PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc

Lima, 17 de setiembre de 2022

N° 254-2022-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 254	Fecha: 17-09-2022
		Página 04 de 06

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

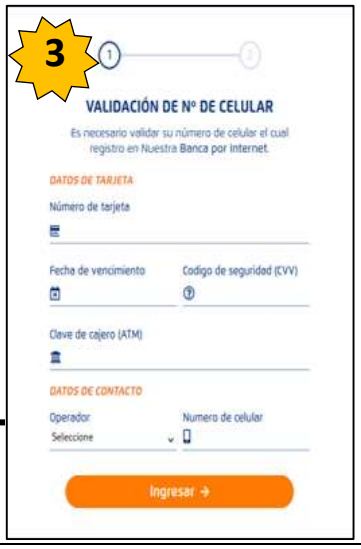
1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes se vienen llevando a cabo una campaña de Phishing, a través de los diferentes navegadores web, dirigido a los clientes y/o usuarios de la entidad bancaria Banco de Crédito del Perú (BCP); el cual, mediante la creación de un sitio web similar al original, solicitan a las posibles víctimas a realizar una supuesta solicitud de validación de datos para adquirir el apoyo económico denominado “Bono Wanuchay ”; otorgado por el gobierno a los productores de la agricultura familiar con menos de dos (02) hectáreas de terreno.

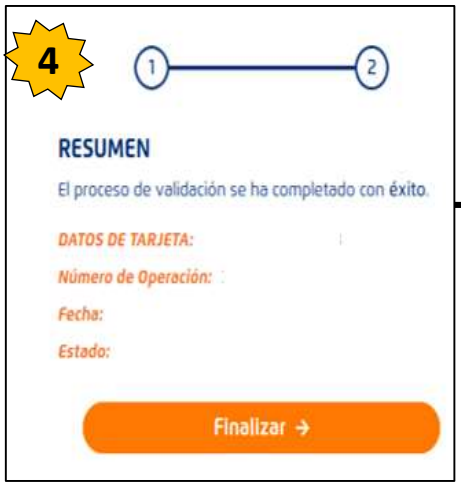
2. **Detalles del proceso de Phishing.**

Solicita realizar una solicitud para adquirir el bono Wanuchay, ingresando datos bancarios como número de tarjeta y clave web.

Requiere validar número de celular registrado en la banca por internet del BCP

Pide ingresar el número de DNI del titular de cuenta bancaria.





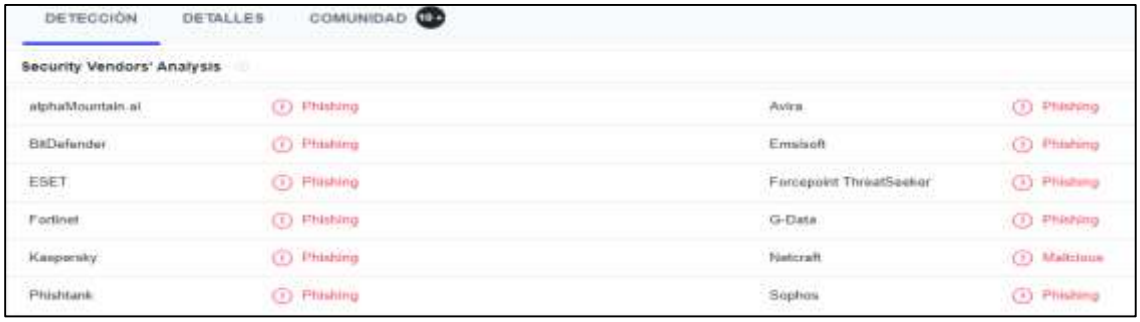
Por último, informa que el proceso de validación se ha completado con éxito, agregando detalles de la operación realizada como N° tarjeta, N° de operación, fecha y estado.

- Existe una similitud entre el fondo y forma de cada sitio web.
- 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.

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

- **INDICADORES DE COMPROMISO:**

  - ✓ **URL:** hxxps://vialbcp-pe[.]com
  - ✓ **Dominio:** vialbcp-pe[.]com
  - ✓ **IP:** 50.87.145.190
  - ✓ **Tamaño:** 80.84 KB
  - ✓ **SHA**-256: 4112434f5be36cd42c190fcf8014be241047f09858bffa1d4615f5a60f51f2d6



4. **Algunas Recomendaciones:**

- Verificar la información en la entidad correspondiente
- Ingresar desde fuente oficiales.
- Corroborar la información en la entidad correspondiente.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.

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

Índice alfabético