DIP. MARTHA SOLEDAD ÁVILA VENTURA
PRESIDENTA DE LA MESA DIRECTIVA DEL
CONGRESO DE LA CIUDAD DE MÉXICO
III LEGISLATURA
P R E S E N T E

Quien suscribe**, OLIVIA GARZA DE LOS SANTOS,** Diputada Local integrante del Grupo Parlamentario del Partido Acción Nacional en el Congreso de la Ciudad de México, III Legislatura, con fundamento en lo dispuesto por los artículos 71, fracción III y 122, numeral A, fracción II de la Constitución Política de los Estados Unidos Mexicanos; 29, Apartado D, inciso a), b); y 30, numeral 1, inciso b), de la Constitución Política de la Cuidad de México; 1, 4, fracción XXI, 12, fracción II, 13 fracción LXIV, LXXIV de la Ley Orgánica del Congreso de la Ciudad de México; y 5, fracción I; 95, fracción II; 96; y 118 del Reglamento de Congreso de la Ciudad de México, todos ordenamientos de la Ciudad de México, someto a la consideración de este órgano legislativo la presente **INICIATIVA CON PROYECTO DE DECRETO POR LA QUE SE ADICIONA LA FRACCIÓN XVII AL ARTÍCULO 231 DEL CÓDIGO PENAL PARA EL DISTRITO FEDERAL CON EL OBJETO DE TIPIFICAR EL DELITO DE PHISHING.** Conforme a lo siguiente:

I. TÍTULO DE LA PROPUESTA.

Iniciativa con proyecto de decreto por la que se adiciona la fracción XVII al artículo 231 del Código Penal para el Distrito Federal con el objeto de tipificar el delito de phishing.

II. PLANTEAMIENTO DEL PROBLEMA

La Ciudad de México enfrenta nuevas problemáticas como son los llamados fraudes electrónicos, no se encuentra tipificados en el Código Penal para el Distrito Federal,

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

por lo que la presente iniciativa busca tipificar los delitos derivados del uso de nuevas tecnologías.

En la era digital, el uso de tecnologías de la información y comunicación ha transformado la vida cotidiana de las personas, facilitando actividades comerciales, laborales, educativas y sociales, sin embargo, como toda nueva herramienta hay sujetos que deciden utilizarlas para fines delictivos, entre los cuales destaca el conocido como “Phishing”, el cual se puede definir como una técnica de ingeniería social utilizada por ciberdelincuentes para obtener información confidencial, como contraseñas, números de tarjetas de crédito o datos personales, mediante el engaño.

El phishing toma su nombre por su homónimo en inglés que hace referencia a la práctica de pescar, deporte para el cual se suele utilizar una carnada y anzuelo que busca atrapar a su presa, lo cual al caso en concreto se traduce a la búsqueda de pescar/obtener información a través de medios fraudulentos, con lo cual se espera obtener información confidencial, como lo sería usuarios y contraseñas de sistemas electrónicos, datos bancarios, suplantación de identidad, transferencia ilegítima de recursos económicos y demás datos con los cuales el perpetrador pueda recibir un beneficio.

Asimismo, se lleva a cabo a través de medios digitales, como correos electrónicos, mensajes instantáneos o sitios web falsos, donde el ciberdelincuente se hace pasar por una persona o entidad confiable para engañar a las víctimas y lograr que revelen sus datos. En México, y particularmente en la Ciudad de México, el crecimiento del uso de internet y las transacciones electrónicas ha incrementado la vulnerabilidad de los ciudadanos ante este tipo de ataques, lo que hace necesario abordar el phishing como delito, con el objeto de su persecución y castigo.

La Ciudad de México, como centro económico, político y cultural del país, ha experimentado una transformación digital acelerada en la última década pues al

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

contar con una población de más de 9.2 millones de habitantes (según el Censo de Población y Vivienda 2020 del INEGI) y una infraestructura tecnológica en constante expansión, la capital del país se ha posicionado como una de las urbes más conectadas del mundo, de hecho la Ciudad de México fue reconocida por el *Guinness World Records* por ser la ciudad más conectada del mundo con 20 mil 500 puntos WiFi[1], sin embargo, este avance también permite que una mayor cantidad de personas trae consigo desafíos significativos en materia de seguridad cibernética, particularmente en relación con delitos como el **phishing**, al ser esta una modalidad de fraude electrónico.

De acuerdo al Kaspersky report, realizado por Kaspersky Lab, la cual es una compañía multinacional dedicada a la seguridad informática, tan sólo las soluciones de dicha empresa bloquearon más de 893 millones de intentos de phishing en 2024, lo que representó un incremento del 26 % con respecto al año anterior, estos intentos buscaron hacerse pasar por redes sociales reconocidas, portales reconocidos de viajes, de comercio electrónico, así como la promesa de “ofertas únicas”, o “premios exclusivos” para así lograr obtener información indebida e incluso la realización de pagos para la obtención de productos o servicios fraudulentos[2].

Ahora bien, esa misma empresa al estudiar el caso de América Latina, encontró que dicha región es una de las zonas de mayor actividad delictiva cibernética, con Brasil a la cabeza y México en segundo lugar, seguido de Perú, Colombia y Ecuador[3], a pesar de lo anterior, la legislación penal vigente en la Ciudad

[1] Gobierno de la Ciudad de México https://gobierno.cdmx.gob.mx/noticias/somos-la-ciudad-mas-conectada-del-mundo/
[2] Kaspersky. (19 febrero 2025). *Kaspersky reports nearly 900 million phishing attempts in 2024 as cyber threats increase*. Obtenido de: https://www.kaspersky.com/about/press-releases/kaspersky-reports-nearly-900-million-phishing-attempts-in-2024-as-cyber-threats-increase
[3] Kaspersky. (15 octubre 2024). *Aumentan en 140% las estafas mediante mensajes falsos en América Latina, revela Kaspersky*. Obtenido de: https://latam.kaspersky.com/about/press-releases/aumentan-en-140-las-estafas-mediante-mensajes-falsos-en-america-latina-revela-kaspersky?utm_source=chatgpt.com

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

de México no contempla de manera específica el phishing como un delito autónomo, lo que genera un vacío legal que dificulta su persecución y sanción efectiva.

El marco legal actual en la Ciudad de México se rige por el Código Penal para el Distrito Federal, el cual contempla delitos relacionados con el fraude y el engaño tipificados en los artículos 230 a 233 BIS, sin embargo, estos artículos no abordan de manera explícita las técnicas digitales utilizadas en el phishing, lo que limita su aplicabilidad en casos donde el delito se comete a través de medios electrónicos.

Tras la pandemia hubo un crecimiento de delitos informáticos en México, pues de acuerdo a un estudio realizado por el Grupo Fractalia[4], señala que aunque internet ya era parte de la vida cotidiana para diversas actividades, el comercio electrónico tuvo un crecimiento de 108% y el uso de herramientas digitales se duplicó en los primeros meses de la pandemia, por lo que en dicho periodo la facturación de tiendas en líneas incrementó 60% y aumentaron las amenazas cibernéticas, pues para el último trimestre de 2020 existían 75% más de probabilidades de ser víctima de un ciberdelito en comparación con 2019.

Las cifras de estos delitos a nivel país pasaron del 2019 a 2021 de 300.3 millones en 2019 a 120 mil millones de intentos en 2021, lo anterior de conformidad con datos de la firma mexicana de ciberseguridad Silikn[5], lo que representa un incremento sin precedentes, y se observa una clara tendencia en donde los ataques se vuelven cada vez más frecuentes, por lo que urge que desde el congreso de la Ciudad de México se tomen medidas concretas para garantizar la ciberseguridad de sus ciudadanos.

---

[4] Grupo Fractalia. (19 noviembre de 2020). El ciberdelito en tiempos de COVID en México. Obtenido de: https://fractaliasystems.com/los-ataques-ciberneticos-aumentan-40-en-mexico-durante-la-pandemia/

[5] Calderón Christopher, 9 de junio 2022, México 'clientazo' de los ciberataques: crecen 42% amenazas por internet. EL FINANCIERO. Obtenido de: https://www.elfinanciero.com.mx/empresas/2022/06/09/aumentan-42-los-ciberataques-con-85-mil-millones-de-intentos-en-mexico/

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

A nivel internacional diversos países han establecido diversas leyes que buscan combatir este delito, precisamente derivado de su prevalencia y el enorme daño que genera a la sociedad, entre las regulaciones realizadas podemos encontrar:

Colombia: Ley 1273 de 2009

Esta ley establece en su artículo 269G establece la suplantación de sitios web para capturar datos personales como un delito, (lo cual es un tipo de phishing), al cual incurre todo aquel que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, así como para aquellos que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza.

Reino Unido de la Gran Bretaña e Irlanda del Norte:

Establecen el delito de “Fraude por representación falsa” en donde se establece que al que realice una representación falsa de forma deshonesta con la intención de obtener un beneficio para si u otra persona, con lo que se genere a alguien más una pérdida o lo expone a un riesgo de pérdida.

Considerándose que es falsa si es inexacta o engañosa, o que en su caso, el sujeto activo sepa que pudiese serlo.

De igual forma se considera que se ha realizado una representación si ésta (o cualquier cosa que la implique) se envía, en cualquier forma, a cualquier sistema o dispositivo diseñado para recibir,

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

transmitir o responder comunicaciones (con o sin intervención humana).

España:

En el Código Penal de aquel país, se establece en su artículo 197 Bis, que al que, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión.

De igual forma dicho artículo establece que la utilización de artificios o instrumentos técnicos, sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión

Como se puede ver, esta legislación ha buscado combatir el phishing desde diversos ángulos, por lo que ahora conviene aprovechar las experiencias extranjeras de tal modo que sea la que mejor responda a las necesidades de México y en particular de nuestra ciudad.

El problema del phishing es prevalente en nuestro país, y así es reconocido por nuestras propias instituciones, pues la propia Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), ha hecho llamados a la población para no dejarse engañar por tácticas de *Phishing*, en donde se hacen pasar por instituciones financieras con el objeto de captar datos personales y bancarios de los usuarios a través de la utilización de la imagen de la

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

institución financiera, para posteriormente cometer fraude con las cuentas de las personas que llegan a caer en el engaño[6].

En el contexto mexicano, el phishing ha desplazado en frecuencia a otras modalidades de fraude digital y se ha convertido en la amenaza cibernética más extendida, según reportes de organismos públicos, los cuales consideran que tan sólo en el año 2023, el 55 % de los consumidores mexicanos afirmó haber sido víctima de algún tipo de ataque de phishing, ya sea a través de enlaces maliciosos o comunicaciones que simulaban provenir de instituciones bancarias o plataformas de pago en línea[7].

El establecer el phishing como un delito específico en la Ciudad de México responde a la necesidad de actualizar el marco legal para hacer frente a las nuevas formas de delincuencia digital, pues la legislación actual no contempla de manera adecuada este tipo de conductas, lo que genera un vacío legal que favorece la impunidad.

La alta prevalencia de ataques de phishing, combinada con la falta de una respuesta legislativa efectiva, justifica la urgencia de esta iniciativa. Al tipificar el phishing como un delito autónomo, se busca proporcionar a las autoridades las herramientas necesarias para investigar y sancionar a los responsables, así como proteger a los ciudadanos de la Ciudad de México de esta creciente amenaza.

Por lo tanto, si consideramos los niveles de incidencia delictiva, tanto a nivel federal como de las entidades federativas, correspondientes a los años 2019, 2020 y 2021, se observa que el nivel de ciberdelincuencia en México ha ido en aumento y que inclusive varias instituciones federales han sido vulneradas, por lo que se

---

[6] Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros [CONDUSEF]. (17 de abril de 2015). *Registra Condusef nuevo caso de "phishing" contra usuarios de BBVA Bancomer* [Comunicado de prensa]. Obtenido de: https://www.condusef.gob.mx/?p=contenido&idc=700&idcat=1

[7] Gutiérrez, N. (31 de mayo de 2024). *Estadísticas de Phishing en Latinoamérica*. Prey Project. Recuperado de https://preyproject.com/es/blog/phishing-en-latinoamerica

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

considera que es urgente que nuestra ciudad implemente medidas políticas, tecnológicas y estratégicas que garanticen la ciberseguridad, lo cual únicamente se podrá lograr con el apoyo de las Fiscalía, otorgándole las herramientas legales que les permita atender este problema, pues ella es la responsable de perseguir los delitos así como el de promover la cultura de la denuncia e investigación de estos.

III. PROBLEMÁTICA DESDE LA PERSPECTIVA DE GÉNERO

Por la naturaleza de la propuesta realizada, se estima que las reformas planteadas no requieren de un estudio de perspectiva de género, toda vez que las reformas no cuentan con la potencialidad de beneficiar o perjudicar el ejercicio de un derecho humano que les pudiese afectar de manera desproporcionada a las mujeres respecto de los hombres.

IV. ARGUMENTOS

En la Ciudad de México, la profundización de la transformación digital en todos los ámbitos de nuestra vida cotidiana ha venido acompañada de una alarmante ola de ataques en materia cibernética, entre los cuales el phishing destaca por su facilidad de propagación y su capacidad de causar perjuicios masivos, en especial en materia económica.

El phishing representa uno de los ciberdelitos más insidiosos y extendidos que afectan a las sociedades modernas, y la Ciudad de México, la cual al extender la capacidad de acceso a la población a la obtención de productos y servicios por internet ha generado un ambiente propicio para que los ciberdelincuentes busquen sacar provecho de dicha situación.

Esta forma de ciberdelito implica que los atacantes empleen técnicas engañosas para inducir a las personas a revelar información sensible, como nombres de usuario, contraseñas, detalles de tarjetas de crédito u otros datos

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

personales, haciéndose pasar por entidades confiables a través de comunicaciones electrónicas.

El phishing es un delito en constante cambio y cuenta con variedades que se van generando conforme a la capacidad tecnológica alcanzada que genera nuevas oportunidades de buscar defraudar a la población, ante la que encontramos:

- Phishing por correo electrónico: correos fraudulentos que imitan fuentes legítimas como bancos o proveedores de servicios para atraer a las víctimas a hacer clic en enlaces maliciosos o divulgar información.

- Spear phishing: un enfoque más dirigido que personaliza los ataques utilizando detalles personales, a menudo obtenidos de redes sociales.

- Whaling: se enfoca en objetivos de alto perfil como ejecutivos corporativos o funcionarios gubernamentales.

- Smishing: ejecutado a través de mensajes de texto SMS con enlaces o solicitudes engañosas.

- Vishing: los atacantes usan llamadas telefónicas para hacerse pasar por organizaciones creíbles.

La naturaleza multifacética y evolutiva de los delitos relacionados con la práctica del phishing subraya la urgente necesidad que desde el Congreso de la Ciudad de México se le establezca como un delito específico dentro de su legislación local, así como el de sus variedades de la forma más amplia posible, de tal forma que se proporcione un marco legal sólido que permita a los fiscales de la Ciudad de México el combatir dicho delito en beneficio de las personas de nuestra capital.

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

Hay estadísticas que indican que “cada 39 segundos tiene lugar un ciber ataque; así que son más de 2 mil 200 casos al día”, alertó Luis Gustavo Parra Noriega, quien apuntó la necesidad de formar y profesionalizar al personal, además de trabajar en colaboración institucional con autoridades de datos y quienes, de alguna manera tienen que trabajar los temas de educación digital, desde las primeras infancias y atacando el problema de la brecha digital, a fin de que esta colaboración pueda hacer frente a las amenazas inherentes al uso de las nuevas tecnologías al interior de los gobiernos y para agilizar trámites y servicios, al utilizar plataformas digitales[8].

Las consecuencias económicas del phishing son profundas y afectan de forma negativa su desarrollo pues con ella se genera una carga significativa entre los habitantes, pues al volverse víctimas de este ciberdelito pierden recursos producto de su trabajo arduo además de que estos en muchas ocasiones dejan de llegar a negocios legítimos que mantienen a flote la economía de nuestra ciudad y país, algunos de los costos asociados al phishing son los siguientes:

- Pérdidas financieras directas: transacciones fraudulentas o accesos no autorizados a cuentas.

- Costos indirectos: honorarios legales, servicios de monitoreo de crédito y tiempo invertido en resolver fraudes.

- Impacto en empresas: interrupciones operativas, pérdida de confianza del cliente y mayores gastos en ciberseguridad.

El marco legal mexicano actual no aborda el phishing con la especificidad necesaria pues si bien el Código Penal Federal incluye el delito de fraude y el así como acceso no autorizado a sistema, pero no menciona explícitamente el phishing ni por nombre ni por sus características únicas, como la ingeniería social, la cual en el contexto de

[8] Infoem. (12 de octubre 2024). *Phishing, amenaza cibernética más extendida en México*. Infoem. Recuperado de https://www.infoem.org.mx/es/contenido/noticias/phishing-amenaza-cibern%C3%A9tica-m%C3%A1s-extendida-en-m%C3%A9xico

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

ciberseguridad hace referencia a las técnicas que usan los ciberdelincuentes para manipular a las personas y obtener información confidencial o comprometer la seguridad basados en la manipulación humana y la psicología, para engañar a la víctima y lograr sus objetivos. De igual forma el Código Penal para el Distrito Federal tampoco contempla el phishing como un tipo penal, por lo que se vuelve necesario atender dicho problema.

A pesar de lo anterior, la Policía Federal del Gobierno Federal ha advertido de la existencia y características de dicho delito[9], la cual define como:

> "El Phishing es una modalidad de estafa, cuyo objetivo es obtener datos, claves, números de cuentas bancarias y tarjetas de crédito, identidad u otros datos para ser usados de forma fraudulenta."

El phishing busca entonces el suplantar la imagen de una empresa o entidad pública, a fin de hacer creer a la víctima que los datos solicitados provienen de un sitio oficial, cuando en realidad lo que se busca es cometer un delito.

La propia policía advierte que en el caso de Internet, para que los mensajes parezcan más reales, las o los delincuentes incluyen un vínculo falso que pareciera dirigir a un sitio web o una ventana emergente que tiene el mismo aspecto que una legítima y que una vez que la o el usuario está en uno de estos sitios web falsos, introduce información personal sin saber que la transmite directamente al delincuente, quien la utilizará para hacer compras, solicitar una nueva tarjeta de crédito o robar su identidad.

En consecuencia, la fiscalía y los órganos jurisdiccionales se ven obligados a encuadrar los hechos conocidos como phishing en tipos penales genéricos, como lo es el acceso ilícito a sistemas, el fraude informático o la usurpación de identidad,

[9] Policía Federal. (8 de enero de 2019). *¿Conoces qué es el Phishing?* Gobierno de México. Recuperado de https://www.gob.mx/epn/policiafederal/articulos/conoces-que-es-el-phishing?idiom=es

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

lo que genera obstáculos para la persecución penal y desincentiva la denuncia ciudadana al prolongar y complejizar los procesos de investigación.

La deficiencia legislativa local contrasta con la creciente sofisticación de los ataques: hoy en día, los ciberdelincuentes emplean técnicas de ingeniería social hiperpersonalizada, como las deepfakes e incluso el establecimiento de portales web casi idénticas a las originales para engañar a usuarios desprevenidos. Al no contar con un tipo penal específico, las autoridades carecen de las herramientas jurídicas para tipificar adecuadamente estos métodos y aplicar sanciones proporcionales al daño patrimonial y moral causado.

El establecer al phishing como un delito específico traería diversos beneficios pues establecer el phishing como delito en la Ciudad de México traería múltiples beneficios pues el contar con una definición clara que abarque todas sus formas, facilitaría su identificación e investigación. Se considera así, que la legislación que se establezca debe de constar con sanciones adecuadas que ayuden a inhibir la práctica de dicho delito.

Esta reforma debe de venir acompañada de una amplia campaña de concientización pública que promueva una cultura de prevención que permita evitar la comisión de dicho delito. Sumado a ello al establecerse el tipo penal que se busca se facilitaría la cooperación con otras jurisdicciones contra delitos transfronterizos con aquellas jurisdicciones que también lo contemplen.

Con la adición de una nueva fracción dedicada al phishing en el Código Penal para el Distrito Federal se busca brindar claridad jurídica: empezando por la definición del concepto, establecería penas privativas de libertad graduadas según el monto defraudado y la concurrencia de agravantes como la afectación de personas vulnerables o la suplantación de dependencias gubernamentales, y permitiría imponer multas proporcionales.

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

La urgencia de esta iniciativa legislativa no puede ser exagerada, ya que el phishing continúa explotando las brechas en la infraestructura legal y de ciberseguridad de la Ciudad de México, poniendo en peligro a sus residentes.

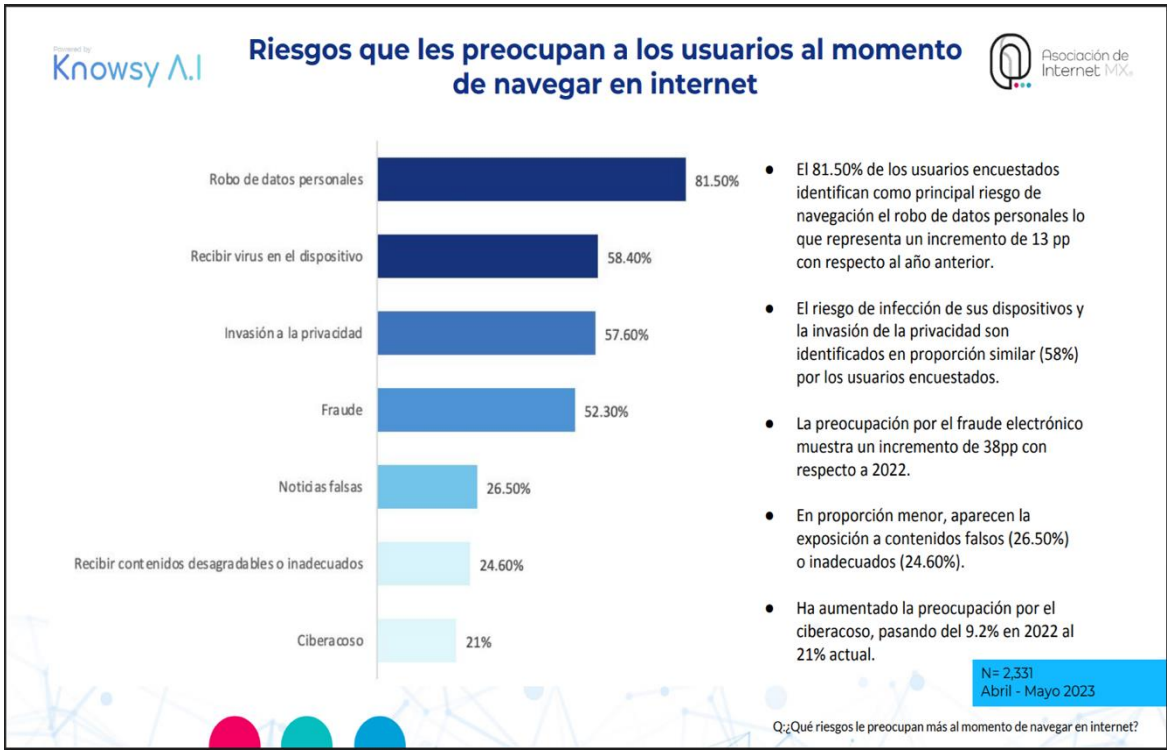
El aumento de incidentes de phishing sirve como una advertencia clara de que, sin acción decisiva, el problema soló empeorará, impulsado por la creciente digitalización de los servicios y la sofisticación de los ciberdelincuentes.

Las leyes actuales, aunque bien intencionadas, no están equipadas para manejar los matices del phishing, tal y como es evidenciado por la dependencia de estatutos amplios de fraude que no abordan explícitamente su naturaleza electrónica y engañosa.

Esta inadecuación no solo obstaculiza el enjuiciamiento, sino que también envía un mensaje de impunidad a los atacantes, que enfrentan poco riesgo de consecuencias significativas.

Se considera así, que el establecimiento de una ley específica anti-phishing señalaría el compromiso de la Ciudad de México con la ciberseguridad, disuadiendo a potenciales infractores a través de repercusiones legales claras y fomentando una cultura de vigilancia entre su población. Una ley proactiva reduciría las pérdidas generadas, protegiendo a las empresas que impulsan el PIB de la ciudad y preservando la confianza del consumidor en las transacciones digitales, lo cual cada día se vuelve vital y viable para nuestra ciudad, se vuelve así necesario el estudiar los Riesgos que les preocupan a los usuarios al momento de navegar en internet por ser este el principal medio por el que se práctica el phishing.

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745



Como se puede ver, la principal preocupación es el robo de datos personales, los cuales normalmente son obtenidos a través de prácticas fraudulentas como el phishing, lo anterior de conformidad con la gráfica realizada por la Asociación de Internet Mx.

Las implicaciones sociales del phishing exigen atención legislativa, ya que afecta desproporcionadamente a grupos vulnerables, entre los que podemos encontrar: residentes ancianos, pequeños empresarios e individuos de bajos ingresos a menudo carecen del conocimiento técnico o los recursos para reconocer intentos de phishing, convirtiéndolos en presas fáciles para los atacantes.

De igual forma se considera que la mejor forma de combatir un delito no es a través de su persecución sino por medio de la prevención, de ahí la importancia de establecer campañas de concientización, la ley empoderaría a los grupos más susceptibles de caer en este tipo de delitos, reduciendo así su vulnerabilidad y

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

mejorando la inclusión digital. Además, el costo psicológico del phishing, incluyendo el estrés y la desconfianza derivada del robo de identidad o la pérdida financiera, afecta la calidad de vida, un costo intangible pero significativo que un marco legal preventivo podría mitigar.

La iniciativa de ley que se propone debe también prever mecanismos de colaboración entre el gobierno capitalino, el Poder Judicial, la Fiscalía General de Justicia y organismos de la sociedad civil especializados en seguridad digital, con el fin de impulsar campañas de prevención educativa, divulgar protocolos de denuncia en línea y consolidar un observatorio ciudadano de ciber amenazas.

Con el establecimiento de este delito, se busca entonces castigar y por tanto inhibir la práctica de estas conductas en beneficio de la población y así evitar afectaciones económicas que pongan en riesgo la estabilidad económica de las personas, así como de los negocios de nuestra ciudad.

El establecer el phishing como delito en la legislación de la Ciudad de México no es meramente una necesidad legal, sino un imperativo estratégico para asegurar su futuro en un mundo cada vez más digital.

La combinación de una definición clara, penas proporcionales, educación pública, responsabilidad empresarial, aplicación especializada, ofrece un enfoque holístico a un problema complejo. Esta iniciativa de proyecto de decreto busca proteger la vitalidad económica de la ciudad, su tejido social y su posición global, posicionándola como un modelo para otras ciudades latinoamericanas que lidian con amenazas similares.

A medida que el phishing evoluciona, también deben hacerlo las defensas legales de la Ciudad de México, con lo cual se da el primer paso crítico hacia la resiliencia, la justicia y la seguridad para todos sus habitantes.

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

Como bien lo plantea la doctrina las fuentes del derecho se dividen en reales y formales. Las formales es en si el proceso parlamentario que da por resultado una norma y las reales las necesidades que generan una legislación con forme la evolución de la población.

Esta iniciativa se basa precisamente en la necesidad de adecuar la ley a una necesidad especifica, generada por la evolución tecnológica, en años anteriores el crecimiento de los medios digitales y la evolución del internet dan por consecuencia adecuar la legislación a esta realidad, ejemplo de esto son los ciber delitos, los cuales son acciones por medios digitales que conllevan al perjuicio o deterioro de la economía, el patrimonio o la moral de los ciudadanos.

Señor Marco Gercke, director del Instituto de Investigación sobre Ciberdelincuencia, Alemania plantea que la ciberdelincuencia como un delito que es parte integrante de la vida cotidiana de individuos y empresas y recalcó que se trata de un delito en constante mutación. Además, indicó que el ciberdelito no es nuevo, que lleva en nuestras vidas desde que el internet se inventó, pero que hasta ahora se le ha considerado como un tema crucial.

Señor José Ramón Agustina, catedrático de Derecho Penal y Criminología de la Universitat Abat Oliba CEU, España: plantea que ahora vivimos en una dicotomía, una realidad híbrida entre el espacio físico y el espacio virtual. Lo peligroso del ciberespacio es que no tiene fronteras y de que las personas no toman en serio su seguridad en el mundo del internet. Finalmente, destacó el gran reto del componente legal y la falta de coordinación entre países por motivo de que el ciberespacio no respeta fronteras.

La Interpol plantea que hoy en día, el mundo está más conectado digitalmente que nunca. Los delincuentes se están aprovechando de esta transformación en línea para atacar, a través de sus puntos débiles, las redes, infraestructuras y sistemas informáticos. Esto tiene una enorme repercusión económica y social en todo el mundo, tanto para los gobiernos, como para las empresas o los particulares.

El phishing, el ransomware y las violaciones de la seguridad de los datos son solo algunos ejemplos de las actuales ciberamenazas, eso sin contar que continuamente están surgiendo nuevos tipos de ciberdelitos. Los ciberdelincuentes son cada vez más ágiles y están mejor organizados, como demuestra la velocidad con que explotan las nuevas tecnologías, y el modo en que adaptan sus ataques y cooperan entre sí de forma novedosa.

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

Los ciberdelitos no conocen fronteras. Los delincuentes, las víctimas y las infraestructuras técnicas están dispersos por múltiples jurisdicciones, lo que resulta muy problemático a la hora de realizar una investigación o emprender acciones judiciales.

Sabemos que este es un problema que ha tenido un gran avance, es común saber de personas que has sido afectadas en su persona o patrimonio por acciones vinculadas con los ciberdelitos, podemos establecer que en menos de una década, estas acciones han aumentado gradualmente y que a últimas fechas el aumento ha sido muy notorio.

Estamos conscientes que esta materia es muy compleja y por lo mismo va evolucionando, por lo cual las leyes tienen que estarse actualizando constantemente para no quedar desfazadas, esta es una de las razones por las que presentamos la presente iniciativa, buscando adecuar nuestro marco legal a las necesidades de la población y de esta forma establecer normas eficientes a las necesidades actuales.

V. FUNDAMENTACIÓN LEGAL, DE CONSTITUCIONALIDAD Y CONVENCIONALIDAD

PRIMERO. El artículo 1 de la Constitución Política de los Estados Unidos Mexicanos establece que todas las personas gozarán de los derechos humanos reconocidos en la Constitución y en los tratados internacionales de los que el Estado mexicano sea parte, es decir, los derechos reconocidos en la constitución deben de ser aplicadas para todos los habitantes de México, independientemente de su situación migratoria.

SEGUNDO. El artículo 16 de la misma Constitución señala que nadie puede ser molestado en su persona, familia, domicilio o posesiones sino en virtud de mandamiento escrito de la autoridad competente. Sin embargo, este derecho a la privacidad y protección individual debe equilibrarse con las necesidades de seguridad y orden público, permitiendo a las autoridades actuar en la prevención y persecución de delitos

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

TERCERO. La Constitución Política de los Estados Unidos Mexicanos, en su artículo 21, establece que la seguridad pública es una función del Estado a cargo de la Federación, las entidades federativas y los Municipios, cuyos fines son salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas, así como preservar el orden y la paz públicos. Es deber del Estado garantizar condiciones que permitan el ejercicio pleno de los derechos y libertades de la ciudadanía. Preservar la seguridad pública necesariamente debe abarcar la ciberseguridad.

CUARTO. El artículo 16, de la Constitución Federal reconoce el "derecho a la protección de sus datos personales

QUINTO. El artículo 122, inciso A, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, establece que la Ciudad de México es una entidad federativa que goza de autonomía en todo lo concerniente a su régimen interior y a su organización política y administrativa y que por consiguiente el ejercicio del Poder Legislativo se deposita en la Legislatura de la Ciudad de México, la cual se integrará en los términos que establezca la Constitución Política de la entidad.

SEXTO. La Constitución Política de la Ciudad de México, establece en su artículo 14 el derecho a la seguridad ciudadana y a la prevención de la violencia y del delito, señalando que toda persona tiene derecho a la convivencia pacífica y solidaria, a la seguridad ciudadana y a vivir libre de amenazas generadas por el ejercicio de las violencias y los delitos. Las autoridades elaborarán políticas públicas de prevención y no violencia, así como de una cultura de paz, para brindar protección y seguridad a las personas frente a riesgos y amenazas.

SÉPTIMO. Que el artículo 11 del Pacto de San José de Costa Rica protege la honra, la dignidad y la vida privada, prohibiendo "injerencias arbitrarias o abusivas en su

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

vida privada, en la de su familia, en su domicilio o en su correspondencia" y garantizando "la protección de la ley contra esas injerencias o esos ataques"

OCTAVO. La Constitución Política de los Estados Unidos Mexicanos, en su artículo 21, establece que la seguridad pública es una función del Estado a cargo de la Federación, las entidades federativas y los Municipios, cuyos fines son salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas, así como preservar el orden y la paz públicos. Es deber del Estado garantizar condiciones que permitan el ejercicio pleno de los derechos y libertades de la ciudadanía.

NOVENO. Es necesario establecer medidas legales que permitan a las autoridades actuar de manera efectiva en la prevención y persecución de delitos, sin menoscabo de los derechos humanos y libertades fundamentales.

DÉCIMO. Otros países y ciudades han implementado normativas que regulan el delito de phishing como medida de seguridad, respetando siempre los derechos humanos y estableciendo excepciones por motivos culturales, religiosos, artísticas, de salud o condiciones climáticas, sirviendo como referencia para la adopción de medidas similares adaptadas al contexto legal y social de la Ciudad de México.

VI. TEXTO NORMATIVO PROPUESTO

Por todo lo antes expuesto y fundado, someto a la consideración del Pleno de este órgano legislativo la presente Iniciativa con proyecto de decreto por la que se adiciona la fracción XVII al artículo 231 del Código Penal para el Distrito Federal con el objeto de tipificar el delito de phishing, en los términos siguientes:

CÓDIGO PENAL PARA EL DISTRITO FEDERAL	
TEXTO VIGENTE	**TEXTO DE LA INICIATIVA**
ARTÍCULO 231.- Se impondrán las penas previstas en el artículo anterior, a quien:	ARTÍCULO 231.- Se impondrán las penas previstas en el artículo anterior, a quien:

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

(…) **Sin correlativo**	(…) **XVII.** A quien haciendo uso de medios de radiodifusión, telecomunicaciones, informáticos o cualquier otro medio de transmisión de para sí o para otro valiéndose de alguna manipulación informática, instrucciones de código, predicción, intercepción de datos de envío, reinyecte datos, use la red de redes montando sitios espejos o de trampa captando información crucial para el empleo no autorizado de datos, suplante identidades, modifique indirectamente mediante programas automatizados, imagen, correo o vulnerabilidad del sistema operativo cualquier archivo principal, secundario y terciario del sistema operativo que afecte la confiabilidad, y variación de la navegación en la red o use artificio semejante para obtener, con el fin de: a) Obtener un beneficio patrimonial para sí o para un tercero; o b) Causar perjuicio patrimonial, reputacional o de cualquier otra índole a otra persona, o la pone en riesgo en su integridad o patrimonio. Si el sujeto activo es empleado o dependiente del ofendido, la pena de prisión se aumentará de dos a cinco años. En el supuesto que el activo tenga licenciatura, ingeniería o cualquier otro grado académico reconocido en el rubro de la informática, telemática o sus afines, la pena se aumentará hasta en cuatro años más, además de una inhabilitación o suspensión para ejercer

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

	su profesión por un término igual al de la pena de prisión impuesta.

VII. DENOMINACIÓN DEL PROYECTO DE LEY O DECRETO

INICIATIVA CON PROYECTO DE DECRETO POR LA QUE SE ADICIONA LA FRACCIÓN XVII AL ARTÍCULO 231 DEL CÓDIGO PENAL PARA EL DISTRITO FEDERAL CON EL OBJETO DE TIPIFICAR EL DELITO DE PHISHING

DECRETO

PRIMERO. Se adiciona la fracción XVII al artículo 231 del Código Penal para el Distrito Federal para quedar de la siguiente manera:

ARTÍCULO 231.- Se impondrán las penas previstas en el artículo anterior, a quien:

(…)

XVII. A quien haciendo uso de medios de radiodifusión, telecomunicaciones, informáticos o cualquier otro medio de transmisión de para sí o para otro valiéndose de alguna manipulación informática, instrucciones de código, predicción, intercepción de datos de envío, reinyecte datos, use la red de redes montando sitios espejos o de trampa captando información crucial para el empleo no autorizado de datos, suplante identidades, modifique indirectamente mediante programas automatizados, imagen, correo o vulnerabilidad del sistema operativo cualquier archivo principal, secundario y terciario del sistema operativo que afecte la confiabilidad, y variación de la navegación en la red o use artificio semejante para obtener, con el fin de:

a) Obtener un beneficio patrimonial para sí o para un tercero; o
b) Causar perjuicio patrimonial, reputacional o de cualquier otra índole a otra persona, o la pone en riesgo en su integridad o patrimonio.

Si el sujeto activo es empleado o dependiente del ofendido, la pena de prisión se aumentará de dos a cinco años.

En el supuesto que el activo tenga licenciatura, ingeniería o cualquier otro grado académico reconocido en el rubro de la informática, telemática o sus afines, la pena

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

se aumentará hasta en cuatro años más, además de una inhabilitación o suspensión para ejercer su profesión por un término igual al de la pena de prisión impuesta.

TRANSITORIOS DE LA REFORMA

PRIMERO. Publíquese en la Gaceta Oficial de la Ciudad de México.

SEGUNDO. El presente decreto entrará en vigor al día siguiente de su publicación en la Gaceta Oficial de la Ciudad de México.

Por lo anteriormente expuesto y fundado, se propone ante el pleno de este Honorable Congreso de la Ciudad de México, la mencionada **INICIATIVA CON PROYECTO DE DECRETO POR LA QUE SE ADICIONA LA FRACCIÓN XVII AL ARTÍCULO 231 DEL CÓDIGO PENAL PARA EL DISTRITO FEDERAL CON EL OBJETO DE TIPIFICAR EL DELITO DE PHISHING.**

ATENTAMENTE

DIPUTADA OLIVIA GARZA DE LOS SANTOS

Doc ID: 7e319ade99ce08eb5832d66bf13967053f650745

Título	Iniciativa phishing
Nombre de archivo	Iniciativa_Phishing_2.docx
Id. del documento	7e319ade99ce08eb5832d66bf13967053f650745
Formato de la fecha del registro de auditoría	MM / DD / YYYY
Estado	Firmado

Historial del documento

ENVIADO	**05 / 13 / 2025** 16:36:54 UTC	Enviado para firmar a Olivia Garza (olivia.garza@congresocdmx.gob.mx) por olivia.garza@congresocdmx.gob.mx. IP: 189.146.137.21
VISTO	**05 / 13 / 2025** 16:38:16 UTC	Visto por Olivia Garza (olivia.garza@congresocdmx.gob.mx) IP: 200.68.183.186
FIRMADO	**05 / 13 / 2025** 16:38:59 UTC	Firmado por Olivia Garza (olivia.garza@congresocdmx.gob.mx) IP: 200.68.183.186
COMPLETADO	**05 / 13 / 2025** 16:38:59 UTC	Se completó el documento.