide to explore how organizations defend against advanced phishing campaigns.

ABOUT GRAYLOG

Graylog delivers a SIEM that works the way teams actually need: full visibility, real detection, and faster investigations—without blowing the budget. Trusted by 50,000+ organizations worldwide, Graylog helps analysts skip the noise and get to what matters. Automate the heavy lifting. Stay focused on real threats. Learn more at graylog.com or connect with us on Bluesky and LinkedIn.