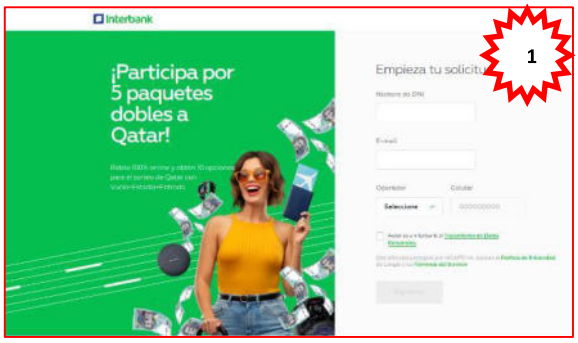
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 149	Fecha: 03-06-2022
		Página 7 de 9

Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	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		

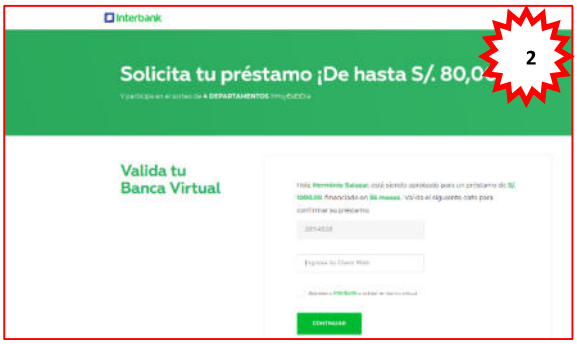
Descripción

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, a través de los diferentes navegadores web, quienes suplantan la identidad del Banco Interbank, dirigido a todos los usuarios y/o clientes de Interbank, indicando que la entidad bancaria viene dando facilidades de adquirir o ampliar un préstamo máximo de 80,000 soles, el cual tiene como finalidad robar información bancaria de las posibles víctimas.

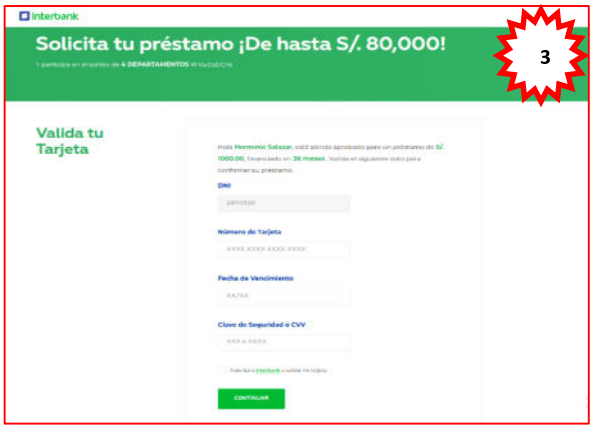
2. Comparación del sitio web oficial y fraudulento.



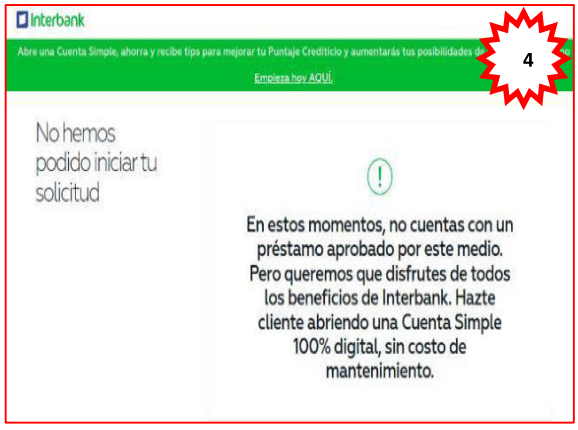
El supuesto sitio web cuenta con los logos y colores característicos del banco Interbank, donde solicita ingresar DNI, E-mail, número telefónico, a fin de empezar una solicitud de préstamo.



Luego, pide a la posible víctima validar la banca virtual de Interbank, ingresado las credenciales de inicio de sesión como usuario y clave web.



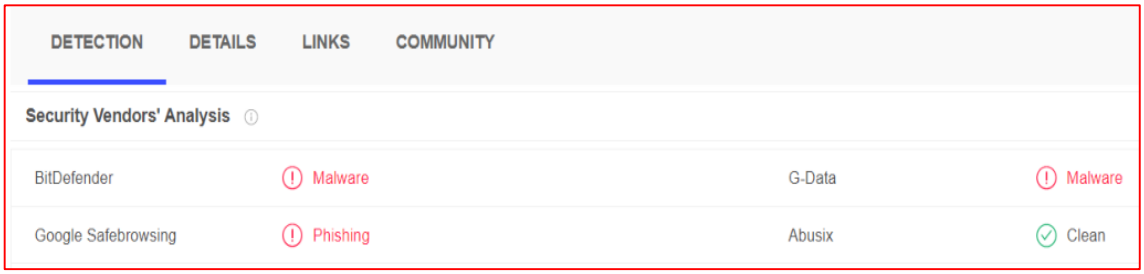
A continuación, requiere ingresar datos bancarios, como número de tarjeta del Banco Interbank, fecha de vencimiento, y clave de seguridad.



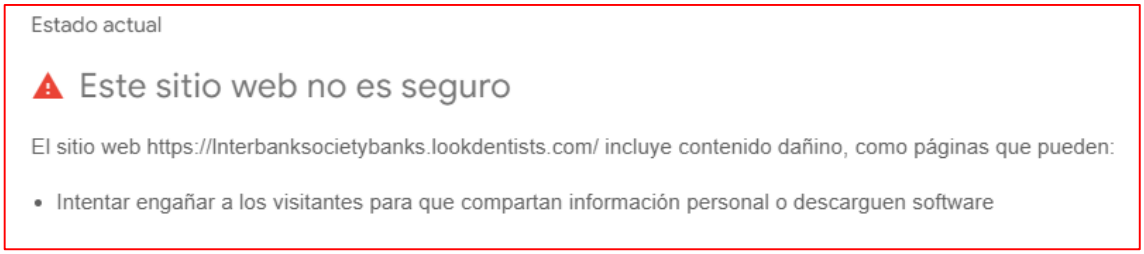
Por último, informa que la entidad bancaria no ha podido iniciar la solicitud de préstamo, debido a que no cuenta con un crédito aprobado.

3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información:

- **URL Malicioso:** hxxps[:]//Interbanksocietybanks[.]lookdentists[.]com
- **Dominio:** lookdentists[.]com
- **IP:** 108[.]167[.]140[.]158
- **Tamaño:** 134.75 KB
- **SHA-256:** 9180a5b0923cee911c62569939925ce9044b4c5ca52315fb3b1aebdda356ceb4



- La navegación segura de Google también cataloga como sitio web **no seguro** o **peligroso**.



4. **Cómo funciona el Phishing:**

- Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- Medios de propagación del Phishing: WhatsApp, telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público o privado, entidad financiera, servicio técnico, etc.)

5. **Referencia:**

- Phishing o suplantación de identidad: Es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

6. **Algunas Recomendaciones:**

- Verificar la información en la entidad bancaria.
- Acceder al sitio web a través de sus fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No brindar información personal a sitios web sospechosos.
- Mantener instalado un servicio de antivirus en el dispositivo.
- Mantener el sistema operativo actualizado del equipo informático.

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