Updated Sender Analysis Rules

1. Spoofed Domains

Description: Check if the sender's domain is a known spoof or lookalike domain.

Example: `paypa1.com` instead of `paypal.com`.

How It Works: Compare the sender's domain against a list of legitimate domains and their common spoofs.

2. Unusual Sender Addresses

Description: Flag emails from addresses with random or suspicious patterns.

Example: `support@random123.com` or `user@xyz.abc`.

How It Works: Use pattern matching to detect unusual email address formats.

3. Domain Age

Description: Flag emails from newly registered domains (e.g., less than 30 days old).

How It Works: Use a WHOIS lookup to determine the domain's registration date.

4. SPF/DKIM/DMARC Validation

Description: Verify if the sender's domain has valid SPF, DKIM, and DMARC records.

How It Works: Check the domain's DNS records for proper email authentication.

5. ReplyTo Address Mismatch

Description: Check if the "ReplyTo" address differs from the "From" address.

How It Works: Compare the "From" and "ReplyTo" headers in the email.

6. IP Reputation & Geolocation

Description: Ensure the sender's IP address belongs to the same country as the domain's registration.

How It Works:

1. Use a WHOIS lookup to determine the domain's registration country.

2. Use an IP geolocation API to determine the sender's IP country.

3. Flag emails where the IP country does not match the domain registration country.

7. Reverse WHOIS Lookup

Description: Identify who registered the domain and check for suspicious patterns.

How It Works: Use a WHOIS lookup to check for recently registered domains, fake registration details, or domains registered by known malicious actors.

8. MX (Mail Exchange) Records

Description: Verify if the sender's domain has legitimate mail servers.

How It Works: Check the domain's MX records to ensure they point to valid mail servers.

9. Lookalike Domains (Typosquatting)

Description: Detect minor alterations in domain names that mimic legitimate domains.

Example: `g00gle.com` instead of `google.com`.

How It Works: Use algorithms to measure similarity between the sender's domain and known legitimate domains.

10. Historical Email Patterns

Description: Check if the sender has a history of legitimate communication with the recipient.

How It Works: Analyze past emails to establish a baseline of normal behavior and flag anomalies.

11. Use of Disposable or Free Email Services

Description: Identify if the email is sent from temporary or disposable email providers.

Example: `10minutemail.com`, `mailinator.com`.

How It Works: Maintain a list of known disposable email domains and flag emails from these domains.

How These Rules Work Together

1. Input: An email is received.

2. Sender Analysis:

Check for spoofed domains and unusual sender addresses.

Validate SPF/DKIM/DMARC records.

Perform IP reputation and geolocation checks.

Conduct a reverse WHOIS lookup.

Verify MX records.

Detect lookalike domains.

Analyze historical email patterns.

Check for disposable email services.

3. Scoring:

Assign scores to each rule based on risk level.

Calculate a total score for sender analysis.

4. Classification:

If the total score exceeds a threshold, classify the email as suspicious.

Benefits of These Rules

Comprehensive Analysis: Combines multiple layers of sender verification.

Proactive Detection: Identifies phishing attempts before they reach the user.

Adaptability: Can be updated with new rules and data sources.