	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°305	Fecha: 25-12-2023
		Página: 5 de 12

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de Smishing o mensaje de texto (SMS) que suplanta la entidad bancaria del 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 Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. **ANTECEDENTES:**

Se identificó, a través de la vigilancia y seguimiento de amenazas en el ciberespacio, una nueva campaña de Smishing o mensajes de texto falso (SMS), realizada por ciberdelincuentes. Esta campaña suplanta la identidad del banco BBVA, con el fin de obtener credenciales de acceso, así como información personal y bancaria de los usuarios.

2. **DETALLES:**

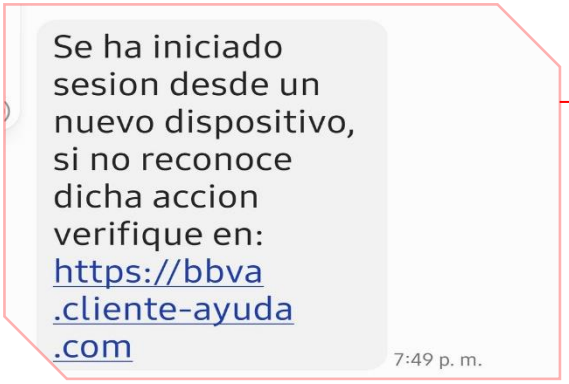


Imagen 1: Mensaje de texto falso (SMS) enviado supuestamente por la entidad bancaria del BBVA, incita a la víctima hacer clic en el enlace adjunto.

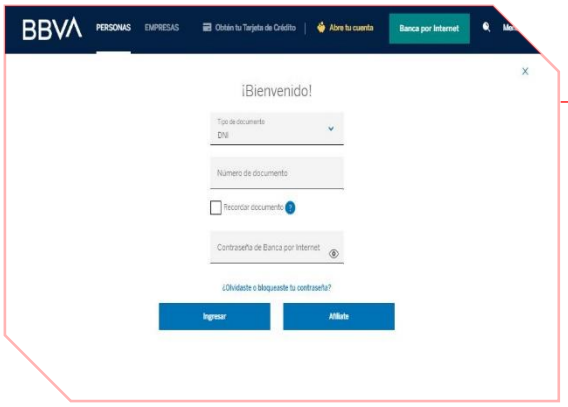
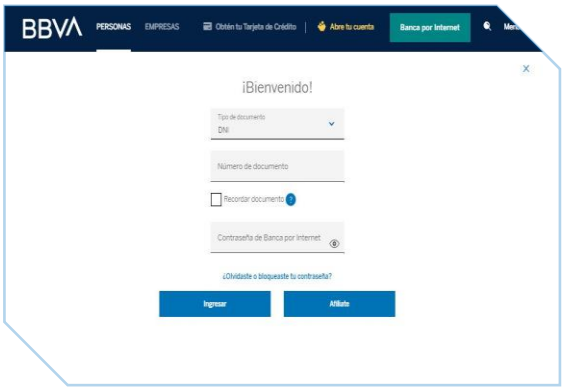


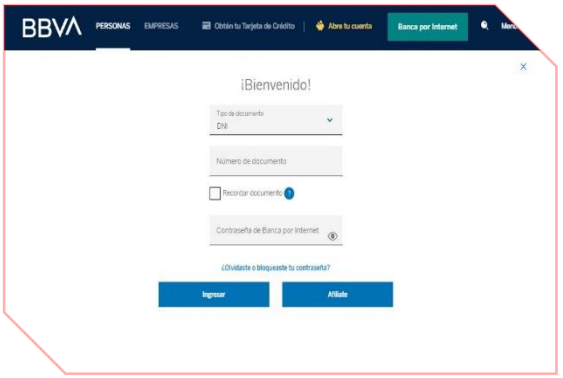
Imagen 2: Después de haber hecho clic, en el enlace, es redirigido al sitio web falso del BBVA, solicitando ingresar las credenciales de acceso tales como el número de DNI y contraseña.

Imagen 3: Una vez ingresada las credenciales de acceso, es redirigido al sitio web oficial del BBVA, aludiendo un aparente error de autenticación; sin embargo, los datos ingresados fueron capturados, por los ciberdelincuentes.

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

SITIO WEB OFICIAL	SITIO WEB FRAUDULENTO
hxxps://www.bbva.pe/	hxxps[:]//bbva[.]cliente-ayuda[.]com/





- 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 BBVA.
- 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 BBVA.

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

Análisis de proveedores de seguridad			
Avira	Suplantación de identidad	BitDefender	Suplantación de identidad
Clúster25	Suplantación de identidad	Emsisoft	Suplantación de identidad
Fortinet	Suplantación de identidad	Datos G	Suplantación de identidad
Kaspersky	Suplantación de identidad	leonico	Malicioso
Netcraft	Malicioso	Sofos	Suplantación de identidad
raiz web	Malicioso	AlfaSOC	Sospechoso

C. Indicadores de compromiso (IoC)

- URL : hxxps[:]//bbva[.]cliente-ayuda[.]com/
- Dominio : bbva[.]cliente-ayuda[.]com
- IP : 172[.]67[.]208[.]96

D. Referencia:

- El smishing es una técnica que consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima red social, banco, institución pública, etc. con el objetivo de robarle información privada o realizarle un cargo económico. Generalmente el mensaje invita a llamar a un número de tarificación especial o acceder a un enlace de una web falsa bajo un pretexto.

3. RECOMENDACIONES:

- Verificar minuciosamente la URL para asegurarse de que corresponda al sitio web oficial.
- Las instituciones bancarias no solicitan la actualización de datos confidenciales en línea.
- Es fundamental 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.
- Es importante abstenerse de compartir la URL con amigos o familiares para evitar riesgos.

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

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°305	**Fecha: 25-12-2023**
		Página: 7 de 12

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 Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. **ANTECEDENTES:**

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, simulado ser la entidad bancaria BBVA, en cual tiene el objetivo de robar credenciales de acceso, datos personales y/o bancarios.

2. **DETALLES:**

Detalles del proceso de Phishing:

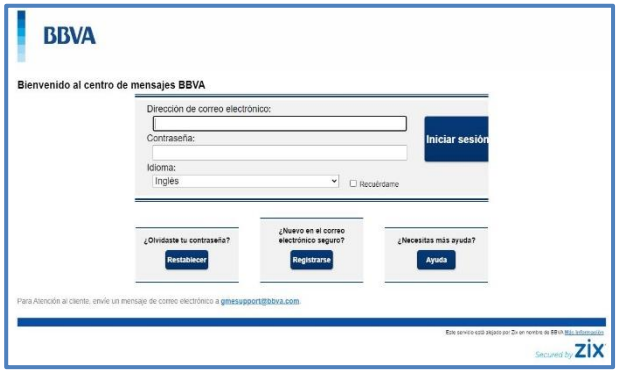
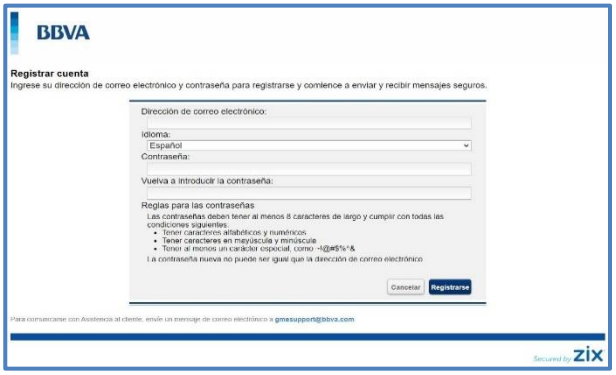


Imagen 1.
Sitio web fraudulenta del Banco BBVA, solicita a las víctimas registrar la dirección del correo electrónico, la contraseña y el idioma para iniciar sesión.

Imagen 2.
Luego de no poder iniciar sesión y darle click en "olvidaste la contraseña" requiere registrar la dirección del correo electrónico, el tipo de idioma y volver a introducir la contraseña para continuar.



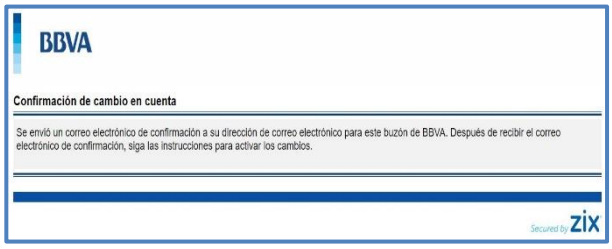


Imagen 2.
Por último, solicita a la víctima confirmar la cuenta, lo cual tendría que ingresar al correo electrónico y completar lo requerido por los atacantes, para luego informar a la víctima que ha ocurrido un error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.

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

Indicadores de compromiso:

- **URL**: hxxps://game-eu-message-portal[.]com/s/loginview[.]jsp?b=bbva
- **Dominio**: juego-eu-mensaje-portal.com
- **SHA-256**: 24e1f50965111719c1b55b04aaf8c094cd8940bdb5b04736d0968c8cc29bd4b5
- **IP**: 91[.]209[.]6[.]51
- **Server:** Apache

B. Otros resultados del análisis:

C. Apreciación de la información:

La presente campaña de Phishing permite a los actores de amenazas obtener las credenciales de acceso a la banca por internet de los usuarios del Banco BBVA.

La propagación del sitio web fraudulento se realiza mediante envió masivos de email, adjuntando enlaces de sitios web fraudulentos con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger, etc. y mensajes de textos SMS.

D. 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.

3. 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.

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