	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 085		Fecha: 11-04-2023
			Página 36 de 43
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Nueva campaña de Phishing que suplanta la entidad bancaria de 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 avanzados ataques cibernéticos, por medio de envíos de correos electrónicos fraudulentos, o también conocidos como Phishing, simulando ser la entidad bancaria BBVA, en el cual tiene el objetivo de robar credenciales de acceso, datos personales y/o bancarios.

2. Detalles del proceso de Phishing:

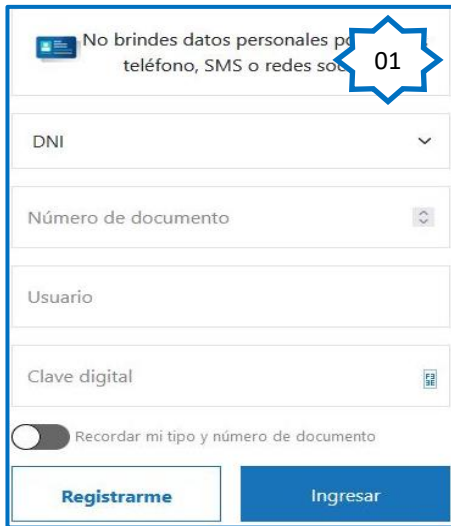


Imagen 1.
Sitio web fraudulenta del Banco BBVA, solicita a la víctima el documento de identidad (DNI), el usuario y clave digital para ingresar.



Imagen 2.
Al ingresar al sitio web fraudulenta, aparece un mensaje, donde la víctima tiene que esperar porque se está vinculando el dispositivo.



Imagen 3.
Luego de esperar, el atacante le solicita a la víctima la verificación de acceso, ya sea en SMS O TOKEN para continuar.




Imagen 4.
Después de completar lo requerido por los atacantes, dentro de unos segundos es redirigido al sitio web fraudulento del banco BBVA, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.

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



- Indicadores de compromiso:

- **URL:** hxtps://bbva-homeacceso[.]com/
- **Dominio:** bbva-homeacceso.com
- **SHA-256:** 9a50136a82e60c31374c9e33aa75b51a291d26b5c0a4f118063b801ff11da9c0
- **IP:** 172[.]67[.]135[.]191
- **SERVIDOR:** Cloudflare
- **TIPO:** texto/html
- **Otros resultados del analisis:**



4. Que es un Phishing:

- Es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

5. Algunas recomendaciones:

- Verificar detalladamente la URL, que corresponda al sitio web oficial del banco BBVA.
- Ingresar desde fuentes oficiales.
- Evitar seguir las instrucciones de sitio web sospechoso o de dudosa procedencia.
- Mantener el antivirus actualizado, ya que es la primera barrera ante posibles ataques cibernéticos.
- Evitar compartir la URL con amigos y/o familiares.

Fuentes de información

- Análisis propio de redes sociales y fuente abierta