Forensic Analysis Report

This report provides an analysis of phishing websites, including geographical hotspots, risk levels, suspicious patterns, sensitive fields, and actionable recommendations. The dataset was collected from PhishTank, which provided 66,661 phishing websites,1,000 websites were successfully scraped and analyzed for suspicious links, metadata, and sensitive forms.Each section includes insights, visualizations, and explanations to assist investigators.

This report is intended to provide a comprehensive overview
of the findings and analysis conducted on the collected data.

1. Geographical Hotspots

- California: 367 occurrences

- Massachusetts: 225 occurrences

- New York: 194 occurrences

- Texas: 53 occurrences

- Missouri: 37 occurrences

- Washington: 12 occurrences

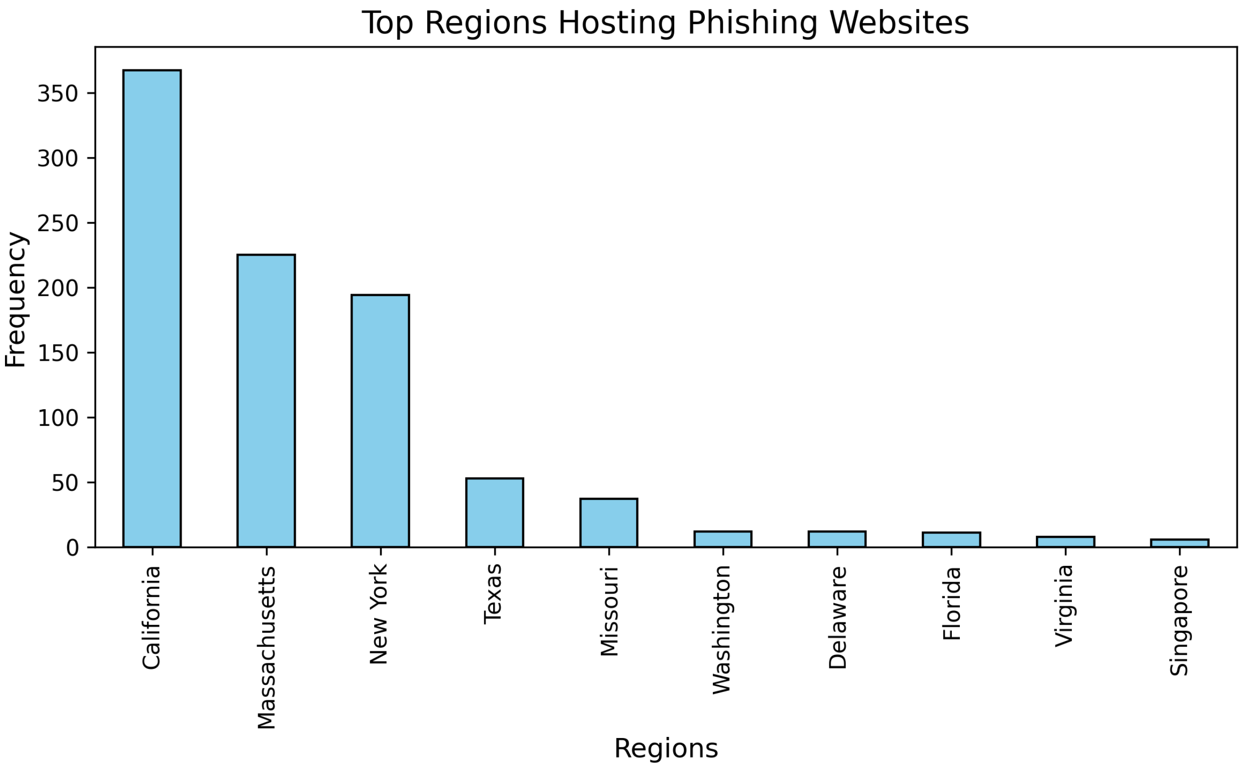
- Delaware: 12 occurrences

- Florida: 11 occurrences

- Virginia: 8 occurrences

- Singapore: 6 occurrences

The chart below highlights the top 10 regions hosting phishing websites. These regions are hotspots for hosting malicious sites, with California and Texas showing the highest occurrences.



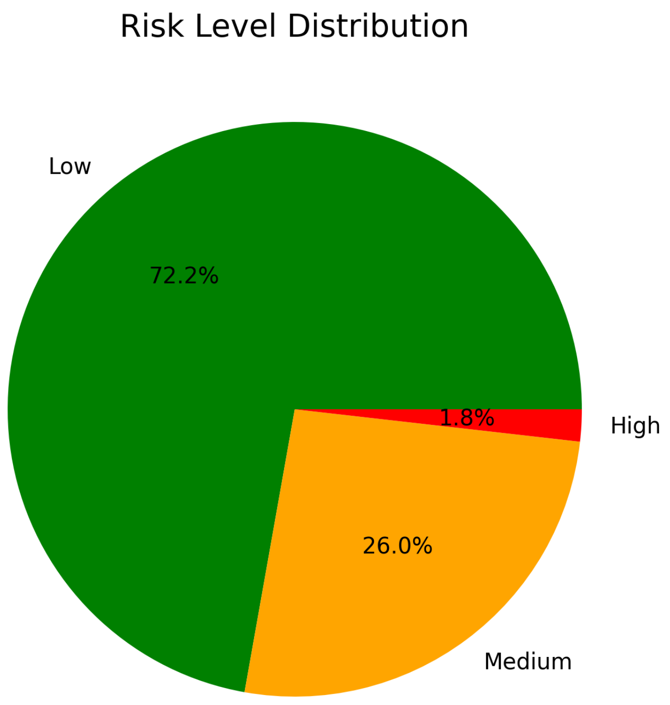
2. Risk Levels Distribution

- Low: 722 websites

- Medium: 260 websites

- High: 18 websites

The pie chart below categorizes phishing websites into risk levels: Low, Medium, and High. High-risk websites are flagged for immediate attention as they exhibit strong phishing indicators, such as suspicious links and sensitive input fields.

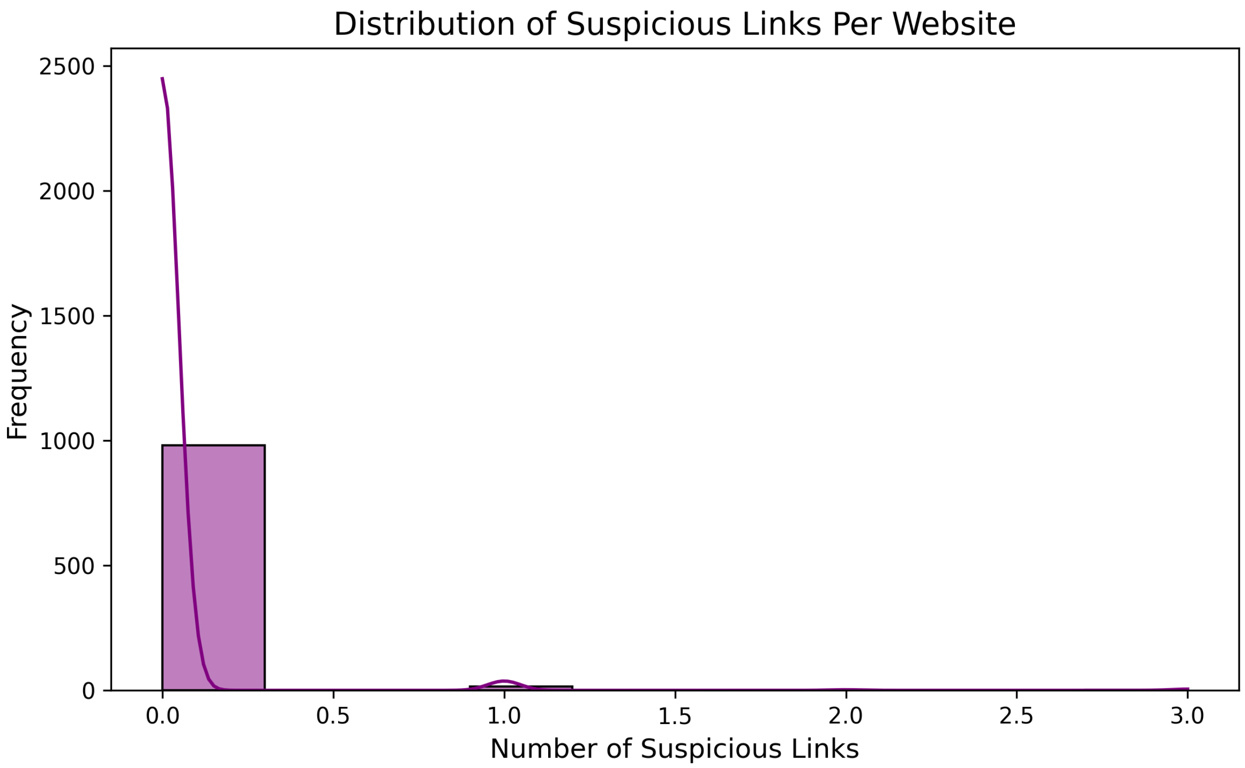


3. Suspicious Links Breakdown

- Total Suspicious Links: 23

- Average Suspicious Links Per Website: 0.02

The histogram below shows the distribution of suspicious links across websites. Websites with high numbers of suspicious links should be prioritized for investigation.



4. Forms with Sensitive Input Fields

- Total Forms with Sensitive Fields: 2

Sensitive fields such as passwords, credit card numbers, and SSNs are often targeted by phishing websites. Investigators should focus on websites containing such forms as they are likely designed to steal user credentials.

5. Recommendations for Investigators

1. Focus on geographical hotspots like California and Texas for targeted analysis.
2. Investigate websites with high-risk levels (e.g., classified as 'High Risk').
3. Pay attention to forms targeting sensitive fields such as passwords and credit card details.
4. Use the suspicious link distribution to identify potential outliers or patterns.