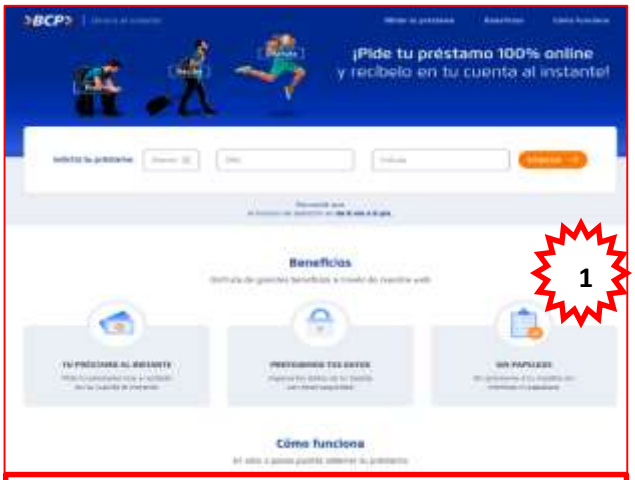
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 282	Fecha: 17-10-2022
		Página 11 de 13

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing suplantando la identidad del Banco de Crédito del Perú - BCP		
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 de Crédito del Perú (BCP); el cual, mediante la creación de un sitio web similar al original, solicitan a las posibles víctimas a realizar una solicitud de préstamo online, ingresando datos personas y bancarios como N° de tarjeta bancaria, clave web, fecha de vencimiento, clave de seguridad, número de contacto, entre otros.

2. Proceso del ataque phishing:



Requiere realizar una solicitud de préstamo online al instante ingresando datos personales

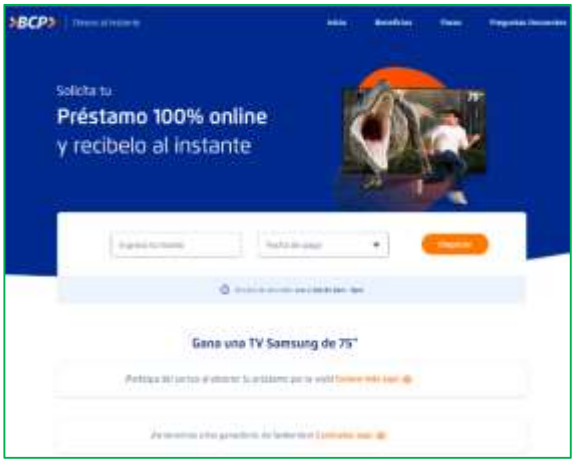
Para continuar con la solicitud pide ingresar la contraseña web

Luego, pide validar datos bancarios del solicitante

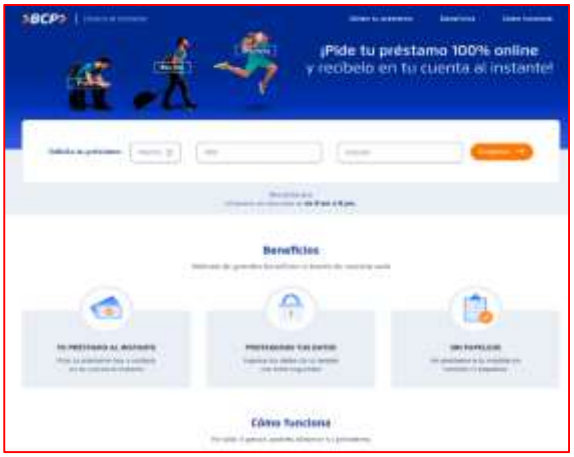
Por último, redirige al sitio web oficial del Banco de Crédito del Perú

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

sitio web oficial
https://www.dineroalinstante.viabcp.com



sitio web fraudulento
hxxps://reactivabeneficioprimavera[.]top



- 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, obteniendo la siguiente información:

- **URL:** hxxps://reactivabeneficioprimavera[.]top
- **Dominio:** reactivabeneficioprimavera[.]top
- **Direcciones IP:** 104[.]21[.]62[.]151
- **Tamaño:** 194B
- **SHA-256:** afca372f9959cb6c46bde573d25172c1b223dac52cba20ffad3c8fc2ea09cc8e

Antiy-AVL	Malicious	Avira	Phishing
BitDefender	Phishing	Certego	Phishing
Comodo Valkyrie Verdict	Phishing	Emsisoft	Phishing
ESET	Phishing	Forcepoint ThreatSeeker	Phishing
Fortinet	Phishing	G-Data	Phishing
Kaspersky	Phishing	Lionic	Phishing
Netcraft	Malicious	Phishing Database	Phishing
Phishtank	Phishing	Sophos	Phishing
Viettel Threat Intelligence	Phishing	Webroot	Malicious

5. Recomendaciones:

- No abrir correos ni mensajes de dudosa procedencia
- Desconfiar de los enlaces y archivos enviados a través de mensajes o correos electrónicos
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Prestar atención en los detalles de los mensajes o redes sociales
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

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