Phishing: Un Enfoque Antropológico sobre la Ingeniería Social y la Ciberseguridad

Phishing: An Anthropological Approach to Social Engineering and Cybersecurity

CARLOS RAMÍREZ CASTAÑEDA
Universidad Nacional Abierta y a Distancia de México - UnADM
cybercrimemx@hotmail.com

Recibido: 26 de marzo de 2026
Aceptado: 15 de abril de 2026

Resumen
El phishing se ha convertido en uno de los vectores de ataque más prevalentes en el panorama de la ciberdelincuencia contemporánea, aprovechándose del factor falible del ser humano como principal superficie de vulneración. Sin embargo, su análisis trasciende los límites de la informática e involucra disciplinas transversales que resultan imprescindibles para el diseño de estrategias de prevención eficaces. El presente artículo adopta un enfoque interdisciplinario que integra perspectivas de la antropología, la psicología social y la ciberseguridad para examinar los mecanismos socioculturales que facilitan el éxito de los ataques de phishing. Se argumenta que la vulnerabilidad ante el phishing no es únicamente técnica, sino que se encuentra profundamente enraizada en sesgos cognitivos, estructuras culturales y dinámicas de poder simbólico que reproducen condiciones de desigualdad digital. La antropología y la psicología podrían ayudarnos a desmenuzar cómo puede impactar el phishing en distintas escalas, contribuyendo a la construcción de una cultura de concientización digital más sólida y contextualizada.
Palabras clave: Phishing, Ingeniería Social, Antropología Digital, Ciberseguridad, Prevención.

Abstract
Phishing has become one of the most prevalent attack vectors in the contemporary cybercrime landscape, exploiting the fallible human factor as the primary vulnerability surface. However, its analysis transcends the boundaries of computer science and involves cross-disciplinary fields that are essential for the design of effective prevention strategies. This article adopts an interdisciplinary approach that integrates perspectives from anthropology, social psychology, and cybersecurity to examine the sociocultural mechanisms that facilitate the success of phishing attacks. It is argued that vulnerability to phishing is not solely technical, but is deeply rooted in cognitive biases, cultural structures, and dynamics of symbolic power that reproduce conditions of digital inequality. Fields such as psychology and anthropology could help us break down how phishing can impact on different scales, contributing to the construction of a stronger and more contextualized culture of digital awareness.
keywords: Phishing, Social Engineering, Digital Anthropology, Cybersecurity, Prevention.

Introducción

En el contexto de la hiperconectividad digital del siglo XXI, el phishing representa uno de los fenómenos sociotécnicos más complejos y persistentes de la ciberdelincuencia. Hablar de phishing es tener en el radar un tema que relaciona a la ciberseguridad con otro tipo de ramas que no son puramente informáticas; el phishing se aprovecha de la parte vulnerable del usuario a nivel psicológico para lograr obtener información privilegiada y/o confidencial, con la finalidad de lograr alguna afectación o vulneración de información de mayor magnitud. Con su alto nivel de efectividad, la influencia de las estructuras sociales posibilita la manipulación, el engaño y el error para la obtención de aquella información relacionada con la identidad digital de cada persona como usuario.

La antropología es una de las ramas que no se puede dejar de lado, pues al analizar el phishing como un fenómeno social que involucra elementos como la confianza y la percepción (existencia o ausencia) del riesgo, dichos elementos se convierten en factores clave para la consecución de un ataque exitoso. En este sentido, autores clásicos como Pierre Bourdieu (1980) y su teoría del habitus ofrecen un marco interpretativo valioso: las disposiciones incorporadas a lo largo de la socialización digital determinan, en gran medida, la capacidad de los individuos para discernir entre interacciones legítimas y fraudulentas en el entorno en línea. Del mismo modo, Marvin Harris (1979) y su materialismo cultural invitan a considerar cómo las condiciones materiales de existencia (para nuestro caso, acceso a dispositivos, nivel educativo, brecha digital) condicionan la vulnerabilidad ante el phishing. Guy Debord (1967), desde otra perspectiva, permite leer el entorno digital como una "sociedad del espectáculo" en la que la apariencia y la simulación son instrumentos de dominación simbólica, condición que los atacantes explotan sistemáticamente.

Es menester desarrollar un análisis riguroso de los factores involucrados en el phishing desde un enfoque psicosocial, considerando que, en la actual era de digitalización, la vida cotidiana se desenvuelve en entornos virtuales que exponen a riesgos la identidad e información confidencial de los usuarios. En este sentido, no se trata únicamente de un problema informático, sino de un fenómeno que exige un abordaje interdisciplinario donde convergen perspectivas como la antropología y otras ciencias sociales.

El presente artículo tiene como objetivo general analizar el fenómeno del phishing desde una perspectiva interdisciplinaria, que articule la antropología, la psicología cognitiva y la ciberseguridad, con la finalidad de identificar los mecanismos socioculturales y cognitivos que facilitan el éxito de dichos ataques, así como proponer lineamientos para el diseño de estrategias de prevención culturalmente situadas. Para ello, se adoptó una metodología de revisión documental sistemática, integrando estudios empíricos, informes de organismos especializados en ciberseguridad y aportaciones teóricas de las ciencias sociales, con el propósito de construir un marco de análisis coherente e interdisciplinario.

La comprensión del comportamiento humano es crucial para fortalecer la ciberseguridad. Las estrategias de phishing se aprovechan de la confianza y las emociones de los usuarios. Por ello, la educación y los estudios relacionados con la ciberseguridad como rama transversal deben considerar la formación de hábitos digitales responsables.

Es importante promover la conciencia sobre los riesgos del phishing y cómo identificar correos electrónicos o mensajes sospechosos. Con una base sólida apoyada en la antropología aplicada a la ciberseguridad, es posible construir un entorno digital más seguro para todos.

Desarrollo del tema
Phishing: definición y contexto

Para conceptualizar y entrar en materia, es necesario precisar el concepto de phishing, definido como un tipo de ataque gestado a través de medios informáticos, basado en la ingeniería social, una técnica de inducción al error o al engaño, cuya finalidad es lograr obtener información privilegiada o confidencial de un usuario (Hadnagy, 2011; Cialdini, 2007). El phishing se encuentra más presente que en épocas anteriores, pues con la digitalización y el alcance tecnológico de una mayoría poblacional, la estandarización del uso de las nuevas tecnologías de la información y la comunicación posibilita una múltiple cartera de acciones negativas en contra de la identidad e integridad de los usuarios, pues entre mayor cantidad de usuarios vertidos en una plataforma, más posibilidades de éxito en el ataque existen,

Como ejemplo de lo anterior, México registra una penetración tecnológica a nivel social de más del 85%, de acuerdo con el 20° Estudio sobre los Hábitos de Usuarios de Internet en México (Asociación Mexicana de Internet, 2024). Este dato adquiere relevancia antropológica cuando se considera que la incorporación masiva de dispositivos digitales en la vida cotidiana no ha estado acompañada de forma proporcional por procesos de alfabetización digital crítica, lo cual genera condiciones estructurales de vulnerabilidad que los atacantes explotan de manera sistemática (Turkle, 2011). Países como Brasil, Colombia, Perú y Ecuador presentan patrones similares de penetración tecnológica acelerada sin formación digital equivalente (Kaspersky, 2024).

El phishing es una técnica que consiste en el envío de comunicaciones como correos electrónicos, mensajes de texto, llamadas telefónicas o páginas web fraudulentas por parte de un ciberdelincuente a un usuario, simulando ser una entidad legítima (red social, banco, institución pública, etc.), con el objetivo de robar información privada, realizar un cargo económico o infectar el dispositivo mediante malware (INCIBE, 2020; Krombholz et al., 2015). Los factores de simulación y suplantación de identidad, propios del engaño, resultan operativos tanto en el plano técnico como en el plano simbólico-cultural.

La ingeniería social constituye el núcleo operativo del phishing y representa la intersección más evidente entre la ciberseguridad y las ciencias sociales. En términos generales, la ingeniería social hace referencia a las técnicas de manipulación que fusionan elementos de la sociología y la psicología con el objetivo de engañar a las personas, provocando que revelen información delicada o lleven a cabo acciones que puedan poner en riesgo su seguridad (Cialdini, 2007; Hadnagy, 2011).

Desde la antropología, es posible interpretar la ingeniería social como una práctica de distorsión ritual: el atacante adopta una máscara social (por ejemplo, la identidad de una institución confiable) y activa esquemas culturales de obediencia, reciprocidad y autoridad que el actor social ha interiorizado a lo largo de su socialización. En este sentido, los principios de influencia social sistematizados por Cialdini (1984) como reciprocidad, compromiso, prueba social, autoridad, simpatía y escasez, no son únicamente mecanismos psicológicos individuales, sino estructuras culturales incorporadas que el "habitus bourdieusiano" reproduce en cada interacción social, incluyendo las mediadas por tecnología.

Harris (1979) señalaba que las prácticas culturales responden, en última instancia, a condiciones materiales de infraestructura y superestructura. En el caso del phishing, las condiciones materiales (dispositivos accesibles, conectividad fragmentada, ausencia

de políticas de cibereducación e incluso brecha digital) configuran una superestructura de vulnerabilidad que beneficia a los atacantes. Por su parte, Debord (1967) permite comprender cómo el entorno digital ha construido una "economía de la atención" basada en la apariencia y el espectáculo, condición que los phishers explotan al diseñar interfaces y mensajes que imitan con fidelidad las apariencias institucionales legítimas.

Dentro del campo de la ciberseguridad, los ciberdelincuentes emplean estas estrategias para adquirir contraseñas, datos bancarios o acceso a sistemas informáticos sin necesidad de utilizar herramientas y técnicas informáticas más complejas. Su método se centra en crear un ambiente que produzca una respuesta anticipada en la víctima, utilizando sus sentimientos y reflejos naturales.

Psicología y persuasión en el Phishing
Mecanismos Emocionales y Sesgos Cognitivos

Los ciberdelincuentes utilizan a su favor acciones basadas en emociones como la curiosidad, el respeto, el temor y la codicia para afectar el comportamiento de sus víctimas. Estas emociones, más que meras vulnerabilidades, pueden ser vistas como vías que facilitan la manipulación de las personas para que se comporten de cierta forma de manera automática, sin utilizar el razonamiento crítico. Es en este punto donde puede mencionarse el concepto de sesgo cognitivo.

Los sesgos cognitivos son distorsiones en el procesamiento de la información que influyen en la toma de decisiones, facilitando errores de juicio que pueden ser explotados en ataques de phishing (Kahneman, 2011; Tversky y Kahneman, 1974). A continuación, se analizan los principales sesgos cognitivos explotados por los atacantes:

- Sesgo del Optimismo: Este sesgo consiste en la tendencia a sobrestimar la probabilidad de resultados positivos futuros y a minimizar las eventualidades negativas que pudieran ocurrir. Los ciberatacantes lo explotan apelando al optimismo de los usuarios digitales con promesas de promociones en productos virales, premios, reducciones de deudas bancarias, beneficios hipotecarios u ofertas de trabajo, con el objeto de inducirlos a hacer clic en un enlace o llenar formularios que los exponen a los atacantes (Torres-Salazar et al., 2020; Sharot, 2011).

- Sesgo de Escasez: En este sesgo, la percepción de que un recurso es limitado o escaso lleva al individuo a otorgarle un mayor valor, generando respuestas de urgencia o acción anticipada. Los atacantes usan esta falla perceptual para apelar a actitudes de protección de recursos que la víctima considera valiosos (Cialdini, 2007; Kahneman, 2011). Mensajes como "Solo quedan 3 lugares" o "Tu cuenta será bloqueada en 24 horas" son ejemplos típicos de activación de este sesgo.

- Sesgo de Reciprocidad: Hace referencia a la necesidad o sentido de obligación de corresponder a un beneficio otorgado por otra persona; los atacantes fingen realizar una supuesta buena acción (un beneficio, una promoción, información relevante) y a cambio las personas creen razonable entregar cierta información. Cialdini (2007) describe la reciprocidad como uno de los principios de influencia más poderosos y universales, enraizado en normas culturales de intercambio que trascienden contextos y sociedades. En el entorno digital, este principio se activa de forma automática cuando el atacante construye un escenario de donación simbólica.

- Sesgo de Autoridad: Se fundamenta en la tendencia a creer como verídica cualquier información aparentemente emitida por una figura de autoridad: jefes de trabajo, instituciones de gobierno, autoridades académicas. Un ejemplo típico es un correo que simula provenir del Servicio de Administración Tributaria, alertando sobre una irregularidad fiscal con urgencia de actuar de inmediato. Milgram (1963) demostró experimentalmente la poderosa inclinación humana a la obediencia ante figuras de autoridad, hallazgo que los phishers aprovechan al suplantar la identidad de instituciones con alto capital simbólico. Bourdieu (1980) nos ayuda a complementar este análisis señalando que el reconocimiento de la autoridad es, en sí mismo, un efecto del campo social y del habitus que el individuo ha construido a lo largo de su trayectoria.

- Sesgo de Anclaje: Las personas tienden a "anclarse" a la primera información recibida, sin profundizar en el análisis posterior. Un mensaje de SMS falso con texto llamativo (los más usuales, "OFERTA", "URGENTE", "PREMIO"), fija la atención del usuario en el estímulo inicial, induciendo el clic sin mayor reflexión. Tversky y Kahneman (1974) identificaron el anclaje como uno de los heurísticos más persistentes en la toma de decisiones bajo incertidumbre, condición que caracteriza el entorno informacional contemporáneo, saturado de estímulos competitivos.

En este punto, posterior a la identificación de los principales sesgos, resulta pertinente hacer referencia a los sistemas de pensamiento desarrollados por Daniel Kahneman (2011), quien en su obra Pensar rápido, pensar despacio distingue dos modos de procesamiento cognitivo: el Sistema 1, caracterizado por ser rápido, intuitivo y emocional, guiado por experiencias previas y patrones heurísticos; y el Sistema 2, más lento, analítico y deliberado, para el entendimiento hacemos el desglose directo de los sistemas y la relación inherente que aparejan a la temática del phishing y la antropología.

De acuerdo con Kahneman (2011), el Sistema 1 es el que se utiliza con mayor frecuencia en las actividades cotidianas, lo que nos hace vulnerables a sesgos cognitivos y errores de juicio. Esta vulnerabilidad se actualiza plenamente cuando los usuarios realizan una revisión veloz y rutinaria de sus plataformas digitales sin percatarse de que están siendo inducidos a un error a través de la ingeniería social. La saturación informacional del entorno digital contemporáneo favorece precisamente las condiciones en las que el Sistema 1 opera de forma predominante, reduciendo la probabilidad de activación del pensamiento analítico (Kahneman, 2011; Sunstein y Thaler, 2009). En este contexto, el tiempo, la prisa, el desconocimiento, el interés y la curiosidad se suman como factores amplificadores de la vulnerabilidad, como se ha mencionado factores de ingeniería social que ayudan a que se lleve con éxito el ataque.

El Sistema 2 es el que se activaría al comenzar a tener mayor conciencia sobre la existencia de estas amenazas digitales. Al intentar evitar los diversos sesgos cognitivos, los usuarios podrían detectar que se trata de un intento de phishing, esto es precisamente lo que persiguen las campañas de concientización digital promovidas por bancos, instituciones financieras y organismos de ciberseguridad, este es un primer acercamiento de resolución y atención a la problemática que representa el phishing. Cabe destacar que para llegar a este punto, se requiere una profundización básica del tema para la comprensión y sobre todo, abordaje y combate directo al phishing.

Marco antropológico del Phishing

El análisis antropológico del phishing permite comprenderlo como un fenómeno estructural, vinculado a disposiciones sociales, condiciones materiales y dinámicas culturales que configuran la vulnerabilidad digital

Pierre Bourdieu (1980), con su concepto de habitus, permite comprender la vulnerabilidad ante el phishing no como una debilidad individual, sino como el producto de disposiciones socialmente construidas. El habitus digital (el conjunto de disposiciones, percepciones y prácticas adquiridas en relación con el entorno digital), determina la probabilidad de que un individuo reconozca o no una interacción fraudulenta. Los individuos con capitales culturales, sociales y económicos limitados presentan habitus digitales menos críticos, lo que los hace objetivos prioritarios para los atacantes (Bourdieu, 1980; Bourdieu y Wacquant, 1992).

Marvin Harris (1979), desde el materialismo cultural, nos permite situar el problema en su contexto material. Las condiciones de producción y distribución de los medios tecnológicos (quién tiene acceso a dispositivos de calidad, a conexiones estables, a educación digital), determinan en gran medida los patrones de vulnerabilidad social ante el phishing en teoría. La brecha digital, lejos de ser una cuestión meramente técnica, es una expresión de desigualdades estructurales que el cibercrimen aprovecha de manera sistemática.

Guy Debord (1967), en "La sociedad del espectáculo", anticipó el advenimiento de una cultura dominada por la apariencia y la representación. En el entorno digital contemporáneo, el phishing puede ser leído como una manifestación extrema de la lógica espectacular: los atacantes construyen representaciones convincentes de instituciones legítimas que operan sobre la superficie de la realidad, explotando la incapacidad del espectador-usuario para distinguir la imagen de la cosa. La autenticidad simulada, por ejemplo, correos que imitan fielmente los logotipos institucionales, páginas web que replican la interfaz de entidades bancarias se convierten en el instrumento central de este espectáculo delictivo.

Desde la antropología contemporánea, Sherry Turkle (2011) ha analizado cómo la vida en pantalla ha reconfigurado la identidad y la confianza social. Turkle señala que la mediación tecnológica de las relaciones crea nuevas formas de vulnerabilidad psicosocial: la confianza en los entornos digitales tiende a ser menos reflexiva y más contextual que en las interacciones cara a cara, lo que facilita el éxito de la suplantación de identidad. Asimismo, Danah Boyd (2014) ha documentado cómo las normas de privacidad y los marcos de relevancia que los jóvenes construyen en las redes sociales pueden divergir significativamente de las concepciones adultas de seguridad, generando vulnerabilidades específicas en este segmento poblacional.

Esta integración de perspectivas antropológicas clásicas y contemporáneas enriquece el análisis del phishing al revelar que sus condiciones de posibilidad no son técnicas, sino estructurales y culturales: el phishing prospera en los intersticios de la desigualdad digital, la confianza mal calibrada y la reproducción acrítica de habitus en entornos sociotécnicos.

Factores culturales y el Phishing

Ahora que se ha comprendido que el phishing se aprovecha de una gran variedad de herramientas de ingeniería social, resulta más evidente que este tipo de ataques pueden personalizarse en función de características culturales específicas de los usuarios

objetivo. Esta capacidad de segmentación cultural convierte al phishing en lo que se denomina un ataque dirigido (Asperis, s.f.).

Diversas empresas y organizaciones especializadas en ciberseguridad recopilan datos sobre el comportamiento de los ataques en distintas partes del mundo. La empresa Kaspersky (2024) realizó un informe sobre las estafas mediante mensajes falsos en la región de América Latina, donde los países más afectados fueron Brasil, México, Perú, Colombia y Ecuador, en ese orden de mayor a menor número de ataques. La modalidad predominante en esta zona geográfica fue el uso de deepvoice y deepfakes potenciados por inteligencia artificial.

Desde una perspectiva antropológica, la preeminencia de estas modalidades en América Latina puede interpretarse a la luz de la teoría de la distancia social de Bourdieu (1980): en sociedades con altos niveles de desigualdad y fragmentación social, la confianza tiende a estructurarse en torno a figuras familiares o cercanas. Los atacantes explotan esta disposición cultural al generar mensajes de voz o video que simulan la identidad de personas conocidas para la víctima, activando así los mecanismos de confianza interpersonal en un contexto fraudulento.

El estudio State of the Phish 2024 de Proofpoint (2024), realizado en ocho países de Europa y Oriente Medio, mostró que el 70% de los usuarios en Emiratos Árabes Unidos, Suecia, Italia y Francia admitieron haber asumido riesgos de ciberseguridad de forma consciente, como compartir contraseñas, abrir mensajes de desconocidos o utilizar equipos laborales para actividades personales. Esto ocurre a pesar de disponer de mayor infraestructura de ciberseguridad, lo que indica que el conocimiento, por sí solo, no modifica el comportamiento.

Este hallazgo es de notable relevancia teórica: la brecha entre conocimiento y conducta ha sido ampliamente documentada en psicología social como "brecha intención-comportamiento" (Sheeran, 2002). En el ámbito digital, factores como la optimización del tiempo, la comodidad y la percepción de invulnerabilidad personal, lo que Sharot (2011) denomina "sesgo del optimismo irrealista"; llevan a usuarios bien informados a actuar de manera riesgosa. Esta paradoja refuerza la necesidad de estrategias de intervención que operen no solo en el nivel cognitivo, sino en el nivel de las disposiciones culturales y los hábitos incorporados.

El informe también reveló que la mayoría de los usuarios en entornos organizacionales considera que la responsabilidad de su seguridad digital recae en sus superiores y no en ellos mismos, mientras que el 83% de los profesionales de seguridad de la información encuestados creen que los empleados son conscientes de su propia responsabilidad (Proofpoint, 2024). Esta disonancia entre la percepción de los responsables de seguridad y la autopercepción de los usuarios reproduce, en el entorno digital, dinámicas de delegación de responsabilidad que Bourdieu (1980) identificaría como efectos del campo: los agentes tienden a naturalizar las reglas implícitas del campo en el que operan, asumiendo posiciones de poder o de subordinación que definen quién "debe" hacerse cargo de cada función.

Impacto social del phishing

El impacto del phishing trasciende la pérdida de información, afectando dimensiones psicológicas, sociales y económicas de las víctimas. En términos antropológicos, el phishing puede entenderse como una forma de violencia simbólica (Bourdieu y Passeron, 1977): el atacante ejerce poder sobre la víctima aprovechando su posición de desventaja en el campo digital, sin que esta lo perciba como tal en el momento del ataque.

Las afectaciones inmediatas que experimenta la víctima incluyen la pérdida de datos personales o sensibles, el acceso no autorizado a cuentas bancarias, la suplantación de identidad y la instalación de malware que puede escalar a ataques de mayor sofisticación, como el ransomware. En un segundo plano, las afectaciones psicológicas son significativas: depresión, ansiedad, estrés postraumático, sentimientos de vergüenza y culpa. Un artículo publicado por la Universidad Nacional Autónoma de México (2016) titulado "Víctimas de cibercrimen sufren depresión y trauma" documenta que las víctimas de ataques en el entorno digital pueden sufrir traumas comparables a los experimentados en agresiones físicas: sensación de invasión de la privacidad, enojo, depresión, culpa e incluso insomnio y desórdenes alimenticios. En casos extremos, se han registrado tendencias suicidas vinculadas a la incapacidad de las víctimas para manejar las consecuencias del ataque, particularmente en casos de extorsión sexual o pérdida total del patrimonio.

Desde la psicología del trauma, Janoff-Bulman (1992) señala que las víctimas de delitos (incluidos los ciberdelitos), experimentan un quiebre en sus "suposiciones básicas" sobre el mundo: la creencia de que el mundo es benevolente, significativo y de que uno mismo es competente y digno de protección. Este quiebre tiene consecuencias duraderas en la capacidad de confianza y en la disposición a participar en entornos digitales, lo que puede generar formas de exclusión digital secundaria.

El phishing no se limita a afectar al usuario directamente atacado; a través de este, puede comprometer organizaciones completas. Un caso paradigmático ocurrido en México fue la propagación del mensaje "¿Eres tú el del video?" a través de Facebook Messenger (WeLiveSecurity, 2021), que se replicó exponencialmente utilizando las listas de contactos de las cuentas comprometidas. Este mecanismo de propagación viral ilustra, en el plano digital, el concepto de contagio social de Gabriel Tarde (1890), quien explicaba la difusión de prácticas e ideas en las sociedades a través de procesos de imitación e irradiación desde centros de influencia. En el caso del phishing, la víctima primaria se convierte, sin saberlo, en vector de contagio para su red social.

En el ámbito organizacional, el phishing puede ser la puerta de entrada a ciberataques más sofisticados que comprometan secretos empresariales, datos financieros o información de terceros, generando responsabilidades legales y pérdidas reputacionales de difícil reparación.

Modelos de vulneración en el Phishng

La literatura especializada en ciberseguridad ha desarrollado diversos modelos para explicar los mecanismos por los que el phishing logra comprometer a sus víctimas, analizaremos algunos de los más aptos para la temática abordada y con base a ello lograr llegar a un punto de entendimiento sobre cómo se hace presente y se marca la diferencia entre cada modelo de vulneración al hablar de phishing:

El modelo de ataque de ingeniería social de Mouton et al. (2016) propone un proceso de cinco fases:

- identificación del objetivo y recopilación de información (reconocimiento);
- selección y diseño del vector de ataque;
- desarrollo del pretexto o narrativa de engaño;
- ejecución del ataque; y
- extracción de la información y cobertura de rastros.

Este modelo resulta especialmente útil para comprender cómo los factores culturales identificados en el apartado anterior se integran en cada fase del ataque: el reconocimiento implica la identificación de vulnerabilidades culturales específicas del objetivo; el diseño del vector de ataque adapta el engaño a las disposiciones culturales del grupo objetivo; y el pretexto aprovecha los sesgos cognitivos descritos anteriormente.

Otro de los modelos para mencionar es el de cadena de ataque de phishing (Phishing Attack Lifecycle) de Krombholz et al. (2015) distingue tres etapas fundamentales:

- preparación, en la que el atacante selecciona la víctima, diseña el mensaje fraudulento y construye la infraestructura de engaño;
- ataque, en la que se ejecuta el envío del mensaje y se espera la respuesta de la víctima; y
- monetización, en la que el atacante explota la información obtenida.

La intersección entre este modelo técnico y el análisis socioantropológico reside, principalmente, en la primera etapa: la efectividad del phishing depende, en gran medida, de la capacidad del atacante para construir un pretexto culturalmente plausible que active los mecanismos de confianza de la víctima.

Finalmente, el modelo de persuasión de Cialdini (1984, 2016), posteriormente aplicado al análisis del phishing por Vishwanath et al. (2011), identifica seis principios de influencia:

- reciprocidad,
- compromiso y consistencia,
- prueba social,
- autoridad,
- simpatía y escasez

Como los mecanismos psicológicos centrales que los atacantes activan en sus víctimas. La relevancia de este modelo reside en que cada uno de estos principios tiene una base cultural específica: la reciprocidad y la autoridad, por ejemplo, varían significativamente en su intensidad y forma de expresión entre culturas colectivistas e individualistas (Hofstede, 1980), lo que explica la diferenciación de las estrategias de phishing observada entre América Latina y Europa en los informes analizados.

Estrategias de prevención y concientización digital

Una de las actividades que los gobiernos pueden llevar a cabo para mitigar y reducir la tendencia de los ataques de phishing son los programas de concientización, no solo con el fin de difundir información, sino con el objetivo de generar un impacto real en la comprensión que los usuarios tienen sobre la importancia de resguardar su información. Como se observó en el caso de los países europeos, no es suficiente contar con infraestructura de seguridad y abundante información si el usuario no dimensiona la importancia de su seguridad en el entorno digital ni su papel de responsabilidad social.

En el panel "Ciberseguridad y privacidad", en el marco del Foro Nacional de Ciberseguridad 2024, el comisionado del INFOEM señaló que la mayor parte de

los ataques y fugas de información que resultaron eficaces en las empresas fueron consecuencia de la falta de profesionalización y capacitación del personal que labora en instituciones que trabajan con datos sensibles.

Desde una perspectiva antropológica y pedagógica, la concientización efectiva requiere ir más allá de la transmisión de información y operar en el nivel de la transformación de habitus (Bourdieu, 1980). Esto implica diseñar intervenciones que partan de los marcos culturales de referencia de los grupos objetivo, que conecten la seguridad digital con valores y prácticas ya incorporadas, y que generen experiencias de aprendizaje situadas que modifiquen las disposiciones y no únicamente los conocimientos declarativos. Por lo anterior es necesario identificar a los sectores primordiales de atención.

- Adultos mayores: Este es uno de los grupos más afectados, dado que muchos de ellos no crecieron con la tecnología y poseen menor conocimiento sobre ciberseguridad. Tienden a conferir mayor confianza a cualquier información que reciben en el entorno digital (El País, 2024). Desde la perspectiva del capital cultural de Bourdieu, los adultos mayores presentan un capital digital más bajo, lo que los ubica en una posición de desventaja estructural en el campo digital. Las estrategias de intervención deben contemplar formatos accesibles, lenguaje familiar y conexión con valores como la protección de la familia y la comunidad.
- Niños y adolescentes: Los jóvenes son otro bastión débil, debido al tiempo que pasan en redes sociales y videojuegos sin supervisión adecuada. El Instituto Nacional de Transparencia (INAI, 2021) ha señalado que este sector es altamente vulnerable, ya que frecuentemente comparte información sin precaución. Boyd (2014) ha documentado cómo los jóvenes construyen normas de privacidad contextualmente específicas que pueden no coincidir con las expectativas de seguridad de los adultos, generando zonas de vulnerabilidad invisibles para las estrategias de prevención tradicionales.
- Trabajadores y funcionarios públicos: Muchas veces, los empleados reciben correos electrónicos fraudulentos que imitan comunicaciones oficiales. De acuerdo con un estudio de Verywell Mind (Cherry, 2024), las personas de entre 35 y 44 años son especialmente propensas a caer en estos engaños debido a la presión laboral y la falta de capacitación en seguridad informática.
- Pequeños empresarios y emprendedores: Debido a recursos limitados para invertir en ciberseguridad y a un mayor uso de correos electrónicos y transacciones en línea sin protocolos seguros, este sector presenta una vulnerabilidad específica ante los ataques de phishing.
- Usuarios con bajo nivel educativo o acceso limitado a información digital: La falta de conocimientos sobre seguridad digital aumenta el riesgo de caer en ataques de phishing. La brecha digital, caracterizada por la intersección entre desigualdad socioeconómica y acceso diferenciado a la tecnología, genera condiciones estructurales de vulnerabilidad que no pueden abordarse únicamente mediante campañas informativas (EasyDMARC, 2022).
- Profesionales de la salud y académicos: Aunque pueda parecer un ámbito alejado del entorno digital, los sectores de la educación y la sanidad son objetivos frecuentes de ciberataques debido al valor de la información que manejan. La digitalización acelerada de estos entornos ha aumentado los riesgos, y los profesionales no siempre reciben entrenamiento adecuado en seguridad informática (El País, 2025).

Un modelo de prevención culturalmente situado debería articular, al menos, los siguientes componentes:

- diagnóstico del habitus digital del grupo objetivo;
- diseño de mensajes y experiencias de aprendizaje que partan de los marcos de referencia culturales del grupo;
- conexión de la seguridad digital con valores centrales del grupo (familia, comunidad, identidad);
- activación del Sistema 2 de pensamiento (Kahneman, 2011) mediante la incorporación de hábitos de verificación y pausa reflexiva antes de proporcionar información en línea; y
- evaluación longitudinal del cambio en las disposiciones y no únicamente en los conocimientos declarativos.

Consideraciones finales

Las consideraciones finales que pueden extraerse del análisis realizado apuntan a que el phishing es un fenómeno sociotécnico complejo cuya comprensión y prevención efectiva requieren una perspectiva genuinamente interdisciplinaria. La relación entre educación digital y concientización constituye una necesidad urgente en un momento histórico en que la mayor parte de la población mundial participa del entorno digital.

El aporte específico del presente artículo reside en la articulación de un marco analítico que integra herramientas conceptuales de la antropología clásica y contemporánea (Bourdieu, Harris, Debord, Turkle, Boyd), con los modelos de vulneración técnica y los hallazgos de la psicología cognitiva (Kahneman, Cialdini, Tversky), para explicar los mecanismos socioculturales que subyacen al éxito del phishing. Este marco permite superar las limitaciones de los enfoques exclusivamente técnicos o psicológicos, ofreciendo una comprensión más integral del fenómeno y sentando las bases para el diseño de estrategias de prevención culturalmente pertinentes.

Es evidente que la especialización de un ataque de phishing no solo descansa en el conocimiento técnico de informática o programación, sino que es la conjunción del aprovechamiento de vulnerabilidades tanto técnicas como psicosociales: la ingeniería social, los sesgos cognitivos y los factores culturales actúan de manera articulada. Las consecuencias tampoco se limitan a la fuga de información sensible, sino que se proyectan en repercusiones negativas a nivel mental, físico, económico y social.

El usuario siempre estará en el centro del fenómeno, pero la diferencia entre un ataque exitoso y su prevención reside no solo en la concientización individual, sino en la transformación de las condiciones estructurales que reproducen la vulnerabilidad: el acceso equitativo a la educación digital, la reducción de la brecha digital, la profesionalización de los equipos de seguridad en las organizaciones y el diseño de políticas públicas de ciberseguridad que reconozcan la dimensión cultural y antropológica del problema. La concientización, en última instancia, debe entenderse no como la transmisión de información, sino como la transformación de habitus: el objetivo no es que el usuario sepa que el phishing existe, sino que incorpore disposiciones de verificación, escepticismo informado y responsabilidad digital como parte de su práctica cotidiana en el entorno digital.

La prevención efectiva no depende únicamente del conocimiento del riesgo, sino de la incorporación de prácticas críticas y reflexivas en el uso cotidiano de las

tecnologías digitales, a la par del entendimiento del contexto en el que los usuarios se encuentran ante una realidad inmersa en el día a día dónde se involucra una estrecha relación con el uso tecnológico.

El phishing tiene diversas aristas de análisis, debemos entender que todos como usuarios de las tecnologías de la información y las comunicaciones estamos expuestos a ser víctimas, esto en una escala mayor dónde la antropología genera un análisis más allá de lo social, hablando incluso de una meta realidad que relaciona diversos elementos entre sí. El usuario siempre estará al centro, pero la diferencia entre un ataque exitoso y la prevención se encuentra en la concientización.

La concientización se convierte en la clave y punto medular para realizar un combate frontal al phishing, y aunque lo identifiquemos a través de distintas ramas que permean toda su existencia y punto de penetración a nivel social, el usuario a través de procesos de aprendizaje a nivel conciencia/prevención podrá salir avante en la detección del mismo.

Referencias

Asociación Mexicana de Internet. (2024). 20° estudio sobre los hábitos de usuarios de internet en México 2024. https://irp.cdn-website.com/81280eda/files/uploaded/20_Habitos_de_Usuarios_de_Internet_en_Mexico_2024_VP.pdf

Asperis. (s. f.). *Ataque dirigido*. https://www.asperis.es/glosario-ciberseguridad/ataque-dirigido/

Bourdieu, P. (1980). Le sens pratique. Les Éditions de Minuit.

Bourdieu, P., & Passeron, J.-C. (1977). La reproducción: Elementos para una teoría del sistema de enseñanza. Laia.

Bourdieu, P., & Wacquant, L. J. D. (1992). An invitation to reflexive sociology. The University of Chicago Press.

Boyd, d. (2014). It's complicated: The social lives of networked teens. Yale University Press.

CERT-MX. (s. f.). Noticia 3019. https://www.cert.org.mx/historico/noticia/index.html-noti=3019

Cherry, K. (2026, March 23). Why we fall for scams. Verywell Mind. https://www.verywellmind.com/why-we-fall-for-scams-8705528

Cialdini, R. B. (1984). Influence: The psychology of persuasion. William Morrow and Company.

Cialdini, R. B. (2007). Influence: The psychology of persuasion (Rev. ed.). HarperBusiness.

Cialdini, R. B. (2016). Pre-suasion: A revolutionary way to influence and persuade. Simon & Schuster.

Debord, G. (1967). La société du spectacle. Buchet-Chastel.

DIF Ciudad de México. (2021, octubre 5). ¿Eres tú el del video? Este es el mensaje de un virus malicioso que ha comenzado a circular [Publicación de Facebook]. Facebook. https://www.facebook.com/DIFCDMX/posts/4999387316754534/

EasyDMARC. (2022). *Estadísticas de phishing: Informe EasyDMARC enero-junio de 2022*. https://easydmarc.com/blog/es/estadisticas-de-phishing-informe-easydmarc-enero-junio-de-2022/

El País. (2024, diciembre 14). La llegada de las compras de Navidad allana el terreno a

los ciberdelincuentes. https://elpais.com/espana/catalunya/2024-12-14/la-llegada-de-las-compras-de-navidad-allana-el-terreno-a-los-ciberdelincuentes.html
El País. (2025, febrero 24). Nuevos actores y herramientas se incorporan a la guerra de la seguridad en internet. https://elpais.com/tecnologia/2025-02-24/nuevos-actores-y-herramientas-se-incorporan-a-la-guerra-de-la-seguridad-en-internet.html
Hadnagy, C. (2011). Social engineering: The art of human hacking. Wiley.
Harris, M. (1979). Cultural materialism: The struggle for a science of culture. Random House.
Hofstede, G. (1980). Culture's consequences: International differences in work-related values. Sage.
IDC Online. (2021, septiembre 17). Jóvenes, la población más vulnerable a ciberataques: INAI. https://idconline.mx/corporativo/2021/09/17/jovenes-la-poblacion-mas-vulnerable-a-ciberataques-inai
INCIBE. (2020). *Phishing*. https://www.incibe.es/aprendeciberseguridad/phishing
Janoff-Bulman, R. (1992). Shattered assumptions: Towards a new psychology of trauma. Free Press.
Kahneman, D. (2011). Thinking, fast and slow. Farrar, Straus and Giroux.
Kaspersky. (2024, octubre 15). Aumentan en 140% las estafas mediante mensajes falsos en América Latina, revela Kaspersky. https://latam.kaspersky.com/about/press-releases/aumentan-en-140-las-estafas-mediante-mensajes-falsos-en-america-latina-revela-kaspersky
Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 22, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005
Milgram, S. (1963). Behavioral study of obedience. Journal of Abnormal and Social Psychology, 67(4), 371–378. https://doi.org/10.1037/h0040525
Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186–209. https://doi.org/10.1016/j.cose.2016.03.004
National Center of Incident Readiness and Strategy for Cybersecurity. (2024). Cybersecurity awareness month 2024. https://security-portal.nisc.go.jp/cybersecuritymonth/2024/
Proofpoint. (2024, February 27). 2024 State of Phish report. https://www.proofpoint.com/es/blog/security-awareness-training/2024-state-of-phish-report
SEON. (2025, February 7). Deepfake: ¿Qué es y cómo funciona? https://seon.io/es/recursos/glosario/deepfake/
Sharot, T. (2011). The optimism bias: A tour of the irrationally positive brain. Pantheon Books.
Sheeran, P. (2002). Intention-behavior relations: A conceptual and empirical review. European Review of Social Psychology, 12(1), 1–36. https://doi.org/10.1080/14792772143000003
Sunstein, C. R., & Thaler, R. H. (2009). Nudge: Improving decisions about health, wealth, and happiness. Penguin Books.
Tarde, G. (1890). Les lois de l'imitation. Alcan.
Torres-Salazar, C., Moreta-Herrera, R., Ramos-Ramírez, M., & López-Castro, J. (2020). Sesgo cognitivo de optimismo y percepción de bienestar en una muestra de universitarios ecuatorianos. Revista Colombiana de Psicología, 29(1), 61–72.

https://doi.org/10.15446/rcp.v29n1.75853
Turkle, S. (2011). Alone together: Why we expect more from technology and less from each other. Basic Books.
Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. Science, 185(4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124
Universidad Nacional Autónoma de México. (2016). Víctimas de cibercrimen sufren depresión y trauma. UNAM
Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, 51(3), 576–586. https://doi.org/10.1016/j.dss.2011.03.002
WeLiveSecurity. (2021, julio 22). ¿Eres tú en este video? Phishing en Facebook Messenger. https://www.welivesecurity.com/la-es/2021/07/22/eres-tu-este-video-phishing-en-facebook-messenger/