Cibercriminales suplantan a Netflix para robar datos de los usuarios

31/10/2022

Los **cibercriminales** utilizan una gran variedad de métodos para infiltrarse en los dispositivos de las personas con el objetivo de robar información para generar ganancias; esta vez están usando a **Netflix**, la aplicación de **streaming** de películas y series para obtener los datos de los **usuarios**.

Sin embargo, a diferencia de la mayoría de los ataques cibernéticos como el phishing, que es el más frecuente, los **ciberdelincuentes** detrás de este método eligen una variante llamada "**smishing**", que consiste en el envío de mensajes **SMS** a las víctimas fingiendo ser una empresa conocida y de gran credibilidad como una red social, un banco o una institución pública, para robarles información o realizar

cargos a sus **cuentas bancarias**.

Estas estafas por internet fueron reportadas en España por la **Oficina de Seguridad del Internauta (OSI)**, institución que indica que los cibercriminales que usan esta forma de ataque tienen la finalidad de llevar a sus víctimas a pasarelas de **pago** para robar su **información personal**.

Cómo funciona el smishing con Netflix

El objetivo de los **cibercriminales** es que los usuarios entreguen sus credenciales de acceso a su cuenta de **Netflix** y para ello engañan a sus víctimas haciéndose pasar por la empresa de tecnología y le indican que se han producido **problemas en el pago** de su **suscripción**, por lo que deberán reingresar a sus cuentas.

“Smishing”, que consiste en el envío de mensajes SMS a las víctimas fingiendo ser una empresa conocida y de gran credibilidad como una red social, un banco o una institución pública, para robar información a los usuarios. (foto: Cinco

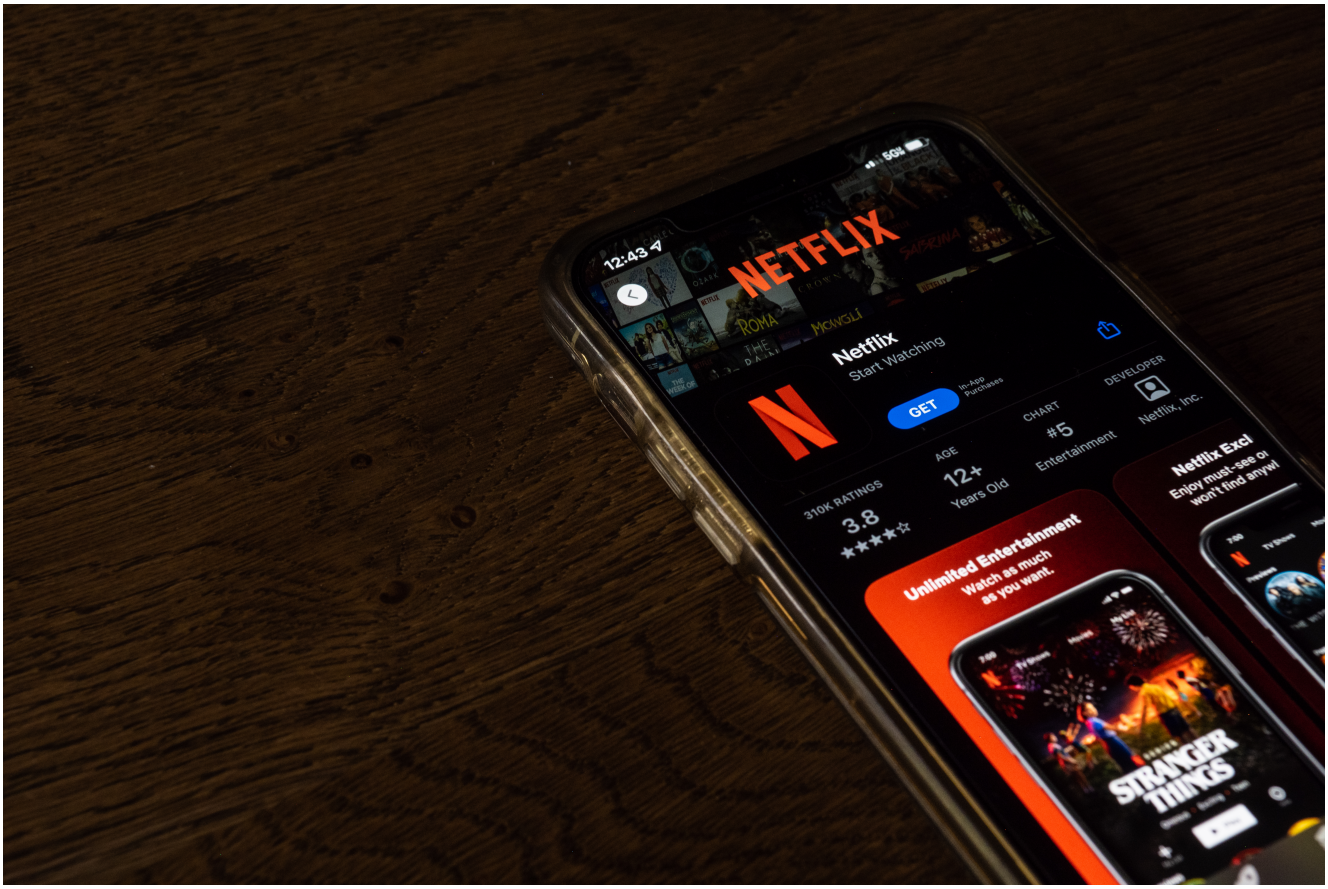
Días)

Además, para aumentar el nivel de presión bajo el que se encuentra la víctima, el **SMS** que le llega a la víctima indica que para poder realizar la transacción solo se tiene un periodo de **24 horas** o, en su defecto, se establece una **fecha límite específica** que no le de oportunidad al usuario de analizar fríamente la situación.

Junto al mensaje que fue enviado a las víctimas, los **ciberdelincuentes** ingresan un enlace a un **sitio web falso** que tiene una apariencia muy similar a la que usa **Netflix** en realidad.

Una vez que caen en el engaño, las **víctimas** introducen su nombre de usuario y **contraseña** en los campos establecidos para esos datos, pero en lugar de ingresar a su perfil son redirigidos a otra **página web** que les indica que su cuenta fue suspendida y se deberá introducir nuevamente la **información bancaria** para ingresar a la cuenta.

“Su último débito falló, por favor actualice sus métodos de pago para beneficiarse de nuestros servicios”, es el mensaje que aparece en la pantalla de la página web falsa que pretende sustituir a **Netflix**. Entonces, aparece el botón ‘Siguiente’ que, una vez se pulsa, despliega un formulario que debe completar el usuario con la **información de facturación**.



Los cibercriminales indican que el inicio de sesión de la víctima falló debido a un problema con el método de pago. De esta forma los usuarios entregan su información bancaria a los cibercriminales. Foto: Getty Images

Una vez realizados todos los pasos que indica el supuesto **sitio web** de Netflix, el usuario pasará por un supuesto proceso de **verificación por SMS** y luego de haber indicado el **número de teléfono** al que lo desea recibir, llegará un mensaje de texto con un enlace que redirige a la página web real de **Netflix** para que no se produzca ninguna sospecha por parte del usuario hasta que sea demasiado tarde.

Cómo evitar ser una víctima

Las estafas que involucran **mensajes SMS** no son una novedad y los usuarios sí pueden prevenir estas situaciones si se encuentran correctamente **informados**. Para empezar, si una persona recibe una comunicación por parte de cualquier empresa cuyos **servicios** no hayan sido contratados, es un **indicador** de

que lo más probable es que se trate de un intento de **ataque cibernético**.

Además, en este tipo de situaciones el usuario debe evitar pulsar el **link** del usuario pues no se sabe a qué tipo de páginas redirigen estos **enlaces**.

Además, en este tipo de situaciones el usuario debe evitar pulsar el **link** del usuario pues no se sabe a qué tipo de páginas redirigen estos enlaces. Sin embargo, en caso de que sí se haya ingresado al **sitio web falso**, las personas deben prestar mucha atención a la dirección del sitio.

En ocasiones pueden presentarse **errores ortográficos** como “Nettflix” o “Netfliix”, mientras que otros casos puede reemplazarse el **dominio** .com por otro que haya sido desarrollado únicamente para este tipo de engaños. Finalmente una actitud de **prevención** puede ser de gran ayuda en este tipo de situaciones para evitar ser una víctima más de **ciberataques**.

Fuente: Infobae