//UCIENCIA/23
CONVENCIÓN CIENTÍFICA INTERNACIONAL

Temática: Inteligencia Artificial y Ciencias de Datos aplicadas a la ciberseguridad

Modelo para la detección de ataques de phishing contra el servicio de correo electrónico

Antonio Hernández Dominguez [1*], Walter Baluja García [2]

[1] Universidad de las Ciencias Informáticas (UCI), La Habana, 19370 Cuba. ahdominguez@uci.cu
[2] Ministerio de Educación Superior (MES), La Habana, 19370 Cuba. walterb@uci.cu

[*] Autor para correspondencia: ahdominguez@uci.cu

Resumen
El phishing es un método de suplantación de identidad electrónica en el que se utilizan técnicas de ingeniería social para engañar a los usuarios y revelar información sensible. Al destruir la confianza de los usuarios en las redes de datos, el phishing tiene un efecto negativo en el ciberespacio. Desafortunadamente, ninguna entidad es inmune a estos ataques, por lo que deben implementar un plan ordenado de prevención, con el objetivo de reducir los riesgos ante una exposición directa. Aunque la capacitación y el entrenamiento de los usuarios suele ser una medida muy eficaz, debe ser combinada con medidas técnicas, dada la creciente tendencia innovadora de los atacantes y la diversidad de los esquemas de ataque de phishing. En los últimos años se han utilizado diversos mecanismos para detectar ataques de phishing. El papel desempeñado por las técnicas de aprendizaje automático supervisado ha sido significativo, principalmente por los niveles de eficacia obtenidos en la detección de estos ataques. La precisión de la solución anti-phishing depende del conjunto de rasgos, los datos de entrenamiento y el algoritmo de autoaprendizaje. Por tanto, el presente artículo tiene el objetivo de proponer un modelo que permita aumentar la eficacia en la detección de ataques de phishing contra el servicio de correo electrónico.

Palabras clave: Phishing, detección de Phishing, Aprendizaje Automático, correo electrónico.