Resumen

En la actualidad se vive un proceso pos pandémico en el que el auge de los ataques de Ingeniería Social especialmente tipo Phishing, se aprovechan del eslabón más débil de la ciberseguridad que es el ser humano. Los usuarios están ahora expuestos constantemente en Internet y al uso de dispositivos electrónicos por lo que son susceptibles a este tipo de ataques. El objetivo del presente estudio es desarrollar una plataforma web para entrenamiento de ataques de Phishing en correos electrónicos mediante la utilización de metodologías ágiles, al combinar seguridad y psicología cognitiva. Para el cumplimiento del mismo, se utilizaron los lineamientos de la metodología de diseño de la ciencia. Así mismo, para la revisión de literatura se aplicó la guía metodológica de Bárbara Kitchenham, cuyos resultados indican que una manera de implementar seguridad cognitiva es mediante la aplicación de teorías de juego. Por esta razón, se diseñó e implementó un algoritmo con teorías de juego capaz de clasificar por el nivel de conocimiento para el proceso de entrenamiento de los usuarios en la plataforma web, la cual se desarrolló mediante la metodología ágil SCRUM. Los resultados del entrenamiento revelan que, en una población de 59 usuarios, entre ellos 33 estudiantes y 26 profesionales, los profesionales según su score fueron en su mayoría por los caminos establecidos como difíciles, es decir tuvieron una alta tasa de éxito y por ende una alta detección. Por el contrario, los estudiantes fueron por los caminos intermedios y difíciles, con un nivel de detección media. Cabe recalcar que se realizó un análisis del nivel de detección por la edad y género. Por otra parte, se implementó en la plataforma un cuestionario de percepción de riesgo con el fin de obtener el nivel de percepción de los usuarios. No obstante, este es un primer pilotaje para lograr su validación a nivel psicológico.

Palabras clave: Phishing, seguridad cognitiva, psicología cognitiva, percepción de riesgo.

Abstract

We are currently experiencing a post-pandemic process in which the rise of social engineering attacks, especially phishing attacks, are taking advantage of the weakest link in cybersecurity, which is the human being. Users are constantly exposed to the Internet and electronic devices and are therefore susceptible to this attack. This study aims to develop a web platform for training Phishing attacks in emails using agile methodologies, combining security and cognitive psychology. For the fulfillment of the same, we used the guidelines of the Design Science methodology. Likewise, for the literature review, Barbara Kitchenham's methodological guide was applied, whose results indicate that one way to implement cognitive security is by using game theories. For this reason, an algorithm with game theories capable of classifying by knowledge level was designed and implemented for the user training process on the web platform, which we developed using the agile SCRUM methodology. The training results reveal that, in a population of 59 users, including 33 students and 26 professionals, the professionals, according to their score, mainly went through the paths established as complex, i.e., they had a high success rate and therefore a high detection. On the contrary, the students went through the intermediate and challenging paths with a medium detection level. We should emphasize that we perform an analysis of the level of detection by age and gender. On the other hand, a risk perception questionnaire was implemented on the platform to obtain the users' level of perception. However, this is the first pilot to achieve its validation at a psychological level.

Keywords: Phishing, cognitive security, cognitive psychology, risk perception.