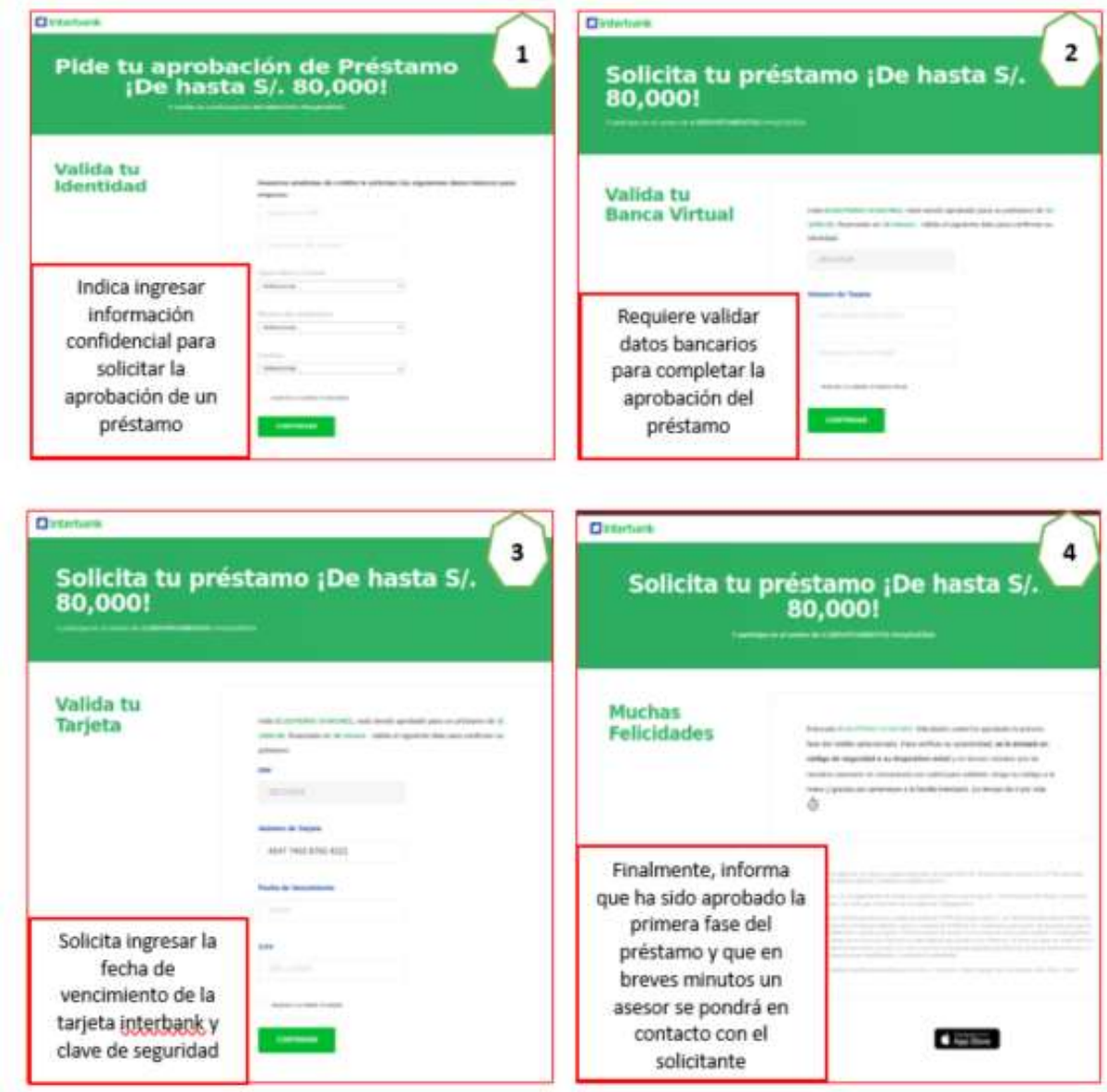
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 286	Fecha: 21-10-2022
		Página 09 de 11

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantando la identidad de la entidad Bancaria 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		

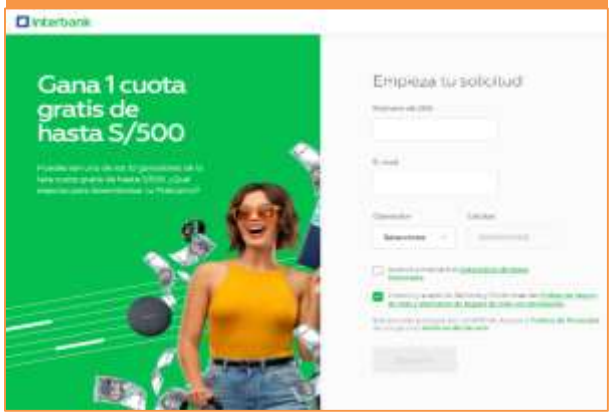
Descripción

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 de la entidad bancaria Interbank; el cual, mediante la creación de un sitio web similar al original, solicitan a las posibles víctimas a requerir la aprobación de un supuesto préstamo de hasta 80,000 soles, ingresando datos personas y bancarios como DNI, N° de celular, contraseña, N° de tarjeta, fecha de vencimiento, clave de seguridad, entre otros.
2. **Imagen**: Detalle del proceso del Phishing:



3. Comparación del sitio web oficial y fraudulento.

Sitio web oficial
https://interbank.pe/solicitar/prestamo/efectivo/inicio

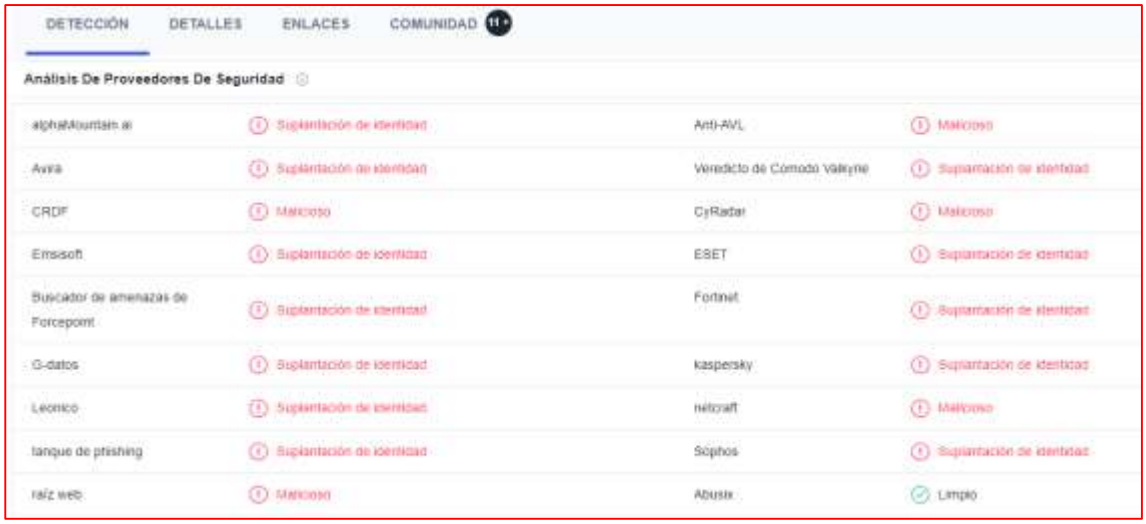


Sitio web fraudulento
hxxps://reactivate-primaveraoctubre[.]site

- 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, toda vez 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://reactivate-primaveraoctubre[.]site
  - Dominio: reactivate-primaveraoctubre[.]site
  - IP: 104.21.67.220
  - Tamaño:
  - 871.65 KB
  - SHA-256: a00198c4f9dd09d858c09b0a9440c1119aa4e17f41e006da57843ff017b888cb



5. Recomendaciones:

- Verificar la información en la entidad correspondiente
- Las entidades bancarias no solicitan realizar actualización de datos de manera online o virtual.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.

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