Herramienta de Detección de Correos Phishing

1. Diseño de la Herramienta

La herramienta fue desarrollada como un sistema automático capaz de detectar correos electrónicos sospechosos de phishing en una cuenta Gmail, usando una combinación de técnicas heurísticas, APIs de seguridad, y análisis de contenido. Está escrita en Python y estructurada en módulos: conexión, análisis, puntuación y reporte.

Se diseñó con el objetivo de ser escalable, automatizable e integrable en flujos de trabajo reales, con enfoque profesional y comercial.

Una de las decisiones clave fue empaquetar la herramienta como .exe para facilitar su uso en entornos no técnicos, como pequeñas oficinas o clientes sin formación en ciberseguridad.

De este modo, no es necesario abrir el código ni usar una terminal: solo se ejecuta y trabaja automáticamente en cualquier PC con Windows, aunque también se generó aparte para Linux.

2. Funcionalidad

La herramienta permite:

- Conectarse a una cuenta **Gmail real mediante IMAP**, utilizando credenciales OAuth o contraseña de aplicación.

- Leer correos nuevos y analizar su contenido (remitente, asunto, cuerpo, enlaces y adjuntos).

- Identificar señales comunes de phishing como:

    - Enlaces ofuscados o en base64.
    - Dominios o remitentes sospechosos.
    - Lenguaje alarmante o genérico.
    - Adjuntos peligrosos (.exe, .bat, .js, .zip).

- Consultar APIs de reputación como:

    - **Google Safe Browsing**.
    - **OpenPhish**.

- Asignar una **puntuación de riesgo** con base en los indicadores anteriores.

- **Etiquetar automáticamente los correos peligrosos** en la cuenta Gmail con la etiqueta “posible-phishing”.

Todo esto ocurre sin necesidad de intervención del usuario. Al ejecutar el .exe, los cambios se reflejan directamente en la bandeja de entrada de Gmail, marcando los correos peligrosos de forma clara.

Además, para facilitar las pruebas sin necesidad de introducir datos personales ni acceder a una cuenta propia, la herramienta ya viene preconfigurada con una cuenta de correo de prueba que contiene múltiples ejemplos reales de phishing. Esto permite demostrar toda la funcionalidad de la aplicación de forma inmediata, segura y efectiva, ideal para presentaciones, auditorías y formación.

Durante el desarrollo, se realizaron pruebas reales con más de 50 correos de phishing recopilados de fuentes públicas y campañas simuladas. Esto ayudó a ajustar los umbrales de puntuación y mejorar la fiabilidad de detección.

3. Uso Comercial y Monetización

Esta herramienta fue desarrollada con una visión comercial clara. La idea es ofrecer el servicio de análisis de seguridad de correos electrónicos a empresas, profesionales independientes o usuarios preocupados por la ciberseguridad.

Se utiliza una cuenta de correo de prueba conectada mediante APIs para:

- Mostrar en tiempo real cómo se detectan amenazas reales.
- Entregar análisis detallados a los clientes como valor añadido.
- Ofrecer el servicio en modalidad SaaS (Software como Servicio) o auditoría puntual.

Esto nos permite monetizar el uso de la herramienta a través de:

- Planes de suscripción para monitoreo continuo.
- Servicios por demanda (auditoría puntual de cuentas).
- Consultoría y personalización del sistema para entornos específicos.

4. Ventajas

- **Automatización completa** del análisis de correos.
- **Uso de APIs confiables** para detección más precisa.
- **Aplicación práctica y vendible**, validada con ejemplos reales.
- **Interfaz adaptable** y fácil de ampliar.
- **No requiere conocimientos técnicos**: el .exe lo hace accesible a cualquier persona.

5. Limitaciones y Futuras Mejoras

- Dependencia de conexión estable a internet y APIs externas.

- Actualmente está centrado en Gmail; en el futuro se puede extender a Outlook, Yahoo, etc.

- Se planea incorporar **modelos de inteligencia artificial** para mejorar la precisión de detección y reducir falsos positivos.

Resumen del Código

Este script en Python **detecta posibles correos de phishing automáticamente** en una cuenta de Gmail. Funciona de la siguiente manera:

1. **Se conecta a tu correo** usando IMAP.
2. **Lee correos no leídos** de la bandeja de entrada.
3. Analiza:
    - **Contenido del correo** (cuerpo y asunto).
    - **Remitente**.
    - **Enlaces incluidos**.
    - **Adjuntos sospechosos**.
4. Usa **listas de palabras clave y dominios sospechosos** (como "verifica tu cuenta", "haz clic aquí", etc.) para evaluar si es phishing.
5. Consulta servicios como:
    - **Google Safe Browsing**
    - **OpenPhish**

6. Si el correo parece sospechoso:
    - Se **etiqueta automáticamente** como posible-phishing en Gmail.
    - Se **mantiene como leído** o no leído dependiendo del resultado.

¿Cómo detectar el phishing?

El sistema utiliza listas y patrones como:

- Palabras clave sospechosas ("verifica tu cuenta", "ganaste un premio", etc.).
- Dominios peligrosos o acortadores (bit.ly, tinyurl.com...).
- Enlaces codificados en base64.
- Correos que usan lenguaje urgente ("expira en 24h", "acción inmediata"...).
- Archivos adjuntos sospechosos (.exe, .zip, .bat, etc.).

Cada señal suma puntos. Si la **puntuación supera un umbral**, se considera posible phishing.

Credenciales de Acceso para Pruebas:

Para facilitar las demostraciones y pruebas de la herramienta sin necesidad de usar cuentas personales, se proporciona una cuenta de correo de prueba preconfigurada. Esta cuenta contiene múltiples correos reales de phishing recopilados y es utilizada por defecto al ejecutar la aplicación.

Credenciales de acceso a la cuenta de prueba:

- 📧 Correo electrónico: wolfcuentaprueba@gmail.com
- 🔑 Contraseña: pepe2001. (tiene un punto al final)

⚠️ *Esta cuenta está diseñada únicamente para fines educativos y demostrativos. No se recomienda usarla para el envío o recepción de correos personales.*