Revista Científica Multidisciplinar G-ner@ndo
ISSN: 2806-5905

Estrategias innovadoras para mitigar la suplantación de identidad en redes sociales.
Innovative strategies to mitigate identity theft on social networks.

Richard Alejandro Macías-Lara, Jair Oswaldo Bedoya-Benavides, Juan Carlos Manchay Orbea, Gilbert Nazareno Vivero, Rodolfo Marlon Mina Angulo

CONFLUENCIA DE INNOVACIONES CIENTÍFICAS
Enero - junio, V°5-N°1; 2024

✓ **Recibido:** 298/03/2024
✓ **Aceptado**: 09/04/2024
✓ **Publicado:** 30/06/2024

PAIS

- Ecuador, Esmeraldas
- Ecuador, Esmeraldas
- Ecuador, Esmeraldas
- Ecuador, Esmeraldas
- Ecuador, Esmeraldas

INSTITUCIÓN

- Universidad Técnica Luis Vargas Torres de Esmeraldas.
- Universidad Técnica Luis Vargas Torres de Esmeraldas.
- Universidad Técnica Luis Vargas Torres de Esmeraldas.
- Universidad Técnica Luis Vargas Torres de Esmeraldas.
- Universidad Técnica Luis Vargas Torres de Esmeraldas.

CORREO:

alejandro.macias@utelvt.edu.ec
jair.bedoya.benavides@utelvt.edu.ec
juan.manchay.orbea@utelvt.edu.ec
gilbert.Nazareno@utelvt.edu.ec
marlon.mina.angulo@utelvt.edu.ec

ORCID:

https://orcid.org/0000-0003-2164-3171
https://orcid.org/0009-0009-7180-1749
https://orcid.org/0000-0003-1404-1383
https://orcid.org/0000-0002-8971-5277
https://orcid.org/0000-0002-5823-1034

FORMATO DE CITA APA.

Macías-Lara, R. Bedoya J. Manchay, J. Vivero, G. Mina, R. (2024). Estrategias innovadoras para mitigar la suplantación de identidad en redes sociales. Revista G-ner@ndo, V°5 (N°1,). 544 -561.

Resumen

La suplantación de identidad, también conocida como robo de identidad, constituye un desafío creciente en el entorno digital actual. A medida que nuestra vida cotidiana se integra cada vez más con la tecnología, es crucial abordar esta amenaza que puede tener repercusiones devastadoras para las víctimas, con el propósito de resaltar la importancia crítica de combatir la suplantación de identidad en la sociedad contemporánea. En este contexto, diversos estudios han propuesto estrategias para combatir este problema. Por ejemplo, Cheng et al. (2017) sugieren el desarrollo de sistemas de detección avanzados basados en inteligencia artificial, mientras que Goga et al. (2015) resaltan la importancia de integrar múltiples fuentes de información. Además, Khaled et al. (2018) proponen campañas de concientización y educación dirigidas a los usuarios para fortalecer su capacidad de protegerse. La implementación exitosa de estas estrategias promete un futuro más seguro y confiable para los usuarios en línea. Al mitigar los riesgos de suplantación de identidad y otros delitos cibernéticos, se fortalece la confianza en las plataformas en línea y se fomenta un entorno digital más inclusivo y accesible para todos. En última instancia, la colaboración entre individuos, empresas, gobiernos y profesionales de seguridad cibernética es fundamental para mantener la integridad y la confianza en un mundo digital en constante cambio. Este enfoque proactivo no solo protege la integridad de los usuarios, sino que también fortalece la confianza en las plataformas en línea, fomentando así un entorno digital más seguro y fiable para todos.

Palabras clave: identidad digital, suplantación de identidad, estrategias, redes sociales.

Abstract

Identity theft, also known as identity theft, is a growing challenge in today's digital environment. As our daily lives become increasingly integrated with technology, it is crucial to address this threat that can have devastating repercussions for victims, with the purpose of highlighting the critical importance of combating impersonation in contemporary society. In this context, several studies have proposed strategies to combat this problem. For example, Cheng et al. (2017) suggest the development of advanced detection systems based on artificial intelligence, while Goga et al. (2015) highlight the importance of integrating multiple sources of information. In addition, Khaled et al. (2018) propose awareness and education campaigns aimed at users to strengthen their ability to protect themselves. The successful implementation of these strategies promises a safer and more reliable future for online users. By mitigating the risks of phishing and other cybercrimes, trust in online platforms is strengthened and a more inclusive and accessible digital environment is fostered for all. Ultimately, collaboration between individuals, businesses, governments, and cybersecurity professionals is critical to maintaining integrity and trust in an ever-changing digital world. This proactive approach not only protects the integrity of users, but also strengthens trust in online platforms, thus fostering a safer and more trustworthy digital environment for all.

Keywords: digital identity, identity theft, strategies, social networks.

Introducción

En la era digital, nuestra identidad se ha expandido más allá de las fronteras físicas y se ha visto reflejada en nuestras actividades en línea (Baldini et al., 2020; Olivero et al., 2020). Actualmente, dependemos de la tecnología digital para comunicarnos, realizar transacciones financieras y almacenar nuestros datos personales. Por esta razón, la dependencia creciente en los sistemas digitales e informáticos también ha traído consigo una serie de vulnerabilidades y riesgos, entre ellos la suplantación de identidad (Martínez–Ferrer & Ruiz, 2017; Reznik, 2013).

En este sentido, la suplantación de identidad, también conocida como robo de identidad, es un riesgo cada vez más relevante en el panorama digital actual. De este modo, a medida que nuestras vidas se entrelazan más estrechamente con la tecnología, los delincuentes cibernéticos han encontrado nuevas formas de aprovecharse de esta dependencia(Lux & Calderón, 2020). Esta actividad delictiva puede tener consecuencias devastadoras para las víctimas, desde la pérdida económica hasta el daño a la reputación personal.

El objetivo principal de este artículo es resaltar la importancia crítica de combatir la suplantación de identidad en la sociedad contemporánea. La proliferación de ataques cibernéticos y el incremento de casos de robo de identidad han generado una sensación de vulnerabilidad entre los usuarios de la tecnología digital. En este sentido, es fundamental concienciar a las personas sobre las medidas de seguridad que pueden implementar para proteger su información personal y prevenir fraudes. Además, la suplantación de identidad no solo afecta a individuos, sino que también tiene repercusiones en instituciones financieras, empresas y gobiernos. Por lo tanto, abordar este problema es esencial para garantizar la integridad y seguridad de las transacciones financieras, la protección de la propiedad intelectual y la preservación de la confianza en las instituciones públicas y privadas.

En este artículo, se explorarán las diversas formas en que la suplantación de identidad puede ocurrir en redes sociales, así como las estrategias y medidas de seguridad que los

individuos y las empresas pueden emplear para protegerse. Además, se examinarán las tecnologías emergentes y las mejores prácticas que podrían ser clave en la lucha contra este problema creciente.

Estado del arte.

Los delitos informáticos abarcan una amplia gama de actividades ilegales que se realizan en el entorno digital. La suplantación de identidad es solo uno de los muchos delitos informáticos que las personas pueden enfrentar en la era digital. Otros ejemplos incluyen el fraude en línea, el robo de información personal, el phishing y la manipulación de datos (Macías-Lara et al., 2022).

En este sentido, el uso empresarial de los datos en redes sociales ha adquirido una relevancia significativa en la última década. Pues, las empresas utilizan las redes sociales para recopilar información sobre las preferencias, comportamientos y opiniones de los consumidores (McCourt, 2022). Este análisis de datos permite comprender mejor a su audiencia, personalizar estrategias de marketing y mejorar la toma de decisiones comerciales. Además, el monitoreo de las redes sociales también permite a las empresas detectar posibles casos de suplantación de identidad y proteger la reputación de su marca. El uso ético y responsable de estos datos es fundamental para construir relaciones sólidas con los clientes y garantizar la seguridad y privacidad de su información personal (Jurado et al., 2022).

Los insights en el ámbito de la suplantación de identidad son fundamentales para comprender las tendencias y patrones que rodean este fenómeno. Estos insights pueden provenir del análisis de datos de ataques cibernéticos, comportamientos delictivos en línea y vulnerabilidades en sistemas informáticos. Al obtener estas perspicacias, las empresas y las entidades encargadas de la seguridad cibernética pueden anticipar y responder de manera proactiva a las amenazas de suplantación de identidad. Los insights también pueden revelar las deficiencias en las medidas de seguridad existentes y destacar áreas específicas que requieren

mayor atención. Asimismo, al comprender los motivos y metodologías detrás de los ataques de suplantación de identidad, se pueden implementar estrategias más efectivas para la prevención y detección temprana (Burt, 2020)

La suplantación de identidad, también conocida como robo de identidad, se define como el acto de usurpar la identidad de otra persona con el fin de cometer fraude, robo o cualquier otra actividad delictiva. Por ende, esta práctica puede llevarse a cabo a través de medios digitales, como el robo de información personal en línea o la creación de perfiles falsos en redes sociales. Es así que la suplantación de identidad puede causar daños significativos a las víctimas, desde pérdidas financieras hasta daños en su reputación, cabe mencionar que es crucial estar alerta y tomar medidas proactivas para protegerse contra esta amenaza cada vez más presente en el entorno digital (Marr, 2023; Calzolari, 2023; Olivero et al., 2020; Marshall & Tompsett, 2005).

La suplantación de identidad digital no solo representa una amenaza para los individuos, sino que también impacta significativamente a las empresas, bancos e instituciones educativas. En el entorno empresarial, el robo de identidad puede dar lugar a la falsificación de transacciones comerciales, el acceso no autorizado a información confidencial y la pérdida de reputación y confianza por parte de los clientes (Thomson, 2022). Los bancos son otro objetivo frecuente de la suplantación de identidad, ya que los delincuentes buscan acceder a cuentas bancarias, solicitar préstamos fraudulentos y realizar transacciones ilegales en nombre de sus víctimas. Del mismo modo, en el ámbito educativo, los estudiantes y el personal pueden ser blancos de suplantación de identidad para acceder a calificaciones, informes académicos o recursos financieros (Estancona, 2023). Es imperativo que todas estas entidades implementen medidas de seguridad robustas, como la verificación en dos pasos, el cifrado de datos y la educación sobre ciberseguridad, para protegerse contra la suplantación de identidad digital (Gulhane & Manwar, 2021).

Las tecnologías emergentes, como la inteligencia artificial, el blockchain y la biometría, juegan un papel crucial en la protección contra la suplantación de identidad en redes sociales y otros entornos digitales. La inteligencia artificial puede ser utilizada para detectar patrones de comportamiento anómalos que podrían indicar intentos de suplantación de identidad. A través del análisis de grandes volúmenes de datos, los algoritmos de inteligencia artificial pueden identificar discrepancias y alertar a los usuarios y a las plataformas sobre posibles actividades fraudulentas. Por otro lado, el blockchain ofrece una forma segura de almacenar y verificar la identidad digital, mediante la descentralización y la criptografía. Además, puede proporcionar un registro inmutable de las transacciones de identidad, lo que reduce significativamente la posibilidad de suplantación. Asimismo, la biometría, que se basa en rasgos físicos únicos como huellas dactilares, reconocimiento facial y escaneos de iris, ofrece un método altamente confiable para autenticar la identidad de los usuarios. La implementación de la biometría en las plataformas digitales puede dificultar en gran medida la suplantación de identidad, ya que los datos biométricos son inherentemente personales y difíciles de replicar (Ghafourian et al. 2023).

Es evidente que la suplantación de identidad representa una amenaza significativa en el mundo digital actual, y se necesitan mayores esfuerzos para abordar esta vulnerabilidad. Asimismo, es necesario identificar y explotar las brechas en la seguridad cibernética que los delincuentes pueden aprovechar para realizar ataques de suplantación de identidad. Además, la educación continua y la concientización sobre las últimas técnicas y métodos utilizados por los ciberdelincuentes son esenciales para fortalecer las defensas contra este tipo de actividad delictiva. Asimismo, la colaboración entre instituciones, empresas y entidades gubernamentales es fundamental para desarrollar estrategias integrales de prevención y respuesta ante la suplantación de identidad en la era digital.

Artículos relacionados.

Para llevar a cabo la búsqueda de investigaciones relacionadas con la suplantación de identidad, se realizó una búsqueda exhaustiva en varias bases de datos científicas, incluyendo Research Gate, ACM Digital Library, IEEE Xplore, Elsevier, Springer Nature, Google Scholar, Dialnet y Forbes. La cadena de búsqueda utilizada incluyó términos como "suplantación de identidad", "robo de identidad", "fraude cibernético", "medidas de seguridad", "tecnologías emergentes" y "prevención de la suplantación de identidad". Se aplicaron filtros para incluir estudios y artículos publicados en los últimos 10 años, escritos en inglés o español, con enfoque en la era digital y la protección de la identidad en línea. Este proceso garantizó la inclusión de investigaciones relevantes y actualizadas en el campo de la suplantación de identidad y las medidas de seguridad asociadas.

El estudio de Cheng et al. (2017) se enfocó en analizar los patrones de comportamiento que caracterizan a los usuarios que intentan suplantar la identidad de otras personas en redes sociales. El objetivo de los investigadores fue desarrollar un modelo predictivo que permitiera identificar este tipo de actividades fraudulentas de manera temprana. Para ello, aplicaron técnicas de aprendizaje automático a un gran conjunto de datos de usuarios de Twitter. Los resultados revelaron que factores como la frecuencia de publicaciones, el uso de imágenes de perfil poco comunes y la existencia de cuentas duplicadas son indicadores clave de posibles intentos de suplantación de identidad. Este trabajo aporta valiosos insights para que las plataformas de redes sociales y las empresas puedan implementar mecanismos de detección y prevención de este tipo de fraude

Por su parte, el estudio de Goga et al. (2015) se enfocó en comprender los métodos y técnicas utilizados por los usuarios para suplantar la identidad de otras personas en redes sociales. Los investigadores recopilaron datos de perfiles falsos en plataformas como Twitter y Facebook, y aplicaron técnicas de análisis de lenguaje, patrones de actividad y características

del perfil para identificar patrones distintivos de este tipo de cuentas. Los hallazgos sugieren que los suplantadores a menudo utilizan fotografías de perfil robadas, publican con una frecuencia sospechosa y tienden a tener una red de conexiones poco natural. Este trabajo aporta un valioso marco de referencia para que las empresas y plataformas de redes sociales puedan desarrollar sistemas de detección y bloqueo de cuentas que intentan suplantar identidades.

El estudio de Khaled et al. (2018) exploró los impactos y consecuencias de la suplantación de identidad en redes sociales, tanto para los usuarios víctimas como para las empresas afectadas. Los investigadores recopilaron y analizaron casos de estudio de este tipo de fraude, utilizando entrevistas y revisión documental. Los resultados indican que la suplantación de identidad puede tener efectos negativos significativos, como daños a la reputación, pérdidas económicas y problemas legales. Además, las empresas a menudo enfrentan desafíos para detectar y responder de manera efectiva a estos incidentes. Este trabajo resalta la importancia de que las empresas y plataformas de redes sociales implementen estrategias proactivas para prevenir y mitigar los riesgos asociados con la suplantación de identidad.

Por otro lado, el estudio de Meligy et al. (2015) se enfoca en el desarrollo de un sistema de identificación de perfiles falsos en redes sociales. El objetivo es proponer una solución tecnológica para mitigar la suplantación de identidad, identificando perfiles falsos y evitando posibles fraudes o crímenes. Se destaca la importancia de integrar distintas fuentes de información, incluyendo un componente de comparación de imágenes y la implementación de un módulo de deep learning para discernir perfiles falsos de reales. El proyecto se desarrolló bajo la metodología Scrum y se espera un crecimiento exponencial una vez implementado. Se menciona la necesidad de refinar las reglas de validación para identificar perfiles falsos que no pertenecen a personas famosas o influencers, así como la posibilidad de utilizar inteligencia artificial para automatizar el proceso de consulta y verificación de perfiles. Este estudio aporta en esta investigación para combatir la suplantación de identidad en redes sociales mediante el desarrollo

de un sistema de identificación de perfiles falsos, utilizando tecnologías como la comparación de imágenes y la inteligencia artificial para mejorar la detección de perfiles fraudulentos, contribuyendo así a la seguridad y protección de los usuarios en línea frente a ciberdelincuentes.

Del mismo modo, el estudio de Munoz and Guillén (2020) tuvo como objetivo detectar perfiles falsos en redes sociales utilizando técnicas de aprendizaje automático, logrando una tasa de detección del 96% en perfiles de Instagram. Los resultados obtenidos destacan la eficacia de este enfoque para identificar perfiles fraudulentos, lo que puede fortalecer las estrategias de seguridad en línea. En conclusión, el uso de algoritmos de aprendizaje automático en la detección de perfiles falsos aporta una herramienta innovadora para combatir la suplantación de identidad en redes sociales, mejorando la autenticidad y protección de la identidad digital de los usuarios en entornos digitales.

En la misma línea, la investigación de Subba et al. (2023) publicada como "Herramienta de Inteligencia Artificial para la Detección de Cuentas Falsas en Redes Sociales en Línea" se centra en el desarrollo de un sistema basado en inteligencia artificial para identificar perfiles falsos en plataformas de redes sociales. El objetivo principal es mejorar la seguridad de los usuarios al detectar de manera eficiente cuentas maliciosas que puedan comprometer la privacidad y la integridad de la información en línea. La metodología aplicada implica el uso de redes neuronales artificiales entrenadas con conjuntos de datos de cuentas falsas y reales para clasificar nuevos perfiles. En el resumen, se destaca la importancia de proteger la información personal en entornos digitales y la relevancia de la inteligencia artificial en la detección de amenazas cibernéticas. Las conclusiones resaltan la efectividad de la herramienta propuesta para identificar perfiles falsos con precisión y rapidez, lo que contribuirá significativamente a fortalecer la seguridad en las redes sociales en línea. Este estudio aportará al campo de la ciberseguridad al ofrecer una solución innovadora respaldada por tecnologías avanzadas de inteligencia artificial para combatir la proliferación de cuentas falsas en entornos virtuales.

Para finalizar, el artículo en el Aun et al. (2023) desarrollan un modelo de aprendizaje profundo RNN-LSTM capaz de identificar con alta precisión diferentes tipos de ataques de ingeniería social en publicaciones de redes sociales, como suplantación de identidad y phishing. Utilizando un pipeline de detección que analiza la fuente, el grafo social y el sentimiento de las publicaciones, el modelo logra clasificar estas amenazas con 0.84 de precisión y 0.81 de tasa de recuerdo, superando a otras técnicas de aprendizaje automático. Estos resultados demuestran que el análisis lingüístico y semántico es efectivo para la detección temprana de ataques de ingeniería social, pudiendo contribuir a fortalecer las estrategias de las plataformas para combatir la suplantación de identidad en redes sociales.

La suplantación de identidad es un problema que afecta a estudiantes, profesionales, personas de todas las edades y empresas. La creciente conectividad digital ha expuesto a todos a riesgos de seguridad cibernética, lo que subraya la importancia de estar informado y tomar medidas preventivas. Los jóvenes estudiantes, en particular, son un grupo vulnerable, ya que utilizan activamente la tecnología en su vida académica y personal. Es crucial que todos los estudiantes estén educados sobre los peligros de la suplantación de identidad y estén equipados con conocimientos para protegerse en línea. Asimismo, cualquier avance en la protección contra la suplantación de identidad beneficiará a toda la sociedad al promover un entorno digital más seguro y confiable para todos.

Resultados y discusión.

En este estudio se han recopilado y analizado datos y resultados de artículos relacionados en referencia a la suplantación de identidad en la sociedad actual. Además, se ha examinado el panorama legal y regulatorio respecto a la suplantación de identidad, identificando vacíos y áreas de mejora para la protección de los individuos.

Los resultados arrojan que la suplantación de identidad en las redes sociales puede ocurrir de diversas maneras, lo que pone en riesgo la información personal y la reputación de los usuarios. De este modo, las maneras más comunes son: a) a través de perfiles falsos, donde los delincuentes crean cuentas que se hacen pasar por otra persona, ya sea un conocido, una celebridad o incluso una institución. Estos perfiles falsos pueden utilizarse para enviar mensajes engañosos, propagar información falsa o realizar actividades ilegales en nombre de la persona suplantada; y, b) el phishing, donde los criminales envían mensajes o correos electrónicos que parecen ser de una fuente legítima, como una red social o una empresa, para engañar a los usuarios y obtener sus credenciales de inicio de sesión u otra información personal. Además, el secuestro de cuentas es otra táctica común utilizada por los suplantadores de identidad en las redes sociales, donde acceden de forma no autorizada a la cuenta de una persona y la utilizan para difundir contenido malicioso o realizar actividades fraudulentas. No obstante, cabe recalcar que las plataformas de redes sociales también tienen la responsabilidad de implementar medidas de seguridad efectivas para proteger la integridad de sus usuarios y prevenir la suplantación de identidad.

Por otra parte, en aspectos legales, la suplantación de identidad en Ecuador se define como la acción de atribuirse sin autorización la identidad de otra persona (Art. 187, COIP). El COIP sanciona este delito con pena privativa de libertad de uno a tres años, la cual aumenta de uno a cinco años si se busca obtener un beneficio económico, causar daño a la víctima o cometer otro delito.

Con estos antecedentes se hace necesario a continuación, presentar las siguientes estrategias para combatir la suplantación de identidad en redes sociales:

Tabla1: Estrategias para empresas

Estrategia	**Descripción**

Implementación de verificación de identidad robusta	Utilizar métodos de verificación de identidad más sólidos, como la verificación en dos pasos.
Monitoreo proactivo de actividad sospechosa	Utilizar herramientas de monitoreo de actividad en tiempo real para detectar comportamientos sospechosos.
Desarrollo de algoritmos de detección de perfiles falsos	Invertir en tecnologías de aprendizaje automático para identificar y bloquear perfiles falsos.
Fortalecimiento de políticas y regulaciones	Revisión y mejora del marco legal y normativo para abordar de manera más efectiva los delitos de suplantación de identidad en el entorno digital.
Campañas de concientización y educación	Implementación de programas de capacitación y divulgación dirigidos a los usuarios de redes sociales sobre los riesgos de la suplantación de identidad.
Colaboración entre plataformas y autoridades	Fomento de la cooperación entre las plataformas de redes sociales, organismos reguladores y fuerzas de seguridad para el intercambio de información.

Tabla 2: Estrategias para personas comunes en redes sociales

Estrategia	Descripción
Mantener información personal privada	Limitar la cantidad de información personal compartida en redes sociales y configurar la privacidad adecuadamente.
Verificar la autenticidad de las solicitudes de amistad	Antes de aceptar solicitudes de amistad, verificar la autenticidad de los perfiles y solo aceptar solicitudes de personas conocidas.
No compartir contraseñas ni información confidencial	Recordar que las plataformas legítimas nunca solicitarán información confidencial a través de mensajes privados.
Utilizar autenticación en dos pasos	Habilitar la autenticación en dos pasos siempre que sea posible para añadir una capa adicional de seguridad.

Análisis de sentimientos y semántica de publicaciones	Aplicación de modelos de procesamiento de lenguaje natural para detectar indicios de intención maliciosa en el contenido de las publicaciones.
Integración de múltiples fuentes de información	Implementación de soluciones que combinen el análisis de perfiles, publicaciones, conexiones y otras fuentes de datos relevantes para tener una visión holística de posibles amenazas.

Por otra parte, la lucha contra la suplantación de identidad en el entorno digital requiere un enfoque integral que combine la sensibilización, la implementación de medidas de seguridad robustas y la adopción de tecnologías innovadoras. En la búsqueda de soluciones efectivas, es crucial examinar las tecnologías emergentes y las mejores prácticas que podrían ser clave en la lucha contra este problema creciente. El desarrollo de sistemas de autenticación biométrica, el uso de inteligencia artificial para la detección de comportamientos fraudulentos y la implementación de métodos de cifrado más sólidos son solo algunas de las innovaciones tecnológicas que tienen el potencial de fortalecer la seguridad en línea y mitigar el riesgo de suplantación de identidad. Además, la colaboración entre gobiernos, instituciones financieras, empresas y expertos en ciberseguridad es fundamental para desarrollar estrategias efectivas que aborden este desafío en constante evolución. Así pues, la conciencia y la preparación son fundamentales en la batalla contra la suplantación de identidad en el mundo digital, y la adopción de tecnologías emergentes desempeñará un papel vital en la protección de la identidad y la seguridad de los usuarios en línea.

Discusión.

La implementación de las estrategias propuestas para combatir la suplantación de identidad en redes sociales promete un futuro más seguro y confiable para los usuarios en línea.

Los hallazgos de diversos estudios enfocados en la detección temprana de perfiles falsos, el análisis de patrones de comportamiento y la colaboración entre plataformas y autoridades respaldan la efectividad de estas medidas (Cheng et al., 2017; Goga et al., 2015; Khaled et al., 2018). Al desarrollar sistemas de detección avanzados basados en inteligencia artificial y análisis de sentimientos, las empresas pueden anticipar y neutralizar intentos de fraude con mayor eficacia (Meligy et al., 2015; Munoz & Guillén, 2020). Este enfoque proactivo no solo protege la integridad de los usuarios, sino que también fortalece la confianza en las plataformas en línea, fomentando así un entorno digital más seguro y fiable para todos (Subba et al., 2023).

Además de abordar los desafíos actuales de la suplantación de identidad, la implementación de estas estrategias sienta las bases para un futuro más resiliente frente a amenazas cibernéticas emergentes. La integración de múltiples fuentes de información y el fortalecimiento de políticas y regulaciones proporcionan un marco sólido para abordar no solo la suplantación de identidad, sino también otras formas de fraude en línea (Cheng et al., 2017; Goga et al., 2015). Al mismo tiempo, las campañas de concientización y educación dirigidas a los usuarios fortalecen la capacidad de las personas para protegerse y responder ante posibles amenazas, creando una cultura de seguridad digital que perdura en el tiempo (Khaled et al., 2018, Meligy et al., 2015). Esta perspectiva proactiva no solo previene incidentes futuros, sino que también reduce los costos asociados con la recuperación y mitigación de ataques cibernéticos.

En última instancia, la implementación exitosa de estas estrategias tiene el potencial de transformar el paisaje digital, donde la confianza y la seguridad son elementos centrales en la interacción en línea. Al mitigar los riesgos de suplantación de identidad y otros delitos cibernéticos, las personas y las empresas pueden aprovechar plenamente los beneficios de la conectividad digital sin temor a ser víctimas de fraudes o violaciones de privacidad (Munoz & Guillén, 2020; Subba et al., 2023). Este futuro prospectivo promueve un entorno digital inclusivo

y accesible para todos, donde la protección de la identidad y la seguridad en línea son prioridades fundamentales respaldadas por tecnologías avanzadas y colaboraciones efectivas entre todos los actores involucrados.

Conclusiones

La suplantación de identidad es un problema en constante evolución que plantea desafíos significativos en la era digital. A medida que nuestra vida cotidiana se entrelaza cada vez más con la tecnología, es crucial estar al tanto de las vulnerabilidades y riesgos asociados con la suplantación de identidad. En este sentido, la protección de la información personal y la prevención de fraudes deben ser prioridades tanto a nivel individual como para las instituciones financieras, empresas y gobiernos.

Es imperativo que se fomenten medidas de seguridad proactivas para contrarrestar la suplantación de identidad, y que se promueva la concienciación sobre las estrategias disponibles para protegerse en el entorno digital. Además, el desarrollo y la implementación de tecnologías emergentes, junto con la adopción de las mejores prácticas en seguridad cibernética, son esenciales para mitigar este problema en evolución.

La lucha contra la suplantación de identidad requiere una colaboración entre individuos, empresas, gobiernos y profesionales de seguridad cibernética, con el fin de mantener la integridad y la confianza en un mundo digital en constante cambio.

Referencias bibliográficas

Aun, Y., Gan, M., Wahab, N H A., & Guan, G H. (2023, January 1). Social Engineering Attack Classifications on Social Media Using DeepLearning. , 74(3), 4917-4931. https://doi.org/10.32604/cmc.2023.032373

Baldini, G., Barrero, J., Draper, G., Duch-Brown, N., Eulaerts, O., Geneiatakis, D., Joanny, G., Kerckhof, S., Lewis, A., Martin, T., Nativi, S., Neisse, R., Papameletiou, D., Hernández-Ramos, J L., Reina, V., Ruzzante, G L., Sportiello, L., Steri, G., & Tirendi, S. (2020, January 1). Cybersecurity, our digital anchor : a European perspective. https://doi.org/10.2760/352218

Burt, T. (2020, September 29). Microsoft report shows increasing sophistication of cyber threats. https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/

Calzolari, A. (2023, March 31). Suplantación de coautorías en repositorios científicos virtuales. https://doi.org/10.51987/revhospitalbaires.v43i1.254

Cheng, J., Bernstein, M., Danescu-Niculescu-Mizil, C., & Leskovec, J. (2017, November 10). Anyone Can Become a Troll: Causes of Trolling Behavior in Online Discussions. Computer science bibliography. https://dblp.org/rec/journals/corr/ChengBDL17.html

Ecuador. Asamblea Nacional. (2014). Código Orgánico Integral Penal. Registro Oficial No. 180, Quito, Ecuador. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Estancona, A. (2023, December 14). Responsabilidad de las entidades financieras ante el hackeo de cuentas bancarias. En particular, casos de “phising”. https://dialnet.unirioja.es/servlet/articulo?codigo=8897911

Ghafourian, M., Sumer, B., Vera-Rodríguez, R., Fiérrez, J., Tolosana, R., Moralez, A., & Kindt, E. (2023, February 21). Combining Blockchain and Biometrics: A Survey on Technical Aspects and a First Legal Analysis. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2302.10883

Goga, O., Venkatadri, G., & Gummadi, K P. (2015, October 28). The Doppelgänger Bot Attack. , 141-153. https://doi.org/10.1145/2815675.2815699

Gulhane, P N., & Manwar, Y V. (2021, December 15). Introduction to Cyber Security - A Review. https://doi.org/10.32628/ijsrst218674

Jurado, C., Macías-Lara, A., Leyva, A., Sacón-Klinger, A., & Choez, C. (2022, December 12). Vinculación con la sociedad: capacitación para el buen manejo de las tecnologías por parte de la Universidad Técnica “Luis Vargas Torres” de Esmeraldas. G-ner@ndo, 3(2), 15. https://revista.gnerando.org/revista/index.php/RCMG/article/view/45/42

Khaled, S., El-Tazi, N., & Mokhtar, H. (2018, January 24). Detecting Fake Accounts on Social Media. IEEE Xplore. https://doi.org/10.1109/BigData.2018.8621913

Lux, L M., & Calderon, G R O. (2020, June 29). El delito de fraude informático: concepto y delimitación. Revista chilena de derecho y tecnología (En línea), 9(1), 151-151. https://doi.org/10.5354/0719-2584.2020.57149

Macías-Lara, R A., Boné-Andrade, M F., Angulo, F Q., Loor, J J M., Estupiñan-Troya, G., & Vizuete, J D R. (2022, April 30). Casos frecuentes, penalización y prevención de los delitos informáticos en el Ecuador: una breve revisión sistemática. , 3(2), 231-243. https://doi.org/10.51798/sijis.v3i2.324

Marr, B. (2023, April 7). The Dark Side Of Technology: Navigating The Threat Of Digital Impersonation. https://www.forbes.com/sites/bernardmarr/2023/04/07/the-dark-side-of-technology-navigating-the-threat-of-digital-impersonation/

Marshall, A M., & Tompsett, B C. (2005, January 4). Identity theft in an online world. https://www.sciencedirect.com/science/article/pii/S0267364905000683

Martínez–Ferrer, B., & Ruiz, D F. (2017, October 22). Dependencia de las redes sociales virtuales y violencia escolar en adolescentes. 2(1), 105-105. https://doi.org/10.17060/ijodaep.2017.n1.v2.923

McCourt, A. (2022, December 5). Social Media Mining: The Effects of Big Data In the Age of Social Media. https://law.yale.edu/mfia/case-disclosed/social-media-mining-effects-big-data-age-social-media

Meligy, A M., Ibrahim, H M., & Torky, M. (2015, February 8). A Framework for Detecting Cloning Attacks in OSN Based on a Novel Social Graph Topology. , 7(3), 13-20. https://doi.org/10.5815/ijisa.2015.03.02

Munoz, S D., & Guillén, E. (2020, December 1). A dataset for the detection of fake profiles on social networking services. https://doi.org/10.1109/csci51800.2020.00046

Olivero, M A., Bertolino, A., Mayo, F J D., Escalona, M J., & Matteucci, I. (2020, June 1). Digital persona portrayal: Identifying pluridentity vulnerabilities in digital life. Journal of information security and applications, 52, 102492-102492. https://doi.org/10.1016/j.jisa.2020.102492

Reznik, M. (2013, October 16). Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation. https://digitalcommons.tourolaw.edu/lawreview/vol29/iss2/12/

Subba, R., Amrutha, N., & Shanmukha, P. (2023, December 13). Artificial Intelligence Tool for Fake Account Detection from Online Social Networks. Research Gate, 14(1), 243-254. https://ir.mallareddyecw.com/id/eprint/500/

Thomson, R. (2022, February 14). Synthetic identity – a new path for government fraude. https://legal.thomsonreuters.com/en/insights/article