	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 132	**Fecha: 06-06-2023**
		Página 23 de 25

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de Phishing que suplanta 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 ataques avanzados de Phishing, dirigidos a usuarios de la entidad del Banco de Crédito del Perú (BCP), con el objetivo robar credenciales de acceso, datos personales y bancarios.

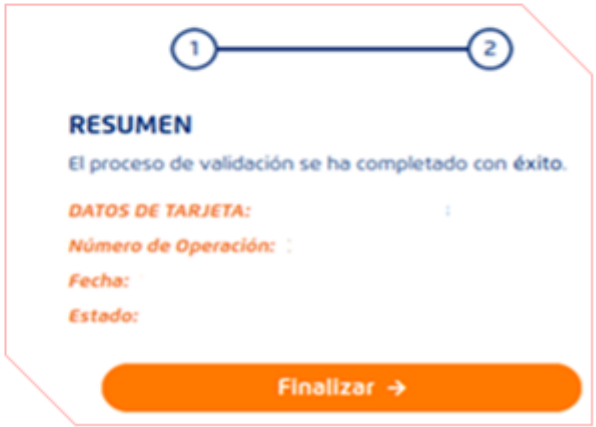
2. Detalles del proceso de estafa.

Imagen 1: Solicitud de ingreso de las credenciales de acceso (DNI, N.º de tarjeta y clave de internet de 6 dígitos)

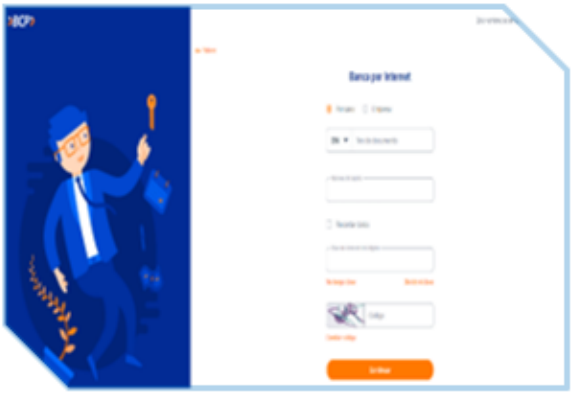
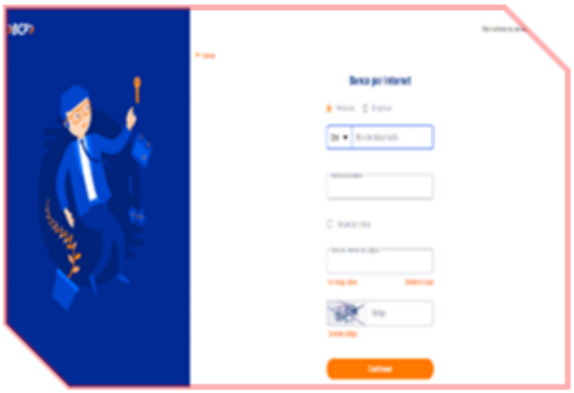
Imagen 2: Luego de ingresar las credenciales de acceso, requiere ingresar el DNI.

Imagen 3: Seguido solicita validar el número de celular y datos bancarios en la Banca por Internet.

Imagen 4: Por último, indica que la validación de datos ha sido exitosa.



3. Comparación del sitio web oficial y sitio web falso del BCP:

SITIO WEB OFICIAL https://loginunico.viabcp.com/#/tarjeta-sesion	SITIO WEB FRAUDULENTO hXXps[:]//vvvvwebzonasengunra[.]com/view?cgi=Liy40Ni9kLRV9iQOV2o2
	

- Existe una similitud entre el fondo y forma de cada sitio web.
- La diferencia está en el dominio, debido a que el sitio web fraudulento no coincide con el sitio oficial del BCP.
- Ambos sitios webs, poseen el ***PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS),*** lo que hace más convincente a que las víctimas accedan a dicho sitio web.

4. Proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD – PHISHING:

DETECCIÓN | DETALLES | COMUNIDAD

Análisis de proveedores de seguridad ⓘ — ¿Quieres automatizar los cheques?

Avira	Suplantación de identidad	BitDefender	Suplantación de identidad
CyRadar	Malicioso	Buscador de amenazas de Forcepoint	Suplantación de identidad
Fortinet	Suplantación de identidad	G-datos	Suplantación de identidad
Leonico	Suplantación de identidad	Búsqueda segura	Malicioso
Sophos	Suplantación de identidad	raíz web	Malicioso

5. Indicadores de compromiso (IoC)
   - URL : hXXps[:]//vvvvwebzonasengunra[.]com/view?cgi=Liy40Ni9kLRV9iQOV2o2
   - Dominio : vvvvwebzonasengunra[.]com
   - SHA-256 : 80c3fe2ae1062abf56456f52518bd670f9ec3917b7f85e152b347ac6b6faf880
   - IP : 198[.]54[.]115[.]232

6. 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.

7. Algunas recomendaciones:
   - Verificar detalladamente la URL, que corresponda al sitio web oficial.
   - Las entidades bancarias no solicitan actualización de datos confidenciales de manera online.
   - Ingresar desde fuentes oficiales.
   - No seguir las instrucciones de sitio web sospechoso.
   - Mantener el antivirus actualizado.
   - Evitar compartir la URL con amigos y/o familiares.

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