	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 013	**Fecha: 14-01-2023**
		Página 10 de 13

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Ataque mediante phishing dirigido al 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 financiero		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que los ciberdelincuentes vienen realizando una campaña de envío masivo de correos electrónicos falsos, supuestamente del Banco BBVA, advirtiendo que ***"Su cuenta ha sido suspendida temporalmente",*** adjuntando un enlace detrás del botón ***"Acceder a mi"*** que, al ser pulsado, redirige a la víctima, a un sitio web falso que simula ser el oficial, con el objetivo de robar las credenciales de acceso, información personal y/o financiera.

   - Proceso del ciberataque:

Figura 1. Correo inicial que llega a la víctima.

Figura 2. Solicitud para ingresar las credenciales de acceso (DNI, usuario y clave web).

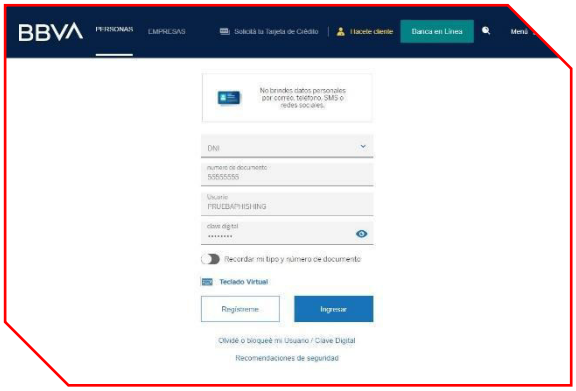


Figura 3. Seguidamente, debe ingresar el código de verificación enviado por SMS.

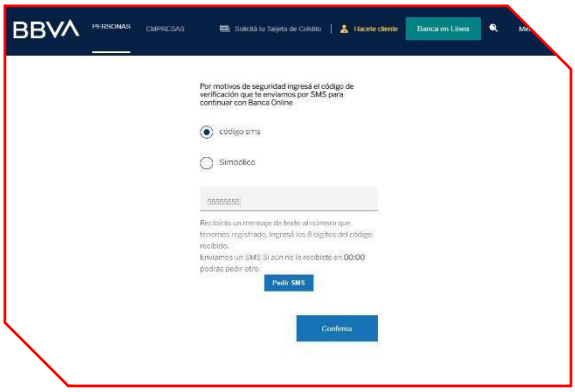
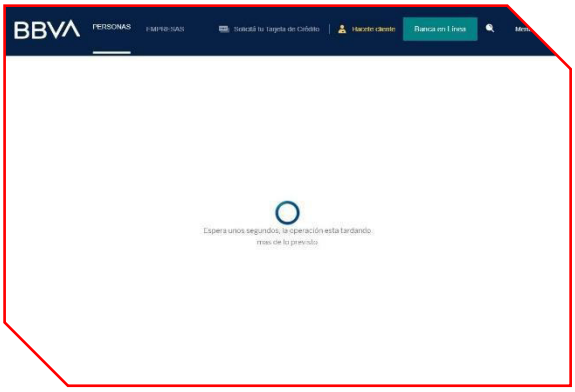


Figura 4. Al final, parece validar los datos, pero en realidad la información fue robada por los ciberdelincuentes.



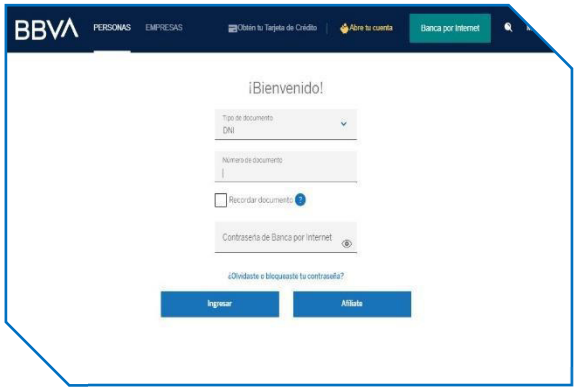
- Comparación de los sitios web legítimo y falso del Banco BBVA:

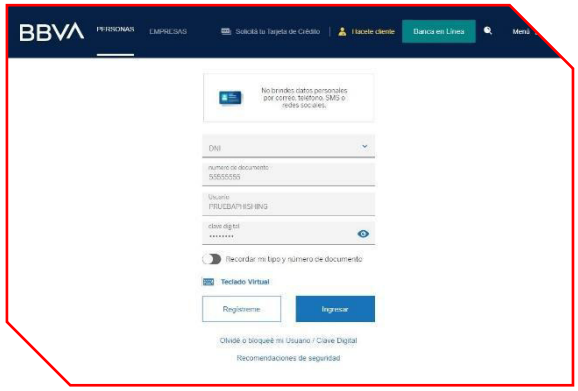
SITIO OFICIAL

URL: https://www.bbva.pe/

SITIO FRAUDULENTO

URL: hXXp[:]//c1631155[.]ferozo[.]com/#/Loader[.]aspx

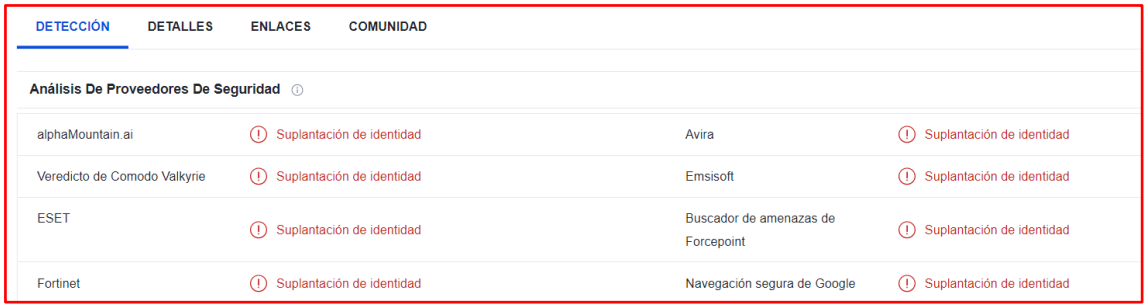




- Existe similitud en imagen, logotipo, fondo, color y escritura.
- No tiene certificado de seguridad de protocolo HTTPS.
- El dominio se hace pasar por el sitio oficial, pero no coinciden.

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

- Indicadores de compromisos:
  - **URL:** hXXp[:]//c1631155[.]ferozo[.]com/#/Loader[.]aspx
  - **Dominio:** c1631155[.]ferozo[.]com
  - **Dirección IP:** 200[.]58[.]110[.]176
  - **Código:** 200
  - **Longitud:** 1.10 KB
  - **SHA-256**: a4fd7c904aac1629098e274680ef0554e1057a29bf1f5c98aaea0410915fb32f



- Phishing:
  - Es un tipo de ataque de ingeniería social, que consiste en la utilización de envió masivo de email, los cuales se disfrazan para que parezcan proceder de una fuente de confianza. Estos emails están diseñados para engañar a las víctimas y conseguir que proporcionen información personal o financiera.

- Características de un phishing:
  - Contiene errores ortográficos
  - No se respeta el formato (justificado)
  - Algunos emails son de alerta o urgencia
  - Tienen adjunto documento o URLs

3. Recomendaciones:

- Evitar ingresar los datos de autenticación en las URL que recibas por correo electrónico.
- Escribir directamente la URL de la entidad en el navegador.
- Sospechar de todos aquellos mensajes alarmantes que tengan tono de urgencia y contengan faltas de ortografía o erratas.
- No divulgar la información a amigos, familiares o terceros.
- Utilice un programa antivirus actualizado, ya que es la primera línea de defensa contra un ciberataque.

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