Guía para prevenir el Pharming

HACIENDA
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

CONDUSEF
COMISIÓN NACIONAL PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS

ift INSTITUTO FEDERAL DE TELECOMUNICACIONES

Guía para prevenir el Pharming

El **pharming** es una combinación de los términos "phishing" y "farming" que significa cultivo y "phishing" que representa una técnica nueva y más complicada para acceder a información personal o bancaria de otra persona.

De acuerdo con la **CONDUSEF**, el pharming es aquella práctica que consiste en la redirección a una página de internet falsa mediante ventanas emergentes, con el objetivo de robar información.[1]

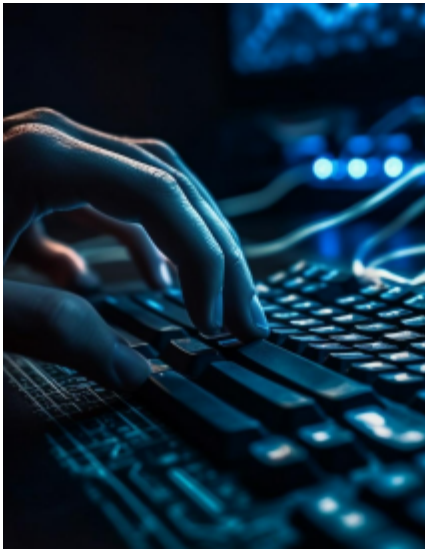
A través de esta actividad se busca obtener beneficios económicos e información privilegiada, muchas veces para la generación de estafas.[2]

1 CONDUSEF, Tipos de fraude. Disponible en: **https://www.condusef.gob.mx/?p=tipos-de-fraude**

2 Patiño Corona, Juan, PHARMING, LA EVOLUCIÓN DE UN ATAQUE, DGTIC-UNAM. Disponible en: **https://revista.seguridad.unam.mx/numero-02/pharming-la-evoluci%C3%B3n-de-un-ataque**

I. ¿Qué es el Pharming

Esta práctica aprovecha la **vulnerabilidad del software** de los servidores con la intención de modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP de una entidad, ya sea que se hagan pasar por los sitios de banca electrónica o de pago para redirigirlos a una otra IP que se aloja en una página web falsa (la misma que fue introducida por el ciberdelincuente) y, de esta forma obtener las claves de acceso a las diferentes cuentas.[3]



3 INCIBE. Glosario de términos de ciberseguridad, Una guía de aproximación para el empresario. Disponible en: **https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf**

II. ¿Cómo se lleva a cabo?

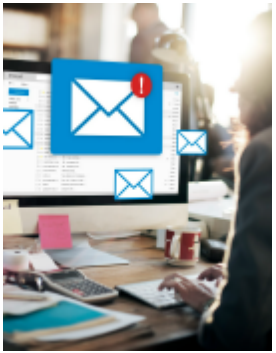
El pharming se puede realizar de dos formas: mediante **el hackeo de ordenadores individuales o por la contaminación de servidores DNS**, (este sistema traduce las direcciones web en direcciones IP para que se pueda navegar en internet):

- En el primer caso, los ciberdelincuentes infectan tu ordenador con un virus que cambia el **archivo de hosts**, que es el que asocia las direcciones web con las IP.

- En el segundo caso, los ciberdelincuentes atacan **el servidor DNS**, cambiando el dominio que se puede ver en el buscador, con lo que pueden afectar a miles o millones de usuarias o usuarios al mismo tiempo.[4] Por ejemplo, si quieres acceder a tu Banca en línea, puedes escribir la dirección web en tu navegador, pero en vez de llevarte al sitio real, te redirige a uno falso que imita su apariencia. Allí, te piden que introduzcas tu usuario y contraseña, y así los ciberdelincuentes pueden acceder a tu cuenta bancaria.

4 Kaspersky, ¿Qué es el pharming?, 2021. Disponible en: **https://latam.kaspersky.com/resource-center/definitions/pharming**

III. Diferencias
entre el phishing
y el pharming



El Instituto Nacional de Transparencia **(INAI)** señala que, el phishing es una práctica que consiste en usurpar **la identidad de una empresa u organización gubernamental**. Se hacen llegar correos electrónicos a la víctima con un enlace a una página aparentemente legal, pero que en realidad es falsa, en donde piden datos personales para después cometer el fraude.[5]

Esta práctica también es utilizada para simular ser **entidades financieras o bancarias** con el objetivo de tomar sin autorización de la persona su información personal.

El pharming en muchas ocasiones omite el mensaje que utiliza como gancho para atraer la atención de la persona, y de esta forma, pone a disposición de la o el usuario la dirección electrónica errónea de una manera más sencilla y sutil.

5 INAI, COMUNICADO INAI/248/21. "PHISHING, PHARMING, SMISHING Y VISHING, PRÁCTICAS PARA COMETER FRAUDES DIGITALES, ALERTA INAI". Disponible en:
https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-248-21.pdf

IV. Consecuencias

- Usurpación de identidad.
- Robo de tus cuentas bancarias.
- Robo de tus cuentas de correo y redes sociales, así como contraseñas de acceso a diversas aplicaciones.
- Pérdida de información personal.
- Daño en los equipos ya que pudieron sufrir alguna infiltración de malwares.

V. Recomendaciones
para evitar ser
víctima de pharming

1. Evita ingresar a **links y descargar archivos de origen desconocido**.
2. Instala un **antivirus** en tus dispositivos electrónicos.
3. Comprueba que la dirección electrónica esté **escrita de forma correcta**.
4. Procura instalar una herramienta que te permita **bloquear ventanas** emergentes en los sitios a los que accedes.
5. Evita abrir correos electrónicos de los que no se puedan confirmar su **veracidad o procedencia**.
6. Evita dar **clic en anuncios** o ventanas emergentes que te digan que has ganado **un premio, viaje o sorteo**.

7. Verifica que el sitio al que ingresas tenga un **“candado”** al principio del enlace electrónico y, posteriormente comience con **https://**.
8. Evita consultar tus cuentas personales y compartir información personal cuando utilices dispositivos de **carácter público** o que estén conectadas a redes públicas.
9. Tus contraseñas o NIPs **no deben ser fáciles de adivinar**, evita utilizar fechas de nacimiento, números telefónicos o cualquier dato relacionado con tu identidad.
10. Utiliza mecanismos para establecer verificaciones de varios pasos.
11. Procura hacer uso de una **VPN (Virtual Private Network, o red privada virtual)** cuando accedas a internet.

Para mayor información consultar:

- CONDUSEF, Tipos de fraude. Disponible en: **https://www.condusef.gob.mx/?p=tipos-de-fraude**
- INAI, COMUNICADO INAI/248/21. “PHISHING, PHARMING, SMISHING Y VISHING, PRÁCTICAS PARA COMETER FRAUDES DIGITALES, ALERTA INAI”. Disponible en: **Comunicado INAI-248-21.pdf**
- INCIBE. Glosario de términos de ciberseguridad, Una guía de aproximación para el empresario. Disponible en: **https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf**
- Kaspersky, ¿Qué es el pharming?, 2021. Disponible en: **https://latam.kaspersky.com/resource-center/definitions/pharming**
- Patiño Corona, Juan, PHARMING, LA EVOLUCIÓN DE UN ATAQUE, DGTIC-UNAM. Disponible en: **https://revista.seguridad.unam.mx/numero-02/pharming-la-evoluci%C3%B3n-de-un-ataque**