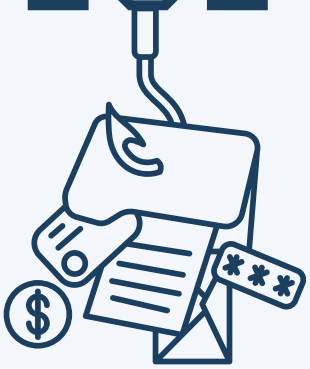
2024



10 Phishing Analysis Tools

FOLLOW

CYBERMATERIAL

PhishTool

PhishTool offers a robust set of features designed for effective phishing detection and response, tailored for both individual users and professional teams:

- PhishTool Enterprise: Offers tools for real-time collaboration and rapid email triaging, ideal for cybersecurity teams and service providers. It integrates easily with systems like Microsoft 365 and Google Workspace
- PhishTool Community: A free version for individuals, providing tools for reverse engineering and analyzing phishing emails with access to Open Source Intelligence (OSINT)
- User Interface: Features an intuitive UI that guides users through automated analysis and contextual email metadata analysis, helping to quickly address phishing threats
- API Integration: Supports integration with third-party threat intelligence platforms, enhancing its real-time threat detection capabilities
- Analysis Tools: Includes heuristic detection and the capability to generate detailed forensic reports for actionable insights into phishing incidents

For additional information, vist: PhishTool Community

ThePhish

ThePhish is an automated phishing email analysis tool that offers a range of features to streamline and enhance the phishing detection process. Here's a summary of its capabilities:

- Comprehensive Automation: ThePhish automates phishing email analysis by extracting and evaluating observables like IP addresses and URLs from the email content.
- Integrated Platforms: It utilizes TheHive for case management, Cortex for observable analysis, and MISP for sharing threat intelligence on identified threats.
- Enhanced Analysis Capabilities: Features specialized analyzers for tasks such as domain verification, link expansion, and attachment scanning.
- Customizable Whitelisting: Allows users to create whitelists using exact matches or regular expressions to prevent the analysis of known safe entities, reducing false positives.
- Real-time Communication: Employs a Mailer responder to send analysis verdicts directly to users, facilitating quick responses to phishing threats.

For more details and setup instructions, you can visit the project's GitHub page

PhishTank

PhishTank provides several features that are useful for combating phishing:

- Community Contributions: Users can submit and verify suspected phishing URLs, fostering a collaborative approach to identifying threats.
- Developer API: Offers a robust API that allows integration of PhishTank's data into other applications, supporting multiple data formats.
- Phishing Database: Provides a searchable database of verified phishing URLs for research and prevention purposes.
- Open Data Access: PhishTank ensures that all phishing data is freely accessible, promoting transparency and widespread usage.
- Backed by Cisco Talos: Operated by Cisco's Talos Intelligence Group, ensuring reliable and informed security insights.

For more detailed information, visit PhishTank

OpenPhish

OpenPhish provides several key features focused on delivering timely and actionable phishing intelligence:

- Phishing Intelligence: OpenPhish provides detailed insights on phishing trends, including data on targeted brands and sectors.
- Phishing Feeds: Offers real-time updates on phishing URLs and associated data, available through various subscription levels.
- Comprehensive Database: Maintains an up-to-date database with detailed forensics on phishing URLs, useful for cyber incident analysis.
- API Integration: Supplies an API for developers to integrate phishing intelligence directly into security applications.
- Flexible Applications: Supports diverse cybersecurity tasks, from URL verification to pattern analysis in phishing threats.

For further details or to access these services, visit OpenPhish

Cuckoo Sandbox

Cuckoo Sandbox is an open-source automated analysis system that analyzes suspicious files and URLs in a virtual environment.

Here are its key features focused on URL analysis:

- Versatile URL Analysis: Examines suspicious URLs to detect phishing, malicious redirects, and exploit kits across multiple platforms like Windows, Linux, macOS, and Android.
- Behavior Tracking: Monitors activities like downloads, redirects, and scripts triggered by URLs.
- Network Traffic Analysis: Captures and analyzes all URL-generated traffic, including encrypted SSL/TLS data.
- Threat Detection: Integrates with tools like YARA for deeper inspection of suspicious URLs.
- Customizable Environments: Simulates various browsing setups for tailored URL analysis.

For more information, visit Cuckoo Sandbox

Email Veritas

Email Veritas is an email security platform designed to protect users from phishing threats and enhance email safety.

Here are its key features:

- Phishing Detection: Identifies and flags potential phishing emails to prevent malicious attacks.
- URL and File Verification: Allows users to verify the legitimacy of URLs and files received via email.
- Threat Intelligence: Provides insights into email threats, including domain proximity activity and message origin analysis.
- Data Loss Prevention (DLP): Implements policies to prevent unauthorized sharing of sensitive information.
- Integration with Email Clients: Offers extensions for Google Workspace and Microsoft Outlook to enhance email security within existing workflows.

For more information, visit Email Veritas

AbuseIPDB

AbuseIPDB is a platform that enhances internet safety by enabling users to report and check IP addresses associated with malicious activities.

Here are its core features:

- IP Reporting: Users can report suspicious IP addresses to help create a shared database of malicious IPs.
- IP Checking: Offers tools to check an IP's report history and its associated abuse confidence score.
- API Integration: Provides API access for automated IP checking and reporting, suitable for system integrations.
- Blacklisting: Maintains an updated blacklist of high-risk IP addresses based on community reports.
- Security Tool Integration: Supports integration with various security tools, enhancing its functionality within different tech environments.

For more details, you can explore AbuseIPDB

PhishTitan

PhishTitan by TitanHQ is a powerful phishing protection tool for Microsoft 365, designed to enhance email security with the following features:

- AI-Driven Protection: Utilizes advanced AI and machine learning to detect and neutralize sophisticated phishing threats in real time.
- Comprehensive Scanning: Integrates seamlessly with M365 to scan all emails, bolstering defenses against threats missed by conventional security measures.
- URL and Email Filtering: Employs dynamic URL rewriting and time-of-click protection to ensure safety from malicious links at the moment they are accessed.
- Rapid Remediation: Features instant remediation capabilities that quickly remove harmful emails across all user inboxes, minimizing the risk of damage.
- Ease of Use and Support: Offers a user-friendly interface for easy setup and management, supported by robust customer service to assist users effectively.

For more information, visit TitanHQ's PhishTitan page

CheckPhish

CheckPhish by Bolster AI is a comprehensive tool designed to protect against phishing and typosquatting attacks. Here are the key features of CheckPhish:

- Real-Time URL Scanning: Provides in-depth threat analysis including screenshots and hosting details for rapid phishing detection.
- Domain Monitoring: Monitors domain registrations and phishing pages, covering over 1300 TLDs to protect against typosquatting.
- Email Link Protection: Integrates with Microsoft Outlook to scan and block malicious email links, enhancing email security.
- Phishing Scanner: Delivers a comprehensive scanner for web domains and URLs to quickly identify malicious content.
- Community Engagement: Supports a user community for sharing best practices and learning how to combat phishing.

For more information or to use these features, visit CheckPhish

IsItPhish

IsItPhish is a real-time phishing detection tool that leverages machine learning technology to identify phishing URLs. Here are the key features of IsItPhish:

- Machine Learning Detection: IsItPhish uses advanced machine learning algorithms to analyze over 140 million URL syntax features, enabling it to detect zero-day phishing attacks with a high degree of accuracy.
- High Accuracy Rate: The tool boasts an impressive accuracy rate of 97%, allowing it to effectively distinguish between phishing and legitimate URLs.
- Real-Time Analysis: IsItPhish operates in real-time, providing immediate assessments of URLs to determine their safety, which is crucial for preventing phishing attacks as they happen.
- Speedy Response: The service ensures quick response times, with most queries processed in less than 200 milliseconds, minimizing any disruption to user experience.
- Continuous Improvement: Constantly improves detection algorithms for reliability.

For more details, visit IsItPhish.

Tool Overview

Phishtool: PhishTool Community

ThePhish: GitHub page

PhishTank: PhishTank

OpenPhish: OpenPhish

Cuckoo Sandbox: Sandbox

Email Veritas: EV

AbuseIPDB: AbuseIPDB

PhishTitan: PhishTitan page

CheckPhish: CheckPhish

IsItPhish: IsItPhish