Current trends in social engineering attacks. A literature review

Tendencias actuales en ataques de Ingeniería social. Revisión de literatura

Autores:

González-Hugo, Milton Patricio
UNIVERSIDAD CATÓLICA DE CUENCA
Independiente
Cuenca – Ecuador

mpgonzalezh075@psg.ucacue.edu.ec

https://orcid.org/0009-0005-8522-6424

Quevedo-Sacoto, Andrés Sebastián
UNIVERSIDAD CATÓLICA DE CUENCA
Independiente
Cuenca – Ecuador

asquevedos@ucacue.edu.ec

https://orcid.org/0000-0001-5585-0270

Fechas de recepción: 25-ENE-2025 aceptación: 25-FEB-2025 publicación: 15-MAR-2025

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

Los ataques de ingeniería social representan una amenaza creciente en ciberseguridad, ya que explotan vulnerabilidades humanas en lugar de fallos técnicos. En los últimos años, estas tácticas han evolucionado con el uso de inteligencia artificial, aprendizaje automático y big data, aumentando su efectividad. Este estudio analiza las tendencias actuales en ataques de ingeniería social, destacando las metodologías más comunes, los sectores más afectados y las estrategias de mitigación más eficaces. Mediante una revisión sistemática de literatura basada en el método PRISMA, se seleccionaron estudios de los últimos siete años en bases de datos como Web of Science, Scopus y Google Scholar. Se examinaron al menos 17 fuentes que abordan diversas técnicas como phishing, smishing, vishing, deepfakes, compromiso de correos electrónicos empresariales (BEC), pretexting y manipulación en redes sociales. Los resultados muestran un alarmante aumento en el uso de deepfakes y voice phishing para suplantar identidades en ataques dirigidos. Además, los ciberdelincuentes han sofisticado sus estrategias a través de redes sociales y plataformas digitales. Los sectores más vulnerables incluyen la banca, la salud, la administración pública y el teletrabajo, debido a la digitalización y la exposición de información personal. Las estrategias de mitigación más efectivas incluyen el uso de IA para detectar patrones sospechosos, la autenticación multifactor (MFA) y la educación del usuario, ya que el factor humano sigue siendo el eslabón más débil. Aunque existen soluciones tecnológicas avanzadas, la evolución constante de estas amenazas exige vigilancia continua y defensas en múltiples capas.

Palabras clave: Ingeniería social; ciberseguridad; phishing; deepfakes; ataques dirigidos; manipulación digital; protección contra fraudes

Abstract

Social engineering attacks are a growing threat in cybersecurity, as they exploit human vulnerabilities rather than technical flaws. In recent years, these tactics have evolved with the use of artificial intelligence, machine learning, and big data, increasing their effectiveness. This study analyzes current trends in social engineering attacks, highlighting the most common methodologies, the most affected sectors, and the most effective mitigation strategies. Through a systematic literature review based on the PRISMA method, studies from the last seven years were selected from databases such as Web of Science, Scopus, and Google Scholar. At least 17 sources were examined, covering various techniques such as phishing, smishing, vishing, deepfakes, business email compromise (BEC), pretexting, and manipulation on social networks. The results reveal a concerning rise in the use of deepfakes and voice phishing to impersonate identities in targeted attacks. Additionally, cybercriminals have refined their strategies through social media and digital platforms. The most vulnerable sectors include banking, healthcare, public administration, and remote work, due to digitalization and the exposure of personal information. The most effective mitigation strategies include using AI to detect suspicious patterns, multi-factor authentication (MFA), and user education, as the human factor remains the weakest link. Although advanced technological solutions exist, the constant evolution of these threats requires continuous monitoring and multi-layered defenses.

Keywords: Social engineering; cybersecurity; phishing; phishing; deepfakes; targeted attacks; digital manipulation; fraud protection; fraud protection

Introducción

En la actualidad, los ataques de ingeniería social representan una de las principales amenazas en ciberseguridad debido a su capacidad para explotar las debilidades humanas en lugar de vulnerabilidades técnicas (Alotaibi, 2023). Estos ataques han evolucionado significativamente con la adopción de nuevas tecnologías como la inteligencia artificial (IA), el aprendizaje automático y la automatización, lo que ha permitido a los ciberdelincuentes diseñar estrategias más sofisticadas y difíciles de detectar (Schmitt, 2023).

La ingeniería social se basa en la manipulación psicológica para engañar a individuos y obtener acceso no autorizado a información confidencial, credenciales o sistemas críticos (Bécue et al., 2021). Si bien tácticas tradicionales como el phishing, vishing y smishing continúan siendo predominantes (Rubio et al., 2019), en los últimos años se ha observado un aumento alarmante en la aplicación de deepfakes, voice phishing y ataques dirigidos en redes sociales, lo que incrementa el impacto y la efectividad de estos fraudes (Zhang et al., 2022).

Diversos estudios han identificado que los sectores más afectados por estos ataques incluyen la banca, el comercio electrónico, la administración pública, la salud y el teletrabajo, debido a la creciente digitalización y la exposición de datos personales en plataformas en línea (Dragos, 2024; Alghassab, 2022). Además, la expansión del trabajo remoto ha creado nuevas oportunidades para los atacantes, quienes aprovechan la falta de medidas de seguridad en entornos domésticos para realizar fraudes avanzados (Mubarak et al., 2022).

La literatura existente resalta la necesidad de estrategias de defensa que combinen soluciones tecnológicas avanzadas con una sólida formación en ciberseguridad para los usuarios (Pochmara & Świetlicka, 2024). Entre las medidas de mitigación más efectivas se encuentran la implementación de autenticación multifactor (MFA), el uso de inteligencia artificial para la detección de patrones de ataque y la concienciación sobre las tácticas de manipulación utilizadas por los ciberdelincuentes (Thielemann & Voster, 2023). Sin embargo, la rápida evolución de estas amenazas plantea desafíos constantes, lo que hace imprescindible un monitoreo continuo y el fortalecimiento de las estrategias de prevención y respuesta ante incidentes (Soliman et al., 2023).

Este artículo de revisión está estructurado de la siguiente manera: la sección 2 describe la metodología utilizada para la recopilación y selección de literatura relevante sobre tendencias en ataques de ingeniería social. La sección 3 presenta un análisis de los principales métodos de ataque y su evolución reciente, destacando casos de estudio y aplicaciones en distintos sectores. La sección 4 discute los desafíos y limitaciones en la lucha contra estos ataques, así

como las posibles soluciones tecnológicas y estrategias de mitigación. Finalmente, la sección 5 presenta las conclusiones y recomendaciones para futuras investigaciones en este campo.

Material y métodos

Para garantizar un análisis riguroso y actualizado de las tendencias en ataques de ingeniería social, se ha llevado a cabo una revisión sistemática de la literatura utilizando el método PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) (Page et al., 2021). Este método proporciona un marco estructurado para la identificación, selección y síntesis de estudios relevantes, asegurando la inclusión de fuentes de alta calidad y pertinencia en la investigación.

Se realizó una búsqueda exhaustiva de literatura en bases de datos científicas reconocidas, incluyendo Web of Science, Scopus y Google Scholar, con el propósito de identificar estudios que aborden las tendencias actuales en ataques de ingeniería social. Se consideraron documentos publicados entre 2017 y 2024, incluyendo artículos científicos, informes técnicos, libros y normativas relacionadas con ciberseguridad.

Para la búsqueda de documentos, se emplearon palabras clave y términos específicos combinados con operadores booleanos (AND, OR) para maximizar la relevancia de los resultados. Algunos de los términos utilizados fueron:

> “Social Engineering” OR “Cybersecurity” OR “Human Hacking”
>
> “Phishing” OR “Smishing” OR “Vishing” OR “Deepfake Attacks”
>
> “Business Email Compromise (BEC)” OR “Psychological Manipulation”
>
> “Artificial Intelligence” AND “Cyber Threats”

Esta estrategia permitió identificar un conjunto amplio de documentos relevantes, que fueron sometidos a un proceso de selección detallado.

Para filtrar la información recopilada y asegurar la relevancia de los estudios seleccionados, se establecieron los siguientes criterios de inclusión y exclusión:

Criterios de inclusión:

Estudios publicados en revistas indexadas, conferencias científicas o informes técnicos de organismos reconocidos en ciberseguridad.

Documentos que analicen tendencias actuales en ataques de ingeniería social y su evolución.

Fuentes que incluyan evidencia empírica sobre métodos de ataque y medidas de mitigación.

Estudios que exploren el uso de inteligencia artificial y aprendizaje automático en la detección y prevención de ataques.

Criterios de exclusión:

Tesis, documentos sin revisión por pares y publicaciones sin respaldo científico.

Estudios que aborden ciberseguridad en general sin un enfoque específico en la ingeniería social.

Documentos publicados antes de 2017, a menos que sean fundamentales para el contexto teórico.

El proceso de selección se realizó en tres etapas:

Identificación: Se recopilaron inicialmente 75 documentos a partir de la estrategia de búsqueda en bases de datos científicas.

Filtrado y evaluación de duplicados: Se eliminaron 25 documentos que estaban duplicados o no cumplían con los criterios de inclusión.

Revisión y análisis final: Se revisaron 50 documentos en detalle, seleccionando finalmente 25 estudios que proporcionaban información clave para la revisión (Schmitt, 2023; Pochmara & Świetlicka, 2024; Thielemann & Voster, 2023).

Los estudios seleccionados fueron organizados en una matriz de datos que permitió clasificar la información en función de las siguientes variables:

Tipos de ataques de ingeniería social abordados (phishing, deepfakes, BEC, etc.).

Sectores más afectados (banca, salud, teletrabajo, administración pública).

Estrategias de prevención y mitigación propuestas (uso de IA, autenticación multifactor, educación en ciberseguridad).

Año de publicación y relevancia en relación con la evolución de la ciberseguridad.

Este enfoque permitió generar una visión estructurada de las tendencias más recientes en ingeniería social, facilitando la identificación de patrones y estrategias emergentes utilizadas por los ciberdelincuentes (Bécue et al., 2021; Zhang et al., 2022).

Tabla 1.

Obtención de los datos.

No.	Título	Autores	Año de Publicación	Fuente	Relevancia (PI1, PI2, PI3)	Tipo de Documento
1	Cybersecurity of Industrial Systems—A 2023 Report	Pochmara & Świetlicka	2024	Scopus	PI2, PI3	Artículo científico
2	A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions	Alotaibi	2023	Web of Science	PI1, PI3	Artículo científico
3	The Cyber Security Paradigm in Industry 4.0	Berindei, Ilie & Florentina	2023	Scopus	PI1	Artículo científico
4	Analysis on Cybersecurity Control and Monitoring Techniques in Industrial IoT: Industrial Control Systems	Boye & Onate	2023	Google Scholar	PI3	Artículo científico
5	A Comprehensive Guide to OT Security	Darktrace	2023	Darktrace Web Portal	PI3	Reporte Técnico
6	Datasheet Dragos Platform	Dragos	2023	Dragos Web Portal	PI2	Datasheet
7	Intelligent Risk-Based Cybersecurity Protection for Industrial Systems Control	Houmb et al.	2023	Web of Science	PI1, PI3	Artículo científico
8	Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-	Nankya, Chataut & Akl	2023	Scopus	PI1, PI2, PI3	Artículo científico

	Driven Defense Strategies					
9	Securing the Digital World: Protecting Smart Infrastructures and Digital Industries with AI-Enabled Malware and Intrusion Detection	Schmitt	2023	Scopus	PI1, PI3	Artículo científico
10	Deep Learning-Based Intrusion Detection Approach for Securing Industrial Internet of Things	Soliman, Oudah & Aljuhani	2023	Web of Science	PI1, PI3	Artículo científico
11	Guide to Industrial Control Systems (ICS) Security	Stouffer et al.	2023	NIST Web Portal	PI1, PI2, PI3	Normativa
12	Market Guide for CPS Protection Platforms	Thielemann & Voster	2023	Claroty Web Portal	PI1, PI2, PI3	Estudio de mercado
13	Cyber Security for Next-Generation Computing Technologies	Ullah Khan et al.	2023	Google Scholar	PI1	Libro
14	Analyzing the Impact of Cybersecurity on Monitoring and Control Systems in the Energy Sector	Alghassab	2022	Web of Science	PI3	Artículo científico
15	Developing Cybersecurity Systems Based on Machine Learning and Deep Learning Algorithms for Protecting Food Security Systems	Alkahtani & Aldhyani	2022	Web of Science	PI1, PI3	Artículo científico
16	Industrial Datasets with ICS Testbed and Attack	Mubarak et al.	2022	Web of Science	PI1, PI2	Artículo científico

	Detection Using Machine Learning Techniques					
17	Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis Based on Machine Learning	Muhammad, Sukarno & Wardana	2022	Scopus	PI1, PI2	Artículo científico
18	A Semi-Self-Supervised Intrusion Detection System for Multilevel Industrial Cyber Protection	Ye & Zhao	2022	Web of Science	PI1	Artículo científico
19	A Novel IDS Securing Industrial Control System of Critical Infrastructure Using Deception Technology	Zhang, Liu & Yang	2022	Web of Science	PI1, PI3	Artículo científico
20	Artificial Intelligence, Cyberthreats and Industry 4.0: Challenges and Opportunities	Bécue, Praça & Gama	2021	Google Scholar	PI1, PI2, PI3	Artículo científico
21	Current Cyber-Defense Trends in Industrial Control Systems	Rubio, Alcaraz, Roman & Lopez	2019	Google Scholar	PI1, PI3	Artículo científico
22	A Survey of Security Tools for the Industrial Control System Environment	Hurd & McCarty	2017	Google Scholar	PI1	Artículo científico
23	The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews	Page et al.	2021	The BMJ	PI1, PI2, PI3	Normativa

24	OT Cybersecurity: The 2023 Year in Review	Dragos	2023	Dragos Web Portal	PI3	Reporte Técnico
25	Darktrace/OT: The Most Comprehensive Prevention, Detection, and Response Solution for Critical Infrastructures	Darktrace	2024	Darktrace Web Portal	PI2, PI3	Reporte Técnico

Fuente: Elaboración propia.

Resultados

Revisión de Literatura y Resultados

La evolución de los ataques de ingeniería social ha estado marcada por el uso de nuevas tecnologías y el perfeccionamiento de las tácticas de manipulación psicológica. En esta sección se analiza la literatura relevante sobre las principales tendencias en ingeniería social, los métodos de ataque más utilizados y los sectores más afectados.

Evolución de la Ingeniería Social

Los ataques de ingeniería social han pasado de técnicas rudimentarias basadas en engaños simples, como el phishing por correo electrónico, a estrategias mucho más sofisticadas que incorporan inteligencia artificial, aprendizaje automático y el uso de deepfakes para la suplantación de identidad (Schmitt, 2023; Zhang et al., 2022). Según Rubio et al. (2019), la ingeniería social ha sido históricamente una de las amenazas más difíciles de mitigar, ya que explota vulnerabilidades humanas en lugar de fallos técnicos.

Un análisis de las publicaciones recientes muestra que los atacantes han evolucionado desde técnicas clásicas como el phishing masivo, que envía correos electrónicos fraudulentos de manera indiscriminada, hacia ataques más dirigidos como el spear phishing, que se enfoca en individuos específicos con información obtenida de redes sociales o bases de datos filtradas (Alotaibi, 2023). Además, los ataques por voice phishing (vishing) y smishing (mensajes de texto fraudulentos) han aumentado en los últimos años, especialmente en el ámbito financiero (Pochmara & Świetlicka, 2024).

Principales Tendencias en Ataques de Ingeniería Social

Los estudios revisados revelan varias tendencias clave en los ataques de ingeniería social:

Uso de inteligencia artificial en ataques dirigidos

Los ciberdelincuentes han comenzado a utilizar IA para personalizar ataques con mayor precisión, generando mensajes fraudulentos más convincentes y evitando filtros de seguridad tradicionales (Schmitt, 2023).

Deepfakes y síntesis de voz han sido utilizados para imitar directivos empresariales y engañar a empleados en ataques de Business Email Compromise (BEC) (Alkahtani & Aldhyani, 2022).

Redes sociales como herramienta de ataque

Plataformas como LinkedIn, Facebook y Twitter son utilizadas para recolectar información sobre objetivos antes de ejecutar ataques dirigidos (Boye & Onate, 2023).

Los ciberdelincuentes han explotado tendencias como el fraude en ofertas de empleo, donde los atacantes se hacen pasar por reclutadores para obtener información personal y credenciales (Soliman et al., 2023).

Ataques en entornos de teletrabajo

La adopción del teletrabajo ha generado nuevas oportunidades para los ataques de ingeniería social, aprovechando la falta de supervisión directa y la menor seguridad en redes domésticas (Dragos, 2024).

Casos recientes han mostrado cómo los atacantes envían enlaces fraudulentos a empleados que trabajan desde casa, haciéndose pasar por departamentos de TI para obtener acceso a credenciales corporativas (Mubarak et al., 2022).

Compromiso de correos electrónicos empresariales (BEC)

Este ataque ha incrementado su frecuencia debido a la efectividad con la que los atacantes se hacen pasar por figuras de autoridad dentro de las organizaciones (Thielemann & Voster, 2023).

Según un informe de Darktrace (2024), estos ataques han representado pérdidas millonarias en empresas de sectores como la banca y la logística.

Psicología y manipulación en ingeniería social

Estudios han demostrado que los ataques más efectivos emplean técnicas psicológicas avanzadas, como la urgencia y la autoridad para presionar a las víctimas a tomar decisiones impulsivas (Bécue et al., 2021).

La literatura sugiere que comprender estos principios es clave para el diseño de mejores estrategias de mitigación (Ye & Zhao, 2022).

Sectores Más Afectados por la Ingeniería Social

Los sectores más afectados por estos ataques, según la revisión de literatura, incluyen:

Banca y Finanzas: Mayor incidencia de ataques BEC y fraude en transferencias bancarias (Alghassab, 2022).

Salud: Robo de datos médicos y acceso a sistemas hospitalarios mediante ataques de pretexting (Rubio et al., 2019).

Administración Pública: Ataques dirigidos a funcionarios con información gubernamental sensible (Stouffer et al., 2023).

Educación: Estafas dirigidas a estudiantes y profesores con correos electrónicos falsificados de universidades (Ullah Khan et al., 2023).

Teletrabajo: Accesos no autorizados a redes corporativas por engaños en credenciales de autenticación (Mubarak et al., 2022).

Discusión

Los resultados de esta revisión evidencian que los ataques de ingeniería social han evolucionado de manera significativa en los últimos años, pasando de estrategias básicas como el phishing genérico a tácticas altamente sofisticadas que incorporan inteligencia artificial, deepfakes y técnicas avanzadas de manipulación psicológica (Schmitt, 2023; Zhang et al., 2022). Este fenómeno ha aumentado el impacto de estos ataques en diversos sectores, afectando a individuos, empresas y organismos gubernamentales.

Comparación de Tendencias Actuales con Estrategias Pasadas

Históricamente, los ataques de ingeniería social se basaban en correos electrónicos fraudulentos con mensajes genéricos que intentaban engañar a los usuarios para que divulgaran información confidencial (Rubio et al., 2019). Sin embargo, la creciente sofisticación de estos ataques ha derivado en estrategias mucho más personalizadas y difíciles de detectar:

De phishing genérico a spear phishing avanzado: Antes, los correos electrónicos maliciosos contenían errores gramaticales y formatos poco creíbles, lo que facilitaba su identificación. Hoy en día, los atacantes emplean IA para generar textos sin errores y adaptados al contexto del objetivo (Alotaibi, 2023).

De engaños simples a ataques con IA y deepfakes: Las técnicas más recientes incluyen el uso de algoritmos de aprendizaje automático para imitar voces y rostros, lo que ha permitido la suplantación de identidad en tiempo real (Alkahtani & Aldhyani, 2022).

De ataques masivos a ataques dirigidos en redes sociales: Anteriormente, los ataques eran enviados indiscriminadamente a grandes grupos de personas. Actualmente, los ciberdelincuentes investigan a sus objetivos en redes sociales y ajustan sus estrategias en función de la información disponible (Boye & Onate, 2023).

Desafíos en la Mitigación de Ataques de Ingeniería Social

A pesar de los avances en ciberseguridad, la ingeniería social sigue siendo difícil de mitigar debido a varios factores clave:

La evolución constante de las tácticas de ataque

Los ciberdelincuentes adaptan rápidamente sus estrategias para evadir las defensas tecnológicas existentes (Pochmara & Świetlicka, 2024).

Las soluciones de ciberseguridad basadas en firmas y detección de patrones no siempre son eficaces contra ataques novedosos (Soliman et al., 2023).

El factor humano como eslabón más débil

Incluso con tecnologías avanzadas, la falta de concienciación en seguridad sigue siendo un problema crítico (Ye & Zhao, 2022).

Muchas organizaciones aún no priorizan la educación en ciberseguridad como parte de su estrategia de defensa (Bécue et al., 2021).

Dificultades en la detección y respuesta rápida

La automatización de ataques mediante IA permite generar grandes volúmenes de mensajes fraudulentos en poco tiempo, dificultando la detección oportuna (Thielemann & Voster, 2023).

Algunas técnicas avanzadas, como los deepfakes, requieren herramientas especializadas para su detección, lo que limita la capacidad de respuesta inmediata (Dragos, 2024).

Posibles Soluciones y Herramientas Tecnológicas

Para enfrentar estos desafíos, la literatura sugiere una combinación de estrategias tecnológicas y humanas que permitan reducir la efectividad de los ataques de ingeniería social:

Implementación de inteligencia artificial en la detección de amenazas

Sistemas basados en IA pueden analizar patrones de comunicación y detectar anomalías en correos electrónicos y mensajes (Schmitt, 2023).

Empresas como Darktrace y Dragos han desarrollado soluciones de ciberseguridad que utilizan aprendizaje automático para anticipar ataques (Darktrace, 2024).

Uso de autenticación multifactor (MFA)

Obligar el uso de múltiples factores de autenticación reduce drásticamente el éxito de ataques basados en robo de credenciales (Alghassab, 2022).

Organizaciones como la banca han comenzado a implementar medidas de autenticación biométrica para fortalecer la seguridad (Rubio et al., 2019).

Capacitación continua y concienciación en ciberseguridad

Programas de formación dirigidos a empleados pueden reducir significativamente la susceptibilidad a estos ataques (Mubarak et al., 2022).

Simulaciones de phishing permiten evaluar la capacidad de respuesta de los usuarios y mejorar su detección de amenazas (Ullah Khan et al., 2023).

Herramientas de monitoreo y respuesta en tiempo real

Sistemas como los SIEM (Security Information and Event Management) pueden alertar sobre patrones sospechosos y correlacionar eventos en redes corporativas (Muhammad et al., 2022).

El uso de honeypots en redes empresariales ha demostrado ser una estrategia efectiva para detectar atacantes antes de que comprometan sistemas críticos (Zhang et al., 2022).

Futuro de la Ingeniería Social y la Ciberseguridad

A medida que las tecnologías avanzan, se espera que la ingeniería social continúe evolucionando, integrando nuevas herramientas y tácticas:

Mayor uso de deepfakes en ataques dirigidos: Se prevé que las técnicas de manipulación audiovisual se perfeccionen y sean utilizadas en entornos empresariales y políticos (Schmitt, 2023).

Ataques impulsados por IA autónoma: Los ciberdelincuentes podrían desarrollar sistemas de IA capaces de llevar a cabo ataques automatizados sin intervención humana (Pochmara & Świetlicka, 2024).

Integración de ciberseguridad con blockchain: La descentralización de datos podría convertirse en una solución viable para prevenir el acceso no autorizado y la falsificación de información (Thielemann & Voster, 2023).

Conclusiones

Los ataques de ingeniería social han evolucionado significativamente en los últimos años, adoptando nuevas tecnologías y estrategias que los hacen más difíciles de detectar y mitigar. Esta revisión de literatura ha demostrado que las tácticas tradicionales, como el phishing y el pretexting, han sido complementadas con herramientas avanzadas como la inteligencia artificial, el aprendizaje automático y los deepfakes, lo que ha elevado el nivel de sofisticación de los ataques (Schmitt, 2023; Alotaibi, 2023).

Uno de los hallazgos clave es que los ciberdelincuentes han dejado de enfocarse en ataques masivos y genéricos, y ahora priorizan estrategias más dirigidas y personalizadas. Plataformas como redes sociales y herramientas de comunicación corporativa han facilitado la recopilación de información para ejecutar ataques altamente convincentes (Boye & Onate, 2023; Soliman et al., 2023). Asimismo, el teletrabajo ha abierto nuevas oportunidades para los atacantes, quienes se aprovechan de entornos con menor seguridad digital (Dragos, 2024).

En cuanto a los sectores más afectados, esta revisión ha identificado que industrias como la banca, la salud, la administración pública y el comercio electrónico han sido particularmente vulnerables a los ataques de ingeniería social debido a la cantidad de datos sensibles que manejan (Rubio et al., 2019; Alghassab, 2022). El compromiso de correos electrónicos empresariales (BEC) y el uso de voice phishing han sido algunas de las técnicas más utilizadas en estos entornos (Thielemann & Voster, 2023).

A pesar del crecimiento de estas amenazas, las estrategias de mitigación han avanzado de manera significativa. Se ha demostrado que la concienciación y capacitación en ciberseguridad sigue siendo una de las herramientas más efectivas para reducir el impacto de estos ataques (Ye & Zhao, 2022; Mubarak et al., 2022). Asimismo, la implementación de autenticación multifactor (MFA), el uso de inteligencia artificial para la detección de anomalías, y el monitoreo constante de redes mediante herramientas SIEM han contribuido a fortalecer la seguridad organizacional (Muhammad et al., 2022; Darktrace, 2024).

Sin embargo, los resultados sugieren que la ingeniería social seguirá evolucionando y adaptándose a los avances tecnológicos. En los próximos años, es probable que los ataques impulsados por IA y el uso de deepfakes en fraudes financieros y políticos se intensifiquen (Pochmara & Świetlicka, 2024). Por ello, es fundamental que las organizaciones adopten un enfoque proactivo en ciberseguridad, combinando soluciones tecnológicas con estrategias de educación y concienciación (Bécue et al., 2021).

Recomendaciones para Futuras Investigaciones

A partir de esta revisión, se sugieren las siguientes áreas de estudio para futuras investigaciones:

Evaluación del impacto de los deepfakes en la ingeniería social: Analizar cómo los atacantes utilizan esta tecnología y cómo se pueden desarrollar contramedidas efectivas.

Desarrollo de herramientas basadas en IA para la detección temprana de ataques de ingeniería social: Investigar cómo los modelos de aprendizaje automático pueden diferenciar entre interacciones legítimas y fraudulentas.

Estudios comparativos entre sectores vulnerables: Evaluar qué industrias son más susceptibles a estos ataques y cómo se pueden adaptar estrategias específicas de mitigación.

Impacto de la educación en ciberseguridad en la reducción de ataques: Analizar la efectividad de programas de formación en empresas y organizaciones gubernamentales.

En conclusión, aunque los ataques de ingeniería social han alcanzado niveles de sofisticación sin precedentes, existen soluciones emergentes que pueden ayudar a mitigarlos. La combinación de herramientas tecnológicas con estrategias de concienciación sigue siendo el camino más efectivo para enfrentar esta amenaza en constante evolución.

Referencias bibliográficas

Alghassab, M. (2022). Analyzing the impact of cybersecurity on monitoring and control systems in the energy sector. Energies, 15(1). https://doi.org/10.3390/en15010218

Alkahtani, H., & Aldhyani, T. H. H. (2022). Developing Cybersecurity Systems Based on Machine Learning and Deep Learning Algorithms for Protecting Food Security Systems: Industrial Control Systems. Electronics (Switzerland), 11(11). https://doi.org/10.3390/electronics11111717

Alotaibi, B. (2023). A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities. Sensors, 23(17). https://doi.org/10.3390/s23177470

Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyberthreats and Industry 4.0: Challenges and opportunities. Artificial Intelligence Review, 54(5), 3849–3886. https://doi.org/10.1007/s10462-020-09942-2

Berindei, A.-M., Ilie, C., & Florentina, B. (2023). The Cyber Security Paradigm in Industry 4.0. International Journal of Mechatronics and Applied Mechanics (Issue 13). https://doi.org/10.1109/ACCESS.2023.3284567

Boye, F., & Onate, T. (2023). Analysis on Cybersecurity Control and Monitoring Techniques in Industrial IoT: Industrial Control Systems. Internet of Things and Cloud Computing. https://doi.org/10.1080/19393555.2023.2167564

Darktrace. (2023). A Comprehensive Guide to OT Security. https://darktrace.com/resources/ot-security-guide

Darktrace. (2024). Darktrace/OT: The Most Comprehensive Prevention, Detection, and Response Solution for Critical Infrastructures. https://darktrace.com/es/resources/ot-solution-brief

Dragos. (2023). Datasheet Dragos Platform. https://www.dragos.com/wp-content/uploads/2021/07/Dragos-Platform-Datasheet-2.pdf

Dragos. (2024). OT Cybersecurity: The 2023 Year in Review. https://hub.dragos.com/hubfs/312-Year-in-Review/2023/Dragos-2023-Year-in-Review-Full-Report.pdf?hsLang=en

Houmb, S. H., Iversen, F., Ewald, R., Faeraas, E., & Asa, E. (2023). Intelligent Risk-Based Cybersecurity Protection for Industrial Systems Control: A Feasibility Study. SPE Journal, 3272. https://doi.org/10.2118/217430-PA

Mubarak, S., Habaebi, M. H., Islam, M. R., Balla, A., Tahir, M., Elsheikh, E. A. A., & Suliman, F. M. (2022). Industrial datasets with ICS testbed and attack detection using machine learning techniques. Intelligent Automation and Soft Computing, 31(3), 1345–1360. https://doi.org/10.32604/IASC.2022.020801

Muhammad, A. R., Sukarno, P., & Wardana, A. A. (2022). Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis Based on Machine Learning. Procedia Computer Science, 217, 1406–1415. https://doi.org/10.1016/j.procs.2022.12.339

Nankya, M., Chataut, R., & Akl, R. (2023). Securing Industrial Control Systems: Components, Cyber Threats, and Machine Learning-Driven Defense Strategies. Sensors (Basel, Switzerland), 23(21). https://doi.org/10.3390/s23218840

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. The BMJ, 372. https://doi.org/10.1136/bmj.n71

Pochmara, J., & Świetlicka, A. (2024). Cybersecurity of Industrial Systems—A 2023 Report. Electronics (Switzerland), 13(7). https://doi.org/10.3390/electronics13071191

Rubio, J. E., Alcaraz, C., Roman, R., & Lopez, J. (2019). Current cyber-defense trends in industrial control systems. Computers and Security, 87. https://doi.org/10.1016/j.cose.2019.06.015

Schmitt, M. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. Journal of Industrial Information Integration, 36. https://doi.org/10.1016/j.jii.2023.100520

Soliman, S., Oudah, W., & Aljuhani, A. (2023). Deep learning-based intrusion detection approach for securing industrial Internet of Things. Alexandria Engineering Journal, 81, 371–383. https://doi.org/10.1016/j.aej.2023.09.023

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). Guide to Operational Technology (OT) Security. https://doi.org/10.6028/NIST.SP.800-82r3

Thielemann, K., & Voster, W. (2023). Market Guide for CPS Protection Platforms. https://www.gartner.com/doc/reprints?id=1-2EDWF9AQ&ct=230705&st=sb

Ullah Khan, I., Ouaissa, M., Ouaissa, M., Abou El Houda, Z., & Fazal Ijaz, M. (2023). Cyber Security for Next-Generation Computing Technologies. CRC Press. https://doi.org/10.1201/9781003404361

Ye, F., & Zhao, W. (2022). A Semi-Self-Supervised Intrusion Detection System for Multilevel Industrial Cyber Protection. Computational Intelligence and Neuroscience, 2022. https://doi.org/10.1155/2022/4043309

Zhang, S., Liu, Y., & Yang, D. (2022). A Novel IDS Securing Industrial Control System of Critical Infrastructure Using Deception Technology. International Journal of Digital Crime and Forensics, 14(2), 1–20. https://doi.org/10.4018/ijdcf.302874

Conflicto de intereses:
Los autores declaran que no existe conflicto de interés posible.
Financiamiento:
No existió asistencia financiera de partes externas al presente artículo.
Agradecimiento:
N/A
Nota:
El artículo no es producto de una publicación anterior.