PHISHLABS

Phishing Incident Response

Expert analysis and automated response to user-reported threats

Expert Analysis and Automated Response to User-Reported Threats

Phishing attacks target enterprises and their employees on a daily basis. Unfortunately, phishing accounts for more than 90 percent of data breaches[1] and the average cost of a breach is $3.86 million[2] Technological barriers, while essential, are not sufficient to mitigate the threat posed by phishing. For this reason, it is critical to leverage employees as a layer of the security infrastructure.

Timely analysis of user-reported phishing attacks can significantly reduce the risk of a major security incident. However, many enterprises do not have the resources and processes in place to quickly analyze and respond to all messages reported by users. Emails are often ignored or set aside for later analysis, and potential threats go undetected.

Phishing Incident Response is a managed service that provides near real-time monitoring, expert analysis, and automated response to user-reported emails. By partnering with our two 24/7 Security Operations Centers, enterprise security teams can rapidly detect and respond to the email-based threats that reach the inboxes of end users. Additionally, the PhishLabs team can perform in-depth forensic payload analysis when advanced threats are found.

Stop Threats Missed by Security Technologies

Phishing Incident Response helps enterprises detect and stop the phishing attacks that go undetected and unblocked by email and network security technologies. Suspicious emails reported by end users are monitored in near real-time, providing full visibility into the threats that make it into employee inboxes.

These potential attacks are analyzed via a robust process that combines purpose-built automation with anti-phishing experts. This process ingests all user-reported messages, identifies threats, and extracts threat indicators from emails and payloads. These threat indicators are delivered via TAXII in STIX format, enabling automatic integration with third-party security tools.

This process detects and mitigates phishing threats within minutes of an email being reported by a user.

Around -the-Clock Threat Monitoring

Forty-four percent of professionals[3] stated that they check work emails while on vacation, with 1-in-10 checking hourly. Based on a typical seven day work week, data shows that this constant connectedness correlates with user-reported emails landing in the abuse box outside of typical hours and even on the weekends.

For most organizations, these reported emails can end up sitting for days, weeks, or an indefinite amount of time without analysis.

With Phishing Incident Response, reported emails are rapidly analyzed regardless of the time they are reported. With expert review and threat severity categorization, only threats that need to be addressed are brought to your team's attention.

Respond to Attacks With Complete Threat Context

With a vast and expanding digital threat landscape, it's critical to quickly identify and understand the elements of a threat targeting your organization.

PhishLabs' team of experts review and analyze digital risks on your behalf, allowing your team to prioritize and focus on risks that matter the most. Threats identified by the PhishLabs SOC teams can be escalated to the R.A.I.D. for in-depth forensic analysis. This is ideal for advanced and/or targeted threats that pose higher risk.

In this scenario, R.A.I.D. threat analysts reverse-engineer advanced payloads and correlate attacks against our global intelligence to provide a complete picture of the threat.

This includes delivering intelligence on relevant attack campaigns, patterns, and threat actors.

Armed with this intelligence, security operations and incident response teams can take immediate action to counter and mitigate advanced and/or targeted threats.

Taking Down Malicious Content and Reducing Risk

PhishLabs' Incident Response service focuses on eliminating malicious threats that target your employees. When you partner with PhishLabs, our SOC teams will analyze malicious or unauthorized content when it is reported or detected, and if necessary, move quickly to take the threat offline.
Due to our strong relationships with numerous hosting providers and social platforms, we are able to quickly and efficiently take down malicious content. With a 99 percent takedown success rate on confirmed phish and an estimated window of under five hours for takedowns, your employees and organization will be more secure.

Strengthening Security Across the Enterprise

PhishLabs' Phishing Incident Response is a component of a holistic security offering provided by PhishLabs that is designed to protect your enterprise, your employees, and your customers, which includes:

- Digital Risk Protection
- Security Awareness Training

1. 2017 Verizon Data Breach Digest: Perspective is Reality
2. 2018 Ponemon Institute Cost of a Data Breach: Global Overview
3. American Psychological Associate survey

PHISHLABS

As a managed services provider with more than 15 years of experience finding and stopping threats outside the traditional network perimeter, PhishLabs is the ideal partner to help cyber security teams protect their enterprise, brands, and customers from digital risks.

PhishLabs Managed Threat Intelligence and Mitigation services make it easier than ever to manage risks across email, domain, social media, mobile, dark, deep, and open web vectors. Our expert-driven, managed approach goes beyond do-it-yourself tools to ensure the digital risk protection outcomes enterprises want.

To learn more, visit www.phishlabs.com.

@PhishLabs

linkedin.com/company/phishlabs