

Phisherescudo 3D

Datos Persoais

Miguel Colmenero Fernández
Noelia Pena Romero
Divina Pastora Franciscanas Ourense

Resumo

O proxecto consiste no deseño dunha APP orientada á protección contra ciberataques no fogar. O phishing é un fraude dixital que tenta enganar ás persoas para roubar contraseñas e datos persoais. Para detectalo, crearemos un pequeno sistema automático con capacidade de analizar correos electrónicos e determinar se poderían ser un intento de phishing. Empregaremos un buzón de proba Mamilpit e un sistema de detección n8n. Despois procedermos ao desenvolvemento en 3D do phisherescudo. Para empregar o 3D axudarémonos con tecnoloxía fusión 360º para crear e optimizar modelos tridimensionais precisos no entorno dixital. Despois de deseñar a carcasa do router, empregaremos PCBs creados por nós, e moita electrónica para que sexa o mellor invento creado por humanos.

Introducción

A idea principal do proxecto é construír un entorno de probas seguras onde os correos poidan ser analizados pola Intelixencia Artificial que lles asignará unha puntuación de risco. Segundo a puntuación, o sistema decidirá se o correo é seguro ou debe considerarse perigoso.

Os obxectivos educativos do proxecto son:

- ➔ Explicar que é o phishing.
- ➔ Demostrar como a Intelixencia Artificial pode axudar a mellorar a ciberseguridade.
- ➔ Amosar como se poden automatizar procesos sen intervención humana.
- ➔ Concienciar sobre a importancia de analizar os correos antes de confiar neles.

Propósito do traballo

Aínda que é un prototipo educativo, este tipo de sistemas xa se empregan en empresas reais para protexer a empregados e clientes fronte a ataques dixitais. O proxecto amosa como combinando automatización e intelixencia artificial é posible crear ferramentas intelixentes que axuden a previr fraudes online.

Estudo do estado da arte

Mediante busca en redes, atopamos APP para detectar ataques por phishing:

- Scam Search (sitios web falsos, números de teléfono sospeitosos, etc.)
- Virustotal (detectar malware)
- CRDF labs (URLS, correos electrónicos fraudulentos)
- Isit phishing
- Desenmascara.me
- GlobalScam

Hipótese

Deseñar un sistema automático de análise de correos electrónicos para previr ciberataques a través dun buzón de proba Mailpit e un sistema de detección n8n.

Material e Métodos

O proxecto emprega dúas ferramentas principais:

- Mailpit: é un programa que actúa como un buzón de correo de proba. Permite recibir emails nun entorno controlado e seguro, sen empregar unha conta real.
- n8n: é unha ferramenta que permite crear automatizacións. Neste proceso será o “cerebro” que conecta todo.

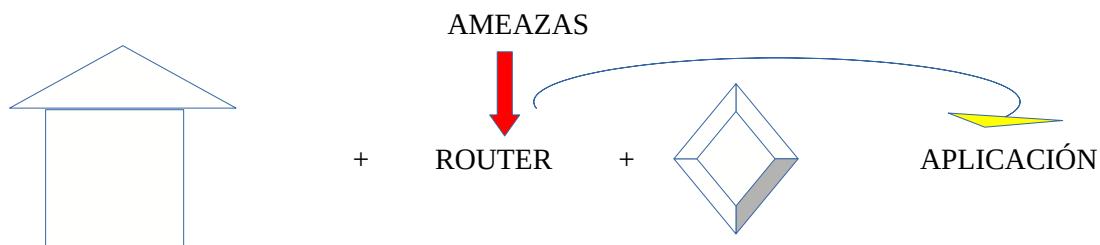
O funcionamento será o seguinte:

- 1- Chega un correo ao buzón de proba (Mailpit).
- 2- n8n detecta automaticamente ese novo correo.
- 3- n8n envía o contido do correo a un sistema de intelixencia artificial (como ChatGPT).
- 4- A intelixencia artificial analiza o texto e devolve unha puntuación de risco (por exemplo, de 0 a 100).
- 5- Se a puntuación é alta, o sistema marca o correo como posible phishing.

Por outra banda, empregaremos o programa Fusión 360º para deseñar a carcasa do router.

Resultados

Unha vez integrado no router o sistema de detección de phishing poderase empregar nos fogares este sistema para previr fraudes dixitais.



Conclusiones

Aprender a detectar ataques de phishing é fundamental para a sociedade

Bibliografía

Implementación y evaluación de un sistema de seguridad anti phishing para la protección de la información utilizando un firewall en procedimientos académicos en línea. 2022.

Hacker. 2008. Anaya multimedia.

Destripa la red. 2007. Anaya multimedia.