Introducción a la Ciberseguridad a Través de Amenazas Cibernéticas

Ricardo Raúl Vaccaro
Maestría en Ciencia de Computadoras
Mentor: Alfredo Cruz, Ph.D.
Departamento de Ingeniería Eléctrica y de Computadoras y Ciencia en Computadoras
Universidad Politécnica de Puerto Rico

Resumen*—La ciberseguridad se ha convertido en uno de los conceptos más importantes de estos tiempos. Esto se debe al avance exponencial tecnológico que ha ocurrido en el siglo XXI. Debido a este avance tecnológico, los estudiantes comienzan a utilizar dispositivos con acceso a la Internet desde edades más tempranas. Esto significa que hay que introducir el tema de la ciberseguridad desde grados más bajos K-12 (Kínder a duodécimo) para ir educando a la futura generación sobre los conceptos de ciberseguridad y las amenazas cibernéticas que puedan identificarlas y no caer víctimas de estas. Por esta razón se desarrollaron tres módulos donde se explicó lo que es ciberseguridad y lo que esto conlleva. Se estaría educando acerca de la Internet, y las amenazas que se pueden encontrar. La población de K-12 es la más vulnerable a caer víctimas de ataques cibernéticos ya que están constantemente en línea lo cual incrementa las probabilidades de ser atacados. Al no estar educados en el tema de ciberseguridad, no reconocen que a pesar de ser una de las creaciones más importantes del siglo XX, en la Internet hay amenazas reales. Desde la pandemia la interacción virtual ha aumentado significativamente.*

Términos Claves – *criptografía, ingeniería social, malware, virus.*

INTRODUCCIÓN

En la profesión de ciencias de computadora, 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, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales. Debido al incremento exponencial del uso del Internet por la pandemia y por los avances tecnológicos, ahora más que nunca es imperativo conocer sobre el tema. Para presentar el concepto de ciberseguridad a los estudiantes de K-12, el autor hizo tres módulos. Estos fueron creados desde los conceptos más generales, hasta los más específicos para así facilitar el aprendizaje al estudiante. De esta manera, el estudiante lee los conceptos generales primero y luego los puede aplicar con el aprendizaje de los módulos.

Estos módulos contienen información, actividades de aprendizaje en línea interactivas, hojas de evaluación, ilustraciones y videos para todo tipo de estudiante. Los módulos fueron creados tomando en cuenta los 3 tipos de aprendizaje principales que son, aprendizaje kinestésico, visual y auditivo [1].

OBJETIVOS DEL PROYECTO

Los objetivos principales de este proyecto son:

- Presentar los conceptos generales de la ciberseguridad a los estudiantes de K-12.
- Presentar a los estudiantes la importancia de la ciberseguridad.
- Crear conciencia sobre lo que significa ser un ciudadano digital y el comportamiento seguro en el Internet.
- Dar a conocer las amenazas cibernéticas más comunes y como defenderse contra estas.
- Introducir los conceptos generales de Ataques Cibernéticos, Ingeniería Social y Ransomware.
- Proveer herramientas para los 3 tipos de aprendizaje principal: kinestésico, visual y auditivo.
- Proveer educación al estudiante sobre las medidas de defensa que puede tomar en contra de estos ataques.

Preguntas de Investigación

A continuación, se establecen las preguntas que ayudaron a desarrollar el proyecto.

- ¿Cómo se puede transmitir el concepto de ciberseguridad a los niños de grados K-12 de manera divertida?
- ¿Cuál es el orden eficiente para transmitir el contenido de los módulos a los niños de K-12?
- ¿Cuáles son los ataques o riesgos cibernéticos más comunes con los que se enfrentan los niños en los grados K-12?
- ¿Qué plataformas de sistema de manejo de aprendizaje son las más efectivas?

Literatura

La percepción general del público es que los ataques cibernéticos ocurren con más frecuencia entre los individuos de edades mayores de 50-80 años. Sin embargo, debido a los avances en la tecnología el uso de esta comienza cada vez más en una edad temprana. Por lo tanto, contrario a la percepción general, el grupo mayormente víctimas de ataques cibernéticos son entre las edades de 18 a 29 años. Esto es debido a que están en línea con más frecuencia, lo cual aumenta las probabilidades de ser víctima de un ciberataque [2].

Un estudio realizado en el 2019 mostró que el 42% de los niños entre las edades de 5 a 7 años tienen una tableta personal. Esto es un incremento de 7% en comparación con el año previo. Esto significa que niños de 5 a 7 años están conectados al Internet sin ningún tipo de conocimiento básico de seguridad. Un estudio realizado en el 2021 encontró que el 49% de los guardianes de los niños nunca habían revisado los accesos o "parental control" que tenían puesto para los niños en sus dispositivos electrónicos [3]. Esto presenta un doble problema, niños que están utilizando dispositivos conectados a el Internet sin conocimiento alguno sobre la ciberseguridad y los guardianes que tampoco tienen conocimiento acerca del tema. El problema que esto causa es que los niños normalmente utilizan los dispositivos de los padres para acceso el Internet. Estos dispositivos luego son llevados por los padres a sus trabajos y si han sido infectados cuando los hijos lo utilizaron, al conectarse a la red de la organización se infectará la misma.

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 este enseñando. Debido a la rápida evolución tecnológica, [4] 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 al Internet a un niño que no ha sido educado sobre los riesgos que existen, es el equivalente de darle un carro sin saber guiarlo y que lo use. En el transcurso ocurrirán accidentes.

Por tal razón [4] alude a que el crimen cibernético ha aumentado consistentemente cada año y a consecuencia de esto, el riesgo de que los niños corren en el Internet incrementa. Bele et al [5], 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.

Contratiempos y Barreras

La creación de estos módulos es relevante como proyecto final de Maestría porque está tratando de resolver un problema que se enfrenta en la vida real. La revisión de literatura respalda el problema que se estableció en la propuesta al igual que el método que se propuso utilizar para la enseñanza de ciberseguridad. Este tema fue de interés y fue escogido por varios motivos. Uno de los motivos es que, como educador de grados elementales de computadora, el investigador ha visto la falta de educación sobre temas de ciberseguridad. Otra razón es que también ha visto como los padres les dan sus celulares o tabletas a los hijos. Es impresionante lo hábil que son los niños con la tecnología y como desde tan pequeños saben utilizarla, por tal razón es importante educarlos desde pequeños. Una última

razón más personal, es que el investigador tiene dos sobrinos de cuatro y nueves años y una sobrina de ocho años y ha visto como los padres le dan sus dispositivos y siente que si está en posición de poder educar a la mayor cantidad de gente posible tiene el deber de hacerlo.

La mayoría de los colegios en Puerto Rico se rigen por el Departamento de Educación y por lo tanto los currículos tienen cierta uniformidad. Aunque el currículo puede cambiar de colegio a colegio. El lugar más razonable para implementar esta educación es en el colegio ya que los niños pasan la mayoría del día en ellos y es donde reciben su educación. Aparte de lo mencionado previamente, es digno como proyecto de Maestría porque indirectamente ataca un problema de seguridad nacional. La tecnología seguirá avanzando y las personas con ella. Por esto, hay que adaptarse o asumir las consecuencias.

Ya ha habido reportes de grupos de hackers controlados por naciones que han intentado penetrar infraestructura esencial. También está bastante documentando como Rusia hackeo las elecciones presidenciales del 2016. Si queremos crear ciudadanos que sepan contrarrestar estas amenazas, tenemos que comenzar a educarlos desde niños. Un ejemplo de la urgencia que deben de tener los gobiernos y educadores en implementar la educación de ciberseguridad en las escuelas y colegios por cuestiones de seguridad nacional es lo que ha ocurrido con la plataforma social conocida como TikTok.

Una noticia de "USA TODAY" publicada el 16 de noviembre de 2022 tiene como titular que el director del FBI admitió que TikTok es una amenaza a la seguridad nacional y está sumamente preocupado. Precisamente las edades que más utilizan esta plataforma social son los jóvenes adolescentes sin tener ningún conocimiento de que esta plataforma muestra un riesgo a la seguridad de la nación americana [6].

SOLUCIÓN AL PROBLEMA EXPUESTO

Para mitigar este problema de falta de educación acerca de la ciberseguridad desde los grados K-12 este proyecto propone desarrollar tres módulos educativos. Cuando se desarrollaron los módulos era importante tener en cuenta que la educación cuando es divertida y atractiva para los niños, estos muestran más interés en aprender [7].

Para los módulos que se propusieron se utilizaron plataformas de manejo de aprendizaje (LMS por sus siglas en ingles). Estas plataformas hicieron el aprendizaje interactivo porque mantuvieron al estudiante comprometido con los módulos en adición a material y actividades desarrolladas por el maestro. Los temas de los módulos fueron seleccionados basado en la revisión de literatura y los riesgos cibernéticos que con mayor frecuencia enfrentan los niños. Los módulos que se propusieron ayudarán a crear una generación educada sobre lo que es la ciberseguridad. Se planteó esto porque a consecuencia del conocimiento que se les estará transmitiendo en el colegio (K-12), sabrán practicar ciberseguridad una vez sean adultos. Ese es otro objetivo de crear los módulos y proveer material y ejercicios para los tres grupos de aprendizaje.

METODOLOGÍA

Para solucionar el problema se crearon tres módulos. Cada uno 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.

Este formato ha sido utilizado por educadores para desarrollar evaluaciones, currículos y métodos instruccionales. Al utilizar la estructura de la taxonomía de Bloom, cada módulo llevo la misma estructura.

La estructura es la siguiente:

- Descripción General del Módulo.
- Objetivos de Aprendizaje.
- Contenido del Módulo.
- Material Instruccional.

- Hojas de Evaluación.
- Referencias.
- Apéndice.

Los temas seleccionados para los módulos se basaron en la revisión de literatura y fueron creados para ser enseñados en un orden especifico, 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

Estos temas se consideraron los más importantes porque son los ataques que con más frecuencia atacan a niños.

El Módulo 1 provee una introducción general de lo que son ataques cibernéticos y términos generales importantes de conocer.

El Módulo 2 expone a los estudiantes a lo que son Ataques de Ingeniería Social, como reconocer este tipo de ataque, cómo y dónde puede ocurrir, que hacer en dicha situación y crear conciencia antes de dar información personal y/o oprimir cualquier enlace que aparenta ser de origen legítimo.

Por último, el Módulo 3 toca el tema de Ransomware. Es importante este tema porque este tipo de ataque está en aumento. También, se ha podido establecer que están apuntando a la infraestructura esencial de la nación como los hospitales.

Se utilizaron presentaciones de PowerPoint, videos y plataformas de manejo de aprendizaje (LMS). En adición, se crearon hojas de evaluación para que el educador se pueda asegurar que el estudiante está comprendiendo los conceptos presentados.

Los recursos educativos se encuentran en los apéndices correspondientes a cada Módulo. En el apéndice se puede encontrar el enlace a la presentación de PowerPoint del Módulo, enlace a videos y plataformas de manejo de aprendizaje. Las plataformas de manejo de aprendizaje se seleccionaron porque proveen reportes individuales de los estudiantes para ver su progreso a través de las lecciones.

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

Figura 1
Orden Secuencial de los Módulos

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

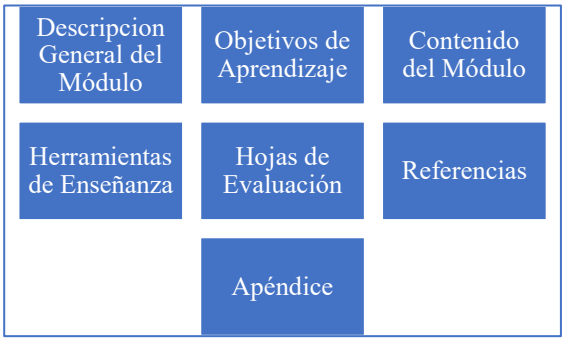


Figura 2
Estructura de los Módulos

La Descripción General de los Módulos provee al educador una descripción breve de la unidad del tiempo estimado de duración y trasfondo acerca del tema del módulo. Los objetivos de aprendizaje del módulo definen los objetivos esperados a cumplir en cada uno en términos del conocimiento adquirido por el estudiante como resultado de la lección del módulo.

El contenido del módulo provee información detallada de como el módulo o lección debe ser presentada además de ofrecer puntos de discusión para el educador.

Las herramientas de enseñanza son recursos adicionales provistos al educador que incluyen: presentación de PowerPoint, Hojas de Evaluación, enlaces a videos complementarios a los temas y enlaces a las plataformas de manejo de aprendizaje.

Cada uno de los tres 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.

En la Figura 3 se ofrece un ejemplo de una diapositiva de la presentación del Módulo 2: Ataques de Ingeniería Social. La diapositiva contiene un listado de los métodos más comunes para llevar a cabo Ataques de Ingeniería Social.

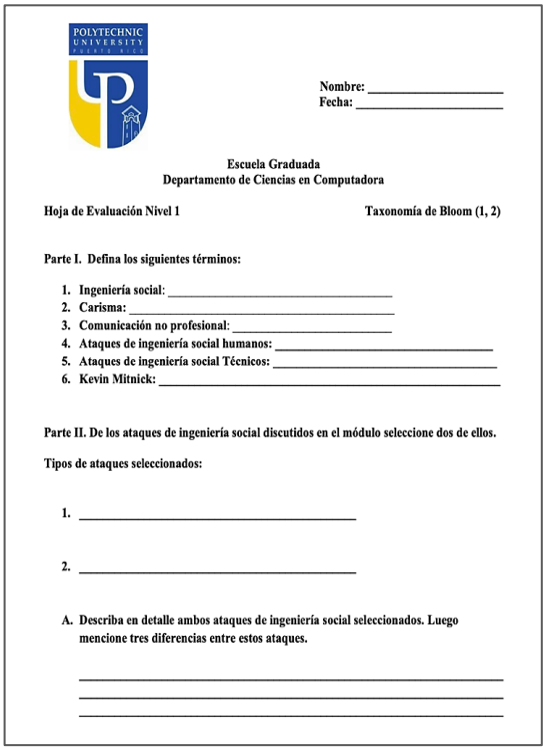
Figura 3
Ejemplo de una Diapositiva de la Presentación Ataques de Ingeniería Social

La Figura 4 muestra uno de los ejemplos de los videos que se utilizaron en el Módulo 3: Ransomware como parte de las Herramientas Instruccionales para el educador.

Figura 4
Herramientas Instruccionales: Ejemplo de Video Acerca de Ransomware

En adición, en las herramientas instruccionales se encuentran hojas de evaluación. Hay tres hojas de evaluación por módulo. Estas hojas se crearon para ser completadas durante cada lección. El propósito de las hojas de evaluación es que el educador pueda corroborar si los estudiantes están logrando los diferentes niveles de la taxonomía de Bloom.

La Figura 5 es un ejemplo de una de las hojas de evaluación. Las hojas de evaluación se diseñaron para evaluar 2 niveles de la taxonomía de Bloom.


POLYTECHNIC UNIVERSITY

Nombre: _____
Fecha: _____

Escuela Graduada
Departamento de Ciencias en Computadora

Hoja de Evaluación Nivel 1 — Taxonomía de Bloom (1, 2)

Parte I. Defina los siguientes términos:

1. Ingeniería social: _____
2. Carisma: _____
3. Comunicación no profesional: _____
4. Ataques de ingeniería social humanos: _____
5. Ataques de ingeniería social Técnicos: _____
6. Kevin Mitnick: _____

Parte II. De los ataques de ingeniería social discutidos en el módulo seleccione dos de ellos.

Tipos de ataques seleccionados:

1. _____
2. _____

A. Describa en detalle ambos ataques de ingeniería social seleccionados. Luego mencione tres diferencias entre estos ataques.

_____
_____
_____

Figura 5
Herramientas Instruccionales: Hoja de Evaluación

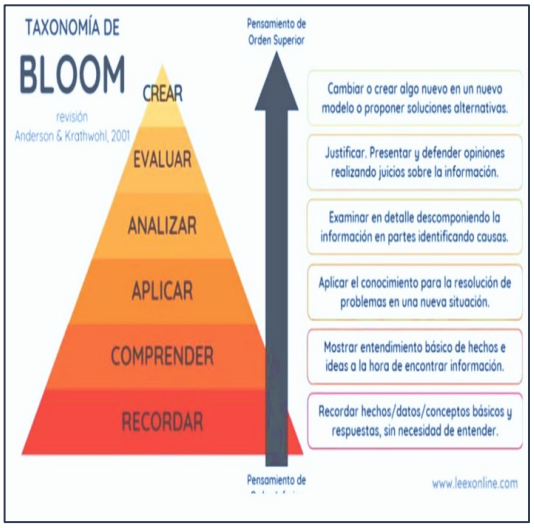


Figura 6
Taxonomía de Bloom y sus Niveles

La Figura 6 representa la jerarquía de la taxonomía de Bloom que fue utilizada para crear los módulos y las hojas de evaluación.

Módulo 1: Ataques Cibernéticos

Descripción General

El primer Módulo comienza discutiendo los conceptos generales que se necesitaran aprender para que el estudiante pueda avanzar al Módulo 2 e igualmente al Módulo 3. Es una introducción general a los varios conceptos que se irán discutiendo en los siguientes dos Módulos. Es esencial que aprendan primero estos conceptos para que así tengan conocimiento de lo que se está discutiendo con más detalle en los siguientes módulos.

Se presenta al estudiante cómo funciona el Internet y como se transmiten los datos a través de esta, al igual que los significados de los conceptos de Ataques de Ingeniería Social y Ransomware.

Objetivos de Aprendizaje

Los objetivos principales de aprendizaje en el Módulo 1 son:

1. Explicar cómo funciona la Internet
2. Explicar lo que es el concepto de Dirección IP.
3. Introducir los ataques cibernéticos más frecuentes.
4. Presentar a los estudiantes maneras de cómo pueden protegerse de los ataques cibernéticos.
5. Proveer diferentes métodos de ejercicios donde puedan identificar el tipo de ataque cibernético y que pueden hacer basado en el escenario provisto en el ejercicio.

Módulo 2 : Ataques de Ingeniería Social

Descripción General

El Módulo 2: Ataques de Ingeniería Social inicia con una discusión sobre el concepto de Ingeniería Social y que significa. Los estudiantes serán expuestos a los diferentes tipos de Ataques de Ingeniería Social. Durante la lección podrán discutir varios escenarios donde está ocurriendo un Ataque de Ingeniería Social. Los estudiantes podrán usar su creatividad para explicar que harán en dicha situación.

Adicionalmente, serán introducidos a conceptos más detallados acerca de Ingeniería Social y los diferentes ataques que caen bajo el renglón de Ataques de Ingeniería Social. Por último, el módulo contiene una breve historia de los primeros Ataques de Ingeniería Social. También se dará un breve trasfondo de Kevin Mitnick, el Ingeniero Social más famoso de nuestra época.

Objetivos de Aprendizaje

Los objetivos de aprendizaje del Módulo 2 son los siguientes:

1. Introducir a los estudiantes a lo que son Ataques de Ingeniería Social.
2. Identificar las características generales en común de todos los Ataques de Ingeniería Social.
3. Identificar al estudiante a los diferentes medios que son utilizados para llevar a cabo Ataques de Ingeniería Social.
4. Explicar cómo en el Internet ocurren los Ataques de Ingeniería Social.
5. Retar al estudiante a tener que utilizar pensamientos críticos y sus habilidades para resolver problemas implementando lo aprendido en el módulo.

Módulo 3: Ransomware

Descripción General

El Módulo 3 está dedicado al tema de Ransomware. Los conceptos esenciales del Ransomware también son discutidos.

Se incluye una breve historia del descubrimiento de los primeros Ransomware. También, se explica lo que ocurre si una computadora es infectada con Ransomware. Se le provee medidas a tomar dependiendo del tipo de Ransomware que haya infectado la computadora.

Al final del módulo tendrán que crear una situación hipotética donde estará ocurriendo un Ataque Ransomware y establecerán que harán para mitigarlo.

Objetivos de Aprendizaje

Los objetivos de aprendizaje del Módulo 3 son los siguientes:

1. Explicar la importancia de poder protegerse contra Ataque Ransomware.
2. Explicar el daño que el Ransomware ocasiona en las computadoras y sistemas informáticos.
3. Identificar cuando están siendo atacados por un Ransomware
4. Proveer diferentes métodos de cómo protegerse en contra del Ransomware.
5. Analizar situaciones hipotéticas y crear sus propias respuestas al ataque basado en lo aprendido.

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 de los módulos puede ver si estos son eficientes en enseñar los conceptos y si se está cumpliendo los 6 niveles de taxonomía de Bloom.

Se tratará de implementar los módulos en el currículo escolar para poder crear retrospectiva acerca de ellos en una situación real. Las hojas de evaluación que fueron creadas para cada módulo servirán de guía para que el educador pueda medir cuanto los estudiantes están 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.

CONCLUSIÓN

El objetivo principal de los 3 módulos que fueron creados fue introducir a los estudiantes a los conceptos de Ataques Cibernéticos, Ataques de Ingeniería Social y Ataques 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.

REFERENCIAS

[1] Educapeques, "3 Tipos de Aprendizaje Según individualidades - portal educapeques," *Portal Educativo de apoyo a Padres, Maestros y Niños en las Tareas Escolares*, 21-Oct-2020. [En línea]. Disponible: https://www.educapeques.com/estimulapeques/tipos-de-aprendizaje.html. [Accedido: 12-Mar-2023].

[2] Admin, "HSB: Young adults most likely to be targeted in cyber attack," *Claims Journal*, 20-Sep-2016. [En línea]. Disponible: https://www.claimsjournal.com/news/national/2016/09/20/273559.htm. [Accedido: 12-Mar-2023].

[3] S. Hazlegreaves and P. enter your name here, "Children are becoming more vulnerable to cybercriminals as IOT device use explodes," *Open Access Government*, 04-Sep-2019. [En línea]. Disponible: https://www.openaccessgovernment.org/children-vulnerable-to-cybercriminals/72665/. [Accedido: 14-Mar-2023].

[4] 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*. [En línea]. Disponible: https://journals.sfu.ca/ijitls/index.php/ijitls/article/view/81. [Accedido: 18-Apr-2023].

[5] 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. [En línea]. Disponible: https://eric.ed.gov/?id=ED557216. [Accedido: 18-Apr-2023].

[6] E. Amankwa, "Relevance of cybersecurity education at pedagogy levels in schools," *Journal of Information Security*, vol. 12, no. 04, pp. 233–249, 2021.

[7] F. Quayyum, "Cyber Security Education for children through gamification," *Proceedings of the 2020 ACM Interaction Design and Children Conference: Extended Abstracts*, 2020.