



Abstracto

La ciberseguridad se ha convertido en uno de los conceptos más importantes de nuestros tiempos. Debido a los avances tecnológicos, desde edades más tempranas los estudiantes comienzan a utilizar dispositivos con acceso a la Internet. Esto significa que se debe introducir el tema de la ciberseguridad desde los grados (K-12). Se estará educando a la futura generación sobre los conceptos de ciberseguridad. La población de K-12 son los más vulnerables a los ataques cibernéticos. Se utilizó la taxonomía de Bloom para desarrollar los 3 módulos. El autor se aseguró que cada módulo funcionó en transmitir los conceptos.

Introducción

En la profesión de ciencias de computadoras, uno de los conceptos más importantes es la ciberseguridad. Dentro de este término, existen múltiples temas que forman este concepto. La ciberseguridad es la práctica de proteger equipos, redes y aplicaciones de software. Debido al incremento exponencial del uso del Internet por la pandemia y por los avances tecnológicos, ahora más que nunca es imperativo introducir el concepto. Los objetivos principales de este proyecto son:

- Introducir a los estudiantes de K-12 con los conceptos generales de la ciberseguridad.
- Introducir a los estudiantes la importancia de la ciberseguridad.
- Dar a conocer las amenazas cibernéticas más comunes y como defenderse contra estas.
- Proveer educación al estudiante sobre las medidas de defensa que puede tomar en contra de estos ataques.

Literatura

La percepción general del público es que los ataques cibernéticos ocurren con más frecuencia entre los individuos de edades entre 50-80 años. El grupo que en realidad está en mayor riesgo son entre las edades de 18-29 años. Son la población en mayor riesgo por la frecuencia que están en línea lo cual aumenta sus probabilidades de ser víctimas de un ciberataque. Un estudio realizado en el 2021 encontró que el 49% de los guardianes de los niños nunca habían revisado los accesos que tenían en sus dispositivos electrónicos [1]. El problema que esto causa es que los niños normalmente utilizan los dispositivos de los padres para acceder el Internet. Luego estos dispositivos son utilizados por los padres y se conectan en la red de la organización y esta queda infectada.

Exposición del Problema

El objetivo principal de toda institución académica es proveerles la mejor educación a los estudiantes. Esta información debe ser transmitida de la mejor manera posible dependiendo el nivel o grado que el educador esté enseñando. Debido a la rápida evolución tecnológica [2], dice que los niños comienzan a utilizar dispositivos electrónicos con acceso a el Internet desde edades más tempranas. El darle un dispositivo electrónico con acceso a el Internet a un niño que no ha sido educado sobre los riesgos que existen en el Internet, es el equivalente a darle un carro sin saber guiarlo. Por tal razón [2], alude a que el crimen cibernético ha aumentado consistentemente cada año y a consecuencia de, el riesgo que los niños corren en el Internet incrementa Bele et al [3], menciona que los niños y adolescentes representan la población más apta con relación al uso de la tecnología. Pero al mismo tiempo son la población más vulnerable. Con estos módulos se atacará este problema.

Metodología

Se crearon tres módulos y cada módulo discute un tema importante acerca de la ciberseguridad. El formato de los módulos fue basado en la taxonomía de Bloom. La taxonomía de Bloom es un sistema de clasificación utilizada para definir y distinguir diferentes niveles de cognición. Los temas seleccionados para los módulos se basaron en la revisión de literatura y fueron creados para ser enseñados en un orden específico, desde lo más simple hasta lo más detallado. Por tal razón, los temas que se propusieron fueron:

1. Módulo 1: Ataques Cibernéticos
2. Módulo 2: Ataques de Ingeniería Social
3. Módulo 3: Ransomware

En la Figura 1 se muestra los módulos creados y en el orden que se deben enseñar.



Figura 1

Orden Secuencial de los Módulo

Al utilizar la estructura de la taxonomía de Bloom, cada módulo llevo la misma estructura.

Metodología continuación

La estructura de los módulos es la siguiente:

1. Descripción General del Módulo
2. Objetivos de Aprendizaje
3. Contenido del Módulo
4. Material instruccional
5. Hojas de Evaluación

La Figura 2 demuestra la estructura utilizada para los módulos. Esta estructura fue la siguiente:



Figura 2

Estructura de los Módulos

Cada uno de los módulos incluye una presentación de PowerPoint de 15 a 20 diapositivas. Esto ayuda al educador a reforzar visualmente los conceptos discutidos en cada uno de los módulos. También, en las herramientas instruccionales se encuentran hojas de evaluación. A continuación, en la Figura 3 podemos ver la pirámide de la jerarquía de la taxonomía de Bloom, la cual fue utilizada para crear los módulos, las hojas de evaluación y las herramientas instruccionales.



Figura 3
Taxonomía de Bloom y sus niveles

Conclusión

El objetivo principal de los 3 módulos que fueron creados fue introducir a los estudiantes a los conceptos de Ataques Cibernéticos, Ataques Ingeniería Social y Ataques de Ransomware. Los módulos se harán disponibles en la base de datos de la Universidad Politécnica de Puerto Rico para el uso de educadores, al igual que las herramientas de aprendizaje. Los enlaces a las plataformas de manejo de aprendizaje también serán incluidos en la base de datos para el uso público. Estas plataformas contienen lecciones interactivas con videos y juegos educativos. Para finalizar, como trabajo futuro se puede utilizar la taxonomía de Bloom para expandir el contenido de los módulos para abarcar más temas.

Trabajo Futuro

Como trabajo futuro, se debería dar seguimientos a los módulos y tratar de que se implementen en el currículo escolar. Así, el autor puede ver si estos son eficientes en enseñar los conceptos y se si está cumpliendo los 6 niveles de taxonomía de Bloom.

Al trabajar como maestro, se tratará de implementar los módulos en el currículo escolar para poder crear retrospectiva acerca de ellos.

Con las hojas de evaluación que fueron creadas para cada módulo servirán de guía para el educador poder medir que los estudiantes estén comprendiendo y aplicando los conceptos aprendidos. Cuando los módulos se implementen en un currículo escolar se medirá la eficacia y se harán las modificaciones necesarias.

Reconocimientos

Quiero agradecer a las siguientes personas que ayudaron en formar este proyecto como requisito de la Maestría de Ciencias de Computadora. Se le agradece al Doctor Alfredo Cruz que fue mentor durante este proyecto. A la Dra. Garriga, Dr. Vicente, Dr. Duffany y a todos los que lograron que este sueño se convirtiera en realidad.

Referencias

[1] Admin, "HSB: Young adults most likely to be targeted in cyber attack," *Claims Journal*, 20-Sep-2016. [Online]. Available: <https://www.claimsjournal.com/news/national/2016/09/20/273559.htm>. [Accessed: 12-Mar-2023].

[2] A. A. A. Shamsi, "Effectiveness of Cyber Security Awareness Program for young children: A case study in UAE," *International Journal of Information Technology and Language Studies*. [Online]. Available: <https://journals.sfu.ca/ijitls/index.php/ijitls/article/view/81>. [Accessed: 18-Apr-2023].

[3] J. L. Bele, M. Dimc, D. Rozman, and A. S. Jemec, "Raising awareness of cybercrime—the use of education as a means of prevention and protection," *International Association for Development of the Information Society*, 30-Nov-2013. [Online]. Available: <https://eric.ed.gov/?id=ED557216>. [Accessed: 18-Apr-2023].