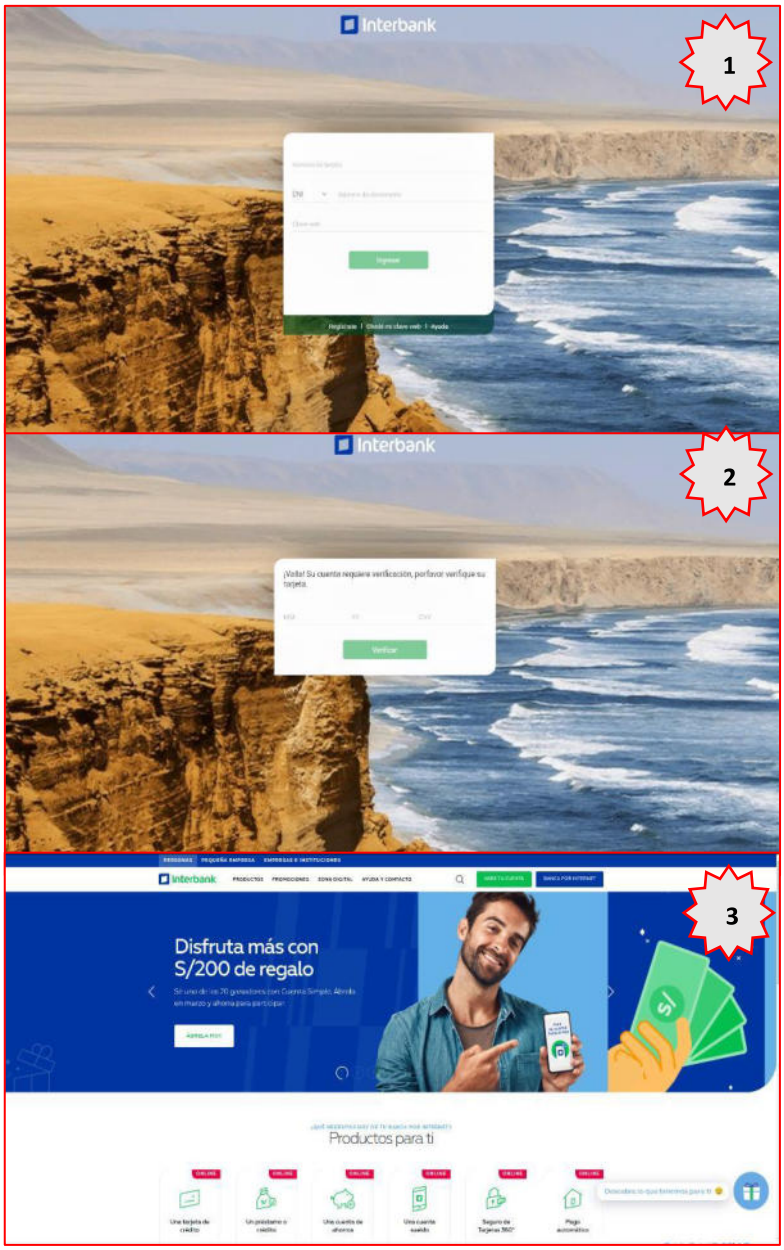
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 068	Fecha: 09-03-2022
		Página 6 de 8

Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ			
Nombre de la alerta	Campaña de Phishing, suplantando la identidad del Banco Interbank			
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. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, por medio de los diferentes navegadores web, dirigido a los clientes y/o usuarios del Banco **INTERBANK**; el cual, mediante la creación de un supuesto sitio web de la entidad bancaria, solicitan a las posibles víctimas a ingresar datos bancarios, como número de tarjeta, DNI y clave web, con la finalidad de apoderarse de manera ilícita de dicha información.

2. **Imagen**: Detalle del proceso del Phishing:



Solicitan a las posibles víctimas ingresar datos bancarios, como Número de tarjeta, DNI y clave web.

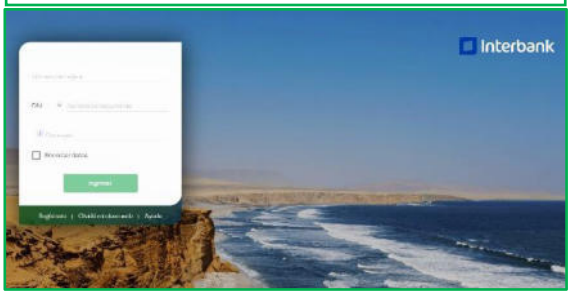
Indica que su cuenta requiere realizar una verificación, para ello la posible víctima debe ingresar datos bancarios de la tarjeta, como fecha de vencimiento y código de seguridad.

Finalmente redirige de forma automática al sitio web original del banco Interbank; aludiendo un aparente error de autenticación. Sin embargo, los datos ya fueron capturados por los ciberdelincuentes.

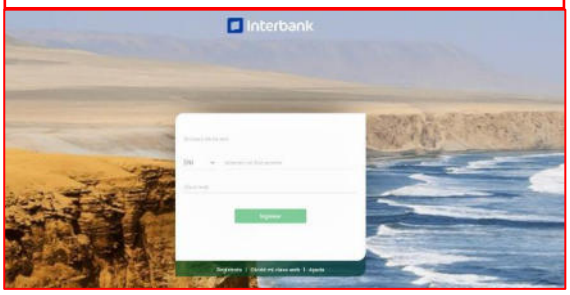
3. Comparación del sitio web oficial y fraudulento.

Dominio

Sitio web oficial
URL: https://bancaporinternet.interbank.pe/login



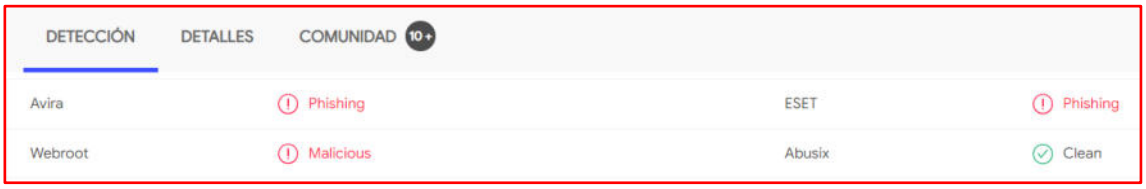
Sitio web fraudulento
URL: hxxps[:]//acceder-interbank[.]web[.]app/#/



- Ambas URL´s utilizan el protocolo HTTPS, lo que hace más convincente a que las víctimas accedan al sitio web.
- La diferencia está en la URL, debido a que el dominio del sitio web fraudulento no coincide con el oficial.

4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como Phishing (suplantación de identidad):

- Indicadores de compromiso:
  - URL: hxxps[:]//acceder-interbank[.]web[.]app
  - Dominio: interbank[.]web
  - IP: 199[.]36[.]158[.]100
  - Tamaño: 3.80 KB
  - SHA-256: 7a6942a564c836cb46b35b1351deb08dd3be862e2c360c2e63be123ff4f7025a



5. Apreciación de la información:

- La presente campaña de Phishing, permite a los actores de amenazas obtener información bancaria de los usuarios del Banco Interbank

- La propagación del sitio web fraudulento se realiza mediante envió masivos de email, adjuntando enlaces de sitios web fraudulentos con la finalidad de obtener información sensible de las víctimas; asimismo, dicho enlace malicioso, es enviado a través de las plataformas digitales como el WhatsApp, Telegram, Messenger y mensajes de textos SMS.

6. Referencia.

- PHISHING: Es un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar.

7. Recomendaciones:

- No brindar información personal y/o bancaria en sitios web de dudosa procedencia.
- Ingresar de forma manual la URL de la entidad correspondiente.
- Verificar la información en la entidad correspondiente.
- No compartir la información con familiares o amigos.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener un software antivirus.

Fuentes de información	Análisis propio de redes sociales y fuente abierta