	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°001	Fecha: 31-12-2023
		Página: 7 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Detección de una nueva 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 Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. **ANTECEDENTES:**

A través del monitoreo y la búsqueda de amenazas en el ciberespacio, se ha detectado que los ciberdelincuentes están llevando a cabo una nueva campaña de Phishing. En esta, suplantan la identidad del Banco de Crédito del Perú (BCP) con el objetivo de robar credenciales de acceso, así como datos personales y bancarios."

2. **DETALLES:**

Imagen 1: Se solicita el ingreso de las credenciales de acceso, que incluyen el DNI, el número de tarjeta y una clave de internet de 6 dígitos.

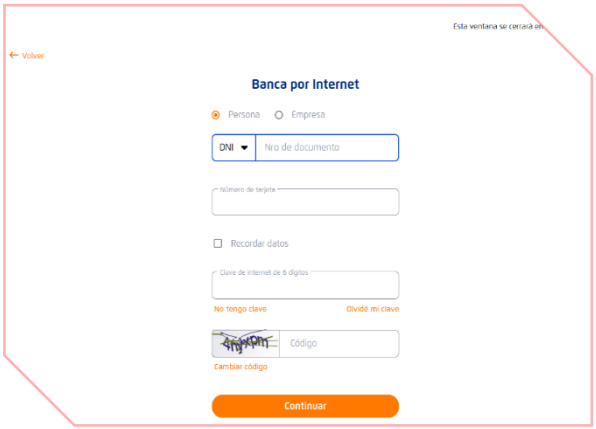


Imagen 2: Después de ingresar las credenciales de acceso, se requiere confirmar el número de DNI.

Imagen 3: Posteriormente, se pide validar el número de celular junto con los datos bancarios asociados a la tarjeta de crédito o débito.

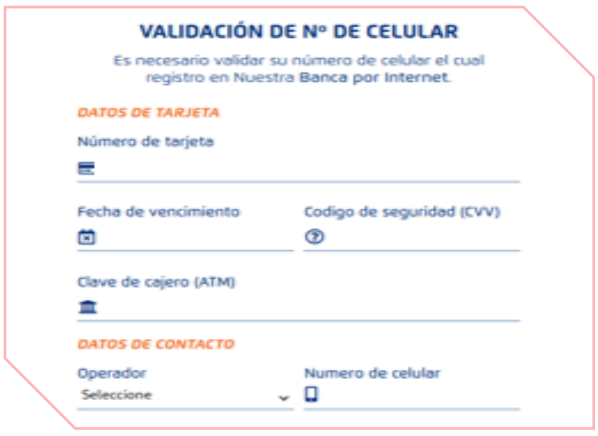
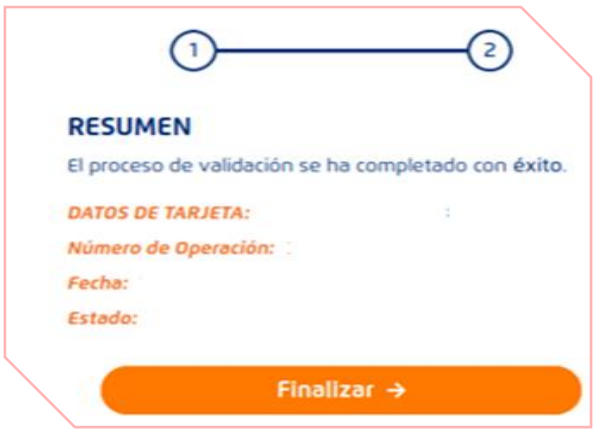
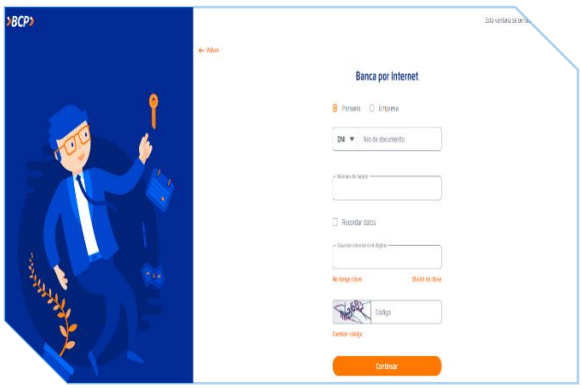


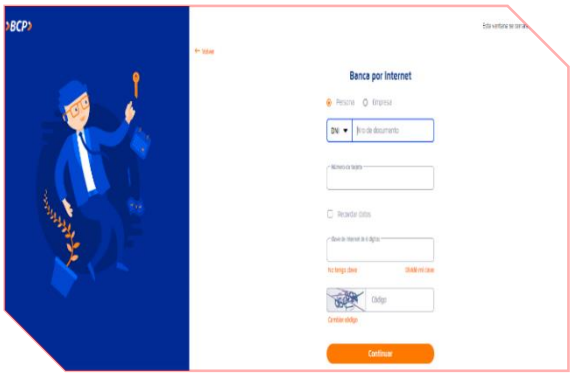
Imagen 4: Finalmente, se indica que la validación de los datos ha tenido éxito.



A. Se realiza una comparación entre el sitio web oficial y el sitio web falso del BCP:

SITIO WEB OFICIAL	SITIO WEB FRAUDULENTO
hxxps://loginunico.viabcp.com/#/tarjeta-sesion	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 web oficial del BCP.
- Ambos sitios webs, poseen el **PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS),** lo que hace más convincente a las víctimas al momento de acceder a dicho sitio web fraudulento del BCP.

B. Los proveedores de seguridad informática emiten alertas sobre la suplantación de identidad, conocida como phishing.

Avira	Suplantación de identidad	BitDefender	Suplantación de identidad
CyRadar	Malicioso	Buscador de amenazas Forcepoint	Suplantación de identidad
Fortinet	Suplantación de identidad	Datos G	Suplantación de identidad
leonico	Suplantación de identidad	búsqueda en seco	Malicioso
Sofos	Suplantación de identidad	raíz web	Malicioso

C. Indicadores de compromiso (IoC)

- URL : hXXps[:]//vvvvwebzonasengunra[.]com/view?cgi=Liy40Ni9kLRV9iQOV2o2
- Dominio : vvvvwebzonasengunra[.]com
- SHA-256 : 80c3fe2ae1062abf56456f52518bd670f9ec3917b7f85e152b347ac6b6faf880
- IP : 198[.]54[.]115[.]232

D. Referencia:

El phishing o suplantación de identidad es un método que los ciberdelincuentes emplean para engañar a los usuarios y lograr que revelen información personal, como contraseñas, datos de tarjetas de crédito, números de cuentas bancarias, entre otros.

3. RECOMENDACIONES:

- Verificar detalladamente la URL, que corresponda al sitio web oficial.
- Tener en cuenta que las entidades bancarias no solicitan actualización de datos confidenciales de manera online.
- Ingresar los datos confidénciales desde fuentes oficiales.
- No seguir las instrucciones de sitio web sospechoso o de dudosa reputación.
- Mantener el antivirus actualizado ya que funciona como primera barrera ante ataques cibernéticos.
- Evitar compartir la URL con amigos y/o familiares.

Fuente de Información:	Análisis propio de redes sociales y fuente abierta.