| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°293 | Fecha: 9-12-2023 |
|---|---|---|
| | | Página: 5 de 9 |

| | | | |
|---|---|---|---|
| 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 Sub familia | G01 |
| Clasificación temática familia | Fraude | | |

Descripción

1. **ANTECEDENTES:**

Se identificó, a través de la vigilancia y seguimiento de amenazas en línea, una nueva campaña de Phishing realizada por ciberdelincuentes. Esta campaña suplanta la identidad del Banco de Crédito del Perú (BCP) con el fin de obtener credenciales de acceso, así como información personal y bancaria de los usuarios.

2. **DETALLES:**

Detalles del proceso de estafa.

**Imagen 1:** Se solicita introducir las credenciales de acceso, que comprenden el número de DNI, el número de tarjeta y una clave de internet de seis dígitos.

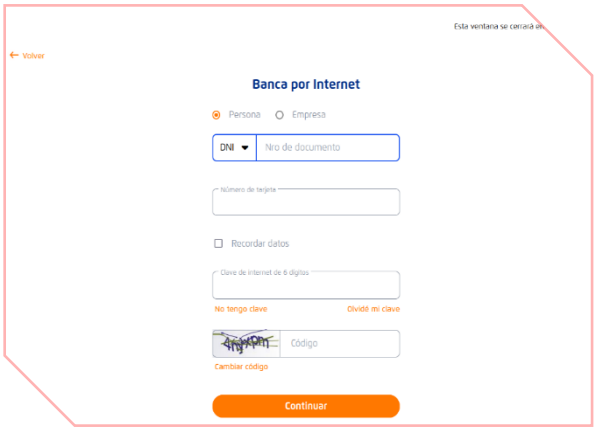



**Imagen 2:** Después de haber ingresado las credenciales de acceso, se necesita verificar el número de DNI para continuar.


**Imagen 3:** A continuación, se pide confirmar el número de teléfono celular y los datos bancarios de la tarjeta de crédito o débito.

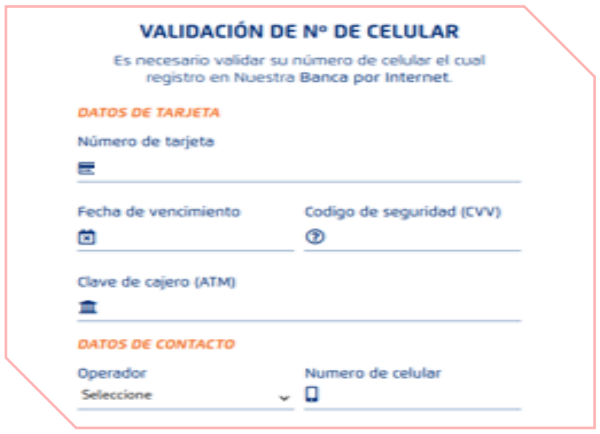
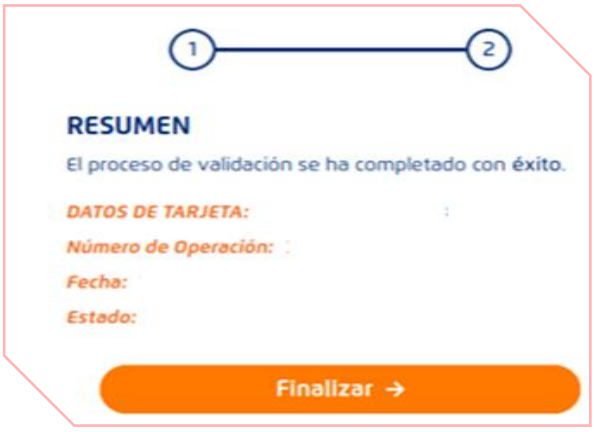
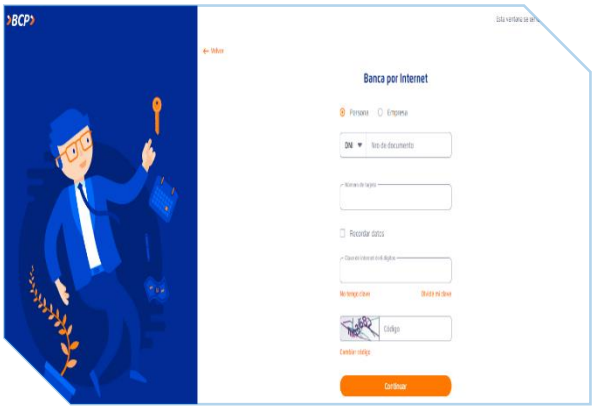


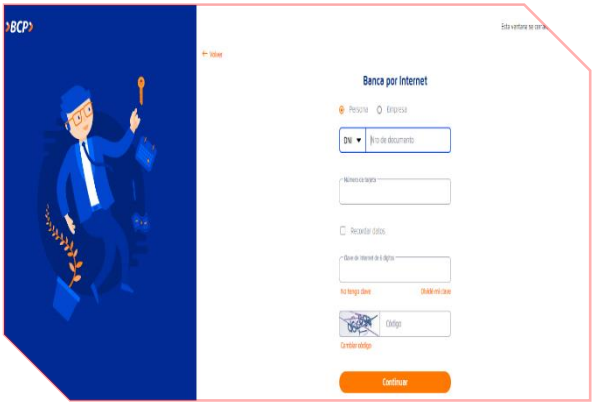

**Imagen 4:** Finalmente, se señala que la validación de los datos ha sido exitosa.



**A.** Comparación entre el sitio web oficial del BCP y el sitio web falso para identificar diferencias y similitudes:

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




- Los dos sitios web tienen una apariencia y estructura similar.
- La diferencia principal radica en el dominio, ya que el sitio fraudulento no concuerda con la dirección oficial del BCP.
- Ambos sitios cuentan con el protocolo seguro de transferencia de hipertexto (HTTPS), lo que puede convencer aún más a las víctimas al acceder al sitio falso del BCP.

**B.** Los proveedores de seguridad informática emiten una alerta sobre el riesgo de suplantación de identidad mediante técnicas de 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:

- Phishing, conocido como suplantación de identidad, es una táctica empleada por ciberdelincuentes para engañar a los usuarios y obtener información personal como contraseñas, datos de tarjetas de crédito o números de cuentas bancarias, entre otros.

**3. RECOMENDACIONES:**

- Verificar minuciosamente la URL para asegurarse de que corresponda al sitio web oficial.
- Tener en cuenta que las instituciones bancarias no solicitan la actualización de datos confidenciales en línea.
- Ingresar datos confidenciales solo desde fuentes oficiales.
- Evitar seguir instrucciones de sitios web sospechosos o de reputación dudosa.
- Mantener el antivirus actualizado sirve como primera línea de defensa contra ataques cibernéticos.
- Abstenerse de compartir la URL con amigos o familiares para evitar riesgos.

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