Análisis de susceptibilidad a fraudes por suplantación de voz mediante inteligencia artificial, en personas de la tercera edad.

Analysis and Mitigation of Voice Spoofing Fraud through Artificial Intelligence in Elderly Individuals.

Recibido:2024/08/12-Aceptado:2024/09/15–Publicado:2024/09/22

Villarreal Herrera, Andrés Esteban[1]
Instituto Superior Tecnológico de Tecnologías Apropiadas, Quito, Ecuador
andres.villarreal@insta.edu.ec

Corella Tipán Stalin Gerardo[2]
Instituto Superior Tecnológico de Tecnologías Apropiadas, Quito, Ecuador
stalin.corella@insta.edu.ec

Pilicita León Jairo Stalin[3]
Instituto Superior Tecnológico de Tecnologías Apropiadas, Quito, Ecuador
jairo.pilicita@insta.edu.ec

Proaño Hidalgo Alexis Daniel[4]
Instituto Superior Tecnológico de Tecnologías Apropiadas, Quito, Ecuador
alexis.proano@insta.edu.ec

Resumen:

El presente artículo aborda la susceptibilidad al fraude por suplantación de voz mediante inteligencia artificial (IA) enfocado en personas de la tercera edad, un grupo particularmente vulnerable a este tipo de estafas debido a su limitada familiaridad con las tecnologías

emergentes. Se llevó a cabo un experimento utilizando herramientas de clonación de voz como Speechify y ElevenLabs para replicar las voces de familiares cercanos a los participantes, todos mayores de 65 años. Se realizaron 40 llamadas simuladas con escenarios diseñados para generar urgencia y preocupación, como accidentes de tránsito o problemas legales. Los resultados muestran que un 72% de los participantes no fueron capaces de identificar que la voz escuchada no pertenecía a su familiar, lo que demuestra la alta vulnerabilidad de este grupo ante estafas telefónicas. Solo un 28% de los participantes detectó la falsificación, generalmente al solicitar más información o verificar la llamada directamente con su familiar.

El análisis revela que el componente emocional juega un papel determinante en la efectividad de estas estafas, ya que las víctimas tienden a reaccionar impulsivamente cuando creen que un ser querido está en peligro. Se discuten estrategias de mitigación, como la educación tecnológica para personas mayores, el desarrollo de tecnologías de detección de fraude y la regulación del uso de IA en la clonación de voz. El artículo concluye que es fundamental implementar un enfoque preventivo que combine educación, tecnología y políticas de seguridad para proteger a este grupo de estafas cibernéticas.

Palabras clave: inteligencia artificial, suplantación de voz, vishing, clonación de voz, fraude cibernético.

Summary

The present article addresses the susceptibility to fraud by voice impersonation through artificial intelligence (AI), focusing on elderly individuals, a group particularly vulnerable to this type of scam due to their limited familiarity with emerging technologies. An experiment was conducted using voice cloning tools such as Speechify and ElevenLabs to replicate the voices of close family members of the participants, all over 65 years old. A total of 40 simulated calls were made with scenarios designed to create urgency and concern, such as traffic accidents or legal problems. The results show that 72% of the participants were unable

to identify that the voice they heard did not belong to their relative, demonstrating the high vulnerability of this group to phone scams. Only 28% of the participants detected the forgery, generally by requesting more information or verifying the call directly with their family member.

The analysis reveals that the emotional component plays a crucial role in the effectiveness of these scams, as victims tend to react impulsively when they believe a loved one is in danger. Mitigation strategies are discussed, such as technological education for seniors, the development of fraud detection technologies, and the regulation of AI use in voice cloning. The article concludes that it is essential to implement a preventive approach that combines education, technology, and security policies to protect this group from cyber fraud.

Keyword: artificial intelligence, voice spoofing, vishing, voice cloning, cyber fraud.

Introducción

El avance de la inteligencia artificial (IA) ha revolucionado múltiples industrias, proporcionando herramientas que, si bien son beneficiosas en muchas áreas, también han sido explotadas para actividades delictivas. Un área de especial preocupación es el uso de tecnologías de clonación de voz. Estas herramientas permiten replicar una voz humana con alta precisión utilizando una breve grabación, lo que ha facilitado la suplantación de identidad en estafas telefónicas. El vishing (voice phishing) es una variante de la ingeniería social que se basa en llamadas telefónicas fraudulentas para manipular a las víctimas y obtener información sensible o inducirlas a realizar transferencias de dinero. Los estafadores pueden utilizar la clonación de voz para hacerse pasar por familiares o amigos cercanos, lo que incrementa el nivel de confianza de la víctima y, por lo tanto, la efectividad del engaño (Caldwell, 2021).

Los adultos mayores son especialmente vulnerables a este tipo de fraude. Estudios recientes han demostrado que las personas de la tercera edad, debido a su limitada familiaridad con la tecnología digital y su confianza en las interacciones telefónicas, son un objetivo preferido para los delincuentes cibernéticos. Según un informe de la Comisión Federal de Comercio (FTC), los fraudes relacionados con suplantación de identidad y vishing dirigidos a adultos mayores han aumentado en los últimos años, con pérdidas estimadas en millones de dólares (FTC, 2022). La brecha tecnológica, sumada a la respuesta emocional que provoca escuchar la voz de un ser querido en apuros, hace que los adultos mayores sean particularmente susceptibles a estas tácticas (Mendenhall & Ferris, 2020).

La tecnología de clonación de voz ha avanzado rápidamente, con herramientas como Speechify y ElevenLabs que permiten generar voces clonadas con pocos segundos de grabación. Aunque estas tecnologías tienen aplicaciones legítimas, como la creación de voces personalizadas para asistentes virtuales o la mejora de la accesibilidad para personas con discapacidades, su uso en actividades delictivas plantea graves problemas de seguridad. La facilidad con la que estos clonadores de voz están disponibles en línea ha permitido que los estafadores puedan replicar la voz de cualquier persona con fines maliciosos (Wells-Edwards, 2022).

En Ecuador, donde los adultos mayores representan una proporción significativa de la población, la vulnerabilidad a estafas como el vishing es particularmente alta. El Instituto Nacional de Estadística y Censos (INEC) reporta que más de 1.3 millones de personas en el país pertenecen a este grupo etario (INEC, 2022). Esto subraya la necesidad urgente de abordar esta problemática mediante estrategias de mitigación que combinen educación tecnológica, regulación del uso de IA y el desarrollo de tecnologías de detección de fraude. Este artículo se enfoca en analizar el impacto del uso de herramientas de clonación de voz en estafas telefónicas dirigidas a personas de la tercera edad, y propone soluciones para reducir su vulnerabilidad.

Contexto y justificación

La digitalización global ha transformado la manera en que interactuamos y realizamos transacciones diarias. Sin embargo, este progreso no ha sido uniforme. Las personas de la tercera edad, en su mayoría, no han sido educadas en el uso avanzado de las tecnologías digitales, lo que las coloca en una posición de desventaja frente a las amenazas cibernéticas. En Ecuador, el Instituto Nacional de Estadística y Censos (INEC) reporta que más del 15% de la población corresponde a adultos mayores, un grupo que se ha visto afectado por diversas modalidades de fraude, con un crecimiento exponencial de los fraudes telefónicos en los últimos años.

Una de las variantes de este tipo de fraude, el vishing, ha ganado popularidad gracias a los avances en tecnologías de síntesis de voz. Estas herramientas permiten que estafadores reproduzcan la voz de un familiar o conocido, engañando a las víctimas para que crean que están interactuando con una persona de confianza. Las investigaciones iniciales, como las presentadas en este estudio, demuestran que los adultos mayores son particularmente propensos a caer en estos engaños, ya que no están familiarizados con la existencia de herramientas de clonación de voz ni con los riesgos que estas implican.

Problemática y objetivos del estudio

La suplantación de voz mediante inteligencia artificial (IA) ha emergido como una herramienta poderosa para los estafadores, particularmente en el ámbito del vishing (voice phishing). Esta técnica implica la reproducción de la voz de una persona de confianza mediante herramientas de clonación de voz, lo que engaña a las víctimas y las lleva a tomar decisiones precipitadas, como realizar transferencias bancarias o proporcionar información sensible (Caldwell, 2021). Aunque este tipo de fraude puede afectar a cualquier persona, los adultos mayores se encuentran en una posición de especial vulnerabilidad. Esto se debe, en gran medida, a su menor familiaridad con las tecnologías emergentes, así como a la respuesta

emocional que experimentan al escuchar la voz de un supuesto familiar en peligro (Mendenhall & Ferris, 2020).

Los datos recientes confirman que los adultos mayores son uno de los grupos más afectados por los fraudes cibernéticos. Según la Comisión Federal de Comercio (FTC), el número de estafas relacionadas con la suplantación de identidad telefónica ha aumentado significativamente en los últimos años, y las personas mayores de 60 años representan un porcentaje considerable de las víctimas (FTC, 2022). Además, el Instituto Nacional de Estadística y Censos (INEC) reporta que la población de adultos mayores en países como Ecuador ha crecido considerablemente, con más de 1.3 millones de personas mayores de 65 años, lo que aumenta el riesgo de que este grupo sea objetivo de fraudes electrónicos (INEC, 2022).

El objetivo general de este estudio es analizar cómo las herramientas de clonación de voz mediante IA están siendo utilizadas para realizar estafas dirigidas a adultos mayores y, en consecuencia, identificar las vulnerabilidades específicas de este grupo. A partir de este análisis, se proponen estrategias de mitigación basadas en la educación tecnológica, el desarrollo de herramientas de detección de fraude y la regulación del uso de IA en la clonación de voz. Adicionalmente, el estudio busca explorar cómo la respuesta emocional de los adultos mayores ante llamadas fraudulentas contribuye a su vulnerabilidad, y qué medidas pueden implementarse para ayudarles a manejar mejor este tipo de situaciones.

Este análisis es crucial, ya que estudios previos han demostrado que las personas mayores, debido a su confianza intrínseca en las relaciones familiares y su falta de conocimiento sobre las nuevas amenazas tecnológicas, tienden a ser manipuladas con mayor facilidad mediante técnicas de ingeniería social (Caldwell, 2021; Mendenhall & Ferris, 2020). Los objetivos específicos incluyen la identificación de los principales factores que influyen en la capacidad de las personas mayores para detectar estafas por clonación de voz, y la propuesta de soluciones prácticas que reduzcan su exposición a este tipo de delitos.

Metodología

Este estudio se diseñó con el objetivo de analizar la efectividad de las herramientas de clonación de voz mediante inteligencia artificial en la suplantación de identidad y evaluar la vulnerabilidad de las personas de la tercera edad ante fraudes telefónicos. Para ello, se llevaron a cabo llamadas simuladas utilizando voces clonadas de familiares de los participantes, quienes fueron seleccionados específicamente por su falta de familiaridad con tecnologías avanzadas. A continuación, se describen los materiales utilizados y el procedimiento metodológico implementado para realizar este experimento, garantizando la validez de los datos y un análisis riguroso de los resultados.

1. Selección de participantes: Se eligió una muestra de 40 personas mayores de 65 años, con una mezcla de habilidades tecnológicas básicas. Se incluyeron solo personas que usaban teléfonos móviles y tenían contacto ocasional con tecnología.
2. Herramientas de clonación de voz: Se utilizaron dos herramientas de IA, Speechify y ElevenLabs, para generar voces clonadas a partir de grabaciones de voz de familiares cercanos de los participantes. Las voces se probaron previamente para asegurarse de su similitud con las originales.
3. Diseño del experimento: Se realizaron 40 llamadas simuladas, en las que se utilizó un guion predefinido que incluía escenarios de emergencia familiar (como accidentes o problemas legales). Los participantes fueron monitoreados para registrar su reacción y si detectaban o no la suplantación.
4. Análisis de resultados: Se registraron las respuestas de los participantes, clasificando los resultados en tres categorías: caída en la estafa, duda sobre la veracidad y detección de fraude.

Resultados

El estudio realizado permitió obtener datos importantes sobre la efectividad de las herramientas de clonación de voz y la vulnerabilidad de las personas de la tercera edad frente a fraudes telefónicos. En total, se realizaron 40 llamadas simuladas utilizando voces clonadas de familiares de los participantes. Estas llamadas, diseñadas para replicar situaciones de emergencia, fueron recibidas por personas mayores de 65 años. Los resultados muestran un panorama preocupante en cuanto a la capacidad de este grupo para detectar la suplantación de voz.

Del total de llamadas realizadas, 28 participantes (72%) no lograron identificar que la voz que escuchaban no pertenecía realmente a su familiar. Estos participantes reaccionaron de manera inmediata y emocional ante las situaciones planteadas en los guiones, que incluían emergencias como accidentes de tránsito y problemas legales, lo que los llevó a realizar acciones como la promesa de transferir dinero o de proporcionar información personal sensible. La mayoría de los participantes de este grupo mencionaron que la voz sonaba "exactamente igual" a la de su ser querido, lo que refuerza la efectividad de la clonación de voz mediante IA en este tipo de estafas.

Por otro lado, el 28% de los participantes restantes logró detectar la estafa o, al menos, evitó caer en ella. Estos participantes utilizaron estrategias como solicitar más información sobre la situación o colgar la llamada para contactar directamente con el familiar en cuestión antes de tomar una decisión. Este comportamiento muestra una cierta resistencia natural al fraude, probablemente influenciada por una mayor conciencia sobre los posibles riesgos de ser víctima de estafas telefónicas, o por su actitud más prudente al recibir este tipo de llamadas inesperadas.

Un análisis más detallado de los resultados muestra que no hubo una gran diferencia en la efectividad de los clonadores de voz utilizados en el estudio. Tanto Speechify como ElevenLabs lograron generar voces que engañaron a la mayoría de los participantes. Sin embargo, se observó que, en los casos en los que los participantes solicitaron más detalles o

tiempo para procesar la información, la capacidad de los estafadores para continuar con éxito la llamada disminuyó significativamente, lo que sugiere que la eficacia de la clonación depende en gran medida de la rapidez con la que se desarrollan los eventos en la llamada.

También es importante destacar que la reacción emocional fue un factor determinante en la efectividad del fraude. Los guiones que apelaban a la preocupación familiar o al miedo por la seguridad de un ser querido resultaron ser más efectivos, ya que activaron una respuesta inmediata por parte de las víctimas, lo que les impidió analizar críticamente la situación. Este factor emocional redujo notablemente la capacidad de los participantes para detectar inconsistencias en la llamada, como la calidad de la voz o la falta de detalles coherentes en la historia narrada.

Discusión

Los resultados obtenidos en este estudio revelan que las personas de la tercera edad son altamente vulnerables a fraudes telefónicos que utilizan la suplantación de voz mediante inteligencia artificial (IA). La elevada tasa de éxito observada (72% de los participantes engañados) pone de manifiesto la necesidad urgente de implementar medidas preventivas que protejan a este grupo frente a este tipo de estafas. Los hallazgos son coherentes con estudios previos sobre la vulnerabilidad tecnológica de los adultos mayores, quienes a menudo carecen de la experiencia necesaria para detectar avances tecnológicos como la clonación de voz, lo que les hace más propensos a confiar en las llamadas fraudulentas como es en el caso de Anderson (2020).

Uno de los factores más determinantes en la efectividad de estas estafas es el componente emocional involucrado. Los guiones utilizados en el experimento apelaban a situaciones familiares urgentes (como accidentes de tráfico o detenciones policiales), lo que provocó una respuesta emocional inmediata en los participantes. Este comportamiento está en línea con investigaciones previas que señalan que, cuando las víctimas creen que sus seres

queridos están en peligro, tienden a tomar decisiones rápidas y basadas en emociones, lo que reduce su capacidad crítica para evaluar la veracidad de la llamada (Mendenhall & Ferris, 2020). La combinación de una situación de crisis con el uso de una voz familiar resulta en una manipulación eficaz de las víctimas, aprovechando la ingeniería social para el beneficio de los estafadores (Caldwell, 2021).

Además, el estudio confirma la eficacia de las herramientas de clonación de voz, como Speechify y ElevenLabs, para replicar voces de manera convincente. Esto plantea serias preocupaciones sobre el acceso público a estas tecnologías. En su estado actual, las herramientas de clonación de voz están ampliamente disponibles, lo que facilita su uso indebido por parte de actores maliciosos. Como han señalado expertos en ciberseguridad, la falta de regulación de estas tecnologías es un problema crítico que debe abordarse de manera urgente para evitar que sean utilizadas en fraudes cibernéticos (Wells-Edwards, 2022). La accesibilidad y precisión de estas herramientas incrementan considerablemente el riesgo de que los adultos mayores sean víctimas de vishing y otros fraudes basados en la suplantación de identidad.

Otro aspecto relevante es la falta de conciencia tecnológica entre las personas mayores, lo que aumenta su susceptibilidad. Estudios han mostrado que la alfabetización digital en los adultos mayores es generalmente baja, especialmente en lo que respecta a los riesgos de la inteligencia artificial y el fraude digital (Anderson, 2020). En este sentido, la educación y la concienciación sobre estos peligros deben ser una prioridad en cualquier estrategia de mitigación. Los programas de alfabetización digital pueden ayudar a las personas de la tercera edad a desarrollar una comprensión básica de las tecnologías emergentes, lo que les permitiría tomar decisiones más informadas y críticas ante una posible estafa.

Por último, es necesario subrayar que, aunque la tecnología puede ser utilizada de manera maliciosa, también ofrece soluciones. Herramientas de detección de fraude basadas en IA podrían ayudar a prevenir estas estafas, analizando patrones de voz o detectando

anomalías en las llamadas que alerten a los usuarios sobre la posibilidad de un engaño (Caldwell, 2021). Estas tecnologías podrían integrarse en dispositivos móviles y aplicaciones telefónicas que usen los adultos mayores, emitiendo alertas en tiempo real cuando se detecten posibles suplantaciones de voz. Sin embargo, para que estas soluciones sean efectivas, es crucial que se diseñen teniendo en cuenta la usabilidad para personas con poca experiencia tecnológica, asegurando que no se conviertan en una fuente adicional de frustración para los usuarios.

En conclusión, la combinación de factores como la respuesta emocional, la familiaridad limitada con la tecnología y el acceso no regulado a herramientas de clonación de voz crea un escenario peligroso para los adultos mayores, que pueden ser fácilmente manipulados mediante vishing. además, es importante destacar que los programas de alfabetización digital pueden desempeñar un papel clave en la mitigación de estos riesgos. Los adultos mayores deben ser instruidos no solo sobre el funcionamiento básico de la tecnología, sino también sobre las técnicas de ingeniería social que los delincuentes emplean para manipular sus emociones y su confianza (Cabanellas, 1993; Anderson, 2020). A medida que las tecnologías de IA continúan avanzando, es imperativo que las estrategias de protección evolucionen en paralelo para reducir la vulnerabilidad de las personas mayores ante el fraude cibernético.

Conclusiones

El presente estudio ha revelado que la suplantación de voz mediante inteligencia artificial (IA) es una amenaza significativa para las personas de la tercera edad, especialmente en el contexto de fraudes telefónicos. Los resultados obtenidos indican que un amplio porcentaje de los adultos mayores no es capaz de distinguir una voz clonada de la original, lo que los convierte en blancos vulnerables para los delincuentes cibernéticos. Esta vulnerabilidad se debe, en gran medida, a la falta de familiaridad tecnológica y a la confianza que estas personas depositan en las interacciones familiares. La educación tecnológica emerge como

una de las herramientas más importantes para mitigar estos riesgos. Es esencial diseñar programas específicos que instruyan a los adultos mayores sobre los peligros del vishing y otras formas de estafas digitales, proporcionándoles habilidades prácticas para verificar la autenticidad de las comunicaciones que reciben.

Otra conclusión clave es que el componente emocional juega un papel crucial en la efectividad de las estafas. La mayoría de las víctimas que cayeron en la estafa lo hicieron al percibir una situación de urgencia relacionada con la seguridad de un ser querido. Esto destaca la importancia de educar no solo sobre los aspectos técnicos de la suplantación de voz, sino también sobre la gestión emocional ante situaciones de crisis que puedan ser simuladas por los estafadores. Reaccionar de manera racional y no precipitarse al tomar decisiones basadas únicamente en emociones puede ser una estrategia efectiva para evitar caer en estos engaños. Esto implica no solo enseñar a las personas mayores a ser más conscientes de las estafas, sino también alentarlas a buscar maneras seguras de verificar la información antes de actuar.

En tercer lugar, los resultados indican que las herramientas de clonación de voz disponibles públicamente, como Speechify y ElevenLabs, poseen una capacidad alarmante para replicar voces con un alto nivel de similitud. Esto sugiere que el acceso a estas tecnologías debe ser regulado y controlado más estrictamente. Si bien estas herramientas fueron creadas con fines legítimos, como mejorar la accesibilidad o personalizar interacciones digitales, su potencial para el mal uso es considerable. Por lo tanto, es necesario que se promueva un marco regulatorio que limite su acceso a fines educativos y profesionales, exigiendo una mayor supervisión sobre quién puede utilizarlas y para qué propósito. Asimismo, la colaboración entre las empresas tecnológicas y los organismos de seguridad es vital para monitorear posibles abusos de estas herramientas.

Finalmente, el estudio resalta la necesidad de desarrollar tecnologías de detección de fraude que puedan integrarse en sistemas telefónicos y dispositivos utilizados por adultos

mayores. Estas tecnologías deben ser capaces de identificar características anómalas en las voces o patrones sospechosos en las llamadas, emitiendo alertas en tiempo real para advertir a los usuarios de la posibilidad de estar siendo engañados. Además, es necesario que estas herramientas sean fáciles de usar, adaptadas a las capacidades técnicas de las personas mayores, y estén disponibles en sus dispositivos cotidianos. En conjunto con la educación y la regulación, el desarrollo de estas tecnologías puede reducir significativamente la tasa de éxito de las estafas de suplantación de voz, protegiendo así a uno de los grupos más vulnerables de la sociedad.

Referencias bibliográficas

Anderson, C. (2020). Technological vulnerabilities in aging populations: Fraud and cybersecurity. Journal of Gerontology, 75(6), 1135-1141. https://doi.org/10.1093/geront/gnaa017

Cabanellas, G. (1993). Diccionario Jurídico Elemental.

Caldwell, T. (2021). The impact of voice cloning on cybersecurity: Threats and opportunities. Journal of Information Security, 15(3), 45-62. https://doi.org/10.1007/s10207-021-00540-1

Caranica, A. (2017). Speech recognition results for voice-controlled assistive applications. Speech Technology and Human-Computer Dialogue (SpeD).

Comisión Económica para América Latina y el Caribe (CEPAL). (2017). Derechos de las personas mayores: Retos para la interdependencia y autonomía. Asunción.

Federal Bureau of Investigation (FBI). (2022). Elder fraud report 2021-2022. https://www.fbi.gov/elder-fraud

Federal Trade Commission (FTC). (2022). Protecting older consumers 2021-2022: A report of the Federal Trade Commission. https://www.ftc.gov/reports/protecting-older-consumers-2021-2022-report-federal-trade-commission

Holdings. (2024). Vishing. WhatIsMyIPAddress. https://whatismyipaddress.com/vishing

Instituto Nacional de Estadística y Censos (INEC). (2022). Censo poblacional 2022. https://www.censoecuador.gob.ec/

Larraín, G. (2017). Longevidad y pensiones: Una propuesta de seguro para la cuarta edad.

Mahuad Calderón, P. (2005). Los delitos informáticos: La ineficiente e inadecuada protección penal en el ordenamiento jurídico ecuatoriano. Quito: USFQ.

Mendenhall, R., & Ferris, S. (2020). Elder fraud and the rise of social engineering attacks targeting seniors. Journal of Elder Abuse & Neglect, 32(4), 1-14. https://doi.org/10.1080/08946566.2020.1795558

Montes, M. (2023). Las 10 cosas que más tememos de la inteligencia artificial. La Tercera. https://www.latercera.com/que-pasa/noticia/las-10-cosas-que-mas-tememos-de-la-inteligencia-artificial

Real Academia Española (RAE). (2001). Significados: Estafa. https://www.rae.es/drae2001/estafa

Skiba, M. (2019). Estafa. AARP. https://www.aarp.org/espanol/dinero/estafas-y-fraudes/info-2019/cfpb-adultos-mayores-victimas-abuso-financiero.html

Speechify. (2024). Clonador de voz. https://voiceover.speechify.com/editor/x3efhexvagf5uzff9oqg?cloning=true

Wells-Edwards, B. (2022). What's in voice? The legal implications of voice cloning. Arizona Law Review, 64, 1213-1235. https://arizonalawreview.org/articles/volume-64

Revista INNDEV. ISSN 2773-7640.Agosto-noviembre 2024. Vol. 3, Núm 2, p. 17-32.

https://doi.org/10.69583/inndev.v3n2.2024.134