28 DE FEBRERO DE 2026

EL ESLABÓN MÁS DÉBIL

DISEÑO ÉTICO DE UNA CAMPAÑA DE INGENIERÍA SOCIAL

CAROL ELIZABETH CORTES BELTRAN
177203
Seguridad informática

Contenido

Introducción 2
Marco teórico 3
Análisis individual de las 8 plataformas 3
Hoxhunt y la Psicología del Aprendizaje Adaptativo 3
Proofpoint y la Estrategia de los Usuarios Altamente Atacados 4
KnowBe4 y la Escalabilidad a Nivel Global 4
Cofense y el Paradigma de la Inteligencia Colectiva 5
Phished y la Automatización Mediante Algoritmos Predictivos 6
NINJIO y el Edutainment como Cambio de Actitud 6
Mimecast y la Formación en el Punto Crítico de Fallo 7
Infosec IQ y la Flexibilidad Operativa mediante Lógica Condicional 8
Tabla técnica comparativa 8
Conclusión 9
Referencias (APA 7) 9

Introducción

En el panorama actual de la seguridad de la información, el paradigma de defensa ha experimentado un cambio drástico. Mientras las organizaciones invierten miles de millones de dólares en perímetros de red robustos, firewalls de última generación y sistemas de detección basados en Inteligencia Artificial, los adversarios han optado por el camino de menor resistencia: el factor humano. La ingeniería social, y específicamente el *phishing*, se ha consolidado como el vector de ataque primario, explotando no las vulnerabilidades del código, sino los sesgos cognitivos y la confianza intrínseca de los usuarios. Bajo esta premisa, el presente proyecto, titulado **"El eslabón más débil: diseño ético de una campaña de ingeniería social"**, se propone abordar la gestión del riesgo humano desde una perspectiva técnica, analítica y profundamente ética.

El concepto de "eslabón más débil" no debe interpretarse como una crítica al usuario, sino como una falla en la estrategia de capacitación corporativa. Para mitigar esta vulnerabilidad, el mercado ha desarrollado plataformas avanzadas de simulación de phishing y concienciación (CBT - *Computer-Based Training*). Este informe técnico inicia con una investigación comparativa de los líderes de la industria: **Hoxhunt, Proofpoint, KnowBe4, Cofense, Phished, NINJIO, Mimecast e Infosec IQ**. El análisis no se limita a la capacidad de envío de correos, sino que profundiza en métricas críticas de resiliencia como el **Click Rate** (tasa de vulnerabilidad), el **Reporting Rate** (capacidad de respuesta activa) y el **Risk Score** (cuantificación predictiva del peligro).

Sin embargo, la implementación de estas herramientas conlleva una responsabilidad ética significativa. El diseño de una campaña de simulación no puede basarse en el engaño malintencionado o la humillación del empleado. Por ello, este proyecto detalla el desarrollo de un **Phishing Quiz interactivo** compuesto por 10 escenarios realistas, diseñados bajo principios de transparencia y retroalimentación formativa. A diferencia de un ataque real, esta simulación busca que el usuario aprenda a identificar los "indicadores de ingeniería social" (SEIs) en un entorno seguro, garantizando la privacidad de los datos y el consentimiento informado.

Finalmente, la efectividad de cualquier programa de concientización reside en su capacidad de medición. Se propone un sistema de puntuación global que trasciende el binomio "aprobado/reprobado", permitiendo a la organización visualizar tendencias de desempeño y áreas de mejora específica. Al integrar el análisis técnico de plataformas profesionales con una ejecución práctica ética, este trabajo busca transformar al usuario de ser el eslabón más débil a convertirse en la primera línea de defensa activa de la organización.

Marco teórico

La ciberseguridad contemporánea ha evolucionado de un enfoque puramente perimetral hacia la **Gestión del Riesgo Humano (Human Risk Management - HRM)**. Este cambio reconoce que el 60% de las brechas de seguridad actuales involucran un elemento humano, ya sea por error, complacencia o manipulación psicológica. La simulación de phishing se posiciona como la herramienta técnica fundamental para medir y mitigar esta vulnerabilidad en un entorno controlado.

1. Métricas Críticas de Resiliencia

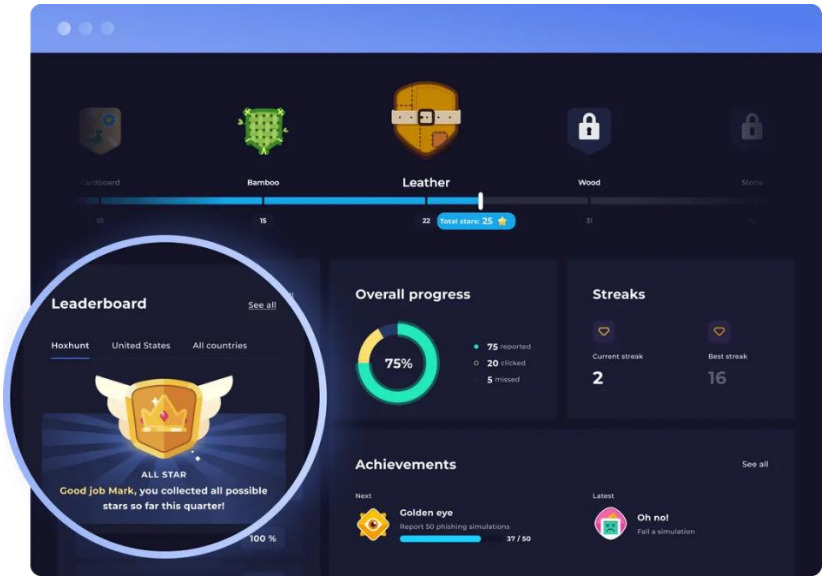
Para evaluar la efectividad de una campaña, las plataformas profesionales han estandarizado tres métricas principales que van más allá del simple "fallo" del usuario:

- **Click Rate (Tasa de Clics):** Porcentaje de usuarios que interactúan con el enlace o archivo malicioso. Aunque es la métrica más común, un valor bajo no siempre indica seguridad, sino que puede reflejar apatía o que el usuario simplemente ignoró el correo sin identificar la amenaza.
- **Reporting Rate (Tasa de Reporte):** Considerada la métrica de éxito más importante. Mide el porcentaje de usuarios que utilizan activamente las herramientas de alerta (como botones de reporte) para informar sobre el correo sospechoso. Una tasa alta indica una cultura de seguridad proactiva.
- **Risk Score (Puntuación de Riesgo):** Algoritmo predictivo que combina el comportamiento histórico (clics previos, reportes, capacitaciones completadas) con el nivel de acceso del usuario a datos críticos de la empresa.

Análisis individual de las 8 plataformas

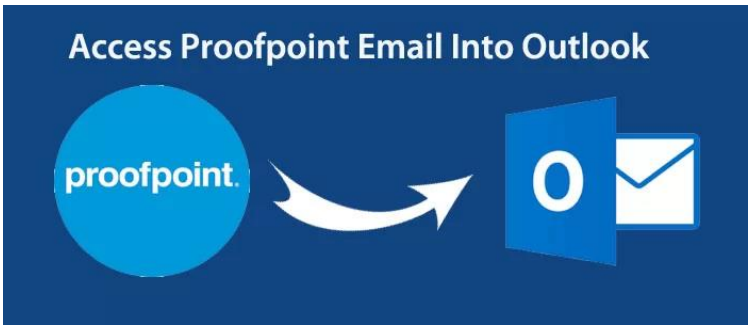
Hoxhunt y la Psicología del Aprendizaje Adaptativo

Hoxhunt redefine la formación en ciberseguridad al alejarse del concepto tradicional de entrenamiento para posicionarse como una plataforma integral de Gestión del Riesgo Humano (HRM). Su núcleo tecnológico se sustenta en algoritmos de aprendizaje automático que personalizan la experiencia de cada colaborador de manera individual. A diferencia de las campañas masivas y estáticas, Hoxhunt distribuye simulaciones en momentos aleatorios, analizando meticulosamente los disparadores psicológicos —como la urgencia, la curiosidad o la apelación a la autoridad— que causan el fallo en un usuario. Desde una perspectiva ética, la plataforma destaca por sustituir el castigo por el refuerzo positivo mediante un sistema de puntos de experiencia, lo que reduce significativamente la fricción operativa entre el departamento de TI y el personal. Su métrica más relevante, el *Shield Score*, no solo mide clics, sino la resiliencia proactiva de la organización ante ataques reales detectados por la propia fuerza laboral.



Proofpoint y la Estrategia de los Usuarios Altamente Atacados

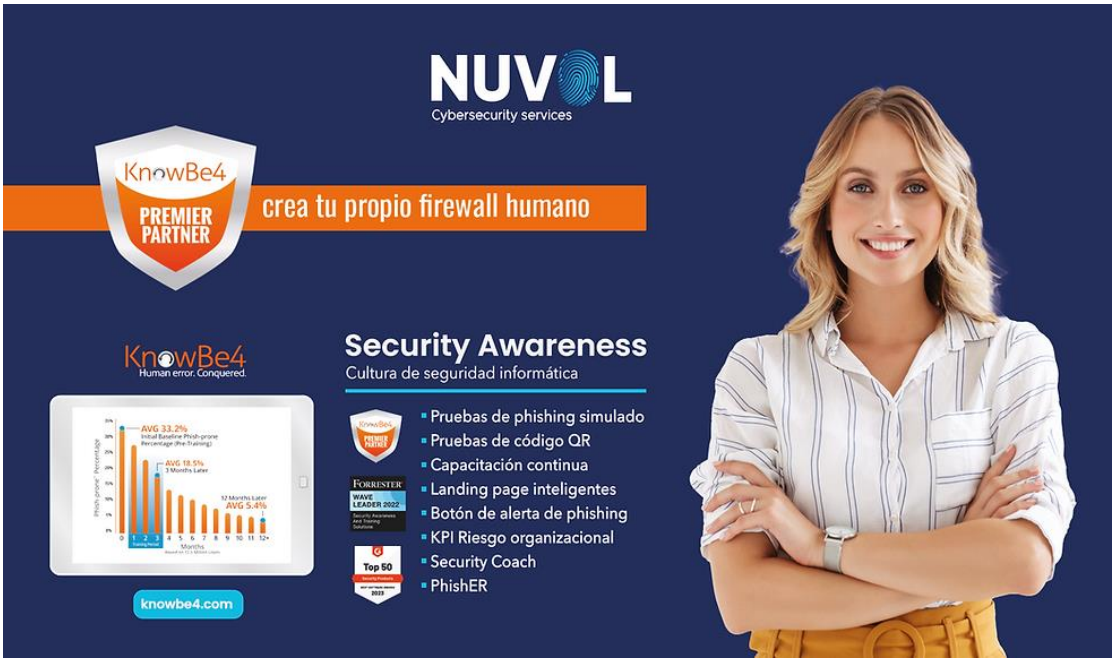
Como referente global en seguridad perimetral, Proofpoint integra la simulación de phishing con su ecosistema de protección de correo electrónico de vanguardia. Su mecanismo diferencial reside en la capacidad de mapear amenazas del mundo real en tiempo real; si sus sensores globales identifican una campaña de malware emergente en un sector específico, la plataforma puede replicar dicho ataque como simulación en cuestión de horas. El pilar de su análisis de riesgo es la clasificación de Personas Muy Atacadas (VAP), lo que permite a los oficiales de seguridad dirigir recursos educativos de manera quirúrgica hacia aquellos individuos con privilegios elevados o perfiles públicos que son blanco constante de actores de amenazas. Aunque su potencia técnica es incomparable, presenta la limitación de requerir un equipo de seguridad altamente especializado para interpretar y accionar la vasta densidad de datos que genera.



KnowBe4 y la Escalabilidad a Nivel Global

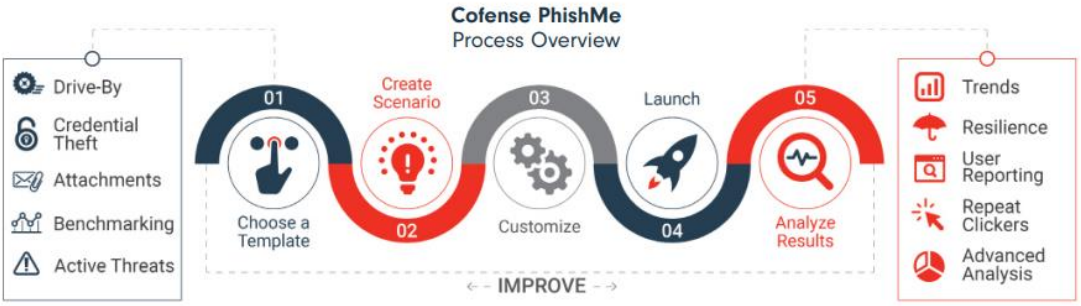
KnowBe4 se mantiene como el líder indiscutible en participación de mercado gracias a una infraestructura diseñada para la escala y el cumplimiento normativo. Su herramienta central, el Programa Automatizado de Concientización sobre Seguridad (AEST), permite estructurar planes de formación anuales basados en

un diagnóstico inicial de madurez digital. Es la plataforma estándar para organizaciones que deben cumplir con marcos legales como GDPR, PCI-DSS o HIPAA, ofreciendo una de las bibliotecas de contenido educativo más extensas de la industria. No obstante, su enfoque masivo puede derivar en una percepción de contenido genérico si no existe una supervisión administrativa que personalice las plantillas. Su indicador crítico de éxito es el *Phish-prone Percentage*, una métrica comparativa que sitúa la vulnerabilidad de la empresa frente a los promedios globales de su industria específica.



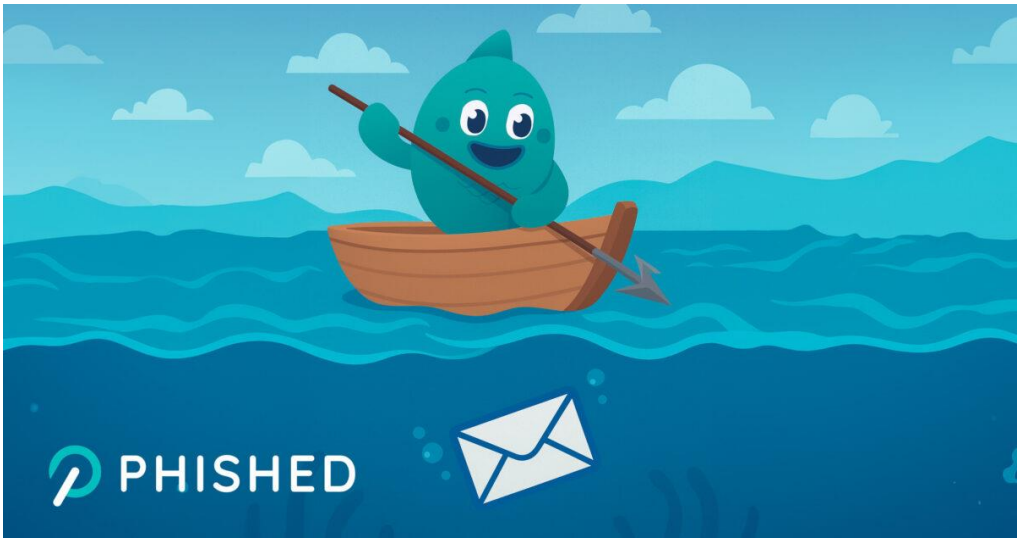
Cofense y el Paradigma de la Inteligencia Colectiva

Cofense se distingue por un enfoque operativo que prioriza el reporte activo sobre la simple detección pasiva. Su filosofía sostiene que un usuario que informa de una amenaza es un activo defensivo superior a aquel que simplemente ignora un correo malicioso. Técnicamente, su arquitectura permite que, tras el reporte de un usuario, sistemas como *Cofense Vision* busquen automáticamente correos idénticos en todos los buzones de la organización para ponerlos en cuarentena, transformando una simulación educativa en una respuesta inmediata a incidentes. Éticamente, esta plataforma promueve una cultura de vigilancia ciudadana digital, donde el empleado deja de ser una víctima potencial para convertirse en un sensor crítico del Centro de Operaciones de Seguridad (SOC). Es la herramienta ideal para empresas que buscan reducir drásticamente su tiempo medio de respuesta (MTTR).



Phished y la Automatización Mediante Algoritmos Predictivos

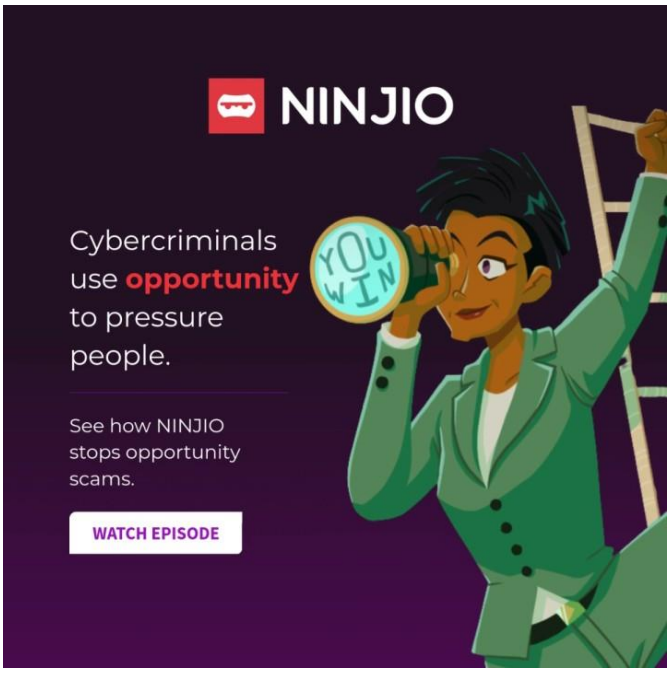
Phished representa la vanguardia de la automatización holística, eliminando la carga administrativa que conlleva la programación manual de campañas. Mediante el uso de una inteligencia artificial propietaria, la plataforma gestiona simulaciones multicanal que abarcan phishing, smishing y vishing, decidiendo de forma autónoma el momento óptimo para intervenir según el nivel de madurez del usuario. Su panel de control destaca por una visualización de datos simplificada que permite a departamentos no técnicos, como Recursos Humanos, monitorear el progreso de la cultura organizacional. El diseño ético de Phished se fundamenta en el respeto al tiempo productivo, utilizando micro-lecciones precisas que evitan la sobrecarga cognitiva y aseguran que el aprendizaje ocurra solo cuando se detecta una brecha de conocimiento real.



NINJIO y el Edutainment como Cambio de Actitud

NINJIO rompe con los esquemas técnicos tradicionales al centrar su eficacia en la retención de memoria a largo plazo a través de la narrativa visual de alta calidad. Su metodología se basa en episodios mensuales de corta duración, producidos con estándares cinematográficos y basados en brechas de seguridad reales y recientes. El valor fundamental de esta plataforma no reside solo en la simulación

del correo, sino en el cambio de mentalidad del colaborador, atacando directamente la apatía hacia la formación técnica aburrida. Aunque su capacidad de personalización técnica a nivel de código es menor que en otras soluciones, su impacto en la empatía y la conciencia humana es superior, siendo la plataforma más eficaz para organizaciones que enfrentan una resistencia cultural profunda hacia las políticas de seguridad.



Mimecast y la Formación en el Punto Crítico de Fallo

Mimecast ofrece una solución profundamente integrada en la infraestructura de red, lo que le otorga una visibilidad excepcional sobre el tráfico de datos y los intentos de suplantación de marca. Su enfoque técnico principal es el entrenamiento en el "punto de fallo", donde un error en una simulación desencadena inmediatamente una página de aterrizaje interactiva que descompone los indicadores de peligro del mensaje. Una de sus capacidades más potentes es la protección contra la explotación de marca, permitiendo simular ataques donde los criminales utilizan la identidad corporativa interna para engañar a los empleados. Gracias a su sincronización nativa con servicios de directorio como Azure AD, Mimecast permite una segmentación granular que asegura que cada grupo jerárquico reciba un entrenamiento acorde a sus responsabilidades técnicas.

Infosec IQ y la Flexibilidad Operativa mediante Lógica Condicional

Infosec IQ se posiciona como una caja de herramientas de alta versatilidad para el oficial de seguridad que exige control total sobre el flujo educativo. Su plataforma permite configurar campañas mediante lógica condicional, lo que significa que la respuesta del sistema varía dinámicamente según la acción del usuario: un reporte exitoso puede generar un correo de reconocimiento, mientras que la introducción de datos en un formulario falso puede asignar automáticamente un módulo de refuerzo de cumplimiento. Destaca por su especialización en roles técnicos y ejecutivos, ofreciendo rutas de aprendizaje diseñadas específicamente para desarrolladores o altos directivos. Finalmente, su *Security Culture Index* proporciona una medición psicométrica de la actitud organizacional, permitiendo distinguir entre el cumplimiento por obligación y una verdadera internalización de los principios de seguridad informática.

Tabla técnica comparativa

El mercado se divide entre soluciones basadas en cumplimiento normativo y plataformas de cambio conductual adaptativo:

Plataforma	Diferencia Técnica y Enfoque	Enfoque de Entrenamiento
KnowBe4	Mayor biblioteca de contenido del mundo; enfoque en cumplimiento (compliance) y escala masiva.	Basado en módulos de larga duración y simulaciones programadas.
Hoxhunt	Plataforma nativa de HRM que utiliza IA para personalizar simulaciones según el rol y nivel del usuario.	Gamificación continua y refuerzo positivo basado en recompensas por reportar.
Proofpoint	Integración profunda con el Gateway de correo; usa amenazas reales detectadas para crear simulaciones.	Entrenamiento basado en roles y niveles de amenaza detectados en tiempo real.
Cofense	Especializado en la "triage" de amenazas reportadas por humanos para acelerar la respuesta a incidentes.	Just-in-time education (capacitación inmediata al momento del error).
NINJIO	Enfoque en micro-aprendizaje mediante episodios estilo serie de televisión basados en ataques reales de la semana.	Storytelling emocional para aumentar la retención de conceptos.
Infosec IQ	Fuertes capacidades de integración y automatización con marcos de trabajo como NIST.	Planes de aprendizaje personalizados y evaluación continua.
Phished	Automatización total mediante IA que elimina la necesidad de gestión manual de campañas.	Entrenamiento adaptativo que escala la dificultad según el progreso del usuario.

Mimecast	Seguridad integrada que combina protección de correo con módulos de conciencia situacional.	Enfoque preventivo y protección de marca frente a suplantación.

3. Enfoques Técnicos y Éticos

Las plataformas modernas están abandonando el entrenamiento "punitivo" (castigo por fallar) en favor de la **retroalimentación formativa inmediata**. Técnicamente, esto se logra mediante la visualización de "Teachable Moments" o indicadores de ingeniería social (SEIs) en el momento exacto del clic. Éticamente, el diseño debe garantizar el **consentimiento informado** y evitar temas sensibles como despidos o crisis personales, priorizando la creación de una "red de sensores humanos" que fortalezca la postura de seguridad global.

Conclusión

El análisis de las plataformas líderes en Gestión del Riesgo Humano (HRM) y el diseño del proyecto "El eslabón más débil" permiten concluir que la ciberseguridad moderna ha dejado de ser un reto exclusivamente técnico para convertirse en un desafío sociocultural. La efectividad de herramientas como **Hoxhunt, KnowBe4 o Proofpoint** no reside únicamente en la sofisticación de sus algoritmos de simulación, sino en su capacidad para transformar la psicología del usuario: de una postura de vulnerabilidad pasiva a una de vigilancia activa.

Se ha demostrado que las métricas tradicionales, como la tasa de clics, son insuficientes por sí solas; el verdadero indicador de resiliencia organizacional es la **Tasa de Reporte (Reporting Rate)**. Una organización segura no es aquella donde nadie comete errores, sino aquella donde los empleados poseen la confianza y el conocimiento para identificar y comunicar anomalías en tiempo real.

Finalmente, el componente ético surge como el pilar fundamental de cualquier estrategia de concienciación. El uso de simulaciones debe alejarse del enfoque punitivo para abrazar el **refuerzo positivo** y el aprendizaje en el punto de fallo. Al tratar al usuario con transparencia y respeto, no solo se mitiga el riesgo de ingeniería social, sino que se construye una cultura de ciberseguridad sostenible donde el ser humano deja de ser el eslabón más débil para consolidarse como la primera línea de defensa de la infraestructura digital.

Referencias (APA 7)

Cofense. (2023). *The 2023 annual state of phishing report*. https://cofense.com/state-of-phishing-2023/

Hoxhunt. (2024). *Human risk management: The psychology behind behavioral change in cybersecurity*. https://www.hoxhunt.com/platform/human-risk-management

Infosec Institute. (2023). *Security awareness training and phishing simulation guide*. https://www.infosecinstitute.com/iq/

KnowBe4. (2024). *2024 phishing industry benchmark report*. https://www.knowbe4.com/phishing-benchmark-analysis

Mimecast. (2023). *The state of email security 2023*. https://www.mimecast.com/resources/ebooks/the-state-of-email-security-2023/

NINJIO. (2024). *The power of storytelling in cybersecurity awareness*. https://ninjio.com/our-solution/

Phished. (2023). *AI-driven behavioral change: A new era of cybersecurity training*. https://phished.io/platform/

Proofpoint. (2024). *2024 state of the phish: An analysis of global IT security trends and user awareness*. https://www.proofpoint.com/us/resources/threat-reports/state-of-the-phish

Teso, G., & Vrizlynn, L. (2022). *Engineering social engineering: A study of human-centric security*. Journal of Cybersecurity Research, 15(2), 112-128.