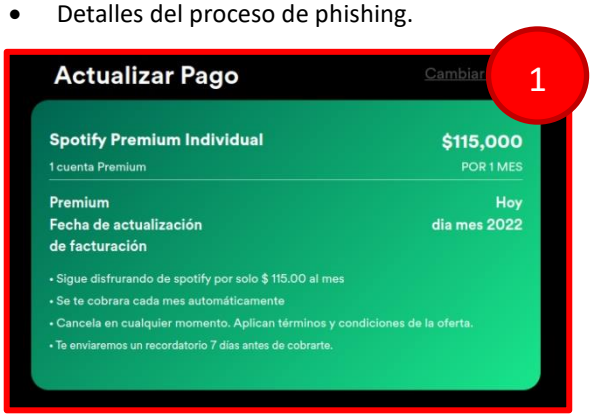
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 071	**Fecha: 23-03-2023**
		Página 22 de 25

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Suplantación de la identidad de la empresa de servicios multimedia Spotify		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	G02
Clasificación temática familia	Fraude		

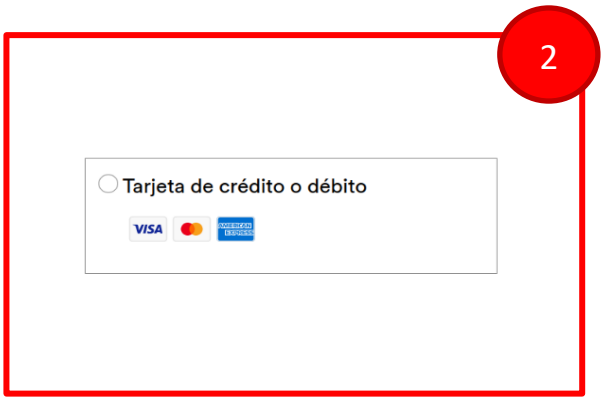
Descripción

1. Mediante el monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, ciberdelincuentes vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad de la empresa de servicios multimedia Spotify (servicio de música, pódcasts y vídeos digitales que te da acceso a millones de canciones y a otro contenido de creadores de todo el mundo), el cual tiene como finalidad robar información confidencial y bancaria de las posibles víctimas como número de tarjeta, fecha de vencimiento, código de seguridad, entre otros.

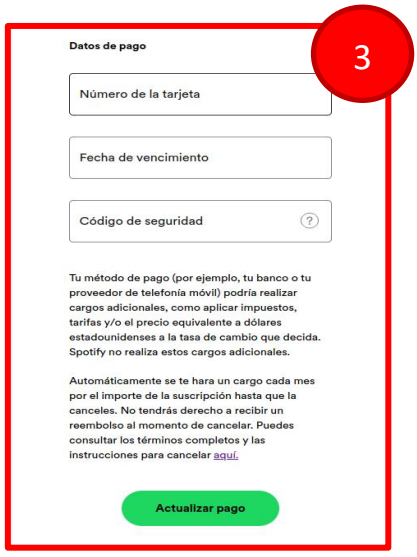
- Detalles del proceso de phishing.



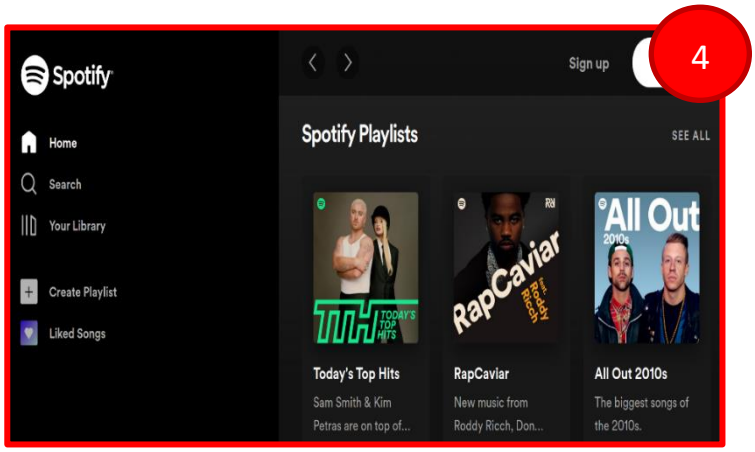
➢ Solicita realizar una actualización de pago de la supuesta cuenta Premium individual de Spotify.



➢ Luego, solicita elegir el tipo de tarjeta crédito o débito, a actualizar.



➢ Requiere ingresar datos bancarios como número de tarjeta, fecha de vencimiento y código de seguridad.



➢ Finalmente, redirige de manera automática al sitio web oficial de Spotify, toda vez que la información ingresada ya fueron captados por los ciberdelincuentes.

2. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

- Indicadores de compromisos:

  - **URL:** hxxps:// www[.]spotifybrasil[.]com
  - **Dominio:** SpotIFyBrasil[.]com
  - **IP:** 89[.]117[.]139[.]96
  - **Tamaño:** 26 KB
  - **País:** Estados Unidos
  - **Proveedor de alojamiento**: Hostinger International Limited

BitDefender	Phishing	CyRadar	Malicious
ESET	Phishing	Fortinet	Phishing
G-Data	Phishing	Google Safebrowsing	Phishing
Lionic	Phishing	Seclookup	Malicious
Sophos	Phishing	Abusix	Clean

3. Otras detecciones:

4. Recomendaciones:

- Utilizar un antivirus actualizado ya que es la primera barrera ante un ataque cibernético.
- Verificar detenidamente la redacción y ortografía de la dirección URL, que coincidan con el sitio web oficial.
- Evitar responder a mensajes enviados (correo electrónico, Whatsapp, SMS y otros), que contengan enlaces de dudosa procedencia.
- No compartir la información con terceras personas, amigos o familiares.
- Acceder al sitio web a través de fuentes oficiales.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta