El robo de identidad en la era digital: tarjetas bancarias en la clandestinidad de la *dark web*

Identity theft in the digital age: bank cards in the underground dark web

Ismael de Jesús Montaño Borboa[1]
Leonardo David Arriaga Ávalos[2]

Fecha de recibido: 22/09/2023
Fecha de aceptado: 17/10/2023

Resumen: La Dark Web es la parte oculta de Internet donde se facilitan actividades ilegales, como la venta de tarjetas bancarias que fueron robadas. Además de que esto representa una conducta criminal, pone en peligro a las instituciones financieras y a sus usuarios. Surge una pregunta importante para esta investigación: ¿cómo acceder a la Dark Web? Se necesitan navegadores y conocimientos específicos y, preferiblemente, una conexión Virtual Privade Network (VPN) para mantener el anonimato.

Asimismo, el robo de identidad en tarjetas bancarias es un delito en el que se obtiene información personal y después es utilizada por otra persona, sin el consentimiento del propietario. Se ha vuelto más común con la proliferación o el uso masivo de Internet y puede tener graves consecuencias legales.

Por otro lado, la prevención del robo de identidad en tarjetas bancarias es crucial, pero ¿cómo hacerlo? Lo importante para evitar este tipo de criminalidad depende, en su mayoría, del usuario de cómo hace uso de sus tarjetas de crédito o de débito. Deben estar alerta, revisar con regularidad sus estados de cuenta y utilizar contraseñas difíciles de descifrar; las instituciones financieras, por su parte, también requieren implementar medidas de seguridad sólidas.

(1) **Catedrático de la Facultad de Derecho y Criminología de la Universidad Autónoma de Nuevo León y miembro del Centro de Investigaciones de Cibercriminalidad, Derecho Digital y Ciberseguridad. Correo de contacto: imontanob@uanl.edu.mx**

(2) **Catedrático de la Facultad de Derecho y Criminología de la Universidad Autónoma de Nuevo León y miembro del Centro de Investigaciones de Cibercriminalidad, Derecho Digital y Ciberseguridad. Correo de contacto: larriagavl@uanl.edu.mx**

Palabras clave: Ciberseguridad, Dark Web, protección de identidad, robo identidad, tarjeta de crédito

Abstract: *The Dark Web is the hidden part of the internet, as it facilitates illegal activities such as the sale of stolen bank cards. In addition to being a criminal behavior, it endangers financial institutions and their users. There is an important question for this research: How to access the Dark Web? To access the Dark Web, specific browsers and knowledge are needed, preferably with a VPN (Virtual Private Network) connection to maintain anonymity.*

Furthermore, identity theft in bank cards is a crime in which personal information is obtained and then used by another person without consent. It has become more common with the proliferation or widespread use of the internet and can have serious legal consequences.

On the other hand, preventing identity theft in bank cards is crucial, but how can it be done? The key to preventing this type of criminal activity largely depends on how users handle their credit or debit cards. Users should remain vigilant, regularly review their account statements, and use hard-to-decipher passwords. Financial institutions should also implement robust security measures.

Key words: *Cybersecurity, Dark Web, identity theft, identity protection, credit card*

Introducción

Actualmente, podemos acceder a gran cantidad de contenido a través de Internet, según sean los gustos de los usuarios, poco a poco sigue creciendo esta red y se agrega más información a cada segundo, pero como todo lo que tiene gran repercusión en nuestra sociedad, llega el momento en que aparecen conductas ilícitas dentro de dicho medio, tal es el caso de la Dark Web (Web Oscura), esa zona de internet donde se puede encontrar, en su mayoría, contenido ilícito.

En la era digital, la Dark Web ha surgido como un rincón clandestino de la red donde la clandestinidad y la ilegalidad se entremezclan en un mundo sin límites aparentes, aunque se deben tener conocimientos adecuados para ingresar a este lugar. A medida que el acceso a la información y las transacciones en línea se vuelven cada vez más comunes, también lo hacen las amenazas que acechan en las profundidades de esta red enigmática. Entre tales amenazas, una de las más preocupantes y devastadoras es el robo de identidad relacionado con tarjetas bancarias.

La Dark Web, conocida por su anonimato y difícil rastreo, ha permitido que los delincuentes encuentren un mercado clandestino para la compra y venta de

diversos productos y servicios. En este trabajo nos centraremos en la venta de información de tarjetas bancarias robadas.

La investigación se focaliza en el comercio ilegal de información de tarjetas bancarias robadas en la Dark Web. Comercio que no sólo afecta a las instituciones financieras, sino también tiene graves consecuencias para las víctimas cuyos datos personales caen en manos equivocadas.

A medida que nos adentramos en este oscuro rincón de la ciberdelincuencia resulta esencial que comprendamos las amenazas que enfrentamos y las medidas que podemos tomar para defendernos. La lucha contra el robo de identidad en tarjetas bancarias en la Dark Web es un desafío urgente e impostergable, y en el desarrollo de este documento exploraremos cómo podemos enfrentarlo juntos en la búsqueda de un mundo digital más seguro y protegido.

1. Descifrando la Dark Web: un viaje a las profundidades de la Web Oscura

En primer lugar, para entrar a estos temas es necesario dejar en claro lo que es la Dark Web, pues a menudo puede confundirse con otro término, que es la Deep Web (Web Profunda), la cual no es más que todo aquello que se encuentra oculto dentro de Internet, que, en sí, es la mayoría de todo lo que se encuentra en la red, es decir, la parte donde se guarda la información privada y personal de los usuarios, archivos en general o cualquier otro contenido que no tiene acceso directo. Un ejemplo serían los videos, fotografías o documentos que guardamos en la nube y sólo nosotros podemos revisarlos o alguna otra persona en específico. Para Allegritti (2018), la Deep Web "no es un lugar físico y concreto, sino un enorme océano virtual de contenidos no indizados".

En el caso de la Dark Web, es una parte específica de la Deep Web que se caracteriza por su intencionalidad de ocultamiento. Aquí es donde se encuentran sitios electónicos que operan de manera anónima y suelen utilizar redes de acceso especializadas, como TOR (The Onion Router) para mantener el anonimato de los usuarios. En este caso podemos tener como ejemplos mercados de drogas, foros de *hacking*, contratación de servicio de sicario, venta de datos robados y fotos de actividades ilegales en general.

La Dark Web ha ido evolucionando y no se tiene una fecha de cuándo apareció, pero es posible afirmar que fue a inicios del siglo XXI, pues la tecnología TOR, la cual utiliza, la desarrolló el Ejército de Estados Unidos en los años noventa para mejorar la privacidad mientras se navega en la red, y

después se comenzó a emplear en páginas *web* que estuvieran fuera de la indexación para que no resultaran de fácil acceso para todos los usuarios, pero con el tiempo comenzó a usarse para actividades ilícitas.

Algo que se debe tener en cuenta es que el acceso y la participación en actividades ilegales en la Dark Web pueden ocasionar graves consecuencias legales. La Dark Web es vigilada de cerca por las fuerzas del orden y las autoridades, y el anonimato no garantiza la impunidad.

La Dark Web cuenta con varias definiciones, y en ocasiones se confunde con otros términos; Ibáñez (2017) la describe como aquella parte de la Deep Web que se encuentra oculta y no es posible tener acceso por los motores de búsqueda tradicionales; se encuentra entre varias capas, y para llevar a cabo la navegación por dichos sitios se requiere un *software* específico, ya que de manera tradicional sería poco factible.

Kaspersky Lab (s.f.) la define como: "Los sitios que no están indexados y a los que solo se puede acceder a través de navegadores web especializados", estas páginas *web* no tienen una indexación como tales, sino que se utilizan túneles de tráfico virtual, los cuales son inaccesibles para los navegadores tradicionales.

Ecija (2017) conceptualiza a la Dark Web como aquel conjunto de páginas electrónicas que se encuentra restringido para su acceso libre, y sólo utilizando ciertos sistemas, como navegadores específicos, VPN u otro sistema, es posible ingresar a estos sitios, que en su mayoría presentan una temática ilegal o controvertida. Recalcamos que no es posible encontrar estas páginas *web* en buscadores como Google, Bing o Yahoo.

Entonces, podemos decir en términos sencillos que la Dark Web es esa parte oculta en Internet a la cual no se tiene acceso de forma fácil, y ofrece sitios *web* relacionados con actividades ilícitas en su mayoría, o que buscan no ser detectados por las autoridades; características que se inscriben en la ilegalidad.

Entre los casos de mayor impacto en la Dark Web, y que fue de gran interés internacional, está el de "Silk Road" (ruta de la seda), que estuvo en funcionamiento entre 2011 y 2013; durante ese tiempo tuvo alrededor de más de 100,000 clientes, lo cual generó ganancias multimillonarias por más de un billón de dólares, y tenía presencia en más de diez países (Finklea, 2015).

Este caso fue llevado a cabo por Ross Ulbricht, quien utilizaba el seudónimo de "Dread Pirate Roberts", y marcó un hito en la compra-venta ilegal utilizando Internet, ya que proporcionaba drogas, armas, documentación falsa, servicio de hackeo y dinero. Todo esto resultó posible gracias a la aparición del Bitcoin, pues éste se convirtió en su principal moneda de cambio (Ribas, 2018).

Gracias a su característica de anonimato y su complejo rastreo, la Dark Web ha facilitado la existencia de un mercado clandestino donde los criminales llevan a cabo transacciones de información de tarjetas bancarias robadas. Este comercio ilícito trae consigo serias repercusiones para las víctimas cuyos datos personales terminan en manos indebidas.

Para acceder a la Dark Web, recalcamos, es necesario algún navegador especial; entre éstos se encuentran programas como TOR, Freenet, I2P, ZeroNet, Brave y otros. Aunque para navegar sólo se requeriría el navegador y una conexión a Internet, no es indispensable pero sí se recomienda contar con una conexión VPN para mantener nuestra conexión segura y anónima lo más que se pueda.

Si bien la mayoría de los contenidos alojados en la Dark Web están vinculados a actividades ilícitas, no todos los usuarios que la visitan buscan necesariamente servicios o productos de este tipo. Su interés, en esos casos, se centra en la fascinación que despierta este espacio, caracterizado por su peligrosidad y misterio. Dicha atracción surgió de la curiosidad inherente de la naturaleza humana, que encuentra en la Dark Web un terreno intrigante (Franco, 2021).

2. Robo de identidad en tarjetas bancarias: un peligro acechante en la *web* oculta

El robo de identidad es un delito en el que un individuo obtiene y utiliza información personal de otro individuo sin su consentimiento. En el caso específico de tarjetas bancarias, esto implica la adquisición y uso indebido de los datos de tal cuenta perteneciente al tarjetahabiente.

En el Código Penal del Estado de Nuevo León, en su capítulo vigésimo sexto, de delitos contra la identidad personal, encontramos el artículo 444, el cual refiere sobre la suplantación de identidad: "Comete el delito de suplantación de identidad quien se atribuya por cualquier medio la identidad de otra persona, u otorgue su consentimiento para llevar la suplantación de su identidad, produciendo con ello un daño moral o patrimonial u obteniendo un lucro o un provecho indebido para sí o para otra persona. Este delito se sancionará con prisión de tres a ocho años y multa de mil a dos mil cuotas".

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef, 2016) define el robo de identidad de la

siguiente manera: "Cuando una persona obtiene, transfiere, utiliza o se apropia de manera indebida, de los datos personales de otra sin la autorización de esta última, usualmente para cometer un fraude o delito".

A pesar de que el robo de identidad no es algo nuevo, aumentó desde la aparición de Internet en nuestro día a día, y podemos encontrar distintas definiciones de lo que sería el robo de identidad, así como de aspectos importantes o básicos, como serían utilizar la información de otra persona sin su consentimiento para llevar a cabo compras, préstamos o trabajos; en resumen, hacerse pasar por alguien que no es (Monastersky y Salimbeni, 2012).

Tal como lo menciona Barba (2018), en el entorno virtual los datos relacionados con la identidad, como nombres de cuenta y contraseñas, se han convertido en objetivos cada vez más atractivos para la delincuencia, lo cual subraya la necesidad apremiante de protegerlos en el mundo digital. Además, se enfatiza que el derecho a la identidad es supranacional y fundamental, y se considera su extensión a otras áreas para fortalecer su protección, tal como se refleja en acuerdos internacionales.

El robo de identidad en tarjetas bancarias ha ido en aumento en los últimos años, si bien las entidades financieras han trabajado en evitar tal tipo de problemáticas, esto no ha impedido el tráfico de información de los usuarios, pues es vendida en la Dark Web, con lo que se evidencia la vulnerabilidad que sigue existiendo y la facilidad con la cual alguien puede adquirir esa información.

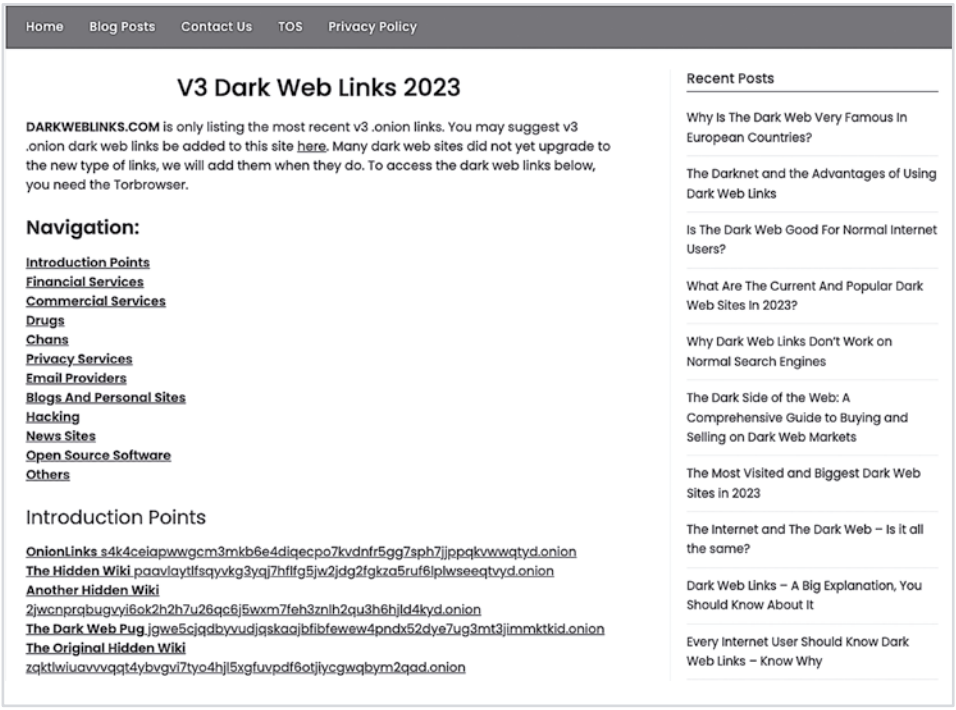
Existen diversas maneras en que los criminales se hacen de datos bancarios, entre las que es posible encontrar el uso de *pishing* o *malware* para obtener información de tarjetas de crédito, y aunque existe gran cantidad de personas afectadas por dichos medios, el de mayor incidencia es a través de la filtración de datos que pudieran tener las instituciones donde se encuentre almacenada nuestra información, pues los criminales suelen accesar a éstas y tener en sus manos la información de miles de personas a un solo clic.

3. Navegando por la Dark Web: un recorrido por lo desconocido

Resulta fácil ingresar a la Dark Web, solamente es necesario un navegador especial y el *link* de la página o al lugar que deseamos entrar dentro de ésta. Existen diversos sitios que nos indican las ligas vigentes para acceder, e incluso

páginas en la *web* tradicional, como lo es Darkweblinks.com, donde podemos visitar un sitio que nos ofrece diversos servicios, desde venta de tarjetas bancarias, drogas hasta hackeos y más.

Figura 1. Darkweblinks.com

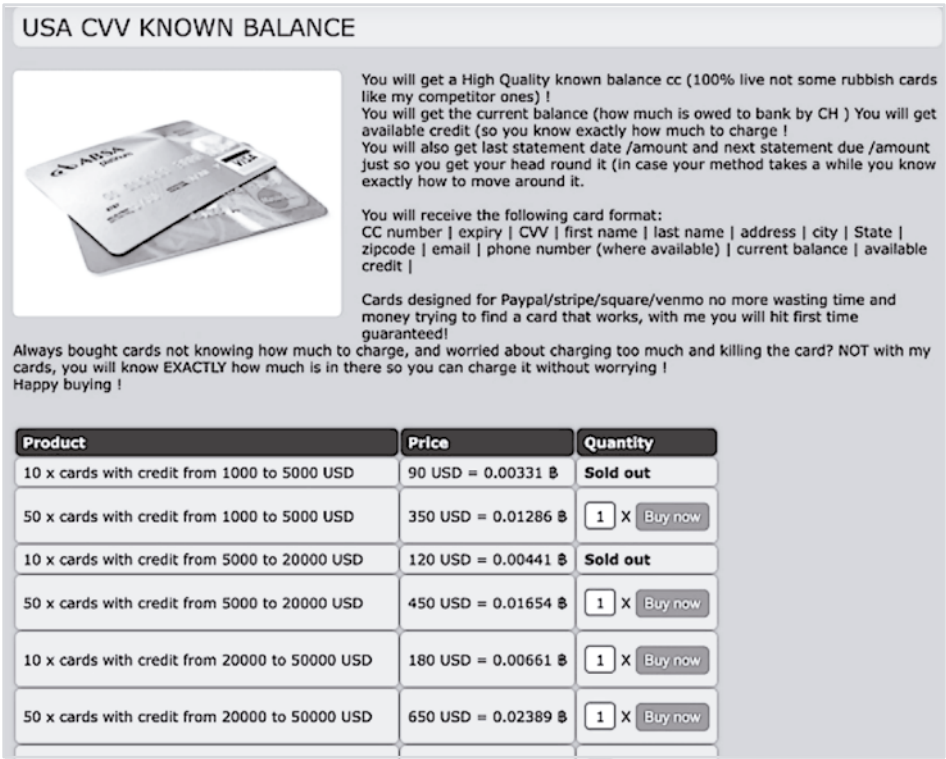


Fuente: Elaboración propia.

En la figura 1 podemos ver las diferentes direcciones onion, es decir, como suelen terminar las páginas que se encuentran en la Dark Web, aunque hay otras que brindan esta información, la cual se enfoca no sólo en los *links*, sino también en dar guías a los usuarios para que puedan navegar.

Dependiendo del servicio que busquemos, es el que seleccionaremos, y para nuestro caso nos enfocaremos en aquellos relacionados con la venta de tarjetas bancarias; resulta claro que existen más sitios como éstos, pero podríamos decir que los mostrados son los más utilizados.

Figura 2. Venta de tarjetas

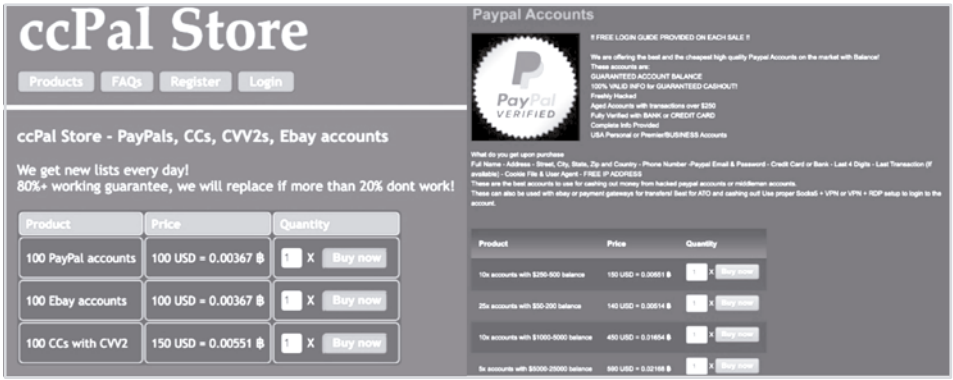


Fuente: Elaboración propia.

En la figura 2 encontramos que se venden diferentes paquetes de tarjetas, en las que indican el monto mínimo y el máximo que en promedio tienen éstas; es posible comprar desde diez tarjetas por 90 dólares, lo cual da como resultado nueve dólares por cada una que contienen un máximo de 5,000 dólares o por el doble de la cantidad se pueden obtener tarjetas por un límite de hasta 50,000 dólares. Y claro, entre mayor sea la compra su precio por unidad disminuye; además, se hace mención de la información de los nombres completos de la persona, su dirección, correo electrónico, número de teléfono y estados de cuenta.

Se debe recordar que para adquirir estos productos es necesario contar con una billetera de Bitcoin, pues tiene un rol muy importante en el anonimato de las dos partes, aunque los precios estén en dólares, el pago en Bitcoin se lleva a cabo al tipo de cambio de ese momento.

Figura 3. Venta de cuentas PayPal



Fuente: Elaboración propia.

De igual forma, está disponible la venta de cuentas PayPal, que, aunque no sea una tarjeta bancaria, contiene saldo y acceso, en su mayoría a más de una tarjeta del usuario, lo cual en los últimos años se ha vuelto más popular tanto por los beneficios como por la facilidad de obtener esta información.

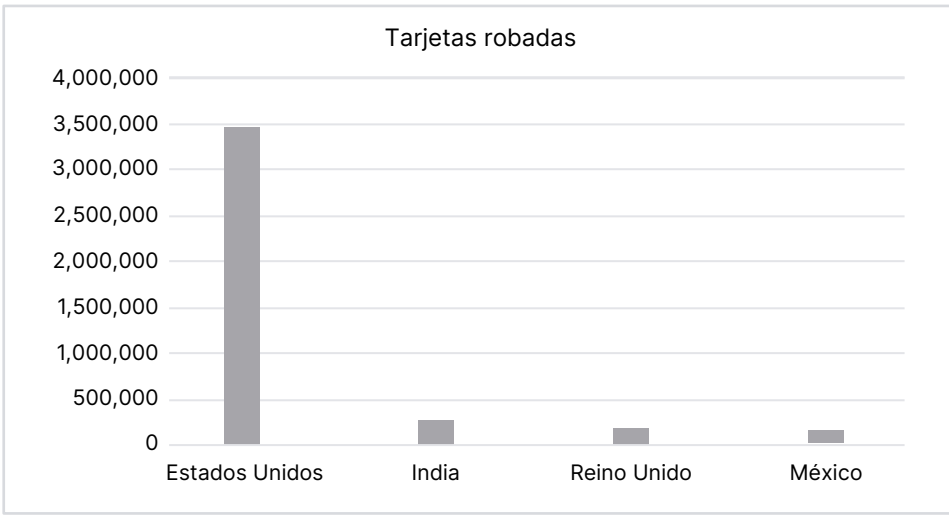
4. Cifras alarmantes de robo de tarjetas bancarias: el impacto global

La magnitud del problema de los robos de tarjetas bancarias es motivo de gran preocupación en el mundo, y uno de los países que se encuentra en la mira constante de esta creciente amenaza es Estados Unidos. Las cifras disponibles reflejan una realidad alarmante que exige nuestra atención.

Según datos proporcionados por NordVPN (2023), Estados Unidos enfrenta un problema desalentador, con aproximadamente 58% de sus tarjetas bancarias en riesgo de que sean robadas o comprometidas. Más aún, un sorprendente 7% de las transacciones realizadas en el país involucran el uso de tarjetas bancarias robadas, lo cual equivale a una cifra sustancial y preocupante.

Los expertos en seguridad financiera advierten que para 2023 los robos de tarjetas bancarias podrían ocasionar pérdidas económicas por un total de 32,960 millones de dólares en Estados Unidos, aproximadamente. Esta cifra da cuenta de la gravedad del problema y pone de manifiesto la importancia de asumir de manera efectiva esta amenaza creciente (NordVPN, 2023).

Gráfica 1. Países con las cifras más altas en tarjetas robadas



Fuente: NordVPN (2023).

Como podemos observar en la gráfica 1, existe una diferencia abismal entre las cifras de Estados Unidos (58%) y los demás países; India en segundo lugar, con alrededor de 218,000 (3.7%); en tercer lugar, Reino Unido, con 164,000 (2.8%); y en cuarto lugar se encuentra México, con 156,000 (2.6%) tarjetas robadas.

Es importante mencionar que entre las tarjetas que más son robadas en el mundo son Visa y Mastercard, ya que estas dos empresas controlan la mayoría del mercado y es más probable que se encuentren en la lista de los criminales.

Continuando con los datos ofrecidos por NordVPN, encontramos que más de la mitad de las tarjetas, específicamente 51.5%, incluían información como direcciones; mientras que un porcentaje significativo también mostraba números de teléfono (39.8%) y direcciones de correo electrónico (28.7%). En el caso de tarjetas de mayor amplitud se detectaron datos como fechas de nacimiento (2.5%) o números de seguridad social (1.8%). Sin embargo, es importante destacar que dicha información adicional aumenta de manera considerable el riesgo de fraude de identidad para las víctimas.

En términos generales, se descubrió que aproximadamente 62.8% de las tarjetas estudiadas contenían algún tipo de información adicional; esto sugiere que la mayoría de las tarjetas robadas fueron obtenidas a través de los métodos de *hacking* mencionados. Además, cerca de 37.2% de estas tarjetas se

obtuvieron mediante intentos de fuerza bruta, aunque es importante recordar que tal cifra representa un límite superior para la fuerza bruta y un límite inferior para los ataques de *hacking*.

Estos patrones variaban según el país de origen de las tarjetas. Cabe mencionar que los registros que carecían de información válida sobre el país seguían una tendencia diferente, ya que la mayoría contenía únicamente datos de la tarjeta; ascendieron a 92.4%. En general, las naciones con mayor número de tarjetas en el conjunto de datos presentaban tasas más altas de información adicional, con excepción de China, que posiblemente se apartaba de esta tendencia debido a su falta de integración con sistemas de información globales y a la naturaleza más cerrada de Internet, así como a las plataformas de compra en línea y las plataformas bancarias chinas.

Además, se observó que cerca de 90% de las tarjetas de la India incluían información adicional, lo cual exponía a las víctimas indias a un mayor riesgo de fraude de identidad. En general, se apreciaba una correlación laxa entre el valor percibido de la víctima y los intentos de *hacking*; los países europeos y las naciones económicamente más desarrolladas registraron tasas más altas de información adicional en las tarjetas robadas. Esto subraya la complejidad de los factores involucrados en los ataques referidos y sus motivaciones.

Por último, algo importante también a considerar, es que países como India y México presentan en su mayoría robos de tarjetas de débito, con 88.67% y 74.34%, respectivamente, las cuales ponen en mayor riesgo el capital de las personas, a diferencia de las tarjetas de crédito.

5. Cuestiones preventivas: proteger datos personales en el mundo digital

Las instituciones bancarias han implementado mecanismos cada vez más eficientes de seguridad para prevenir y detectar el robo de identidad en tarjetas bancarias. Sin embargo, la responsabilidad de salvaguardar cuentas y datos financieros recae no sólo en las entidades financieras, sino también en nosotros como usuarios conscientes.

Es esencial que prestemos atención a las notificaciones que nos envían nuestras instituciones financieras, ya sea a través de mensajes de texto, correos electrónicos o llamadas telefónicas. Estas comunicaciones podrían ser para alertarnos acerca de transacciones sospechosas o actividades inusuales en nuestras cuentas. Una de las mejores prácticas es mantenernos al tanto del

estado de nuestra cuenta bancaria, y al detectar cualquier irregularidad tomar medidas inmediatas para bloquearla. Esto evita que los delincuentes continúen utilizando nuestros datos de manera fraudulenta (Barba, 2018).

Banesco hace recomendaciones sobre qué hacer para evitar ser víctima del robo de nuestra información bancaria; para garantizar la seguridad en línea es esencial seguir una serie de pautas generales. En primer lugar, al acceder a servicios de banca en línea se debe ingresar directamente a través de la URL oficial del banco; se aconseja evitar enlaces de páginas web o correos electrónicos (Banesco, 2020).

Además, nunca se debe responder a correos, formularios o sitios *web* que soliciten datos personales y confidenciales, como contraseñas, números de tarjetas de crédito, códigos de seguridad o acceso. Es fundamental crear contraseñas complejas que incluyan letras mayúsculas y minúsculas, números y caracteres especiales, y asignar una contraseña diferente para cada plataforma en línea que se utilice. Estas contraseñas deben actualizarse cada treinta días, no deben registrarse por escrito y nunca compartirse.

También se sugiera evitar la instalación de aplicaciones de origen desconocido o dudoso en dispositivos personales, mantener actualizado el sistema operativo y el navegador de Internet, además considerar la instalación de un *firewall* y un antivirus en el equipo personal. Finalmente, en caso de sospecha de fraude o robo de cuentas resulta crucial notificar de inmediato al banco correspondiente para tomar las medidas necesarias de seguridad.

En el caso de México, la CONDUSEF (2016) ha proporcionado recomendaciones valiosas para evitar convertirse en víctimas del robo de identidad. Entre éstas se incluye el uso exclusivo de computadoras seguras y actualizadas, así como contraseñas fuertes que no contengan información personal fácilmente identificable. Al realizar compras en línea es fundamental tener precaución al ingresar nuestros datos financieros y verificar que los sitios *web* sean legítimos y seguros.

Asimismo, existen servicios complementarios que mejorarían nuestra seguridad financiera. Por ejemplo, podemos optar por activar las notificaciones de Buró de Crédito, las cuales nos alertarán si alguien intenta solicitar un crédito en nuestro nombre. Asimismo, algunas empresas internacionales ofrecen servicios de monitoreo de nuestra información en línea y rastreo en la Dark Web, lo cual nos permitirá recibir avisos inmediatos en caso de que nuestra información haya sido comprometida en algún momento.

Una práctica esencial es revisar con regularidad los estados de cuenta de nuestras tarjetas bancarias. Al hacerlo podemos identificar de manera temprana cualquier transacción no autorizada y tomar medidas rápidas para resolver el

problema. Por otro lado, debemos ser cautelosos con los correos electrónicos y los sitios *web* que nos soliciten información confidencial, pues podrían ser intentos de *pishing* o sitios maliciosos diseñados para robar nuestros datos.

En resumen, la prevención del robo de identidad en tarjetas bancarias requiere una colaboración activa entre los usuarios y las instituciones financieras. Al seguir estas recomendaciones y mantener una actitud vigilante podemos reducir significativamente el riesgo de resultar víctimas de este tipo de delitos financieros.

Conclusiones

Este artículo ha expuesto la creciente amenaza del robo de identidad relacionado con tarjetas bancarias en la Dark Web, un oscuro rincón de Internet donde el anonimato y la ilegalidad se entrelazan en un mundo sin límites aparentes. Dicha problemática plantea serias preocupaciones tanto para las instituciones financieras como para las víctimas, cuyos datos personales caen en manos indebidas.

La Dark Web, con su difícil rastreo y anonimato, ha facilitado un mercado clandestino en que los delincuentes pueden llevar a cabo transacciones de información de tarjetas bancarias robadas. Este comercio ilícito tiene repercusiones devastadoras en las víctimas y crea graves consecuencias personales y financieras.

Las estadísticas alarmantes acerca del robo de tarjetas bancarias revelan la magnitud del problema; Estados Unidos es uno de los países más afectados. La pérdida económica proyectada para 2023 es significativa, por lo cual se subraya la necesidad urgente de abordar esta amenaza creciente.

El artículo también ofrece pautas preventivas tanto para las instituciones financieras como para los usuarios conscientes. La colaboración activa entre ambas partes es esencial para mitigar el riesgo de caer víctimas de este tipo de delitos financieros. Al prestar atención a las notificaciones, utilizar contraseñas seguras y adoptar prácticas de seguridad en línea podemos reducir la probabilidad de que seamos víctimas de robo de identidad.

En última instancia, la lucha contra el robo de identidad en tarjetas bancarias en la Dark Web es un desafío urgente que requiere la atención de la sociedad en su conjunto. La seguridad en línea y la protección de datos personales son responsabilidades compartidas que deben asumirse con seriedad en la búsqueda de un mundo digital más seguro y protegido.

Bibliografía

Allegritti, P. (2018). *Deep Web: La parte oscura y peligrosa de internet*. España: EDICIONES B.

Álvarez, R. B. (2017). El robo de identidad en México. *Dikê: Revista de Investigación en Derecho, Criminología y Consultoría Jurídica*, (22), 245-260.

Banesco. (2020). Banesco recuerda: ¡En tiempo de contingencia elige la prevención!

Código Penal para el Estado de Nuevo León, Reformado 16 de junio del 2023, artículo 444, México.

CONDUSEF. ¿Sabes qué es el Robo de Identidad? Recuperado de https://www.gob.mx/condusef/articulos/recomendaciones-para-prevenir-el-robo-de-identidad?idiom=es

Ecija, A. (2017). Ciberespacio, Dark Web y Ciberpolicía. *Diario La Ley*, (8940), 1.

Finklea, K. M. (2015). Dark web.

Franco, J. A. R. (2021). Desmitificando a la Deep Web a través de un fugaz viaje por la Dark Web. *Revista Ingeniería, Matemáticas y Ciencias de la Información*, *8*(15), 13-32.

Ibáñez, E. M. (2017). Dark Web y Deep Web como fuentes de ciberinteligencia utilizando minería de datos. *3ª Época*, 74.

Kaspersky, Lab. ¿Qué es la Deep Web y la Dark Web? Recuperado de https://www.kaspersky.es/resource-center/threats/deep-web

Monastersky, D., y Salimbeni, M. (2012). Introducción al robo de identidad. Recuperado de https://dl. dropboxusercontent. com/u/24286331/Robo_de_identidad. pdf.

NordVPN, (2023). La punta del iceberg: 6 millones de tarjetas robadas analizadas. Recuperado de https://nordvpn.com/es/research-lab/6-million-stolen-credit-cards-analyzed/

Ribas Marcos, V. (2018). ¿Qué sabe Internet de nosotros?