



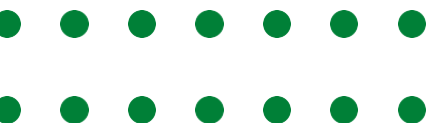
Universidad Veracruzana

USBI Coatzacoalcos



Cartilla de alfabetización informacional

Phishing



Contenido

- 1** Introducción
- 2** Phishing
- 2** Tipos de Phishing
- 5** Recomendaciones
- 7** Bibliografía

INTRODUCCIÓN:

El uso de internet ha aumentado considerablemente en los últimos años, con prácticas tan diversas que van desde el uso de las redes sociales, hasta una compra a través de la web. De acuerdo con el Instituto Nacional de Estadística y Geografía (INEGI, 2023), en México, hay 88.5 millones de usuarios de internet (Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en México 2020).

El desarrollo de las plataformas de la internet ha solidificado a la banca electrónica, la cual facilita el realizar operaciones bancarias como transferencias, consulta de estados de cuenta e inclusive el pago de servicios básicos, por ejemplo; agua potable, energía eléctrica, gas, entre otros.

Para contextualizar un poco más, de acuerdo con el Banco de México, el número de transferencias interbancarias realizadas en un día, a través de internet, a principios del 2002 fue de alrededor de 95 mil, en comparación con las más de 46 millones efectuadas a mediados del 2022. (Baxico, 2023)

El aumento en el uso de operaciones bancarias a través de internet hace que las personas usuarias se familiaricen con las páginas web de las instituciones financieras, correos electrónicos y publicidad que reciben de dichas instituciones. Lo anterior, ha sido aprovechado por delincuentes informáticos para realizar ataques a través de los que obtienen información bancaria y personal de la comunidad usuaria con la finalidad de realizar alguna actividad ilícita, unas de estas es el llamado **Phishing**.

Conocer las estrategias que utilizan las personas delincuentes que practican el phishing podría evitar el robo de información o de algún acto fraudulento contra persona alguna.

PHISHING

Esta técnica ilegal es utilizada con la finalidad de robar la información financiera de una persona, es común que para dicho fin utilicen sitios parecidos a los oficiales. La persona estafadora, conocida habitualmente con el nombre de *phisher*, hace uso de técnicas que le faciliten la obtención de los datos de la persona que es víctima del delito, esto con la finalidad de realizar alguna actividad fraudulenta, como el robo de cuentas bancarias o de datos personales (fecha de nacimiento, domicilio, etc.)



TIPOS DE PHISHING

Phishing por correo electrónico

Consiste en el envío de correos electrónicos con supuesta información de instituciones bancarias, incitando a la persona usuaria a realizar algún movimiento bancario, buscando obtener su información confidencial. Para lo anterior, las personas estafadoras elaboran mensajes que inducen a presionar un enlace que se incluye en el texto, enviando a una página



web similar a la oficial, donde la persona ingresará su información personal; estos datos son captados por un programa denominado *keylogger* y posteriormente enviados a la persona delincuente.

Phishing de software malintencionado:

Este tipo de ataques consiste en programas maliciosos que se envían por correos electrónicos con el supuesto de ser un archivo de confianza, por ejemplo, estados de cuentas bancarias, currículum vitae, invitación a eventos, facturas fiscales, etc.

La persona usuaria al presionar sobre el documento le da acceso al programa para obtener su información personal e inclusive brindarle permiso para que acceda a la red de internet de su hogar o empresa.



Phishing por SMS (smishing)

Es un tipo de actividad ilícita que emplea el envío de mensajes de textos dirigidos a personas usuarias de telefonías móviles; el objetivo es que las personas brinden su información personal a supuestos representantes de una entidad bancaria o financiera, intentando persuadirles de que envíen su información a través del mismo mensaje, solicitándoles introducir su número de cuenta bancaria, tarjeta de crédito, claves o contraseñas, etc.

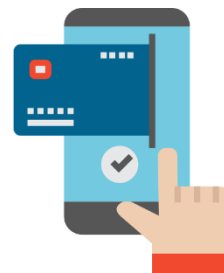


Phishing por voz (vishing)

En las actividades de Phishing por voz, los atacantes, desde centros de llamadas telefónicas fraudulentas, intentan persuadir a una persona a que brinde información personal, e inclusive, lograr que instale programas en forma de aplicación (apps), con los cuales logran acceder de forma remota a los dispositivos



móviles de la persona, ingresando a sus aplicaciones de banco, cuentas personales o de forma permanente a sus teléfonos móviles.



Phishing de objetivo definido:



Los ataques de Phishing normalmente tienen un objetivo generalizado, es decir, miembros de una comunidad financiera e incluso regiones geográficas; en cambio, el Phishing de objetivo definido tiene la finalidad de recabar información de personas específicas, indagando sus estilos de vida, empleos o redes sociales. El objetivo del phisher, en estos casos, es conocer las contraseñas de las cuentas de la posible víctima, para lo cual envían correos electrónicos, mensajes de texto e inclusive campañas de marketing personalizado que inducen a presionar algún enlace o documento adjunto con el cual se roba y envía la información a la persona estafadora, misma que la podría utilizar para situaciones grave como el secuestro y la extorsión.

Los phisher harán uso de frases comunes como:

- Estimado usuario su contraseña tiene fecha de caducidad para el próximo 26 de enero de 2023, presione en el siguiente enlace para realizar la actualización, de lo contrario, su cuenta permanecerá inactiva.
- Estimado “usuario”: Se ha realizado un cargo a tu cuenta por la cantidad de “10,000.00”, si no reconoces esta transacción llama al siguiente número telefónico para realizar la aclaración.
- Accede al siguiente enlace para conocer su adeudo.



- Presione en el siguiente enlace para descargar su estado de cuenta
- ¡Evite sanciones! Revise por favor el siguiente documento.
- Multa por incumplimiento de obligaciones fiscales. Presione en el siguiente enlace para obtener más información.
- ¡FELICIDADES! Fuiste seleccionado en la rifa anual de tu “institución bancaria”, presiona en el siguiente enlace para obtener más información.



RECOMENDACIONES:

Con la finalidad de no ser víctima del Phishing es importante considerar:

- Las instituciones bancarias *no solicitan datos personales a través de correos electrónicos*, si recibes un correo electrónico donde te los piden, lo mejor será corroborar la información a través de una llamada telefónica a tu institución financiera, página web de la entidad, o bien, acudir directamente a una sucursal bancaria.
- No realizar operaciones bancarias en *sitios públicos*, por ejemplo, un cibercafé, o en redes de internet de acceso público (ubicadas en plazas comerciales, parques, etc.) Estos sitios podrían ser un medio vulnerable en sus redes informáticas.
- No prestar atención a correos electrónicos, llamadas telefónicas, sitios web o documentos sospechosos.
- No presionar sobre *documentos adjuntos* en correos electrónicos de dudosa procedencia, estos podrían traer consigo algún programa malicioso.



- No presionar en los enlaces de correos electrónicos, al menos que estos provengan de correos verificados u oficiales.
- No responder mensajes de textos sospechosos o de remitentes desconocidos.
- Si se recibe una llamada que provenga supuestamente de tu entidad bancaria o financiera, verificar la veracidad de esta.
- No revelar a ninguna persona, ni por mensajes ni por correo electrónico, tu información bancaria como: números de cuenta, tarjeta, claves. etc.



Proveer información es como darle a la persona estafadores la llave de tu cuenta bancaria.

Fui víctima de phishing, ahora ¿qué hago?



Si sospechas que fuiste víctima de phishing contacta a las instituciones encargadas de proteger los derechos e información de las personas usuarias de entidades financieras.



Accede a sus sitios oficiales desde los siguientes enlaces:

- CONDUSEF: <https://www.condusef.gob.mx/>
- INAI: <https://home.inai.org.mx/>

BIBLIOGRAFÍA

Baxico. (16 de Enero de 2023). *Sistema de información económica*. Obtenido de

<https://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?accion=consultarCuadro&idCuadro=CF258§or=5&locale=es>

INEGI. (02 de Febrero de 2023). *Encuesta Nacional sobre Disponibilidad y Uso de*

Tecnologías de la Información en los Hogares. Obtenido de ENDUTIH:

<https://www.inegi.org.mx/programas/dutih/2021/>