

**LOS BABY BOOMERS, UNA GENERACIÓN VULNERABLE AL
PHISHING POTENCIADO POR IA**

Modalidad Trabajo De Grado: Diplomado

Marketing de Contenidos y Community Manager: Integrando la Inteligencia
Artificial

Ximena Alexandra Mesa

Cédula de Ciudadanía:1007747266

Director de trabajo de grado

Alban Augusto Blanco Luna

Maestro en Artes Visuales

Universidad de Pamplona

Facultad de Artes y Humanidades

Programa de Comunicación Social

Pamplona

2024

Resumen

La generación de los Baby Boomers se ha catalogado como la población más vulnerable a los ataques conocidos como phishing, esta población posee menos conocimientos tecnológicos que las generaciones más jóvenes. El phishing es una estafa en línea que utiliza correos electrónicos, mensajes de texto y sitios web falsos para robar información confidencial, y ha evolucionado significativamente con la llegada de la inteligencia artificial (IA). La IA ha permitido a los ciberdelincuentes crear mensajes más complejos y personalizados que tienen más probabilidades de robar información confidencial a través de las plataformas más usadas por esta población, como lo son las redes sociales o mensajes de texto. Al crear mensajes más complejos y personalizados, los ciberdelincuentes pueden aumentar la eficacia y la escala de sus ataques.

Estos ataques pueden tener graves consecuencias para los Baby Boomers, provocando importantes pérdidas económicas, robos de identidad y problemas de salud mental como estrés y ansiedad. El robo de información personal y financiera puede acarrear problemas legales e importantes pérdidas económicas. También puede ampliar la brecha digital, ya que la gente no utiliza la tecnología por miedo a ser atacada de nuevo. Para mitigar estos riesgos, es importante poner en marcha programas de alfabetización digital dirigidos a los Baby Boomers que se centren en la educación sobre ciberseguridad y la detección de ataques de phishing. Mejorar las competencias digitales no solo es importante para proteger a los Baby Boomers de los ciberataques, sino también para ayudarles a integrarse en el mundo digital moderno, aprovechar las oportunidades que ofrece la tecnología y reducir la brecha digital.

Palabras clave: Baby Boomers, Phishing, Inteligencia artificial, Ciberataques, Vulnerabilidad tecnológica, Alfabetización digital.

Abstract

Baby Boomers have been labeled as the population most vulnerable to attacks known as phishing, this population is less technologically savvy than younger generations. Phishing is an online scam that uses fake emails, text messages and websites to steal sensitive information, and has evolved significantly with the advent of artificial intelligence (AI). AI has enabled cybercriminals to create more complex and personalized messages that are more likely to steal sensitive information through the platforms most used by this population such as social networks or text messages. By creating more complex and personalized messages, cybercriminals can increase the effectiveness and scale of their attacks.

These attacks can have serious consequences for Baby Boomers, causing significant financial losses, identity theft and mental health issues such as stress and anxiety. The theft of personal and financial information can lead to legal problems and significant financial losses. It can also widen the digital divide, as people do not use technology for fear of being attacked again. To mitigate these risks, it is important to implement digital literacy programs targeting Baby Boomers that focus on cybersecurity education and phishing attack detection.

Improving digital skills is not only important to protect Baby Boomers from cyberattacks, but also to help them integrate into the modern digital world, take advantage of the opportunities offered by technology and bridge the digital divide.

Keywords: Baby Boomers, Phishing, Artificial intelligence, Cyber-attacks, Technological vulnerability, Digital literacy.

Tabla de contenido

Phishing Potenciado por IA: Un Riesgo Emergente para la Generación Baby Boomers	5
Evolución del phishing con la ayuda de la inteligencia artificial	7
La brecha digital de los Baby Boomers	8
Inclusión digital como alternativa	11
Uso de la tecnología; Estadísticas de conexión	12
La alfabetización digital como estilo de vida	15
Estilos de aprendizaje en la población vulnerable	19
Estrategias para reducir la vulnerabilidad de las personas mayores en el entorno digital	21
Conclusiones.....	24
Bibliografía.....	26

Phishing Potenciado por IA: Un Riesgo Emergente para la Generación Baby Boomers

La forma en que la sociedad moderna se comunica y depende de las tecnologías de la información (TIC) ha cambiado radicalmente nuestra forma de vivir, trabajar y comunicarnos. Este fenómeno afecta no sólo a la generación más joven, sino también a la generación de los Baby Boomers, que deben adaptarse a estas nuevas herramientas tecnológicas.

Según la publicación de AnswerNet titulada “De los Boomers a la Generación Z” menciona que esta generación creció en una época en la que predominaban la comunicación cara a cara y los medios de comunicación tradicionales, por lo que la transición a una sociedad digital supone un enorme reto para ellos. Sin embargo, muchos de ellos han utilizado con éxito las TIC para mantener relaciones familiares, participar en el mercado laboral y hacer un uso eficaz de la información y los servicios.

La inclusión digital es importante para todos los grupos de edad, haciendo énfasis en la generación Baby Boomers, debemos garantizar que tengan acceso a equipos tecnológicos y a la formación adecuada para hacer pleno uso de las TIC. Esto contribuye a que puedan beneficiarse de las oportunidades que ofrecen estas tecnologías.

Es importante que la población del adulto mayor conozca las mejores prácticas para la protección de los datos personales y el uso seguro del entorno digital. Con base en esto, Espinet (2007) nos define:

Podemos decir que las TIC son un conjunto de tecnologías basadas en la microelectrónica, la informática y las redes de comunicaciones utilizadas para procesar y transmitir información en formato digital. Las TIC engloban desde

programas de ordenadores hasta los dispositivos de telefonía móvil o Internet.

(p.23)

Sin embargo, estos avances tecnológicos también han traído consigo nuevas formas de ciberamenazas, una de las más persistentes y peligrosas de las cuales es el phishing.

El phishing es un tipo de comportamiento fraudulento cuyo objetivo es robar información confidencial, “diseñados para convencer a una víctima de proporcionar información personal, generalmente realizado para obtener una ganancia monetaria por parte del atacante” (Benavides, Fuertes, Sánchez, & Nuñez-Agurto, 2020, p. 98).

La información confidencial puede obtenerse de forma fraudulenta mediante el envío de correos electrónicos, mensajes de texto o enlaces cifrados que contengan información falsa para inducir a la víctima a facilitar la información solicitada. En el pasado, los ataques se caracterizaban por errores gramaticales u ortográficos, URL de dudosa procedencia e información que no correspondía a la parte solicitada. Incluso los ataques de phishing más simples han demostrado ser eficaces, dejando ver la ignorancia de las víctimas ante estos temas. En este caso, Sastoque y Botero (2016) nos plantean lo siguiente:

Un mecanismo que se ha propuesto para reducir los correos de phishing en tiempo real es el método denominado IBC (Intelligent Based Classification), el cual utiliza un algoritmo de filtrado y clasificación inteligente que detecta los correos electrónicos de phishing por sus propias características. El algoritmo de clasificación detecta ataques de phishing y protege a los usuarios de los enlaces poco fiables, mensajes instantáneos y páginas web; además, puede detectar hasta un 96% de los ataques de phishing en tiempo real. (p.79)

Este tipo de estafa puede afectar a las personas que a menudo desconocen el phishing y otras técnicas de fraude digital. El adulto mayor, como ha tenido poco acceso a la tecnología durante la mayor parte de su vida, puede ser más vulnerable a este tipo de ataques.

Es importante que esta generación tenga buenos conocimientos de seguridad informática. Si saben reconocer los correos electrónicos sospechosos y reconocer las señales de alarma, pueden reducir considerablemente el riesgo de convertirse en víctimas de un fraude. Así ellos se podrán sentir seguros cuando utilizan las TIC, es importante que conozcan los riesgos del phishing y cómo proteger la información personal.

Además, es necesario implementar medidas preventivas como es la colaboración entre generaciones, donde los familiares más jóvenes pueden ayudar al adulto mayor a aprender a utilizar la tecnología de forma segura.

Evolución del phishing con la ayuda de la inteligencia artificial

La inteligencia artificial ha revolucionado el phishing, haciéndolo más sofisticado que nunca. La construcción de estos modelos IA sirve para optimizar y mejorar la automatización de mensajes fraudulentos. La revista El cronista menciona que la firma especializada en seguridad informática Kaspersky asegura que, en América Latina, la cantidad de ataques cibernéticos a través de la IA aumentó un 617 % en este último año.

En ese aspecto, Boden, M. A. (2017), señala que uno de los objetivos principales de la IA era el uso tecnológico, “usar los ordenadores para hacer cosas útiles (a veces empleando métodos muy distintos a los de la mente)”. En este sentido, la IA demostró

ser una herramienta muy completa para solucionar problemas y a la vez poder resolver tareas que antes se exigía el talento humano.

Sin embargo, los hackers o ciberdelincuentes, como se les conoce, aprovechan esta habilidad de la inteligencia artificial para imitar la inteligencia humana y ejecutar estos ataques de phishing, al poseer esta plataforma resultan más persuasivos. Utilizan algunos algoritmos que ya se encuentran automatizados para replicar el lenguaje natural usado por el ser humano, los hackers personalizan y adaptan los mensajes con base en sus necesidades y tácticas de estafa.

La inteligencia artificial facilita la creación y el envío masivo de mensajes de phishing, lo que permite a los agresores llegar a millones de personas a la vez. Los sistemas de inteligencia artificial también pueden adaptarse y evolucionar en tiempo real, ajustando sus tácticas en función de la respuesta de la víctima.

La brecha digital de los Baby Boomers

La generación Baby Boomers, nacida entre los años 1946 y 1964, es particularmente indefensa a los ciberataques, ya que no poseen cierta familiaridad con la tecnología como es el caso de las generaciones más jóvenes, volviéndolos así un blanco fácil de los ciberdelincuentes.

Hay varios factores que hacen que esta generación sea más vulnerable a los ataques de phishing, no crecieron en la era digital, lo que les dificulta las nuevas herramientas y plataformas en línea. Las generaciones mayores pueden no tener la misma formación formal en ciberseguridad que las generaciones más jóvenes.

En ese sentido, la autora Maldonado (2016) comentó lo siguiente en su artículo:

Esta generación en especial se ve forzada a integrarse en un mundo del cual no se siente partícipe. Es así como adapta superficialmente las modas, tendencias, su modo de consumo, su trajín diario y el acercamiento a la vanguardia y nuevos estilos de vida. (p.11)

Nos menciona que los individuos de esta generación pueden experimentar cierta desconexión o falta de identificación con los cambios rápidos y las demandas que les exigen en la sociedad. Pueden sentir la presión de adaptarse.

El autor Rodríguez Izquierdo (2007) hace el siguiente planteamiento:

Se tiende a pensar que las personas mayores no se llevan muy bien con las nuevas tecnologías y utilizan bastante poco las que ya tienen en casa y parece ser que dos de las explicaciones a esas reticencias son: la complejidad y el desconocimiento o falta de información sobre cómo funcionan. Casi todas las personas de edad avanzada son vulnerables a estos prejuicios. Pero nos podemos preguntar, ¿a quién de nosotros no nos ha sucedido lo mismo al empezar a utilizar un ordenador o Internet? (p. 43-44)

Es importante destacar que, inicialmente, se pueden presentar obstáculos. Para la población mayor, al adaptarse al uso de las computadoras e internet, es posible superar estas dificultades y aprovechar las oportunidades que estas herramientas tecnológicas nos pueden brindar. Debemos reconocer que las personas poseen su propio ritmo de aprendizaje y suelen necesitar más asistencia para poder adquirir estas nuevas habilidades digitales.

Los ataques de phishing dirigidos a la generación Baby Boomers pueden tener consecuencias en temas financieros como datos bancarios y números de tarjetas de crédito, al ser robadas provocarán importantes pérdidas económicas. La información

personal robada puede utilizarse para suplantar la identidad de la víctima, lo que conllevaría a problemas legales.

El autor Montañez Ramírez (2023), comenta en su investigación;

También se presentan vulnerabilidades en su falta de conocimiento, por ejemplo, es donde se le miente al Adulto mayor diciéndole que es ganador de un algún premio, cosa que no es cierta, siendo su objetivo que el Adulto mayor de su información confidencial, al hacer clic en esas ventanas recuperan datos de la computadora, ahí es donde proceden a realizar un ataque. (p.43)

Esto podría desembocar en estrés y ansiedad causados por estos ataques cibernéticos, afectando negativamente a la salud mental y el bienestar de la víctima. Por miedo a ser atacados nuevamente, esta generación podría aislarse digitalmente y evitar la tecnología, lo que aumentaría la brecha digital.

Los autores González Barranco, J. L. (2020), en su investigación indican:

El grupo de personas con edad superior a los 50 años tiene un uso de las tecnologías menor, ya que cuando crecieron fueron educados al margen de las tecnologías que iban apareciendo y no tuvieron la posibilidad de conexión a Internet. La masificación de los ordenadores personales no se consiguió hasta finales de los años ochenta y comienzos de los años noventa; por lo que, ni los estudiantes anteriores y los trabajadores posteriores a estos años, no han necesitado el uso del ordenador, alejados de las herramientas informáticas que iban apareciendo en el mercado. Para reducir la brecha digital y la diferencia generacional en el uso de las tecnologías, se suma un motivo, al normal distanciamiento entre generaciones, por eso es necesario buscar estrategias para

alcanzar estos objetivos, mediante la alfabetización digital y el desarrollo de las relaciones interpersonales entre generaciones. (p.35)

Se evidenció cómo enfatizan la importancia de comprender la brecha digital entre los menores de 50 años y las generaciones más jóvenes, una brecha que explica la falta de habilidades tecnológicas que necesitan las generaciones mayores. Para abordar este tema, el autor propone fortalecer la alfabetización digital y los contenidos internacionales como estrategias clave para mejorar la inclusión digital y reducir la brecha tecnológica.

Inclusión digital como alternativa

Con el rápido avance de la tecnología y la aparición de dispositivos digitales en la vida cotidiana, la inclusión digital es muy importante hoy en día para las personas mayores. Este conocimiento no se refiere sólo a la conexión a Internet, sino también a la capacidad de utilizar estas tecnologías de forma eficaz y segura.

Los autores González Barranco, J. L. (2020), mencionan que;

La única posibilidad pasa por la inclusión para los adultos marginados de la generación digital, posibilitando el aprovechamiento de las competencias tecnológicas e incorporarlas a su vida cotidiana y en el desempeño de su actividad laboral, en sus relaciones con los demás, en definitiva, dar oportunidades para el acceso a la información y el conocimiento. (p.35)

Debemos tener claro la importancia de los contenidos digitales ya que este ofrece muchos beneficios a las personas mayores, incluida la mejora de su capacidad para comunicarse con familiares y amigos, acceder a información y servicios de salud y reducir el aislamiento al participar en actividades educativas y recreativas. El acceso a la

tecnología puede ayudar a las personas mayores a mantenerse conectadas, activas y mejorar su calidad de vida y su salud en general.

Para la sociedad, las personas de la tercera edad y las tecnologías son conceptos totalmente separados, debido al trivial concepto de las personas mayores como personas no aptas física y psicológicamente hablando, siendo excluidos de la digitalización por su aprendizaje lento.

Moreno Cuervo & Parra Coutin, M. A. (2016), destacan:

Por medio de la tecnología, el adulto mayor accede a beneficios en cuanto a la interacción social y cultural, en la actividad laboral y formación, también le ofrece un medio de entretenimiento e información; ya que en la interacción con la tecnología no importa el tiempo ni el espacio, el usuario tiene la posibilidad de relacionarse, comprar, vender, realizar trámites, etc., sin importar edad, enfermedad o condición, lo que posibilita mejorar la calidad de vida. La tecnología le permite superar miedos, evitar la soledad, adquirir nuevos conocimientos, interactuar con otras personas, ayudar a sus hijos o nietos, mejorar su actividad laboral y, una vez que se aprende a manejar un aparato tecnológico, el usuario lo utiliza como herramienta de cálculo, comunicación, entretenimiento, entre otras acciones más complejas. (p.4)

Se reconoce que las personas mayores enfrentan muchos desafíos en la inclusión digital. Estos incluyen la falta de habilidades técnicas, la tecnofobia, las discapacidades físicas y mentales y la falta de herramientas y servicios en línea. Estas barreras requieren soluciones simples y específicas que sean fáciles de implementar.

Uso de la tecnología; Estadísticas de conexión

Estos datos muestran que, aunque las generaciones de más edad utilizan la tecnología de diversas formas, también se enfrentan a importantes retos que aumentan su vulnerabilidad ante las ciberamenazas.

Según el instituto de economía digital (ICEMD), los Baby Boomers son menos propensos que las generaciones más jóvenes a poseer un smartphone, con un 68% en comparación con el 95% de los Millennials y el 93% de la Generación X. El 74% de los Baby Boomers posee un ordenador, pero la frecuencia de uso y sofisticación no se compara con la generación de sus nietos, ya que todos poseen diferencias de necesidades y usos.

Gaitán Díaz (2023), nos explica en su trabajo de investigación sobre la adopción digital de esta población mayor. Solo el 78% de los Baby Boomers tiene acceso a Internet en casa, y esta proporción ha aumentado en la última década. Sin embargo, existe una clara disparidad entre los Baby Boomers urbanos y los rurales, siendo estos últimos los que tienen menos acceso a conexiones de banda ancha, lo que limita su participación en la economía digital y la interacción social en línea.

Según las estadísticas del artículo “¿Cómo consumimos contenido según nuestra edad?” destacan que sólo el 57% de los Baby Boomers utiliza plataformas de medios sociales como Facebook, frente al 84% de los Millennials más jóvenes.

Un estudio realizado por la Cámara Colombiana de Comercio electrónico revela que el 52% de los Baby Boomers utiliza servicios de comercio electrónico al menos una vez al mes y el 35% gestiona regularmente su dinero en línea. Sin embargo, la desconfianza en las transacciones digitales sigue siendo alta debido a las preocupaciones por la seguridad, lo que pone de relieve la importancia de educar y promover la confianza en estos servicios.

Las autoras Moreno & Parra (2016), mencionan en su artículo “En Colombia el 88% de los adultos mayores consideran que la tecnología es importante para la vida (Corporación Colombia Digital, 2015) debido a esto, y a que cada vez más las tecnologías de la información y la comunicación (TIC) se han incorporado en los contextos más comunes y frecuentes para los adultos, estos ven aún más necesario aprender a manejar las TIC para tener nuevas oportunidades”.

También enfatizan la importancia de aprender de la tecnología, ya que abre nuevas oportunidades y facilita la adaptación a la sociedad digital actual.

Un artículo publicado por la revista Forbes indica que “Por segundo año consecutivo, Colombia se ha convertido en el país más atacado por ataques cibernéticos, con el 17 % de los incidentes en la región. El Índice de Inteligencia de Amenazas X-Force, compilado mediante el monitoreo de más de 150.000 millones de eventos de seguridad diarios en 130 países, ha destacado que el 71 % de los ciberataques globales ahora se atribuyen a la explotación de identidad”.

El número de ataques en Colombia se puede atribuir a varios factores. En primer lugar, la digitalización en el país ha aumentado el número de ciberataques. Las empresas y los gobiernos adoptan cada vez más tecnologías digitales que ponen en riesgo sus servicios de seguridad. En segundo lugar, el robo de identidad se ha vuelto algo común ya que la web oscura está llena de información personal y otros recursos ilegales, y los ciberdelincuentes pueden usar esa información para todo, desde el robo de identidad.

La Universidad de La Plata publicó un artículo enfocado en “las recomendaciones para evitar ser víctima del phishing”, donde nos indican pasos a realizar para no caer en esta modalidad de estafa cibernética.

- “No envíe información personal usando mensajes de correo electrónico. El correo electrónico, si no se utilizan técnicas de cifrado y/o firma digital, no es un medio seguro para enviar información personal o confidencial.
- No acceda desde lugares públicos. En la medida de lo posible, evite ingresar al sitio web de una entidad financiera o de comercio electrónico desde un cibercafé, locutorio u otro lugar público. Las PCS instaladas en estos lugares podrían contener software o hardware malicioso, destinado a capturar sus datos personales.
- En caso de utilizar dicho ambiente, la mayoría de las instituciones bancarias brindan la posibilidad de utilizar un teclado sobre la pantalla. ¡Utilícelo!”.

Para proteger la información enviada a través de este medio se deben tomar estas precauciones, la información personal puede quedar expuesta a amenazas como robo o interceptación por parte de terceros. Si este es el caso, debes tener cuidado al enviar información confidencial a los usuarios por correo electrónico y considerar opciones más seguras si es necesario.

Debemos tener presente que las computadoras de los sitios públicos pueden ser vulnerables a malware diseñado para recopilar información personal. Estas amenazas potenciales provienen de dispositivos desprotegidos y redes generalizadas. Como precaución, se recomienda evitar esta zona crítica si es posible.

La alfabetización digital como estilo de vida

La alfabetización digital se ha convertido en una herramienta importante para la inclusión social en este mundo cada vez más digitalizado. Sin embargo, la falta de competencias digitales crea desigualdades, donde les limita el acceso a la información, la educación y el empleo y aísla a aquellos que no las dominan.

Debemos promover la alfabetización digital para garantizar la igualdad de oportunidades. Aludido a esto, Andía y Campión (2022), añaden que:

La Multialfabetización se utiliza cada vez más para describir las diversas habilidades y aptitudes que se necesitan para interactuar con la amplia gama de canales de comunicación de los que ahora participamos. Este concepto también reconoce que ser alfabetizado en un mundo digital implica no solo competencia tecnológica, sino también una amplia variedad de práctica. (p.26)

Es importante que las instituciones educativas y los responsables políticos apliquen estrategias para que las personas puedan adquirir las competencias necesarias para navegar y utilizar eficazmente el entorno digital. Con base en esos fundamentos, Espinet, E. (2007), nos menciona que la alfabetización:

Incluye la potenciación de la autonomía de las personas. Es decir, hay que ir más allá del hecho de enseñar a utilizar la tecnología y localizar información. La alfabetización digital debe tener como objetivo que las personas tengan suficiente autonomía para desarrollarse en cualquier situación en el contexto de la sociedad de la información. (p.38)

Para poder caracterizar a nuestra población es importante distinguir los diferentes tipos de alfabetización. Calle González, en su artículo sobre las TICS y la alfabetización, nos menciona los 3 tipos de niveles que existen que reflejan la complejidad y profundidad del uso digital.

Básico: Incluye habilidades básicas como el uso de dispositivos electrónicos (ordenadores, teléfonos inteligentes), navegar por Internet y utilizar el correo electrónico y las aplicaciones básicas de mensajería.

Intermedio: Incluye habilidades avanzadas como aplicaciones ofimáticas (procesador de textos, hojas de cálculo), gestión de archivos, redes sociales y búsqueda de información fiable en internet.

Nivel avanzado: Incluye habilidades en profundidad como la programación, la creación y gestión de contenidos digitales modernos (vídeos, blogs, páginas web), el análisis de datos y el uso de herramientas especializadas en diversos campos.

Es importante hacer la comparación con las generaciones más jóvenes, denominadas nativos digitales, que han crecido en un entorno en el que la tecnología digital se ha hecho presente, por lo que han aprendido intuitivamente las competencias digitales desde una edad temprana.

En el artículo titulado “Boomers versus Millennials y Generación Z” mencionan las principales diferencias entre las generaciones más jóvenes y las mayores, de las cuales se puede resaltar que la llamada “La generación digital” está familiarizada con los dispositivos tecnológicos e internet desde una edad temprana. Esto contrasta con las generaciones mayores, que a menudo no se encuentran con estas tecnologías hasta la edad adulta.

Dado que las generaciones más jóvenes están familiarizadas con la tecnología desde una edad temprana, tienden a adaptarse rápidamente a nuevos dispositivos, aplicaciones y plataformas digitales.

Los nativos digitales utilizan más plataformas sociales para la comunicación, el entretenimiento y la educación, mientras que las generaciones mayores pueden limitarse a unas pocas plataformas y usos funcionales.

Las generaciones más jóvenes tienden a subestimar los riesgos asociados con la seguridad y la privacidad en línea, a pesar de sus habilidades técnicas.

El autor Cruz Aguilar (2020), nos plantea una perspectiva acerca de la alfabetización;

No se trata de imponer un programa pensado para los alfabetizados, de lo que se trata es de observar, dialogar y construir de manera colectiva un programa pensado también por ellos, con ellos, partiendo de la lectura del mundo que ellos realizan, problematizando, confrontando pensamiento y realidad, un programa que integre su palabra, que es la lectura del mundo, que es anuncio y denuncia para transformar. (p.201)

La enseñanza del adulto mayor debe ser aceptada, esto incluye seguimiento y comunicación para comprender las necesidades, intereses y preocupaciones en materia de TIC. Sería fundamental incorporarlos a un proyecto de habilidades digitales, esto les aumentará su confianza y capacidad y hará que esté más interesado en participar más activamente en el aprendizaje de las habilidades digitales que enfrenta el mundo actual.

Además, los programas de alfabetización digital deben centrarse en las realidades y experiencias específicas de los adultos mayores. Esto significa confrontar sus propios pensamientos e ideas sobre la tecnología e identificar problemas y desafíos específicos en el proceso de aprendizaje. Resolver estos problemas juntos crea un ambiente de confianza y colaboración donde las TIC pueden integrarse fácilmente en la vida de las personas.

De manera similar, los programas de alfabetización digital deben priorizar el lenguaje y la experiencia de los adultos. Sus calificaciones y experiencias son herramientas importantes para el desarrollo y el aprendizaje del plan de estudios. Compartir historias e ideas sobre el uso de la tecnología inspira a la comunidad y anima a los participantes a aprender juntos.

Estilos de aprendizaje en la población vulnerable

Cussiánovich (2005) nos plantea que;

Los estilos de aprendizaje son los rasgos cognitivos, afectivos y fisiológicos que sirven como indicadores relativamente estables de cómo las personas perciben interacciones y responden a sus ambientes de aprendizaje, en este caso, el colectivo de personas de edad avanzada de observar cómo estructuran los contenidos, forman y utilizan conceptos, interpretan la información, resuelven los problemas, seleccionan medios de interpretación, etc. Cuanto más se pueda descubrir sobre la manera en que las personas aprenden, mejor podremos diseñar el proceso de formación para fomentar el aprendizaje. (p.7)

Debemos tener presente que cada uno procesa la información de manera diferente, algunas personas ven y aprenden más a través de imágenes, mientras que otras escuchan y aprenden verbalmente. Además, algunas personas aprenden mediante la experiencia. Comprender estas diferencias es esencial para que la educación sea inclusiva y eficaz para todos, y al identificar diferencias en los estilos de aprendizaje entre grupos de adultos, podemos desarrollar estrategias de instrucción para satisfacer estas diversas necesidades.

Puede ser una combinación de diferentes métodos de enseñanza, como video, lectura, discusión grupal y práctica. Al brindar más opciones, los estudiantes aprenden

de acuerdo con sus intereses y estilos de aprendizaje que pueden influir en el acceso de los adultos a la educación en un nivel específico.

Para comprender la seguridad en línea, es importante que los adultos utilicen formas sencillas y fáciles de evitar su mal uso. Sin embargo, se puede modificar la manera en que explicamos al usar tecnicismos, por ejemplo, en lugar de hablar de “malware” o “phishing”, se puede explicar que se trata de un correo electrónico falso cuyo objetivo es engañar a las personas con información personal.

Podemos relacionar la ciberseguridad con las tareas cotidianas, como utilizar las redes sociales o gestionar el correo electrónico, así como comprender y proteger la información. Por ejemplo, explicar cómo ajustar la configuración de privacidad de sus redes sociales para evitar que extraños compartan información personal o cómo detectar spam que engaña a las personas para que se unan a redes maliciosas.

El proceso de enseñanza requiere paciencia y respeto porque entendemos que los adultos necesitan tiempo para aprender nueva información. Colocar ejemplos para explicar cada concepto. Permitir la práctica y la observación para que los adultos puedan mejorar la comprensión a su manera.

Un buen aprendizaje requiere participación activa, por lo que es necesario incluir actividades interactivas para que los adultos puedan aplicar lo que aprenden en un entorno controlado. Esto puede incluir ejercicios, animaciones o ejemplos de actividades seguras en línea.

Es importante brindar orientación a las personas mayores que regresan a sus hogares para garantizar un apoyo continuo. Esto les permite revisar y aplicar lo que han revisado, fortaleciendo su comprensión y capacidad para aplicar el conocimiento de ciberseguridad a situaciones del mundo real.

Estrategias para reducir la vulnerabilidad de las personas mayores en el entorno digital

Mejorar las habilidades informáticas de los adultos es un proceso complejo, ya que se debe proporcionar educación y formación continua. Esto se puede lograr a través de cursos y cursos especializados presenciales y en línea que abarquen desde los conceptos básicos hasta el uso avanzado de la tecnología digital. Es importante proporcionar recursos de aprendizaje específicos, como ejercicios paso a paso y aplicaciones interactivas.

Según el Instituto Colombiano de Bienestar Familiar, es importante ayudar a los adultos mayores a fortalecer sus habilidades digitales para cerrar la brecha tecnológica. Por lo que debemos brindarle un acceso a la tecnología adecuada, ya que es un elemento importante para aumentar la alfabetización digital de las generaciones mayores. El acceso rápido y confiable a Internet también es importante, especialmente para las personas mayores que viven en áreas rurales o de bajos ingresos.

Es importante establecer centros de apoyo tecnológico en las comunidades para ayudar a las personas mayores en el uso de la tecnología digital. Estos centros pueden proporcionar asistencia técnica y orientación sobre el uso de herramientas y software gratuitos.

La corporación StaySafeOnline en su artículo menciona lo fundamental que es que los adultos mayores sigan consejos de seguridad en línea para proteger su privacidad y seguridad en Internet. La seguridad en línea es un tema importante para los adultos. Brindar educación sobre seguridad informática ayuda a los adultos a desarrollar un vocabulario sólido; puede ayudarles a aprender cómo detectar correos electrónicos de phishing y tomar medidas para protegerse del malware. Es muy importante brindar

asesoramiento y capacitación sobre prácticas de privacidad en línea y administrar la seguridad de la información personal.

Debemos fomentar el uso de herramientas digitales en el día a día, al integrar a los adultos en la sociedad digital; es importante fomentar el uso de la tecnología digital en las actividades cotidianas. Tales como banca en línea; telemedicina, esto incluye comprar en línea y comunicarse con familiares y amigos por teléfono. Al mostrarles a las personas mayores el uso correcto y adecuado de la tecnología en su vida diaria, se les animará a aprender y utilizar nuevas herramientas.

También se podrán realizar campañas de sensibilización para educar a las generaciones mayores sobre los peligros del ciberataque y las mejores prácticas para un comportamiento seguro en línea.

Programas de formación: Proporcionar cursos y talleres accesibles para enseñar habilidades digitales a los adultos mayores.

La formación en habilidades digitales desempeña un papel importante a la hora de cerrar la brecha digital entre las personas mayores y ayudarlas a integrarse en la sociedad actual. Estos cursos incluyen una variedad de actividades para enseñar a los adultos cómo utilizar la tecnología de forma eficaz. Existen cursos de diferentes categorías y adaptabilidades:

Cursos de Iniciación: para adultos sin experiencia en tecnología. Cubre temas básicos como computadoras, Internet y el uso del correo electrónico. Utilice el correo electrónico. Los participantes desarrollan las habilidades necesarias para trabajar en un entorno digital. La Red Cultural del Banco de la República ofrece cursos de “Informática básica y recursos digitales para adultos mayores”

Capacitación práctica: estas sesiones interactivas permiten a los adultos aplicar lo que han aprendido en un entorno afectuoso. Aquí conocen herramientas reales y realizan tareas específicas como marketing online, redes sociales o procesamiento de datos. La AARP se une a una organización sin fines de lucro para enseñar tecnología a los adultos mayores, ofreciendo talleres interactivos.

La Universidad Externado de Colombia ofrece cursos virtuales sobre “Curso: Seguridad digital y gestión del riesgo cibernético”. este curso se centra en la importancia de la seguridad en línea y enseña a los adultos cómo prevenir el fraude, proteger la privacidad en línea y administrar contraseñas de forma segura. Identificar riesgos y utilizar prácticas seguras al acceder a Internet y utilizar servicios en línea.

El Ministerio de las TIC realiza el programa “En TIC Confío+”: una década informando a niños y jóvenes sobre los riesgos en Internet”. Este programa promueve el intercambio de información entre padres y jóvenes. Los jóvenes expuestos a la tecnología fomentan la colaboración y la exploración. Los jóvenes utilizan herramientas y aplicaciones digitales para compartir orientación, apoyo y habilidades.

Se deberían implementar cursos de Adaptabilidad y Accesibilidad que estén diseñados para satisfacer las necesidades especiales de adultos con discapacidades físicas o emocionales. Utilizando herramientas y recursos, como pantallas con Zoom o herramientas visuales interactivas, para que todos los participantes puedan beneficiarse de la formación.

De igual manera, existen programas de certificación que permiten a los adultos obtener un certificado completo que refuerza y aplica las habilidades que han adquirido. Estas certificaciones son reconocidas por escuelas o empleadores y pueden ayudar a los adultos a descubrir sus habilidades digitales.

Acceso a la tecnología: Garantizar que todas las generaciones tengan acceso a equipos tecnológicos de calidad y conectividad a Internet.

Apoyo continuo: Crear una red de apoyo en la que los miembros de la generación nativa digital compartan conocimientos y ayuden a las generaciones mayores a superar las barreras tecnológicas.

Conclusiones

Las tecnologías de la información y la comunicación (TIC) avanzan en casi todos los aspectos de nuestras vidas, desde el trabajo, el entretenimiento, hasta las relaciones sociales. Pero junto con estos beneficios, han surgido nuevos desafíos, como el phishing con inteligencia artificial (IA), que crea amenazas nuevas y más sofisticadas.

Básicamente, el phishing consiste en engañar a las personas para que revelen información confidencial, como contraseñas o información financiera, utilizando técnicas engañosas. Tradicionalmente, estos ataques son relativamente fáciles de detectar debido a errores de sintaxis, URL sospechosos o consultas de datos inconsistentes. Sin embargo, con la llegada de la inteligencia artificial, los ciberdelincuentes son mejores para personalizar y adaptar los mensajes de phishing utilizando algoritmos avanzados, lo que dificulta la distinción entre mensajes legítimos e ilegítimos.

El uso de inteligencia artificial para el phishing ha marcado el comienzo de una nueva era de ciberataques en la que los hackers pueden crear y enviar automáticamente mensajes falsos de gran magnitud. Además, la adaptación de estas plataformas de IA hace que los ataques puedan ajustarse rápidamente en función de las reacciones de la víctima, lo que dificulta la detección y prevención.

Muchos Baby Boomers nacieron antes del boom digital y tienen menos conocimientos y experiencia que las generaciones más jóvenes. Su falta de conocimientos técnicos los hace vulnerables a ataques de phishing, especialmente porque no pueden distinguir entre comunicaciones legítimas y fraudulentas.

Para resolver este problema, es necesario promover la alfabetización digital en todas las generaciones. Esto incluye no sólo habilidades técnicas básicas como navegar por Internet o utilizar software de mensajería, sino también una comprensión profunda de los riesgos asociados con el uso de la tecnología y las mejores prácticas en seguridad en línea.

Además, brindar apoyo y recursos claros es fundamental para crear una brecha de productividad digital. Esto incluye programas de capacitación adaptados a las necesidades y habilidades de los adultos mayores, y la creación de redes de apoyo comunitario donde los usuarios experimentados pueden compartir sus conocimientos y habilidades con personas con menos conocimientos tecnológicos.

En definitiva, combatir el phishing aumentado por la IA y proteger a los más vulnerables en línea requiere un enfoque donde se pueda combinar educación, promoción y concienciación pública. Solo trabajando juntos podremos crear un entorno digital que sea seguro y accesible para todos, especialmente para la población vulnerable como es la del adulto mayor.

Bibliografía

Andía Celaya, L., Santiago Campión, R., & Artigas, C. (2022). El reto de la alfabetización digital: De la sustitución a la transformación. Universitat Oberta de Catalunya. Recopilado de: <https://www-digitaliapublishing-com.unipamplona.basesdedatosezproxy.com/a/112350>

AnswerNet. (n.d.). Generaciones y estilos de comunicación. AnswerNet. Recuperado el 22 de mayo de 2024. Recuperado de <https://answernet.com/es/blog-generations-styles-communication/#:~:text=A%20los%20Boomers%20les%20gusta,las%20conversaciones%20cara%20a%20cara>.

Azeez, N. A., Misra, S., Margaret, I. A., Fernandez-Sanz, L., & Abdulhamid, S. M. (2021). Adopting automated whitelist approach for detecting phishing attacks. Computers & Security, 108, 102328. <https://doi.org/10.1016/j.cose.2021.102328>

Banco de la República. (2024, enero 22). Informática básica y recursos digitales para adultos mayores. La Red Cultural del Banco de la República. Recuperado de <https://www.banrepcultural.org/bogota/actividad/informatica-basica-y-recursos-digitales-para-adultos-mayores-1>

Benavides, E., Fuertes, W., Sánchez, S., & Nuñez-Agurto, D. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos: Una revisión sistemática de la literatura. Ciencia y Tecnología, 13(1), 97-104. Recopilado de <https://revistas.uteq.edu.ec/index.php/cyt/article/download/357/407>

Boden, M. A. (2017). Inteligencia artificial. Turner. Recuperado de <https://books.google.com.mx/books?hl=es&lr=&id=LCnYDwAAQBAJ&oi=fnd&pg=P>

[T3&dq=inteligencia+artificial&ots=dsQqx0gOl7&sig=7HmA3cIYdkjViYorW6OJwJruOg#v=onepage&q=inteligencia%20artificial&f=false](https://zaguan.unizar.es/record/121429/files/texto_completo.pdf)

Bunbury Bustillo, E., Osuna-Acedo, S., & Pérez Calle, R. (2022). Las Competencias Digitales en personas mayores: de amenaza a oportunidad (No. ART-2022-131993). Recuperado de https://zaguan.unizar.es/record/121429/files/texto_completo.pdf

Cámara Colombiana de Comercio Electrónico. (2024, abril 2). Accede a los modelos de negocio del comercio electrónico y la transformación digital con un solo clic. Cámara Colombiana de Comercio Electrónico. Recuperado de <https://www.ccce.org.co/noticias/accede-a-los-modelos-de-negocio-del-comercio-electronico-y-la-transformacion-digital-con-un-solo-clic/>

Calle González, S., Torres Belduma, K., & Tusa Jumbo, F. (2022). Las TICs, la enseñanza y la alfabetización digital de la familia. *Transformación*, 18(1), 94-113. Recuperado de http://scielo.sld.cu/scielo.php?pid=S2077-29552022000100094&script=sci_arttext

Camilo, M. R. C. Medidas preventivas de ciberseguridad que debe tener el adulto mayor en Colombia para acceder a internet y sus servicios. Recuperado de <https://repository.unad.edu.co/bitstream/handle/10596/59691/TRABAJODEGRADOCHRISTIANMONTANEZ.pdf?sequence=1>

Cussiánovich, A. (2005, julio). Educando desde una pedagogía de la ternura. Documento presentado en el Instituto Peruano de Educación en Derechos Humanos y la Paz, Lima, Perú. Recuperado de <https://riull.ull.es/xmlui/bitstream/handle/915/20540/Estilos%20de%20aprendizaje%20>

[en%20personas%20de%20edad%20avanzada%20con%20deterioro%20cognitivo%20leve%20y%20moderado%20.pdf?sequence=1&isAllowed=y](#)

Cruz Aguilar, E. (2020). La educación transformadora en el pensamiento de Paulo Freire. *Educere*, 24(78), 197-206. Recuperado de <https://www.redalyc.org/journal/356/35663284002/html/>

Dono, L. (2021, febrero 8). Aprende sobre tecnología con AARP y OATS/Senior Planet. AARP. Recuperado de <https://www.aarp.org/espanol/conoce-aarp/info-2021/oats-senior-planet-tecnologia-adultos-mayores.html>

Ebenezer, L. (2018). Cómo consumen contenido los Baby Boomers vs la Generación Z. Another Blog. Recuperado de <https://blog.another.co/blog/como-consumen-contenido-los-Baby-boomers-vs-la-generacion-z>

Forbes Staff. (2024, febrero 28). Colombia sigue siendo el país con más ataques de ciberseguridad en Latinoamérica, según IBM. Forbes Colombia. Recuperado de <https://forbes.co/2024/02/28/tecnologia/colombia-es-el-pais-con-mas-ataques-de-ciberseguridad-en-latinoamerica>

Gaitán Díaz, M. A. (2023). La adopción digital de la generación Baby Boomers y su relación con el uso de sus servicios financieros digitales. Colegio de Estudios Superiores de Administración - CESA. Recuperado de https://repository.cesa.edu.co/bitstream/handle/10726/5206/MDM_1032450626_2023_1

González Barranco, J. L. (2020). La generación “Baby Boomer” ante la alfabetización digital: Un estudio de caso. Recuperado de

https://redined.educacion.gob.es/xmlui/bitstream/handle/11162/219690/Gonzalez_Barranco_Jose_Luis_TFM.pdf?sequence=1

Grupo ArCERT. (s.f.). Recomendaciones para evitar ser víctima del phishing. Universidad Nacional de La Plata. Recuperado de <https://www.econo.unlp.edu.ar/detise/phishing-3923>

Hernández Domínguez, A., & Baluja García, W. (2021). Principales mecanismos para el enfrentamiento al phishing en las redes de datos. Revista Cubana de Ciencias Informáticas, 15(4), 413-441. Recuperado de http://scielo.sld.cu/scielo.php?pid=S2227-18992021000500413&script=sci_arttext

ICBF. (s.f.). Cómo ayudar a un adulto mayor a fortalecer sus habilidades digitales y cerrar su brecha tecnológica. Recuperado de <https://www.icbf.gov.co/mis-manos-te-enseñan/como-ayudar-un-adulto-mayor-fortalecer-sus-habilidades-digitales-y-cerrar-su>

Infodisa. (2022, diciembre 16). Ciberseguridad para gente mayor. Infodisa. Recuperado de <https://www.infodisa.com/es/ciberseguridad-para-gente-mayor/>

Instituto de la Economía Digital de ESIC (2018). Estudio 6 generaciones de la era digital. Recuperado de https://cdn5.icemd.com/app/uploads/2018/12/Estudio_6-generaciones-de-la-era-digital-.pdf

Lamberti, Carolina. (2024, Enero 4). “Por la IA, los ataques de phishing se dispararon más del 600%: cómo pueden prevenirlos empresas y usuarios”. El Cronista. Recuperado de <https://www.cronista.com/infotechnology/actualidad/por-la-ia-los-ataques-de-phishing-se-dispararon-mas-del-600/>

Maldonado Ibarra, L. C. (2016). Análisis sobre el uso y manejo de la tecnología móvil en las generaciones Baby Boomers y Generación X (Bachelor's thesis, Quito: Universidad de las Américas, 2016). Recuperado de <http://dspace.udla.edu.ec/handle/33000/5454>

Mesa, D. S., & Tabares, R. B. (2015). Técnicas de detección y control de phishing. Cuaderno activa, 7, 75-81. Recuperado de <https://ojs.tdea.edu.co/index.php/cuadernoactiva/article/download/250/242>

Ministerio de Tecnologías de la Información y las Comunicaciones. (2021, septiembre 24). 'En TIC Confío+': una década informando a niños y jóvenes sobre los riesgos en Internet. Recuperado de <https://mintic.gov.co/portal/inicio/Sala-de-prensa/182632:En-TIC-Confio+-una-decada-informando-a-ninos-y-jovenes-sobre-los-riesgos-en-Internet>

Montañez Ramirez, C. C. (2023). Medidas preventivas de ciberseguridad que debe tener el adulto mayor en Colombia para acceder a internet y sus servicios. Universidad Nacional Abierta y a Distancia. Recuperado de <https://repository.unad.edu.co/bitstream/handle/10596/59691/TRABAJODEGRADOCHRISTIANMONTANEZ.pdf?sequence=1&isAllowed=y>

Moreno Cuervo, A., & Parra Coutin, M. A. (2016). Aprendizaje de TIC por parte del adulto mayor. Recuperado de https://repository.upb.edu.co/bitstream/handle/20.500.11912/3313/Monograf%C3%ADa_Aprendizaje%20de%20TIC%20por%20parte%20del%20adulto%20mayor.pdf?sequence=1&isAllowed=y

Ortoll Espinet, E. (2007). La alfabetización digital en los procesos de inclusión social. Universitat Oberta de Catalunya. Recopilado de <https://www-digitaliapublishing-com.unipamplona.basesdedat>

Pérez-Martínez, A. J., & Ruiz-Rubio, A. (2023). Nuevos trabajos y tecnologías: impacto social y vulnerabilidad de las personas mayores. Recuperado de <https://riuma.uma.es/xmlui/bitstream/handle/10630/26959/NUEVOS%20TRABAJOS%20Y%20TECNOLOG%C3%8DAS.pdf?sequence=1>

Plohn, Santiago Adrián. (2022). Aportes en ciberseguridad a través de la Inteligencia Artificial en la detección de patrones compatibles con ciberataques en redes de Internet de las Cosas. (Trabajo Final de Posgrado. Universidad de Buenos Aires.) Recuperado de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-2423_PlohnSA.pdf

Rodríguez Izquierdo, R. M. (2007). Personas mayores y aprendizaje a lo largo de la vida de las tecnologías de la información y la comunicación. Píxel-Bit. Revista de Medios y Educación, 30, 41-48.

Redacción Segurilatam. (2022, agosto 1). Nueva guía con consejos de ciberseguridad para adultos mayores. Segurilatam. Recuperado de https://www.segurilatam.com/actualidad/nueva-guia-con-consejos-de-ciberseguridad-para-adultos-mayores_20220801.html

Rubio-Romero, J., & Fernández-Díaz, E. (2022). Boomers versus Millennials y Generación Z: Alfabetización digital y redes sociales. Ámbitos. Revista Internacional de Comunicación, (57), 83-103.
<https://revistascientificas.us.es/index.php/Ambitos/article/view/23511/21205>

Ruiz, P. E. (2018). Avances en inteligencia artificial y su impacto en la sociedad. Recuperado de: <http://hdl.handle.net/20.500.11912/4942>.

Sandoval Guarín, L. V., Castillo Gamba, F. M., Guevara Amaya, A. E., & Herrera, H. M. (2023). Diseño e implementación de capacitación en adultos mayores para prevenir técnicas de engaños digitales. Recuperado de https://repository.libertadores.edu.co/bitstream/handle/11371/5948/Castillo_Guevara_Sandoval_2023.pdf?sequence=1&isAllowed=y

Sastoque Mesa, D., y Botero Tabares, R. (2016). Técnicas de detección y control de phishing. Cuaderno Activa, 7(1), 75–81. Recuperado de <https://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/250>

StaySafeOnline. (s.f.). Online Safety Tips for Seniors. Recuperado de <https://staysafeonline.org/es/online-safety-privacy-basics/online-safety-tips-for-seniors/>

Universidad Externado de Colombia. (s.f.). Curso: Seguridad digital y gestión del riesgo cibernético. Recuperado de <https://www.uexternado.edu.co/programa/derecho/curso-seguridad-digital-y-gestion-del-riesgo-cibernetico/>