

Alerta de seguridad cibernética	8FPH20-00227-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Mayo de 2020
Última revisión	21 de Mayo de 2020

## NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los loC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los loC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, ha identificado una campaña de Smishing, que se está difundiendo a través de mensaje de texto falso que aparenta provenir de la compañía de streaming Netflix.

La campaña busca persuadir a quienes reciben el mensaje para utilizar el enlace fraudulento adjunto. El mensaje informa que se ha suspendido la suscripción del servicio y para volver disponer de éste, debe actualizar la forma de pago.

Si la persona utiliza el enlace, será dirigido a una web fraudulenta que imita al sitio oficial de netflix, donde se expondrá al robo de sus credenciales y datos de su tarjeta de crédito.

## Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

## Indicadores de compromiso

### Urls Redirecciones:

hxxps://netflix-activa[.]com

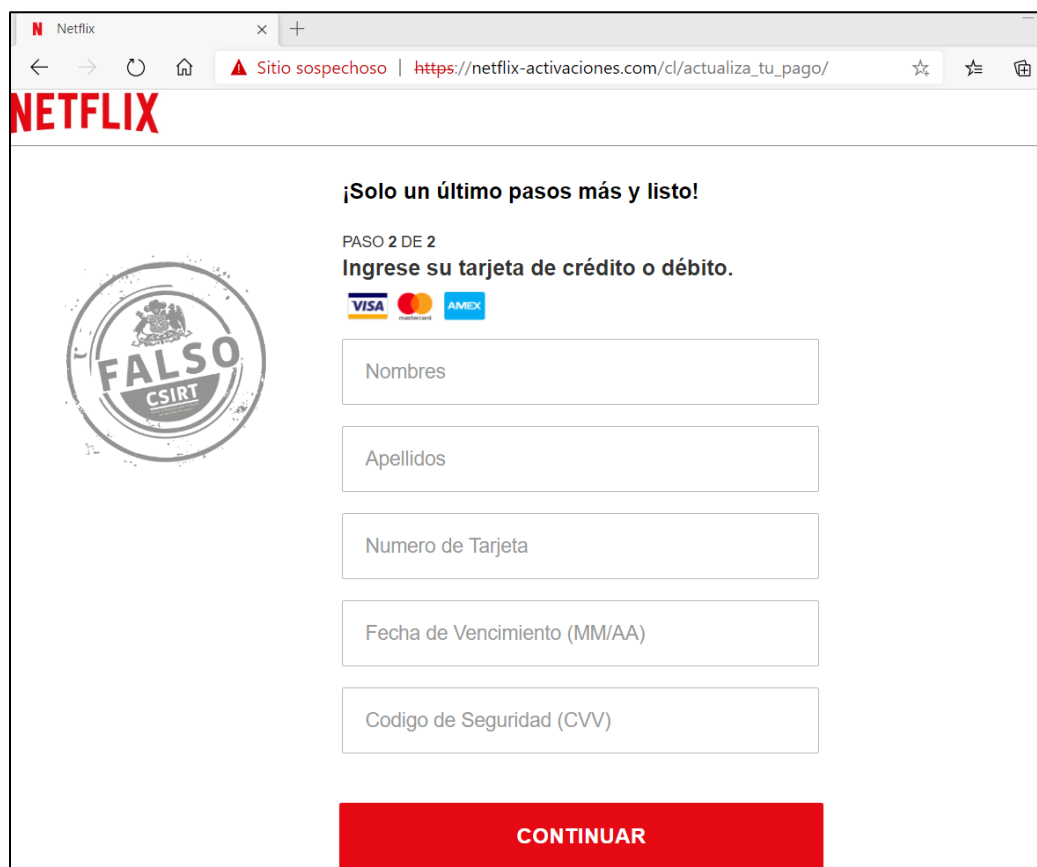
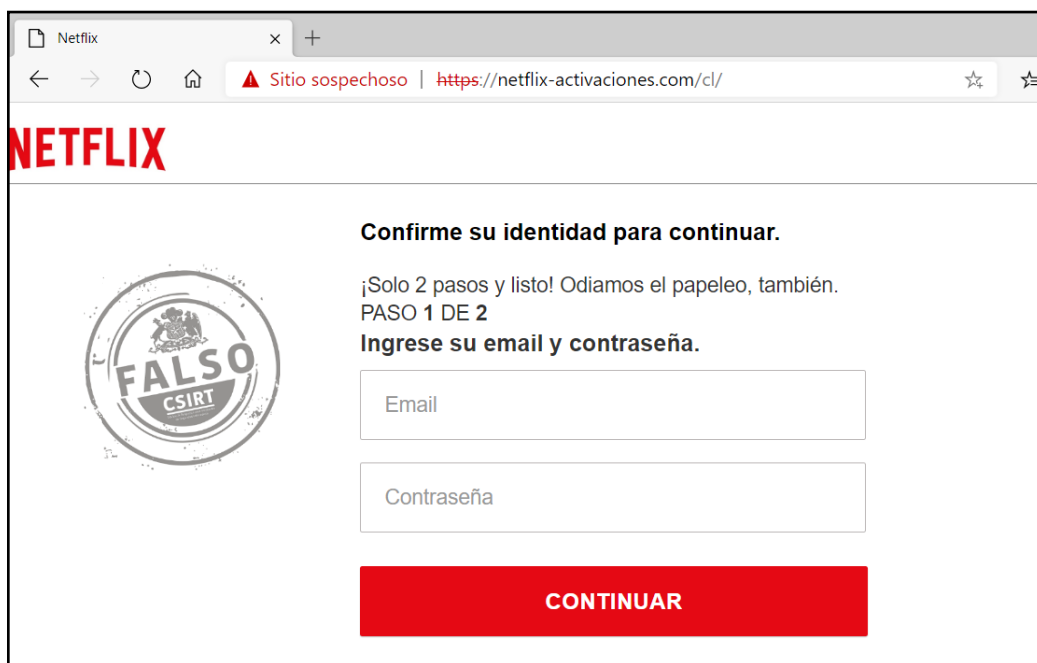
### Urls sitio falso:

hxxps://netflix-activaciones[.]com/cl/

## Imagen del mensaje



## Imagen del sitio



## Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los AntiSpam y SandBoxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.