



## NETFLIX, un engaño de película

Nuevo caso de phishing, técnica para obtener información de usuarios desprevenidos



Con más de 140 millones de usuarios en todo el mundo, la imagen de Netflix sigue siendo utilizada por los cibercriminales para realizar campañas de ingeniería social en las que suplantán la identidad de la popular plataforma de streaming con el objetivo de robar información personal de usuarios desprevenidos.

Por estos días circula un correo en el que se suplanta la identidad de Netflix. El correo indica al destinatario que es necesario verificar su información de inicio de sesión debido a que se había registrado una actividad sospechosa en su cuenta.

A simple vista, un usuario desprevenido podría suponer que se trata de un correo legítimo por parte del proveedor de servicios de series y películas y decidir hacer clic en el botón "ACTUALIZAR" para evitar perder el acceso a su cuenta.

Por supuesto, no estaría verificando que la URL a la que hace referencia el botón presenta las siguientes características:

<https://u10100579.ct.sendgrid.net/wf/click?upn=XXXXXXXXXXXXX>

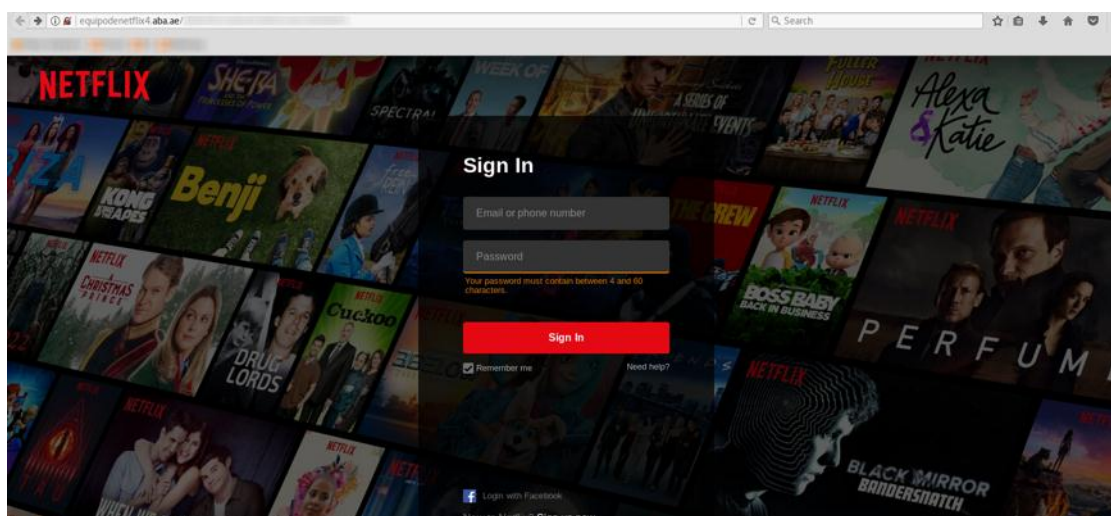
Como se puede apreciar, el enlace no corresponde a ninguna dirección oficial del servicio Netflix; de hecho, ni siquiera aparece el nombre del servicio en alguna parte de la composición de la URL.

Luego de una redirección, seguramente a efectos de evitar protecciones antiphishing, el usuario atacado llegará a un sitio con la siguiente dirección:

<http://equipodenetflix4.aba.ae/f46d63f37e337b21cdcxxxxxxxxxxxxxxxxx/>

En esta URL se puede observar, dentro de la composición del dominio, que se hace referencia a un supuesto equipo de Netflix y que el servidor corresponde a un servicio de hosting gratuito de Emiratos Árabes.

La interfaz del sitio con la que el usuario se encontrará es la siguiente:




Con un diseño igual al del sitio original, la particularidad de esta página es que, independientemente del usuario y clave que se ingresen, no se producirá ningún tipo de verificación de credenciales y se intentará llevar al usuario a una instancia en la que se le solicitará el ingreso de los datos de la tarjeta de crédito asociada a la cuenta.

**NETFLIX**

[Sign Out](#)

STEP 2 OF 2  
**Confirm Your debit or credit card**



?

[CONFIRM YOUR DETAILS](#)

En esta instancia, nuevamente los datos ingresados no serán cuestionados y solo bastará con cumplir con el requisito de longitud en algunos campos. Es decir que ante la inclusión de cualquier información y el pedido de confirmar los datos, el sitio finalmente redireccionará al usuario al portal original de Netflix, habiendo logrado el cometido del robo de credenciales de acceso y los datos de pago de la cuenta.

En un análisis un poco más exhaustivo, se pudo verificar que no se realizaron segundas acciones, como la descarga de algún tipo de malware o la ejecución de algún código adicional que afectara los recursos de la máquina. Por lo tanto, se puede interpretar que se trata de una campaña que busca únicamente el robo de información personal, presumiblemente para vender en el mercado negro (la venta de los datos de una tarjeta de crédito activa ronda los 45 U\$D en la Dark Web) o bien para utilizar en otros ataques dirigidos.

## Como evitar ser víctima en estos ataques

- Siempre evitar acceder a enlaces que llegan inesperadamente por correo electrónico u otros medios.
- Verificar la dirección del remitente y que coincida que con el servicio al que hace referencia.
- Contar con protecciones de seguridad en el dispositivo que puedan hacer de barrera ante estos casos. En el caso de sospechar que pueda ser cierto el mensaje, ya sea porque es un usuario muy activo en esta u otra plataforma, se recomienda acceder a la misma de manera tradicional y verificar ahí si todo está correcto o eventualmente realizar un cambio de credenciales.