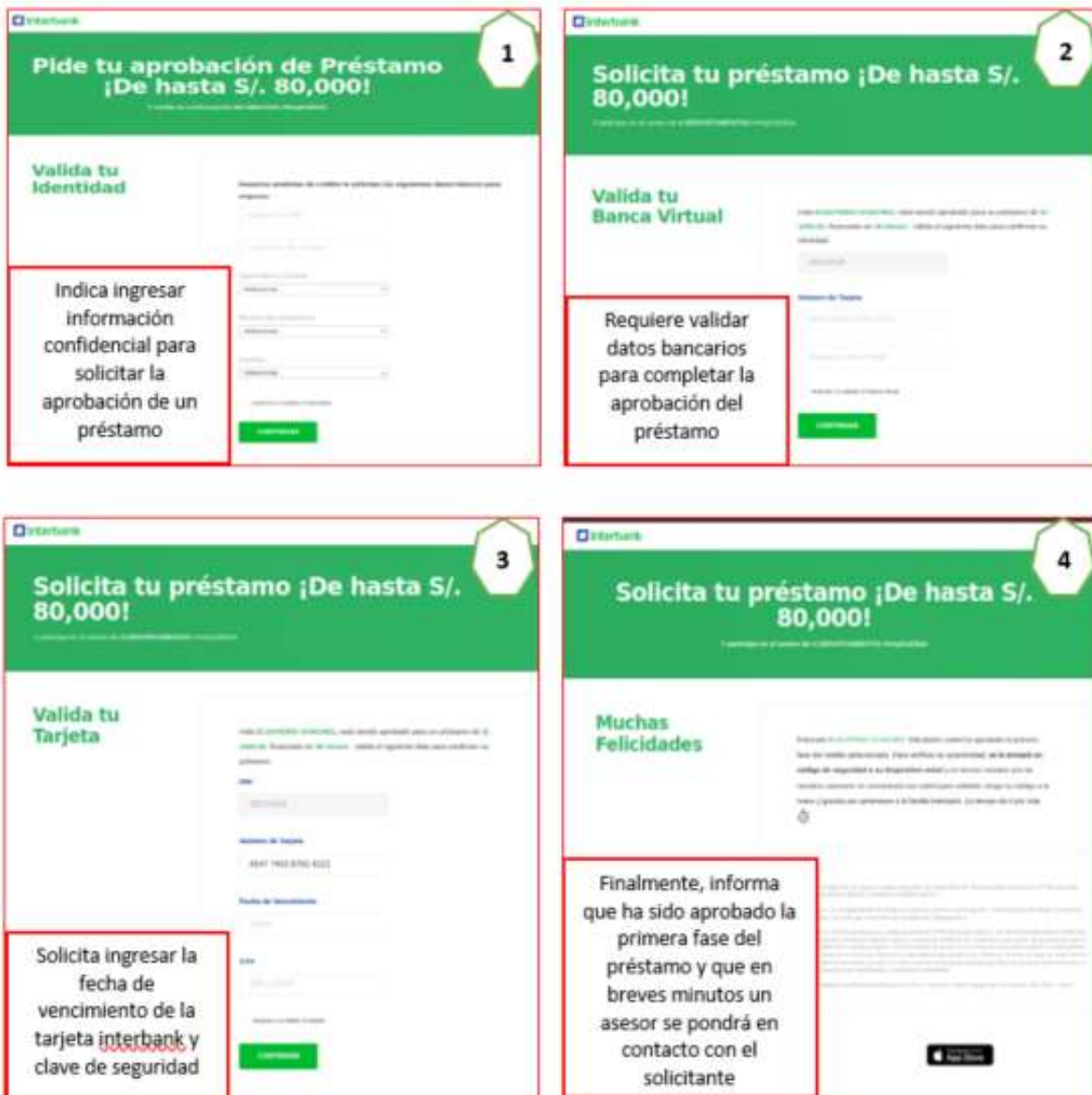


	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 286</b>		<b>Fecha: 21-10-2022</b>
			<b>Página 09 de 11</b>
Componente que reporta	<b>DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ</b>		
Nombre de la alerta	Phishing, suplantando la identidad de la entidad Bancaria Interbank		
Tipo de ataque	Phishing	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.

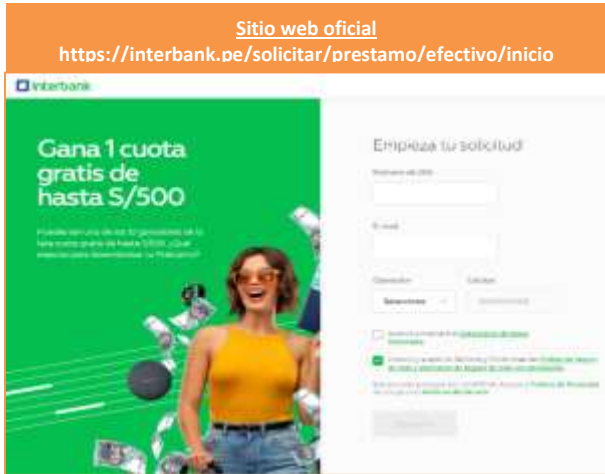
2. **Imagen:** Detalle del proceso del Phishing:



The image displays four sequential screenshots of a phishing website designed to look like the Interbank mobile app. Each screenshot is numbered in a green circle in the top right corner and includes a red-bordered text box with a description of the step:

- Screenshot 1:** Titled "Pide tu aprobación de Préstamo ¡De hasta S/. 80,000!". The form asks to "Valida tu Identidad" (Validate your identity). A red box notes: "Indica ingresar información confidencial para solicitar la aprobación de un préstamo" (Indicates entering confidential information to request loan approval).
- Screenshot 2:** Titled "Solicita tu préstamo ¡De hasta S/. 80,000!". The form asks to "Valida tu Banca Virtual" (Validate your virtual banking). A red box notes: "Requiere validar datos bancarios para completar la aprobación del préstamo" (Requires validating banking data to complete loan approval).
- Screenshot 3:** Titled "Solicita tu préstamo ¡De hasta S/. 80,000!". The form asks to "Valida tu Tarjeta" (Validate your card). A red box notes: "Solicita ingresar la fecha de vencimiento de la tarjeta interbank y clave de seguridad" (Requests entering the Interbank card expiration date and security key).
- Screenshot 4:** Titled "Solicita tu préstamo ¡De hasta S/. 80,000!". The screen shows "Muchas Felicidades" (Congratulations) and a message stating the loan has been approved. A red box notes: "Finalmente, informa que ha sido aprobado la primera fase del préstamo y que en breves minutos un asesor se pondrá en contacto con el solicitante" (Finally, informs that the first phase of the loan has been approved and that an advisor will contact the applicant in a few minutes).

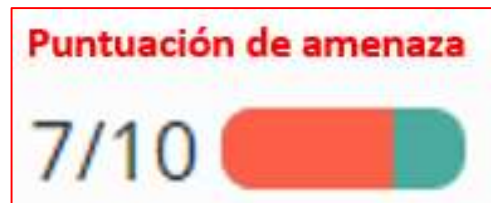
### 3. Comparación del sitio web oficial y fraudulento.



- 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: [https://reactivate-primaveraoctubre\[.\]site](https://reactivate-primaveraoctubre[.]site)
  - Dominio: [reactivate-primaveraoctubre\[.\]site](https://reactivate-primaveraoctubre[.]site)
  - IP: 104.21.67.220
  - Tamaño:
  - 871.65 KB
  - SHA-256: a00198c4f9dd09d858c09b0a9440c1119aa4e17f41e006da57843ff017b888cb



DETECCIÓN	DETALLES	ENLACES	COMUNIDAD
<b>Análisis De Proveedores De Seguridad</b>			
alpha4ourtsis ai	Suplantación de identidad	Anti-AVL	Malicioso
Avya	Suplantación de identidad	Vireducto de Cómodo Valleyne	Suplantación de identidad
CRDF	Malicioso	CyRadar	Malicioso
Ensssoft	Suplantación de identidad	ESET	Suplantación de identidad
Buscador de amenazas de Forcepoint	Suplantación de identidad	Fortinet	Suplantación de identidad
G-datos	Suplantación de identidad	kaspersky	Suplantación de identidad
Leontco	Suplantación de identidad	netcraft	Malicioso
tanque de phishing	Suplantación de identidad	Sophos	Suplantación de identidad
raíz web	Malicioso	Abusix	Limpio

### 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