**What is domain Monitoring: phising analysis?**

**Domain Monitoring: Phishing Analysis** is the process of continuously tracking domain names (web addresses) to detect, analyze, and respond to those that might be created or used for phishing attacks.

Here’s the breakdown:

**1. Purpose**

* **Phishing prevention** – Identify lookalike or suspicious domains before attackers can use them to trick users.
* **Brand protection** – Prevent fraudsters from impersonating your company’s domain.
* **Threat intelligence** – Collect data on attacker infrastructure for further investigation.

**2. How It Works**

1. **Domain Discovery**
   * Monitor **newly registered domains** (NRDs) and subdomains from DNS feeds, WHOIS databases, and zone files.
   * Look for **typosquatting** (e.g., micorsoft.com), **homoglyph attacks** (using similar-looking characters), or **subdomain abuse** (login.example.com.attacker.site).
2. **Risk Scoring**
   * Apply machine learning or rules-based analysis to assign **phishing likelihood scores** based on:
     + Domain name similarity to known brands
     + Hosting location & reputation
     + SSL certificate details
     + WHOIS registration patterns (e.g., privacy-protected, short registration times)
3. **Content & Behavior Analysis**
   * If the domain is live:
     + Capture screenshots of the website.
     + Check for phishing indicators: login forms, fake brand logos, suspicious JavaScript, or credential harvesting scripts.
     + Test for redirection to malicious sites.
4. **Threat Attribution**
   * Correlate with known phishing campaigns, IP addresses, or malware infrastructure.
   * Map the domain to **threat actors** or previously known phishing kits.
5. **Response**
   * Alert security teams or customers.
   * Request **takedowns** via registrars or CERT teams.
   * Add to **blocklists** in email gateways, browsers, or firewalls.

**3. Common Tools & Data Sources**

* **Threat Intelligence Feeds** – PhishTank, OpenPhish, APWG.
* **WHOIS & DNS Data** – WhoisXML, DomainTools, Farsight Security.
* **Certificate Transparency Logs** – For spotting SSL/TLS certs issued to suspicious domains.
* **OSINT Tools** – urlscan.io, VirusTotal, Shodan.
* **Brand Monitoring Platforms** – Detect brand impersonation in domains and email.

**4. Example Use Case**

Imagine your company is *examplebank.com*.  
A domain like examp1ebank-login.com is registered today:

* Domain Monitoring system spots it in **new registrations**.
* Similarity detection flags it as **high-risk**.
* Content scan reveals it’s hosting a **fake login page**.
* The SOC team:
  + Adds it to **email filtering blocklists**.
  + Notifies affected customers.
  + Sends a takedown request to the registrar.

**Data Sources**

**Top Sources for Daily or Real-Time Phishing Feeds**

**1. PhishStats**

* **What it offers**: A real-time phishing data feed pulling from sources like VirusTotal, Google Safe Search, ThreatCrowd, abuse.ch, and Antiphishing.la. It provides updates every **90 minutes** via API or CSV.  
  [Bolster AI](https://bolster.ai/blog/phishing-threat-intelligence?utm_source=chatgpt.com)

**2. OpenPhish**

* **Free community feed**: Updates approximately every **12 hours**.
* **Premium feed**: Updates as frequently as **every 5 minutes**, and includes extra metadata (e.g., targeted brand, language, country).  
  [Bolster AI](https://bolster.ai/blog/phishing-threat-intelligence?utm_source=chatgpt.com)[wiz.io](https://www.wiz.io/academy/must-follow-threat-intel-feeds?utm_source=chatgpt.com)

**3. PhishTank (by Cisco Talos)**

* Community-driven: Users submit suspected phishing URLs, and the community votes on validity.
* Data is accessible via API or downloadable, free to use (with some license restrictions).  
  [Bolster AI](https://bolster.ai/blog/phishing-threat-intelligence?utm_source=chatgpt.com)[Wikipedia](https://en.wikipedia.org/wiki/PhishTank?utm_source=chatgpt.com)

**4. Spamhaus Domain Block List (DBL)**

* A trusted DNS-based blocklist including domains associated with phishing, malware, spam, and abuse.
* Continuously maintained and frequently updated.
* Widely used in email gateways and security filters.  
  [Wikipedia](https://en.wikipedia.org/wiki/The_Spamhaus_Project?utm_source=chatgpt.com)[Bolster AI](https://bolster.ai/blog/phishing-threat-intelligence?utm_source=chatgpt.com)[SOCRadar® Cyber Intelligence Inc.](https://socradar.io/the-ultimate-list-of-free-and-open-source-threat-intelligence-feeds/?utm_source=chatgpt.com)

**5. URLhaus (by abuse.ch)**

* Focuses on malicious URLs used in campaigns (e.g., phishing, malware).
* Provides feeds in multiple formats (ASN, country-specific, TLD) for automated integration.  
  [wiz.io](https://www.wiz.io/academy/must-follow-threat-intel-feeds?utm_source=chatgpt.com)[hunt.io](https://hunt.io/glossary/best-threat-intelligence-feeds?utm_source=chatgpt.com)

**6. PhishFort / Spamhaus Collaboration**

* PhishFort maintains a real-time blocklist of phishing and impersonation domains.
* This data is shared with and distributed by Spamhaus, enhancing reach and reliability.  
  [The Spamhaus Project](https://www.spamhaus.org/resource-hub/phishing/phish-fort-and-spamhaus-working-together/?utm_source=chatgpt.com)

**7. Jarelllama’s Scam-Blocklist (GitHub)**

* Automatically aggregates newly registered scam and phishing domains **daily** (around 16:00 UTC).
* Available in Adblock Plus or wildcard formats; ideal for downloading and consuming in your tooling.  
  [GitHub](https://github.com/jarelllama/Scam-Blocklist?utm_source=chatgpt.com)

**Summary Table**

| **Source** | **Update Frequency** | **Format / Access** | **Highlights** |
| --- | --- | --- | --- |
| **PhishStats** | Every ~90 minutes | API / CSV | Real-time composite feed from multiple sources |
| **OpenPhish** | 12 hrs (free) / 5 min (paid) | Feed / API | Fast updates with rich metadata (premium) |
| **PhishTank** | Continuous | API / Download | Community-verified phishing URLs |
| **Spamhaus DBL** | Continuous | DNSBL / API | High reputation list of phishing/malicious domains |
| **URLhaus** | Continuous | API / CSV feeds | Structured feeds by ASN, country, TLD |
| **PhishFort via Spamhaus** | Real-time | Shared blocklist | Combines PhishFort’s insights with Spamhaus delivery |
| **Scam-Blocklist (GitHub)** | Daily (~16:00 UTC) | File downloads | Newly registered scam/phishing domains |

**Recommendation for Integration**

To maximize coverage and freshness:

1. **Primary feed**: Use **OpenPhish (premium)** or **PhishStats** for near-real-time feed access and easy integration.
2. **Supplementary validation**: Cross-check with **PhishTank** for user-validated confirmations.
3. **Add domain block coverage**: Leverage **Spamhaus DBL** and **PhishFort data** for broader domain protection.
4. **Catch newly registered domains**: Incorporate **Scam-Blocklist** to detect new malicious domain creations early.
5. **For URL-specific threats**: Integrate **URLhaus** if targeting suspicious URLs beyond just domains.

**Example Integration Workflow**

1. **Fetch continuously** from a real-time feed (e.g., OpenPhish premium).
2. **Enrich or validate** entries via PhishTank API.
3. **Block domains** using Spamhaus DBL and/or PhishFort lists.
4. **Track emerging threats** via daily imports from Scam-Blocklist.
5. **Include URL-level detection** using URLhaus feeds for phishing pages.