Transdigital
revista científica

Sociedad de Investigación
sobre Estudios Digitales S. C.
ISSN: 2683-328X

Ensayo Científico

Phishing: métodos de estafa en comercio electrónico en México

Phishing: methods of fraud in e-commerce in Mexico

Iván Huerta
Universidad Autónoma de Baja California, México.
ivan.huerta@uabc.edu.mx

0000-0002-5408-142X

Sección: Ensayo científico
Fecha de recepción: **21/10/2021** | Fecha de aceptación: **11/03/2022**

DOI: https://doi.org/10.56162/transdigital85

Referencia del artículo en estilo APA 7ª. edición:

Huerta, I., (2021). *Phishing*: métodos de estafa en comercio electrónico en México. *Transdigital*, *3*(5), 1-17. https://doi.org/10.56162/transdigital85

Resumen

El comercio electrónico va en aumento con la industria 4.0. Los hábitos de consumo se adaptan a las facilidades de compra y métodos de pago guiados por herramientas digitales tales como terminales de banca móviles o sistemas de pago en las tiendas en línea. Dichas herramientas disminuyen el manejo de dinero en efectivo, brindan velocidad a las transacciones, eliminan la brecha de la distancia al ejecutarse de manera remota y dan al usuario una sensación de seguridad y confianza. No obstante, esto abre la puerta a diversas técnicas de estafas y fraudes digitales cuyos afectados son dos figuras principales: el usuario (de manera directa); y las instituciones bancarias (de manera indirecta), afectando la confianza de los usuarios. Una vez conocidas estas técnicas, el usuario puede recurrir a buenas prácticas de compra en línea y, a su vez, estimular la mejora de sistemas de pago digitales. Mediante un estudio exploratorio descriptivo, el siguiente trabajo aborda y experimenta algunas técnicas de fraude usando herramientas físicas y digitales replicando dichos métodos de estafa. Primeramente, se expone la terminología utilizada en estas prácticas. Posteriormente, se describe su operación o ejecución y, finalmente, se sugieren propuestas para prevenir estafas digitales en plataformas de comercio electrónico.

Palabras clave: Phishing; carding; fraudes bancarios; hackeo de bancos; seguridad en comercio electrónico.

Huerta, I., (2021). *Phishing*: análisis de los métodos de estafa en comercio electrónico en México. *Transdigital*, *3*(5), 1-17. https://doi.org/10.56162/transdigital85

Abstract

E-commerce is on the rise with Industry 4.0. Consumption habits are adapted to the purchasing facilities and payment methods guided by digital tools such as mobile banking terminals or payment systems in e-shops. Such tools reduce cash handling, accelerate transactions through remote executions thus removing the distance gap, and provide the user a feeling of security and confidence. However, this has lead to various scams and digital fraud techniques that affect two main figures: the user (directly); and banking institutions (indirectly), affecting the trust of users and once stimulating the improvement of digital payment systems. Through a descriptive exploratory study, the following work explains and experiments some fraud techniques using physical and digital tools that replicate said fraud methods. First, the vocabulary used in these practices is described, then its operation or execution is described and finally recommendations are suggested to prevent digital scams on electronic e-shops.

Keywords: Phishing; carding; bank fraud; bank hacking; e-commerce security.

Huerta, I., (2021). *Phishing*: análisis de los métodos de estafa en comercio electrónico en México. *Transdigital*, *3*(5), 1-17. https://doi.org/10.56162/transdigital85

1. Introducción

En México los mecanismos de autenticación de identidad de los usuarios durante sus transacciones electrónicas son escasos. Una de las posibles causas de esto es que, hasta hace poco, la Procuraduría Federal del Consumidor (PROFECO) no exigía reglas ni medidas estrictas para la autenticación de usuarios en los portales de comercio electrónico. Actualmente, dicho organismo público cuenta con una base de datos de sitios de ventas la cual permite a los usuarios revisar si estos cumplen con las disposiciones contenidas en la Ley Federal de Protección al Consumidor. Entre enero y noviembre de 2019 se registró un total de 1,461 quejas en el rubro de ventas por internet, con un promedio de conciliación del 74% (PROFECO, 2021).

Debido a esto, los bancos han implementado diversas medidas de seguridad como la verificación de dos pasos, registros de nombres de usuarios con sus contraseñas en bases de datos y tecnologías biométricas, como reconocimiento facial o de huella dactilar. No obstante, la seguridad del patrimonio de los usuarios y la reputación de las empresas sigue estando bajo acecho con los diversos fraudes cibernéticos que diariamente se realizan por internet.

1.1 Fraudes cibernéticos y fraudes tradicionales

Por fraudes cibernéticos se entienden las operaciones y el comercio que se llevan a cabo por internet, como la banca móvil y pagos por celular. Por otro lado, los fraudes tradicionales se entienden como las intervenciones en transacciones hechas en terminales de punto de venta, cajeros automáticos, sucursales, movimientos generados por el banco, etc.

El uso de los datos de tarjetas bancarias en los sistemas de cobro que utilizan los portales es una oportunidad que los estafadores aprovechan con frecuencia. Ejemplos de ello son la banca móvil, pagos por celular y operaciones por Internet. De acuerdo con datos publicados por la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) (2020), al cuarto trimestre de 2020, las quejas por fraudes cibernéticos disminuyeron en 0.4% en comparación al 2019 (Tabla 1).

Tabla1

Comparación de fraudes cibernéticos y tradicionales del 2016 al 2020

	2015	2016	2017	2018	2019	VAR.
Totales	2,704,355	3,917,674	4,974,334	5,364,838	6,614,867	*(2019 vs 2018)*
Cibernéticos	505,141	1,253,371	2,534,834	3,162,217	4,359,807	38%
	19%	32%	51%	59%	66%	-
Tradicionales	2,199,096	2,660,657	2,417,101	2,192,096	2,255,048	3%
	81%	68%	49%	41%	34%	-
Por definir	118	3,646	22,399	10,525	12	-

Nota. Datos de CONDUSEF (2021).

De poco más de 12 millones de pesos reclamados por fraudes cibernéticos, solo el 43% fue bonificado y 84 de cada 100 casos se resolvieron a favor del usuario. Este tipo de fraudes son, en su mayoría, utilizados para desviar recursos y afectar transacciones económicas mediante las compras por internet. Como puede observarse en la Tabla 2, las terminales de punto de venta físicas siguen siendo una de las principales formas de pago debido a la facilidad que hay en el manejo de estos dispositivos.

Tabla 2

Comparación de reclamaciones y resoluciones por fraudes cibernéticos y tradicionales al cuarto trimestre del 2020 en México

	Al cuarto trimestre 2020					
	Reclamaciones iniciadas	Monto reclamado *(mdp)*	Monto reclamado concluido (mdp)	Monto abonado (mdp)	% de abono	% de resolución favorable
Total de fraudes	**8,480,873**	**$19,819**	**$18,611**	**$7,751**	**42**	**77**
Comercio por internet	5,513,910	$6,108	$5,858	$4,586	78	89
Banca móvil	218,529	$1,854	$1,592	$72	5	13
Operaciones por internet P. Físicas	110,243	$3,016	$2,848	$197	7	7
Operaciones por internet P. Morales	23,763	$1,304	$1,225	$73	6	6
Pagos por celular	79	$4	$4	$0	1	8
Subtotal cibernético	**5,866,524**	**$12,285**	**$11,526**	**$4,928**	**43**	**84**
Terminal punto de venta	1,487,048	$3,023	$2,849	$1,072	38	56
Comercio por teléfono	804,836	$914	$837	$601	72	80
Cajeros automáticos	203,699	$821	$805	$102	13	10
Sucursales	116,119	$2,624	$2,452	$995	41	31
Movimientos generados por el banco	1,001	$67	$62	$27	44	41
Corresponsables	700	$6	$5	$4	74	20
Otros bancos	596	$46	$45	$8	18	51
Banca por teléfono	349	$33	$30	$14	47	31
Subtotal tradicional	**2,614,348**	**$7,534**	**$7,085**	**$2,823**	**40**	**59**
Por definir	1	$0.1	$0.1	$0	.0	.0

Nota. Datos de CONDUSEF (2021).

1.2 Etnografía digital y acceso a los grupos de información

La etnografía digital se refiere al estudio del comportamiento de las personas en internet, ya sea de manera individual o grupal (Martínez, et al, 2015). Es relativamente fácil el acceso a comunidades que se reúnen para aprender este tipo de técnicas de estafa. Foros de internet y grupos en aplicaciones móviles como Telegram o WhatsApp sirven como acceso a comunidades que, entre sí mismas, retroalimentan, refuerzan y contribuyen a este tipo de prácticas. En redes sociales como Facebook, los grupos pueden maquillarse cambiando los nombres de la temática. Por ejemplo, un grupo que sirve para la venta de tarjetas de bancarias en Facebook podría tener un título que denote que ese espacio se usa para compartir recetas, juguetes o incluso clubes de matemáticas. Regularmente son grupos privados en los que solamente se tiene acceso mediante una invitación. No obstante, una búsqueda avanzada en Google puede ser suficiente para encontrar diferentes sitios como estos.

1.3 Perfil del atacante

Cuenca Espinosa (2014) perfila al delincuente informático y lo define como poseedor de ciertas características que le permiten llevar a cabo el delito. Las edades pueden ser muy variadas, pero regularmente son jóvenes entre 18 y 25 años, algunos incluso son estudiantes. De manera coloquial, el delincuente informático ha sido llamado hacker, pero ese término merece una atención mayor.

La palabra hacker puede ser muy generalizada, pero de manera técnica, es una persona con conocimientos avanzados en informática que encuentra distintas maneras de realizar acciones o resolver problemas en tecnología. Las categorías que lo caracterizan son tres, dependiendo sus intenciones y fines. Red hat (2021), que es el sitio web de una empresa de desarrollo de software, principal proveedora de soluciones de código abierto y tecnologías en Linux a empresas a nivel mundial, clasifica a los hackers de la siguiente manera:

White Hat (*sombrero blanco*): Es el sinónimo de los *pentesters* (probadores de intrución). Estas personas analizan y examinan redes y sistemas para conocer sus niveles de seguridad y vulnerabilidad. Llevan a cabo o simulan ataques de un intruso para así tomar las medidas adecuadas para prevenir dicho ataque ante estos sistemas en un caso real y

mal intencionado. Estos ataques se ejecutan de manera legal y regularmente dan aviso de sus hallazgos a los dueños de los sistemas, ya sean empresas, instituciones o usuarios particulares (Rodríguez, 2021).

Black Hat (*sombrero negro*)**:** Estos también se conocen como *crackers*. A diferencia del sombrero blanco, estas personas tienen muchos conocimientos en informática y realizan ataques a sistemas ajenos con fines de lucro. Existen casos particulares donde dichos ataques también se realizan como un reto personal o por activismo (ciberactivistas). No obstante, este tipo de fines no pueden incluirse en esta categoría de manera absoluta. Lo que más identifica a un *sombrero negro* es que realiza ataques con fines de lucro, ya sea robar, manipular o restringir información personal de los usuarios (*ransomware*).

Grey Hat (*sombrero gris*)***:*** Conocen las técnicas, los métodos y las herramientas de los de *sombrero blanco*, pero no tienen ningún reparo en actuar, a veces, de manera ilícita. Lo que diferencia a los *sombrero gris* de los *sombrero negro* es que esos ataques no se ejecutan con fines de lucro. En los *sombrero gris* se encuentran ciberactivistas, personas que entran de manera ilegal a sistemas informáticos, pero cuyo fin no es el lucro o intereses personales. Los *sombrero gris* explotan la vulnerabilidad y distribuyen la información de manera general, tanto a *hackers* como a las mismas compañías. No se hacen responsables de lo que pase por difundir esa información.

Lamer (script kiddies): Es una persona que se cree *hacker*, pero que carece de los conocimientos técnicos y lógicas para perpetuar cualquier tipo de ataque. Estas personas acumulan información como libros y videos donde se muestran herramientas para ejecutar los ataques, pero no tienen la intención ni las habilidades para ejecutarlos. Regularmente recurren a herramientas automatizadas y de fácil uso que no necesitan de ningún conocimiento previo para realizar los *hackeos*.

En términos generales, un *hacker* es una persona que encuentra trucos o soluciones a un problema para alcanzar un fin utilizando distintas herramientas. Este término se usa más para el área de informática por ser aplicado a sistemas digitales. Sin embargo, es aplicable para casi cualquier aspecto de la vida. En el caso de las estafas en línea, los actores que interactúan para ejecutar esos ataques forman parte de la categoría: *black hat* o *crackers*.

Huerta, I., (2021). *Phishing*: análisis de los métodos de estafa en comercio electrónico en México. *Transdigital*, *3*(5), 1-17. https://doi.org/10.56162/transdigital85

Esta variante esta identificada por manejar datos de una cuenta o tarjeta bancaria sin conocimiento o consentimiento del dueño. Existen diferentes términos utilizados en esta comunidad, así como herramientas y métodos para hacerse de dichos datos. A continuación, se muestra un pequeño glosario de términos al respecto.

1.4 Terminología del carding y sus herramientas

Bin y “binero": En el mundo del carding existe una subcategoría que se autodenomina bineros. Un bin (Bank Identification Number) son los primeros seis números de una tarjeta bancaria. Estos números manifiestan el tipo de tarjeta, la marca (ya sea visa o master card), país, banco emisor, entre otros. Con un bin pueden generarse diferentes números de tarjeta debido a que la estructura de estas es universalmente conocida como estándar ISO/IEC 7813 (ESET, 2015). Este consiste en 16 dígitos divididos en 4 grupos de 4 dígitos. Pueden tener valores del 0 al 9, número de fecha y expiración y número de seguridad CVV, los cuales se almacenan en tres tracks o zonas ubicadas la banda magnética de la tarjeta. Existen diferentes generadores gratuitos de tarjetas alojados en la red. Los bineros generan estos números de tarjetas y los utilizan para lucrar con ellos, ya sea vendiéndolos, intercambiándolos o haciendo compras por internet.

Carding: Es el uso ilegitimo de tarjetas o datos bancarios. Ya sea de manera física o virtual, se compran bienes y servicios sin consentimiento del poseedor legítimo. Y, en el caso de ser físico, es irrelevante el tipo de tarjeta que este posea (débito, prepago o crédito).

CC: Tarjetas bancarias, cuya estructura es universal y su información es guardada en chips o bandas magnéticas en la misma tarjeta.

Dumps: información completa guardada en las bandas magnéticas de las tarjetas físicas o datos bancarios obtenidos mediante técnicas y herramientas digitales.

Drop: Persona que recibe los paquetes y compras que se efectuaron mediante carding, regularmente recibe una remuneración o una recompensa por brindar ese servicio.

Huerta, I., (2021). *Phishing*: análisis de los métodos de estafa en comercio electrónico en México. *Transdigital*, *3*(5), 1-17. https://doi.org/10.56162/transdigital85

Ingeniería social: La compañía Kaspersky (2021) menciona que la ingeniería social es un conjunto de técnicas utilizadas para engañar a los usuarios con el objetivo de que expongan sus datos confidenciales, ya sea de manera directa o infectando sus equipos con *malware*.

Phishing: Técnica de ingeniería social que consiste en enviar correos electrónicos falsos cuya apariencia parece venir de fuentes confiables como bancos o compañías de servicios. A veces tienen ligas de acceso para que sean redirigidos a los sitios web clonados (*scam*), haciendo creer al usuario que los datos que ingresa están siendo dirigidos al sitio real (Panda, 2021). Aquellos que se dedican al *phishing* constantemente buscan formas nuevas de engañar a los usuarios y cada vez se enfocan más en crear sitios lo más idénticos posible al original. Los jóvenes entre 15 y 30 años son más vulnerables a esta práctica ya que publican sus datos personales de manera más abierta y la posibilidad de que dichos datos sean utilizados de manera ilícita se incrementan (Ibarra et al, 2018).

Scam: página *web* clonada de una original cuya función es redireccionar los datos del usuario a una base de datos o espacio de almacenamiento. El atacante tiene así acceso a los datos. Esta misma página falsa puede estar alojada en distintos servidores utilizando distintos *proxys* o Uniform Resource Locator (URL), dificultando que la página original se pueda ubicar para ponerla en la lista negra de algunos *firewalls*. A este método se le conoce como *Flujo rápido*.

Skimmer: El sitio de seguridad ESET (2015) define los *skimmer* como dispositivos físicos cuya función es almacenar la información que se encuentra en la banda magnética de la tarjeta. Pueden tener formas de boquillas de cajeros automáticos, de lectores de banda del tamaño de un encendedor o, incluso, de terminales móviles.

Spam: La mayoría de los ataques de *phishing* comienzan con un correo electrónico que afirma ser emitido por una empresa de confianza. Al hacer *clic* en la dirección que aparece en el contenido, el usuario es redirigido al sitio *scam*. Existen redes de *spam* donde el atacante solo se enfoca en seleccionar a sus víctimas y enviar correos electrónicos. Dichos datos son redirigidos a otro lugar y de esta manera el verdadero autor del ataque queda limpio de toda culpa, ya que aquellos que efectuaron el ataque fueron los usuarios sin

experiencia (Bernal et al, 2019). De acuerdo con datos mostrados por Kulikova et al (2021) en el sitio web de *securitylist*, en 2020 en América Latina la proporción de *spam* en el tráfico de correo electrónico fue del 50,37% y la mayor parte del *spam* provino de Rusia (21,27%).

Dichos términos son los que se utilizan principalmente en grupos y foros donde se aprende y comparte información para poder cometer estos fraudes. El presente trabajo describe la experiencia de buscar a integrarse en estas comunidades. También de obtener y utilizar las técnicas y herramientas que dichos estafadores utilizan para lograr su cometido.

2. Desarrollo

Para experimentar los métodos de fraude con tarjetas bancarias se llevaron a cabo dos ejercicios. En el primero se tomaron tres tarjetas de débito de distintas instituciones bancarias de México con el fin de clonar sus datos mediante un dispositivo físico conocido como *skimmer* el cual puede apreciarse en la Figura 1. La función de este dispositivo es almacenar los datos de la banda magnética de la tarjeta al deslizarse en él. Los datos de las tarjetas utilizadas en el ejercicio habían expirado y no pueden ser utilizados con fines de lucro. Las tres tarjetas tenían dueño y el propietario dio autorización con plena consciencia del uso que se le daría a las tarjetas.

El segundo ejercicio consistió en llevar a cabo la generación de diez números de tarjetas a través de un *bin* mediante una aplicación abierta y de acceso libre en un sitio *web* de internet. Vale recordar que un *bin* son los primeros seis números de una tarjeta bancaria. Estos números pueden extrapolarse, es decir, pueden generarse miles de tarjetas funcionales distintas modificando unos pocos números de la tarjeta original o los números que se generaron de esta. Una vez generando los números se procede a probar en distintas tiendas en línea para ver qué número *pasa* en los sistemas de pago.

El fin de este experimento fue conocer la facilidad con la que los ciberdelincuentes pueden conseguir números de tarjetas de los usuarios para cometer fraudes.

2.1 Instrumentos utilizados

El skimmer fue adquirido por internet. Su precio osciló entre los 1,500 y los 2,000 pesos mexicanos. El artículo obtenido fue el modelo mini dx3. El skimmer es un aparato del tamaño de un encendedor de bolsillo, incluso puede llevarse como llavero. Dicho dispositivo viene con un disco que tiene su software de instalación, el cual se encarga de extraer los datos del dispositivo y mostrarlos en pantalla.

Se procedió a pasar la tarjeta de la persona través del skimmer y los datos de la banda magnética quedaron almacenados en él. Con el software se extrajo la información, la cual se muestra a continuación en la Figura 1.

Figura 1

Skimmer mini dx3 y *datos de la tarjeta bancaria extraídos*

NO	Track 1	Track 2
	%B5256781777542395^PERFIL EJECUTIVO/PRG ^2008201000000000000000627000000?	;5256781777542395=2008201000006277
2	%B4910896068729963^ ^181222100000000000000003670000000?	;4910896068729963=18122210068036700000
3	%B5579100133744480^NOMINA PREFERENTE /^200720100263000000 ?	;5579100133744480=20072012637

Como se mencionó anteriormente, el software presentó información de la tarjeta, como su tipo, número, fecha de expiración y todo esto se guardó en secciones o *tracks*. El número CVV no lo guarda el *skimmer* ya que no es un dato que se encuentre en la banda magnética de la tarjeta. Sin embargo, no es difícil para el atacante memorizarlo, ya que solo se conforma de tres números.

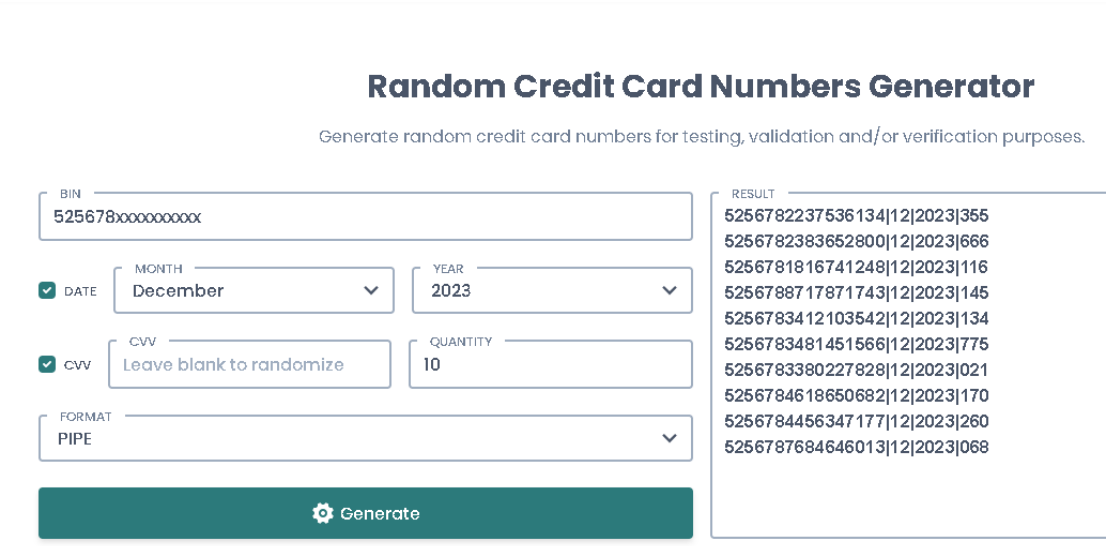
2.2 Obtención del bin y su utilización

El bin consta de los primeros seis números de la tarjeta, así que una vez identificados en cada una de las tres tarjetas se precedió a buscar en internet un sitio web que generara números distintos de las tarjetas raíz de la tarjeta original. Namso es una de las herramientas más utilizadas para este tipo de actividades y puede ser encontrada rápidamente con Google; existen diversos sitios y la gran mayoría son gratuitos.

Los números de tarjeta se generaron con extrema facilidad. Tan solo poniendo los seis dígitos de la tarjeta original se generaron otras 10 distintas. Namso cuenta con campos para introducir los datos de la tarjeta que se desea extrapolar, como se puede observar en la Figura 2.

Figura 2

Números de tarjeta generados por medio de un bin



Las fechas de expiración de las tarjetas fueron puestas al azar ya que la herramienta no genera tarjetas con fechas ya expiradas. Las tarjetas utilizadas expiraron en el año 2020 o 20018. Como puede observarse, puede variar la cantidad de números a generar. En esta

ocasión se generaron diez y el *bin* que se tomó fue de la tarjeta número 1 obtenida por el *skimmer*.

Así es como funciona la extrapolación y los de todas las tarjetas son generados por un algoritmo llamado algoritmo de Luhn, el cual consiste en que una tarjeta es válida si sus números van del 0 al 9. Al invertirse y sumarlos deben dar un múltiplo de diez. Los *bins* que son utilizados dejan de funcionar y, una vez de que el atacante saca el máximo provecho de la tarjeta generada por el *bin*, lo que hace es publicar la información en foros y grupos para que se le dé un uso masivo y se dificulte la localización y el rastreo del uso que se le dio

3. Conclusiones

Como conclusión sobre la aplicación de estos métodos se puede decir que el uso de herramientas para cometer fraudes bancarios digitales es fácil. Conseguir las herramientas, tanto físicas como digitales, es un proceso relativamente sencillo. Prácticamente cualquier persona con pocos conocimientos de informática puede ejecutar estas técnicas de estafa. La manera en la que los usuarios aprenden a desarrollarlas es de manera autodidacta a través de foros o distintos sitios *web*.

A pesar de que los bancos intentan implementar mecanismos de seguridad avanzados, la verdadera vulnerabilidad es la falta de conocimiento del usuario y el fácil acceso a las herramientas de estafa. Se han desarrollado mecanismos para tratar de evitar el fraude cuando está a punto de ser ejecutado, pero el acceso a las herramientas sigue estando disponible para el público en general. Para un usuario que desconoce estas herramientas o métodos es imposible llevar a cabo métodos de prevención.

Paulatinamente, las herramientas de seguridad van mejorando, como la identificación biométrica con el uso de lectores de huella dactilar o de rostro; el *3D secure*, que consiste en enviar un código de acceso único al usuario una vez puestos sus datos de la tarjeta al hacer una compra; e incluso, gracias al *big data* se han implementado mecanismos predictivos que mediante la ejecución de patrones los bancos pueden determinar si se tratan de transacciones reales o estafas.

En esta intervención no pudo observarse un mecanismo de control o regulación para conseguir estas herramientas. La venta de *skimmers* se encuentra abierta al público en general, incluso en tiendas conocidas a nivel mundial ya que estas se ofrecen como herramientas para hacer pruebas. Sin embargo, el uso que puede darse a estas herramientas es totalmente distinto. Los sitios web para la generación de *bins* también son de acceso abierto y gratuitos, lo cual los vuelve fácilmente accesibles y propagables entre quienes llevan a cabo este tipo de actos.

Se sugieren estas recomendaciones para evitar fraudes:

1.- Revisar que los sitios *web* implementen protocolos seguros. Estos comienzan con *https* (Hypertext Transfer Protocol Secure) y trabajando de la mano con *SSL* (Secure Sockets Layer). Estos dos protocolos de internet sirven para la transferencia de datos encriptados en la red y garantiza que la página que se visita es la real y no una falsa (*scam*) que puede obtener los datos del usuario.

2.- Preferentemente, hacer compras con mecanismos de seguridad novedosos como el *3D secure*. El usuario recibe un código de autenticación único a través de un mensaje de texto, a esto se le conoce como *push.* Una vez recibido el código, se pone en el sitio *web* y la transacción se lleva a cabo.

3.- No proporcionar jamás datos personales o de la tarjeta por teléfono. Si esto sucede, el usuario debe ir al banco lo más pronto posible.

4.- En caso de ir a un cajero automático, verificar físicamente y de manera rápida las condiciones del cajero. Por ejemplo, que el teclado no esté despegado, dando pequeños golpes a la boquilla donde se inserte la tarjeta para asegurarse de que esté fija y parpadee, que no haya algo que luzca como lentes o cámaras en la lámina que cubre el tablero de números, etc.

5.- Cuando se pague algún producto o servicio a través de terminal, el usuario debe tener a la vista su tarjeta en todo momento, debe observar a dónde lleva y como usan la tarjeta. Por

ejemplo, la mayoría de las tarjetas tienen *chip*, si la persona hace el cobro pasando la banda magnética en la terminal es una señal de alerta.

6.- Preferentemente, no abrir correos electrónicos que digan que son del banco ni acceso a ligas que vengan en ellos ya que muchos redireccionan a páginas falsas. O bien, pueden ejecutar pequeños programas que hagan una redirección del sitio *web* original a uno falso. Preferentemente, se debe utilizar la aplicación del banco en el teléfono ya que muchos de ellos cuentan con autenticación de huella.

Referencias

Bernal, M., Lizárraga, J., Pinedo J., Flores A., Flores D. (2019). Protocolo para la prevención de ataques de *phishing*. *Revista Digital de Tecnologías Informáticas y Sistemas*. *3*(3). https://www.redtis.org/index.php/Redtis/article/view/34

CONDUSEF (2021). *Página web oficial* de CONDUSEF. https://www.condusef.gob.mx

Cuenca Espinosa, H. A. (2014). *El delito informático: su evolución, punibilidad y proceso penal en el Ecuador*. [Tesis de título publicada]. Pontificia universidad católica del Ecuador. http://repositorio.puce.edu.ec/handle/22000/6966

ESET (2 de abril de 2015). *¿Qué es un skimmer y cómo proteger tu tarjeta de crédito?* https://www.welivesecurity.com/la-es/2015/04/06/que-es-skimmer-como-proteger-tarjeta/

Hernández, M. (16 de mayo 2019). *En 2018 hubo más de 4.3 millones de quejas por fraudes cibernéticos en México. https://www.forbes.com.mx/fraudes-ciberneticos-superan-las-4-3-millones-de-quejas-en-mexico/*

Ibarra, R., Olivarría, M., Zaragoza, J., Qui, S., Otáñez O. (2018). Métodos para evitar el phishing, mediante el uso de las tecnologías. *Revista Digital de Tecnologías Informáticas y Sistemas*. 2(2). https://www.redtis.org/index.php/Redtis/article/view/16

Kaspersky (2021). *Ingeniería social: definición. https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering*

Kulikova, T., Shcherbakova, T., Sidorina, T. (15 de febrero 2021). *El spam y el phishing en 2020*. https://securelist.lat/spam-and-phishing-in-2020/92784/

Martínez, L., Ceceñas, P., & Leyva, M. (Eds.). (2015). *Tecnologías de la Información y Comunicación en el Ámbito Educativo: Etnografía*. Red Durango de Investigadores Educativos, A. C.

Panda (2021). *¿Qué es el Phishing?* https://www.pandasecurity.com/es/security-info/phishing/

PROFECO (21 de febrero de 2021). *Revista Profeco comportamiento de tiendas virtuales* https://www.gob.mx/profeco/prensa/revisa-profeco-comportamiento-de-tiendas-virtuales?state=published

Red hat (2021). *Atacantes y Vulnerabiliades.* https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-attackers_and_vulnerabilities

Rodríguez Llerena, A. E. (2021). Herramientas fundamentales para el hacking ético. *Revista Cubana de Informática Médica*, *12*(1), 116-131. https://www.medigraphic.com/cgi-bin/new/resumen.cgi?IDARTICULO=94154

Huerta, I., (2021). *Phishing*: análisis de los métodos de estafa en comercio electrónico en México. *Transdigital*, *3*(5), 1-17. https://doi.org/10.56162/transdigital85