

DEFENDING THE ENTERPRISE IN THE AGE OF DECEPTION

Understanding the Threat Landscape



graylog

Phishing attacks remain one of the most persistent and damaging vectors for security breaches across organizations of all sizes. According to the [UK Government Cyber Security Breaches Survey 2025](#), this type of attack is the most prevalent and disruptive approach, experienced by 85% of businesses.

While the overall prevalence of cyber breaches has shown some improvement—43% of UK businesses reported breaches in 2024 compared to 50% in 2023—the sophistication of attacks continues to increase. The survey highlights a growing consciousness among organizations that increasingly sophisticated methods, such as AI impersonation, have broken through to the mainstream in phishing campaigns. The digital threat landscape continues to evolve at an alarming pace across the world, and these findings are likely similar no matter the country.

Particularly concerning is the increased incidence of certain damaging outcomes, with businesses reporting a significant increase in temporary loss of access to files or networks (7%, up from 4% in 2024). The survey also reveals that phishing attacks were often cited as time-consuming to address due to their volume and the need for investigation and staff training.

In the United States, the [FBI](#) reported cybercrime losses reached a record \$16.6 billion last year for consumers and businesses, primarily driven by scams such as deceptive emails tricking employees into transferring funds to criminals' accounts.

These findings underscore the critical need for comprehensive log management and analysis for security teams managing diverse technology environments. However, the challenge extends beyond mere data collection — it's about cutting through the noise that overwhelms security operations centers daily. Graylog's real-time log enrichment and precision risk scoring filter out the noise, reducing alert fatigue by up to 99.9%, ensuring teams spend less time chasing false positives and more time focusing on genuine threats.

Building on proven frameworks like MITRE ATT&CK® or the Cyber Kill Chain® helps analysts sharpen detection capabilities and systematically address phishing campaigns. With Graylog, security teams can operationalize these models to drive down mean time to identify (MTI) and mean time to respond (MTTR) — enabling faster decisions with fewer blind spots across the attack surface.

From user and entity behavior analytics (UEBA) to Detection Chains, Graylog strengthens analyst readiness by providing the tools needed to surface hidden threats, detect phishing campaigns in motion, and stay ahead of evolving attacker tactics — all without adding operational overhead. Graylog's centralized log collection and SIEM capabilities become essential here, providing the visibility and analytical depth needed to detect and respond to phishing threats across your entire infrastructure.



85%
of businesses
have
experienced a
phishing attack



7%
of businesses
report a
significant
increase in loss
of access to files
or networks

Five Essential Strategies to Combat Phishing Threats

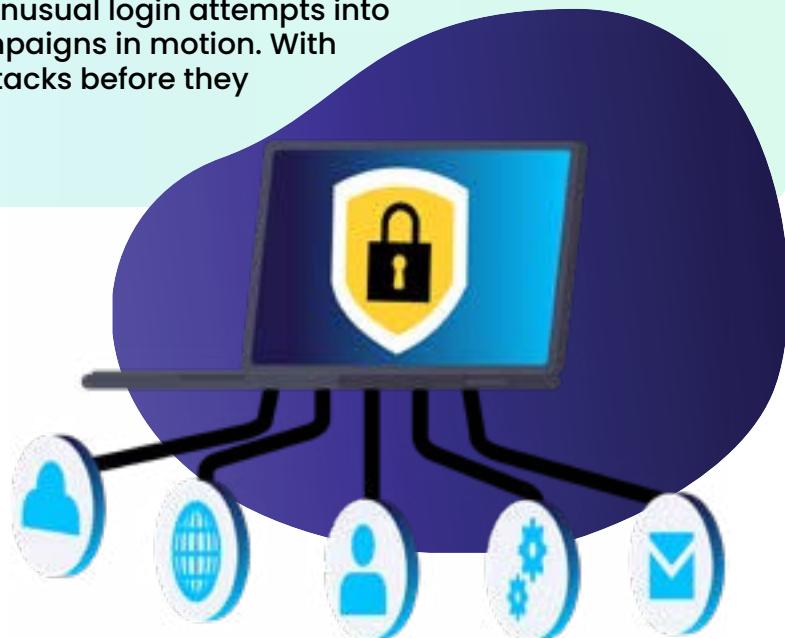
At Graylog, we've designed our platform to help organizations defend against evolving phishing campaigns. Based on our experience with thousands of customers worldwide, here are five essential strategies you can implement using Graylog's capabilities:

1. Leverage Multi-Source Log Collection for Cross-Channel Detection

Graylog's ability to ingest logs from virtually any source enables you to correlate events across your entire infrastructure. Configure Graylog to aggregate and analyze logs from email systems, web proxies, firewalls, endpoints, and authentication servers simultaneously. While siloed tools see fragments, effective correlation connects the dots to spot the attacks others miss. In a phishing scenario where an attacker sends a malicious email, harvests credentials, and gains access — all in a tight window — most tools treat each event as unrelated noise. Modern correlation engines surface the full story.

Per field correlation flags anomalies when multiple failed logins from a single user suddenly flip to success — same field, different behavior providing critical insight. Cross-source correlation ties together logs from email gateways, endpoint agents, and authentication servers, so a phishing link in a message, a browser callout, and an unfamiliar login get correlated and alerted. Time-based sequencing that tracks event order and timing allows you to map the full attack path — from inbox to intrusion — faster than attackers can pivot.

This isn't just alerting. It's correlated visibility that turns isolated signals into clear threats. Graylog's powerful search capabilities allow you to create correlation rules that identify these suspicious patterns across different channels. These rules transform what appears as suspicious email interactions followed by unusual login attempts into clear indicators of successful phishing campaigns in motion. With proper correlation, analysts catch these attacks before they escalate.



2. Monitor Email Authentication with Dashboard Visualizations

Implement email authentication protocols like DMARC, SPF, and DKIM, then use Graylog's dashboard capabilities to visualize their effectiveness. Our dashboard features for security monitoring make it easy to track authentication patterns in real-time and identify potential weak points in your email security architecture. With Graylog's alerting feature, you can receive immediate notifications when authentication anomalies occur, allowing for rapid response to potential spoofing attempts.



3. Implement User Behavior Monitoring with Analytics

Graylog's analytics capabilities allow organizations to establish baseline patterns for user activities and identify anomalies that might indicate compromised credentials. The platform processes authentication logs, access records, and network traffic to detect unusual behaviors such as logins from new locations, access to sensitive systems outside normal patterns, or unexpected data transfers.

The anomaly detection capabilities — enhanced by Illuminate content packs — enable targeted analysis that goes beyond simple threshold-based alerts. For instance, the system can highlight irregular login times, access from unfamiliar geographic locations, or unusual interactions with critical systems. These automated detectors help surface potential phishing-related threats quickly while reducing alert fatigue by focusing on truly anomalous behavior rather than generic thresholds.

This focused approach provides early warning of credential compromise from phishing attacks while minimizing noise through context-specific detectors tailored to each environment. Rather than relying on false positive rates, Graylog's targeted methodology ensures alerts are meaningful and actionable.



4. Automate Phishing Response with Pipelines and Integrations

When phishing attacks succeed, rapid response is critical. Automated workflows can be configured to trigger when suspicious patterns emerge — isolating affected systems, initiating credential resets, and preserving forensic evidence.

Custom HTTP notifications enable posting targeted messages (including event data) to any reachable API endpoint, while script-based notifications can pass event data to local scripts. This flexibility allows interaction with existing systems via REST API or script — whether triggering firewalls to isolate compromised hosts, automatically disabling accounts of suspected phishing victims, or performing real-time reputation lookups on email data.

These integration capabilities connect with existing security tools through Graylog's extensive API, enabling SOC teams to respond to incidents in minutes rather than hours through custom workflows tailored to specific security infrastructure needs.



5. Measure Security Awareness with Custom Reporting

With Graylog's reporting capabilities, security awareness can transform from a checkbox exercise to a measurable security control. Graylog helps you track the effectiveness of your anti-phishing training by collecting and analyzing data on simulated phishing exercise results, user reporting rates for suspicious emails, and security incident metrics. Graylog's customizable reports make these metrics visible to leadership, demonstrating the direct connection between security awareness and business risk.



Looking Ahead

Phishing will remain the dominant attack vector for years to come. Effective security operations require not just powerful tools, but the ability to extract actionable intelligence from diverse data sources. Graylog's centralized log management platform transforms raw security data into actionable insights, helping you build a powerful defense against even the most sophisticated phishing campaigns. The battle against phishing demands more than alert fatigue – it requires visibility that drives decisive action.

Graylog transforms your defense strategy by ingesting comprehensive email data for richer context while integrating continuously updated, high-efficacy detection rules from TruKno through Graylog Illuminate. These rules map directly to MITRE ATT&CK frameworks and adapt to evolving phishing tactics in real-time, cutting through noise to surface genuine threats.

With Graylog anchoring your security operations, you gain the precision to detect, analyze, and neutralize phishing campaigns—without compromise.

The battle against phishing is not just about technology – it's about creating a security ecosystem where visibility drives action. With Graylog at the center of your security operations, you gain the comprehensive visibility needed to detect, analyze, and respond to phishing threats before they impact your business.

[**Request a demo today >**](#)



ABOUT GRAYLOG

Graylog is the no-nonsense SIEM that cuts through noise and complexity. It delivers what security teams need most: full visibility, faster investigations, and smarter detection—without trade-offs or surprise costs. From automated workflows to correlation and anomaly detection, Graylog helps analysts move faster and stay focused. With a product suite spanning Graylog Enterprise, Security, API Security, and Open, we support everyone from large enterprises to lean teams. Trusted by over 60,000 organizations around the world. Learn more at graylog.com or connect with us on [Bluesky](#) and [LinkedIn](#).

