Sehr gut. Unten findest du eine **erweiterte Liste** verdächtiger Keywords, aufgeteilt nach **Betreff**, **Absender**, **Textinhalt**, **technische Trigger** und **Social-Engineering-Phrasen**. Diese Keywords sind speziell dafür geeignet, Spam-, Phishing- und betrügerische E-Mails **frühzeitig zu erkennen**.

🟥 BETREFF (`Subject`)

Weitere verdächtige Phrasen und Wörter, die häufig in Phishing- und Scam-Mails verwendet werden:

- „Letzte Chance“
- „Letzte Erinnerung“
- „Zahlungsverzug“
- „Zahlung erforderlich“
- „Ihr Konto ist in Gefahr“
- „Sicherheitswarnung“
- „Aktualisieren Sie Ihre Informationen“
- „Dringende Mitteilung“
- „Verifizierungsanfrage“
- „Neuer Loginversuch erkannt“
- „Ihr Konto wurde kompromittiert“
- „Wichtige Mitteilung“
- „Ungewöhnliche Aktivitäten“
- „Jetzt handeln“
- „Aktion erforderlich“
- „Benachrichtigung über verdächtige Aktivität“
- „Systembenachrichtigung“
- „Bestellbestätigung“ (wenn du nichts bestellt hast)

🟧 ABSENDER (`From`, `Return-Path`)

Zusätzliche Anzeichen in der E-Mail-Adresse oder Domain:

- „-security“
- „-verifikation“
- „user-update“

- „login-alert“
- „sicherheitscenter“
- „kunden-support“
- „noreply@paypal-security.com“
- „verify-apple@icloud-alert.com“
- Domains mit:
    - `xn--` (IDN-Spoofing)
    - `update-` oder `secure-` Prefix
    - `email-verification`
    - Zahlencode-Domains (z. B. `secure12345-login.net`)
    - kostenlose Hosting-Domains wie `.tk`, `.ml`, `.ga`, `.cf`, `.gq`

🟩 MAIL-INHALT (Body, HTML, Plaintext)

Häufige Trigger-Phrasen und Begriffe:

- „Jetzt bestätigen“
- „Daten eingeben“
- „Sie müssen handeln“
- „Kostenpflichtig, wenn Sie nicht reagieren“
- „Konto wird geschlossen“
- „Verifizierungsprozess“
- „Zahlung ausstehend“
- „Zahlung nicht erfolgt“
- „Nicht autorisierte Zahlung“
- „Zurückerstatten“
- „Jetzt überweisen“
- „Aufladung erforderlich“
- „Laden Sie das Dokument herunter“
- „Datei im Anhang“
- „Dokument geöffnet werden“
- „Sensible Daten“
- „Verschlüsseltes Dokument“

- „Passwort erforderlich“
- „Ungewöhnliches Verhalten“
- „Aktivitätsbenachrichtigung“
- „Apple ID wurde gesperrt“
- „Neues Gerät erkannt“
- „Verdächtige IP-Adresse“

🟦 TECHNISCHE INDIZIEN (HTML, Anhänge, Links)

Diese Begriffe deuten auf potenziell **schädlichen Code oder Anhänge**:

- `src="data:text/html;base64,..."`
- `.scr`, `.vbs`, `.exe`, `.js`, `.jar`, `.zip`, `.rar`
- `<form>`-Tags im Mailbody
- `onclick=`, `onload=`, `document.write(`
- verdächtige Linkverweise wie:
  - `bit.ly`, `tinyurl.com`, `shorte.st`, `ow.ly`
  - Redirect-Links mit `?redirect=`
  - Missmatch zwischen Linktext und URL

🟨 SOCIAL ENGINEERING PHRASES

Diese Phrasen versuchen psychologisch zu drängen:

- „Wenn Sie nicht handeln, …“
- „Sofortiger Zugriff“
- „Verpassen Sie diese Gelegenheit nicht“
- „Vertraulich“
- „Nur für Sie“
- „Ihre Daten wurden kompromittiert“
- „Diese Nachricht wird automatisch gelöscht“
- „Dies ist keine Werbung“
- „Wichtig für Ihre Sicherheit“
- „Bitte vertrauen Sie uns“

✅ HINWEIS ZUR ANWENDUNG

Du kannst diese erweiterten Listen verwenden, um:

- **Listenbasierte Scans** durchzuführen (`any(keyword in ...)`)
- **Gewichtete Prüfungen** umzusetzen (höhere Punkte bei technisch gefährlichen Mustern)
- **Individuelle Keyword-Gruppen** je nach Betreff, Body, Sender

Wenn du willst, kannst du die Keywords auch **in JSON/YAML-Dateien** speichern, um sie dynamisch zu laden und leicht zu pflegen.

Wenn du eine Blacklist-, Keyword- oder Regelverwaltungsstruktur brauchst, erkläre ich sie dir sehr gerne. Sag einfach Bescheid.