	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°012	Fecha: 13-01-2024
		Página: 8 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de Phishing que suplanta a la entidad bancaria de 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 Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que los ciberdelincuentes vienen llevando a cabo una campaña de envío masivo de correos electrónicos falsos, que pretenden ser de la entidad bancaria de Interbank, en el asunto del mensaje advierten ***"Le hacemos llegar una notificación debido a que su cuenta Interbank ha sido bloqueada, esto puede ser debido al ingreso sospechoso a su cuenta de terceros a través de banca por internet ",*** incluido un enlace oculto detrás del botón ***"Ingresa aquí"*** que, al ser pulsado, redirige a la víctima, a un sitio web falso de Interbank que simula ser el oficial, con el objetivo de robar las credenciales de acceso, información personal y/o financiera.

2. DETALLES:

Figura 1. Al abrir el enlace brindado a la víctima, le informa que su cuenta ha sido bloqueada y tiene que ingresar sus datos.

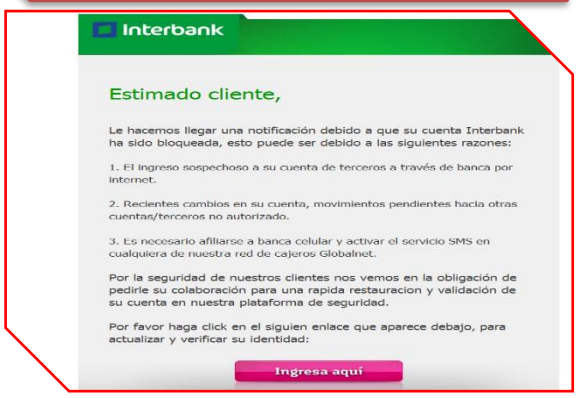


Figura 2. Al ingresar, le pide registrar la solicitud para ingresar las credenciales de acceso (DNI, y clave web).

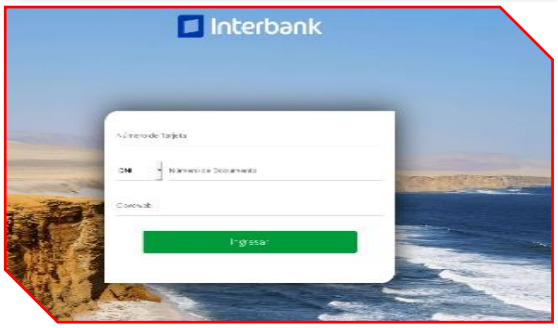


Figura 3. Posteriormente, parece validar los datos, pero en realidad la información fue robada por los ciberdelincuentes.

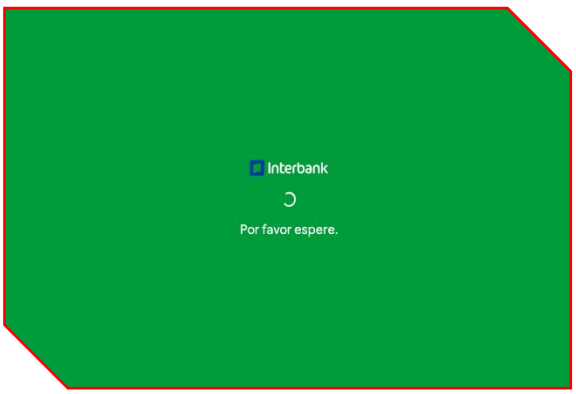
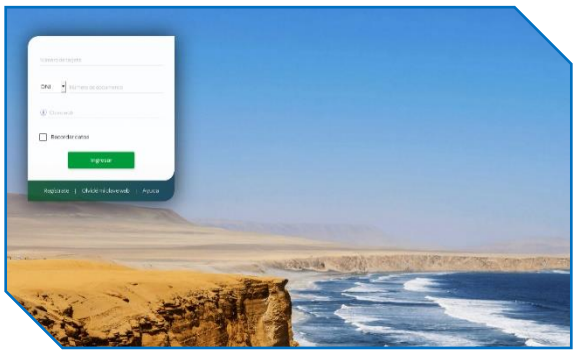


Figura 4. El supuesto sitio web redirige de forma automática al sitio web oficial del banco Interbank; sin embargo, los ciberdelincuentes ya obtuvieron los datos proporcionados por la víctima que luego son usados para realizar acciones sin el consentimiento del titular.

- Comparación de los sitios web legítimo y falso del Banco Interbank:

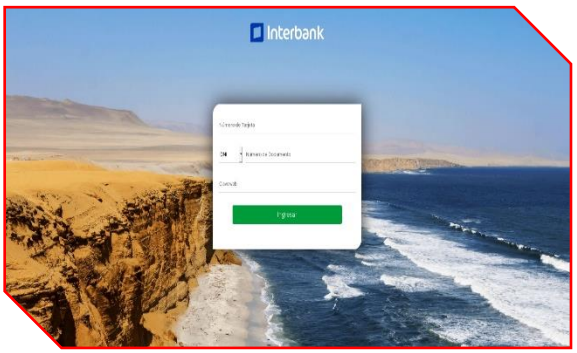
SITIO OFICIAL

URL: https://bancaporintenet.interbank.pe/login



SITIO FRAUDULENTO

hxxps://interbank-acceso[.]com/files/login[.]php?user=true



- Existe similitud en imagen, logotipo, fondo, color y escritura.
- Tiene certificado de seguridad de protocolo HTTPS.
- El dominio se hace pasar por el sitio oficial, pero no coinciden.

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

- Indicadores de compromisos:
  - **URL:** hxxps://interbank-acceso[.]com/files/login[.]php?user=true
  - **Dominio:** acceso-interbancario[.]com
  - **Dirección IP:** 91[.]215[.]85[.]21
  - **Código:** 200
  - **Longitud:** 6.11 KB
  - **SHA-256**: cad5ecd494a1579584c3a9eaf8db8a430f6a2e6fe8aa0a3943bae530678810d2

3. RECOMENDACIONES:

- Evitar ingresar los datos de autenticación en las URL que recibas por correo electrónico.
- Escribir directamente la URL de la entidad en el navegador.
- Sospechar de todos aquellos mensajes alarmantes que tengan tono de urgencia y contengan faltas de ortografía o erratas.
- No divulgar la información a amigos, familiares o terceros.
- Utilizar un programa antivirus actualizado, ya que es la primera línea de defensa contra un ciberataque.

Fuente de Información:	Análisis propio de redes sociales y fuente abierta.