ANÁLISIS DEL CRECIMIENTO DE PHISHING EN LOS ÚLTIMOS AÑOS

William Omán Hernández Ortega[1] , César Sajhid Osuna Jiménez [1], Belem Nuñez Peraza[1], Vazquez Delgado Miguel Eduardo[1]

[1] Universidad Autónoma de Sinaloa, Facultad de Informática Mazatlán (México)

Resumen

La presente investigación muestra información recopilada con relación a él “Phishing”, donde se evidencia cómo es que ataca a la sociedad. Expone un análisis del crecimiento que ha tenido en los últimos años recurriendo a documentación y gráficos, además de un formulario donde se exhiben las causas del cúmulo de casos con respecto a este tipo de estafa.

Palabras clave: Phishing, investigación, crecimiento, estafa, delito.

Abstract

The present investigation shows information compiled in relation to "Phishing", where it is shown how it attacks society. It exposes an analysis of the growth it has had in recent years using documentation and graphics, in addition to a form where the causes of the accumulation of cases regarding this type of scam are exhibited.

Keywords: Phishing, research, growth, scam, crime.

1 INTRODUCCIÓN

El Internet es una tecnología que ha traído un cambio revolucionario en la vida moderna y algunas actividades socioeconómicas, como la comunicación, compras en línea, el comercio, las redes, el entretenimiento, entre otras.

En los últimos años, el crecimiento de la conectividad a Internet aumentó las actividades de fraude cibernético, los delincuentes han visto esto como una oportunidad de transferir esos delitos que hacían en un entorno físico a un entorno virtual. Hay muchos tipos de delitos que se hacen de forma online, uno de los que más crecimiento ha tenido durante los últimos años es el phishing [1].

El phishing es un delito cibernético que consiste en atraer al usuario para que proporcione información sensible y confidencial al atacante. Por lo regular los datos que quieren saber acerca del usuario son detalles de la tarjeta de crédito, nombre de usuario y contraseñas, datos bancarios, etc. Estos ataques de phishing ocurren a través de correos electrónicos maliciosos, mensajes de texto y llamadas telefónicas. Luego de obtener la información, el atacante podría cometer delitos como pérdidas financieras y robos de identidad, etc [2].

El phishing es una actividad que hoy en día suele ser muy común, pero tiene registros que van desde años atrás. La primera vez que se escuchó hablar de este tipo de delito fue en el año 1987 en una conferencia dónde Jerry Félix y Chris Hauck hicieron referencia al término a causa de un documento titulado “Sistema de Seguridad: La perspectiva de un Hacker" [3].

Desde entonces este tipo de fraude cibernético ha ido en aumento de forma muy alarmante y ha evolucionado con los años hasta convertirse en lo que se conoce hoy en día como phishing. Del año 2000 hasta 2003, los estafadores utilizaban URL, registro de pantalla, mensajería instantánea (IM) y chat de retransmisión de Internet (IRC) para atacar a las víctimas. Unos años más tarde, en 2006, los estafadores atacan primero a las víctimas a través de Voz sobre Protocolo de Internet (VoIP) y en 2007, se perdieron más de 3 000 millones de USD por estafas de phishing[4].

Según (McCabe, 2016) entre el período de octubre de 2013 a febrero de 2016, el FBI recibió informes de estafas comerciales por correo electrónico por un monto total de pérdidas de $2.3 mil millones. Esta pérdida es sólo a través de estafas de correo electrónico comercial y no incluye las pérdidas por medio de otras estafas de phishing [5]. Otro ataque de phishing se presentó en 2011, donde hubo una serie de ataques en contra de empresas de seguridad con alto prestigio, entre ellas RSA. Esto demostró que los peligros de los ataques de Phishing, o vulnerabilidades de seguridad debido al factor humano, no se limitan a la ingenuidad de los usuarios finales, ya que los técnicos también pueden ser víctimas [6].

En cuanto a la investigación se espera realizar un análisis acerca del crecimiento del phishing durante los últimos años y localizar las causas del incremento de víctimas, así como encontrar las tasas de desinformación de la sociedad.

2 METODOLOGÍA

La presente investigación fue realizada por medio de un análisis referente al phishing, su significado y el crecimiento que ha obtenido a lo largo de los años, los datos obtenidos fueron gracias a una revisión bibliográfica en documentos de tipo: journals, revistas y artículos científicos con relación al phishing, todo esto con la tarea de encontrar conceptos y estadísticas las cuales ayudaran para analizar su crecimiento.

La encuesta que se hizo a través de formularios de google, fue dirigida al público en general, en donde se abordan preguntas sobre el conocimiento y experiencias de los entrevistados. Las preguntas que se realizaron son las siguientes:

- ¿Es consciente de que existen delitos especializados en el robo de información con fines de lucro?
- Cuando alguna persona o empresa le manda algún correo ¿Suele comprobar de quien proviene el correo?
- ¿Conoce usted alguna víctima o usted ha sido víctima de robo de información por medio de un enlace (Phishing)?
- Del uno al diez ¿Qué tan informado está acerca del Phishing?
- A menudo se suelen recibir correos en nombre de bancos, donde se suele pedir los datos del usuario mediante una liga, para una supuesta validación, ¿ha recibido algún correo de este tipo?
- ¿Cuándo crees que has recibido más estos tipos mensajes o correos por Phishing: Antes del COVID o después del COVID?

El objetivo de realizar esta encuesta es medir el nivel de desinformación sobre el phishing. Así como la opinión de la gente que no tiene tanto conocimiento acerca de los delitos cibernéticos, para así poder entender por qué el phishing ha tenido un crecimiento acelerado durante los últimos años.

3 RESULTADOS

Con base a la investigación realizada de tipo documental, se destaca que el phishing ha tenido un aumento significativo conforme el avance de los años y cada vez es más común que usuarios sean afectados por phishing.

Según los informes anuales de APWG (Anti-Phishing Working Group) se muestra un crecimiento de los ataques de phishing de 2015 a 2020 por trimestres. También se habla de que en el tercer trimestre de 2019, la cantidad de ataques de phishing aumentó a 266 387, que es el nivel más alto en tres años desde finales de 2016. Esto fue un 46% más que los 182 465 del segundo trimestre, y casi el doble de los 138 328 vistos en el cuarto trimestre de 2018. La cantidad de correos electrónicos de phishing únicos informados a APWG en el mismo trimestre fue de 118 260. Además, se encontró que el número de marcas a las que se dirigieron las campañas de phishing fue de 1.283 (figura 1) [7].

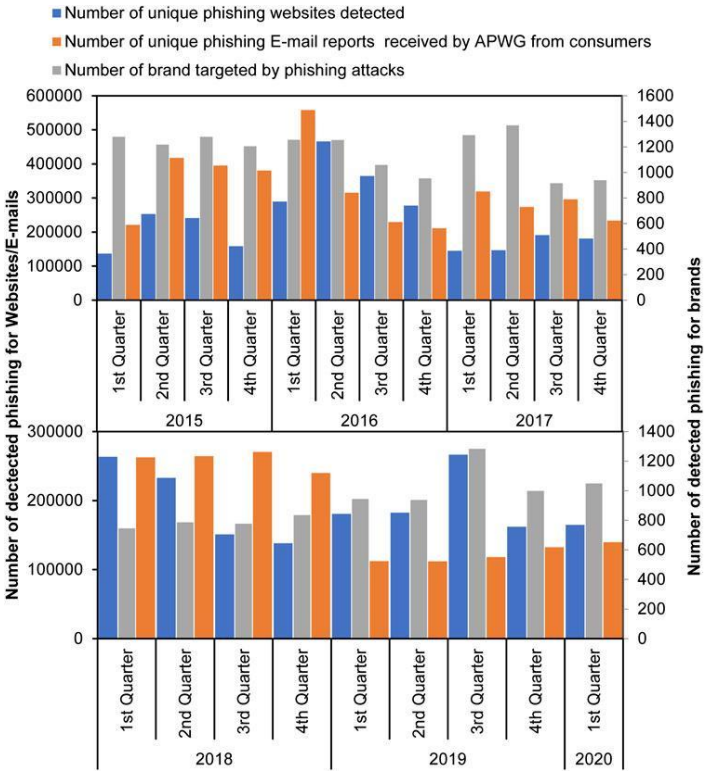

Figura 1. Se muestra el crecimiento de los ataques de phishing entre 2015 y 2020 por trimestres según los datos recopilados de los informes anuales del APWG [7].

Para hablar del aumento de actividades de phishing, también se debe de conocer las causas del por qué ocurren este tipo actividades ilegales. No se puede afirmar con certeza la principal razón por la cual ha habido este crecimiento. Hay diversos factores que propiciaron este crecimiento de la actividad de phishing, algunos de estos factores pueden ser: la desinformación sobre ésta actividad, la falta de seguridad de algunas personas o empresas con respecto a estos tipos de delitos, entre otras cosas.

Es por eso, que se decidió hacer una encuesta a 51 personas de forma aleatoria donde se de por medio de formularios de google para poder identificar qué tanto se está informado acerca del phishing.

Las siguientes gráficas nos muestran el porcentaje de las respuestas que dieron los usuarios con respecto a las preguntas realizadas:

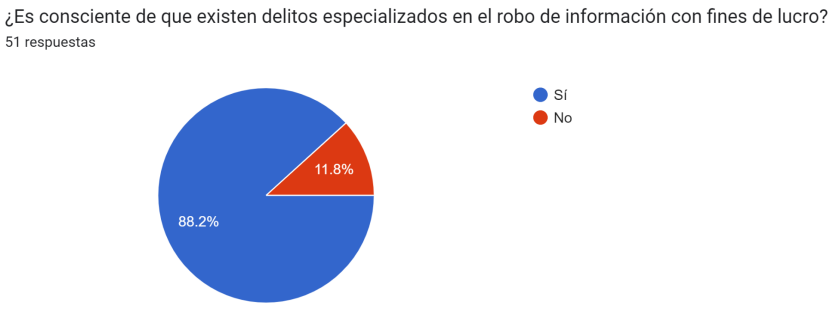

Figura 2. En esta gráfica se muestra la primera pregunta de la encuesta la cual nos permite observar que el 88.2% de las personas encuestadas tienen conocimiento acerca de delitos informáticos.

Figura 3. En la siguiente gráfica se puede comprobar la cantidad de personas que mediante el recibimiento de correos, se comprueba el remitente, dónde el destinatario puede observar si se analiza de dónde proviene o no, la cantidad de personas en total de 50, fue el 44% dando en total que mayormente el uso de destinatarios es acostumbrado a leer sus correos provenientes.

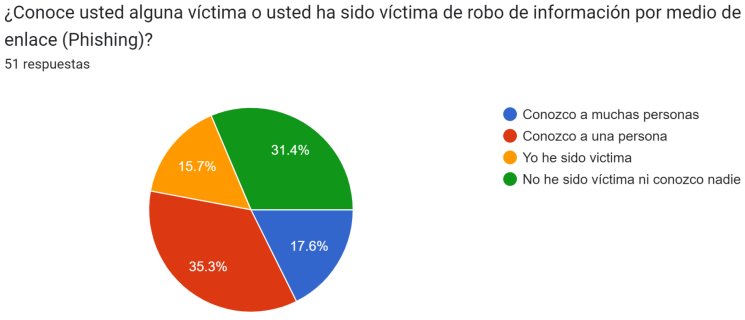

Figura 4. La cantidad de 35.3% que fue encuestada en la representación de la siguiente gráfica se da a visualizar la cantidad de víctimas que han ido cayendo a lo largo del tiempo entre una gran cantidad y una sola persona.

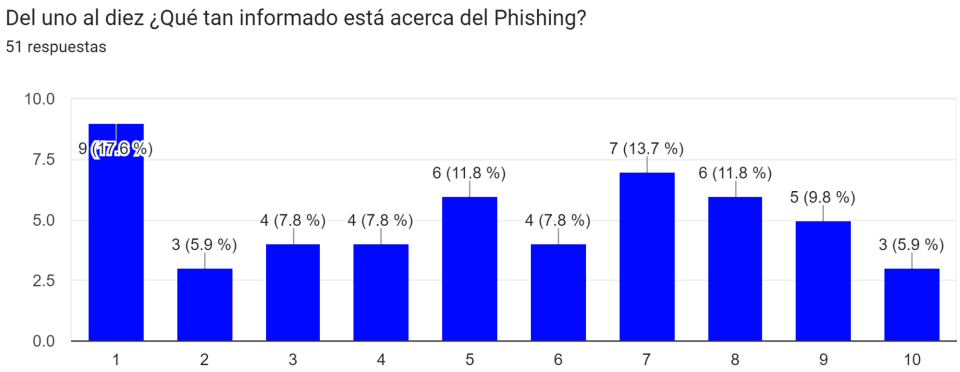

Figura 5. La gráfica representa que tan informados están los encuestados acerca del phishing, los resultados nos indica que la mayoría de personas no es consciente del phishing.

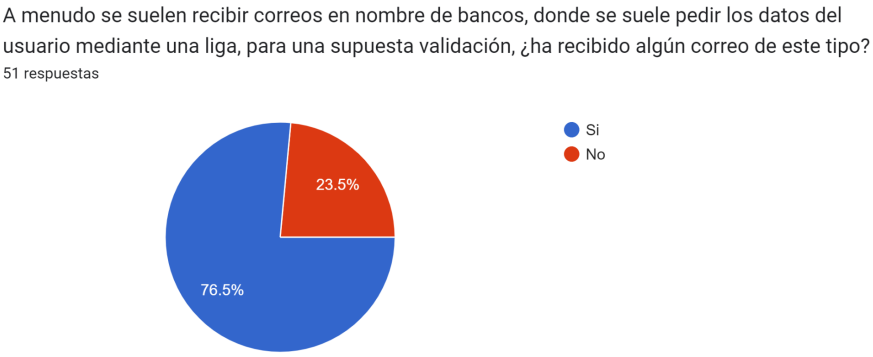

Figura 6. Refiriéndose al recibimiento de correos donde se recibe una liga de datos de bancos para una estafa, el más de 76.5%

Figura 7. En la siguiente gráfica nos muestra que el 72.5% de las personas ha notado que hubo un crecimiento de intentos de estafa con respecto al phishing posterior al COVID-19

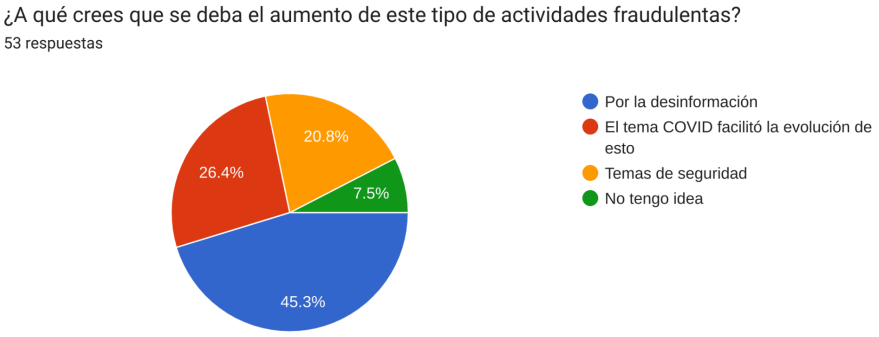

Figura 8. En la siguiente gráfica nos muestra que un poco menos de la mitad de personas encuestadas cree que el aumento de este tipo de actividades delictivas se debe a la desinformación.

4 CONCLUSIONES

El phishing ha tenido un aumento en los números de casos desde 2015 hasta ahora, entre 2015 y 2017 se tuvo un índice de e-mails reportados muy alto y los años posteriores se detectaron más sitios web de phishing que e-mails reportados. En conclusión con la *figura 5*, el phishing no ha tenido un crecimiento tan exponencial, esto gracias a que cada vez más personas conocen sobre el phishing y los delitos informáticos, pero también se debe decir que se han mantenido a un nivel alto estos años.

Las gráficas que se realizaron a partir de la encuesta nos sirvieron para comprobar el nivel de conocimiento que tienen las personas acerca del Phishing. Se puede decir que con base a los resultados obtenidos, las personas saben mínimamente que existen las estafas informáticas y tienen una especie de desconfianza ante los tipo de correos de spam, esta desconfianza se puede deber, gracias a que conocen a terceras personas, las cuales hayan comentado acerca de esta problemática, o bien ellos mismos hayan sido víctimas. A pesar de que la sociedad ya conoce sobre esta estafa informática, no asocia estos problemas con la palabra “Phishing” y tampoco está del todo informada respecto al tema. Se puede decir que la desinformación es una de las principales causas del aumento de víctimas en estos delitos, sin embargo, la gente ya tiene un poco de conocimiento acerca de esta estafa y puede ser que gracias a esto, en los próximos años el número de víctimas de phishing pueda disminuir.

REFERENCIAS

[1] A. A. Ubing, S. Kamilia, A. Abdullah, N. Jhanjhi y M. Supramaniam, "Phishing Website Detection: An Improved Accuracy through Feature Selection and Ensemble Learning", International Journal of Advanced Computer Science and Applications, vol. 10, n.º 1, 2019. Accedido el 14 de noviembre de 2022. [En línea]. Disponible: https://doi.org/10.14569/ijacsa.2019.0100133

[2] A. Shankar, R. Shetty y N. K. Badari, "A Review on Phishing Attacks", International Journal of Applied Engineering Research, vol. 14, n.º 9, p. 5, 2019.

[3] "Phishing History - The Earliest Phishing Scams". Bright Hub.https://www.brighthub.com/internet/security-privacy/articles/82116/ (accedido el 14 de noviembre de 2022).

[4] M. M. Ali y N. F. Mohd Zaharon, "Phishing—A Cyber Fraud: The Types, Implications and Governance", International Journal of Educational Reform, p. 105678792210829, marzo de 2022. Accedido el 16 de noviembre de 2022. [En línea]. Disponible: https://doi.org/10.1177/10567879221082966

[5] K. Leng Chiew, K. Sheng Chek Yong y C. Lin Tan, "A survey of phishing attacks: Their types, vectors and technical approaches", Expert Systems with Applications, vol. 106, p. 20, 2018.

[6] E. Benavides, W. Fuertes y S. Sanchez, "Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura", Ciencia y Tecnología, vol. 13, n.º 1, pp. 97–104, junio de 2020. Accedido el 15 de noviembre de 2022. [En línea]. Disponible: https://doi.org/10.18779/cyt.v13i1.357

[7] Z. Alkhalil, C. Hewage, L. Nawaf y I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy", Frontiers in Computer Science, vol. 3, marzo de 2021. Accedido el 9 de noviembre de 2022.