



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
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 01 de Mayo de 2022

ALERTA INTEGRADA DE SEGURIDAD DIGITAL



N° 119-2022-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.

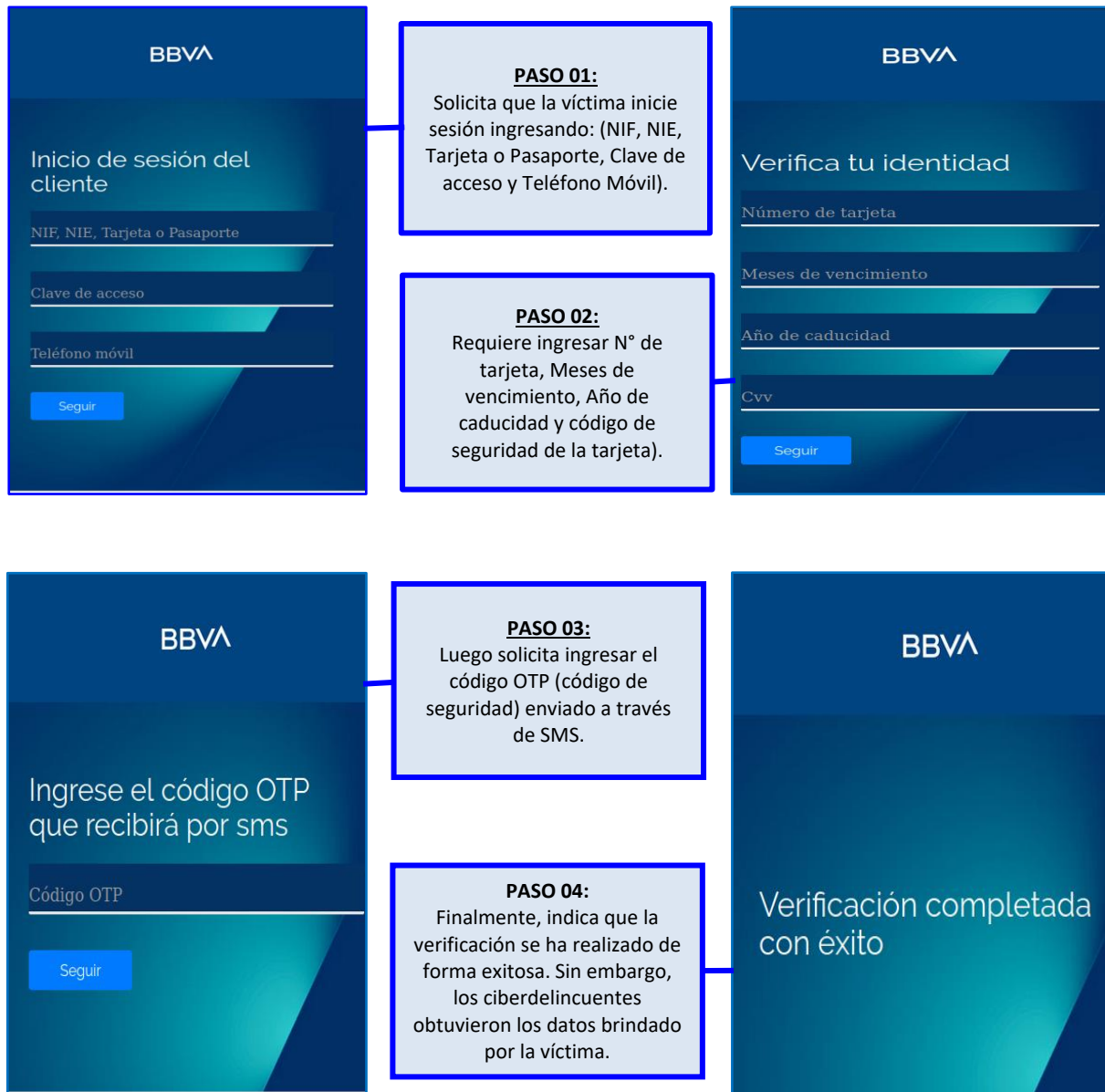
Contenido

| | |
|--|---|
| Phishing, suplantando la identidad del Banco BBVA..... | 3 |
| Índice alfabético | 5 |

| | | | |
|---|--|----------------------|--------------------------|
|  | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 119 | | Fecha: 01-05-2022 |
| | | | Página 3 de 5 |
| Componente que reporta | DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ | | |
| Nombre de la alerta | Phishing, suplantando la identidad del Banco BBVA. | | |
| 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, a través de los diferentes navegadores web, quienes suplantando la identidad del Banco **BBVA**, indicando que la entidad bancaria necesita realizar una “**verificación de datos**” del titular de la cuenta, el cual tiene como finalidad robar información confidencial y bancaria de las posibles víctimas como número de tarjeta, clave de internet, número de celular, fecha de vencimiento, código de seguridad, entre otros.
2. Imagen: Detalles del proceso de estafa del Phishing.



3. La comparación del sitio web oficial y sitio web fraudulento:

SITIO OFICIAL

https://www[.]bbva[.]es/personas/banca-online/notificaciones.

Dominio

SITIO FRAUDULENTO

https://www[.]notificacion-bbvaa[.]be/

- ❖ Existen diferencias entre el fondo y forma de cada sitio web, lo que hace convincente a que las víctimas accedan al sitio web.
- ❖ Ambas URL's utilizan los protocolos de red HTTPS.
- ❖ La diferencia está en la URL, debido a que el dominio del sitio web fraudulento no corresponde con el oficial.

4. URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información:

- **URL Malicioso** : hxxps[:]//www[.]notificacion-bbvaa[.]be/
- **Dominio** : www[.]notificacion-bbvaa[.]be
- **IP.** : 212.109.222.125
- **Tamaño** : 7.46 KB
- **SHA-256** : 851f87276cbbc251242f21ee8276586d4be665076bda0ff6af58fb00e6cd8417

| DETECTION | DETAILS | COMMUNITY |
|----------------------------|-----------|-------------------------|
| Security Vendors' Analysis | | |
| ADMINUSLabs | Malicious | AlienVault |
| alphaMountain.ai | Phishing | Avira |
| BitDefender | Phishing | CyRadars |
| ESET | Phishing | Forcepoint ThreatSeeker |
| Fortinet | Phishing | G-Data |
| Google Safebrowsing | Phishing | Lionic |
| Phishing Database | Phishing | Sophos |
| Webroot | Malicious | Abusix |
| | | Clean |

Otras detecciones:

https://www.notificacion-bbvaa.be

Etiquetas: Phishing y otros fraudes

Puntuación multiescaneo: **02** / 17 MOTORES

Amenazas detectadas:

- Alto Riesgo (Webroot.Com)
- Suplantación De Identidad (Avira.Com)

5. Algunas Recomendaciones:

- Verificar la fuente de la información recibida.
- Sospechar si hay errores gramaticales en el texto de correos recibidos.
- Revisar que el texto del enlace coincida con la dirección web de la entidad al ingresar.
- Revisar periódicamente el estado de cuentas bancarias.
- Verificar la información en la entidad correspondiente.
- Mantener instalado un software antivirus.

Fuentes de información

- Análisis propio de redes sociales y fuente abierta

Índice alfabético

| | |
|-------------------------|---|
| amenazas | 3 |
| antivirus | 4 |
| celular | 3 |
| ciberdelincuentes | 3 |
| ciberespacio..... | 3 |
| Dominio | 4 |
| Phishing | 3 |
| plataformas | 4 |
| robar información..... | 3 |
| seguridad digital | 4 |
| SHA-256 | 4 |
| web | 4 |