UIDE
Powered by
Arizona State University

eig Business School

Maestría en

CIBERSEGURIDAD

Trabajo de investigación previo a la obtención del título de

Magíster en Ciberseguridad

AUTORES:

Ing. Diana Patricia Macancela Macero

Ing. María Fernanda Ramos Villacreses

Ing. Miguel Ángel Rojas Bravo

Ing. Geovanny Fernando Samaniego Sani

TUTORES:

Cortés Lopez Alejandro

Reyes Chacón Iván Galo

Simulación de ataques de Phishing y desarrollo de un Plan de Concienciación para mejorar la seguridad cibernética a nivel de usuario final

Quito, Octubre 2024

Resumen

Actualmente, el phishing es una de las técnicas de ingeniería social más empleadas para engañar a las personas y obtener información sensible, como credenciales y datos financieros, entre otros, a través de correos electrónicos. En Ecuador, la evolución del phishing refleja un aumento de delitos informáticos, lo que destaca la necesidad de proteger los datos y fomentar la colaboración entre autoridades. El objetivo de este proyecto de investigación es diseñar y ejecutar simulaciones de ataques de phishing, para lo cual primero se diseñaron un conjunto de plantillas basadas en los tipos de ataques más comunes creando correos con carácter de urgente. Luego, se configuró una herramienta seleccionada para llevar a cabo las simulaciones en un entorno controlado. Después de ejecutar los ataques, se realizó un monitoreo y se registró las respuestas de los usuarios, como: la cantidad de personas que abrieron enlaces, hicieron clic e ingresaron datos, mismos que fueron recopilados y analizados para identificar patrones de comportamiento y posibles vulnerabilidades. Se utilizó la herramienta GoPhish, que fue configurada en una máquina virtual de Kali Linux con la cual se simularon los ataques realistas y se evaluó la conciencia de las personas sobre estos riesgos. Los resultados obtenidos nos permitieron elaborar un plan de concientización, que está basado en la definición de estrategias, cuyo objetivo es educar y sensibilizar a los usuarios sobre los riesgos inherentes al phishing y proporcionarles las recomendaciones para mejorar la seguridad y evitar caer en este tipo de ataques.

Palabras Clave: Phishing, Simulación, Ataque, Victima, Vulnerabilidades, Concienciación, Gophish

Abstract

At the present, phishing is one of the most widely used social engineering techniques to deceive people and obtain sensitive information, such as credentials and financial data, among others, through emails. In Ecuador, the evolution of phishing reflects an increase in cybercrime, which highlights the need to protect data and foster collaboration between authorities. The objective of this research project is to design and execute simulations of phishing attacks, for which we first designed a set of templates based on the most common types of attacks by creating urgent emails. Then, a selected tool was configured to perform the simulations in a controlled environment. After executing the attacks, we monitored and recorded user responses, such as the number of people who opened links, clicked and entered data, which were collected and analyzed to identify behavioral patterns and potential vulnerabilities. We used the GoPhish tool, which was configured on a Kali Linux virtual machine to simulate realistic attacks and evaluate people's awareness of these risks. The results obtained allowed us to elaborate an awareness plan, which is based on the definition of strategies, whose objective is to educate and sensitize users about the risks inherent to phishing and provide them with recommendations to improve security and avoid falling into this type of attacks.

Keywords: Phishing, Simulate, Attack, Victim, Vulnerabilities, awareness, Gophish