	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 066	Fecha: 07-03-2022
		Página 7 de 9

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**			
Nombre de la alerta	Campaña de 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, dirigido a clientes y/o usuarios del Banco BBVA, por medio de la creación de un sitio web fraudulento de la entidad bancaria, solicitan a las posibles víctimas ingresar las credenciales de inicio de sesión del sitio web, como nombre de usuario, DNI y clave web.

2. Proceso del ataque phishing:

Imagen 01: El sitio web falso del Banco BBVA, solicita a la víctima, ingresar sus credenciales de acceso (número de documento, usuario y clave digital).

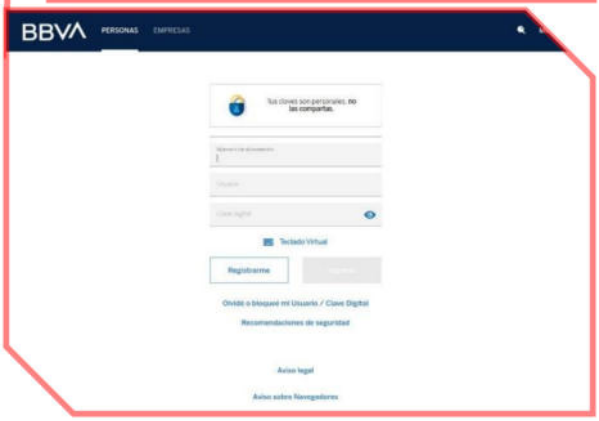


Imagen 02: Al hacer click en <Ingresar>, informan a través de una ventana emergente que debe: ***"Ingresar el código de seguridad que ha sido enviado por SMS".***

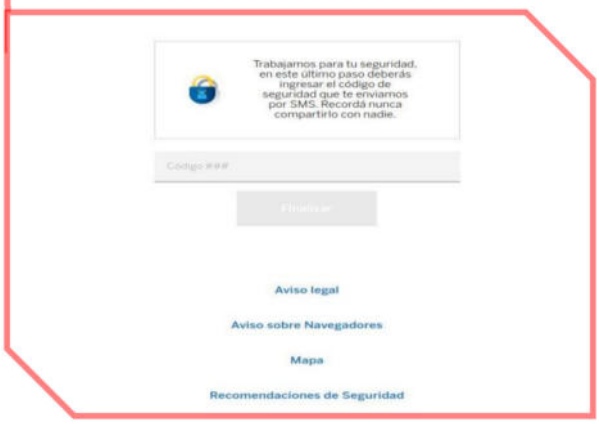
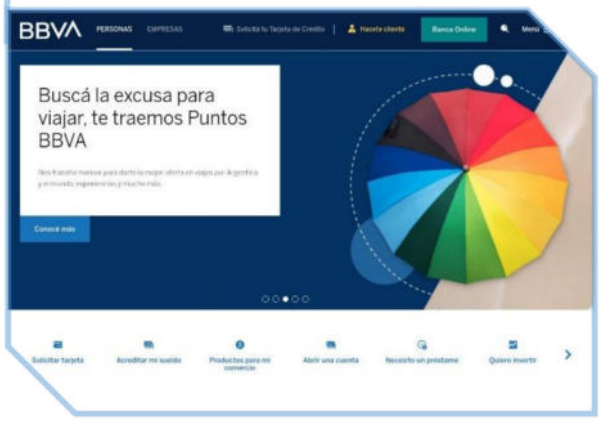


Imagen 03: Luego de 30 segundos, dan a conocer que el token ingresado a expirado, solicitando volver a escribir dicho código de seguridad.

Imagen 04: Finalmente redirige de forma automática al sitio web oficial del Banco BBVA, aludiendo un aparente error de autenticación; sin embargo, los datos ya fueron capturados por los ciberdelincuentes.



3. Comparación el sitio web oficial y sitio web fraudulento:

- Existen similitudes entre el fondo y forma de cada sitio web.
- Ambas URL´s utilizan el protocolo HTTPS, lo que hace más convincente a que las víctimas accedan al sitio web.
- La diferencia está en la URL, debido a que, el dominio del sitio web fraudulento no coincide con el oficial.

4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogada como Phishing (suplantación de identidad):

- Indicadores de compromiso:

  - URL: hxxp[:]//tecnología[.]ibbca[.]com[.]br
  - Dominio: tecnologia.ibbca.com.br
  - Dirección IP:142[.]4[.]31[.]235
  - Tamaño: 70.78 KB
  - SHA-256: e48b9988a3bab1af43a87e0574910950f0230036666bb225294a5332c7ff29af

DETECCIÓN | DETALLES | COMUNIDAD

ADMINUSLabs	Malicious	Avira	Phishing
CRDF	Malicious	CyRadar	Malicious
Emsisoft	Phishing	Fortinet	Phishing
Lionic	Malicious	Netcraft	Malicious
SafeToOpen	Phishing	Sophos	Phishing
Webroot	Malicious	Abusix	Clean

5. Recomendaciones:

- Evitar abrir correos electrónicos de usuarios desconocidos.
- No brindar información personal a sitios web de dudosa procedencia.
- No compartir la información con familiares y/o amigos.
- Verificar la información en la entidad correspondiente.
- Ingresar desde fuentes oficiales.
- Mantener instalado un software antivirus.

Fuentes de información	Análisis propio de redes sociales y fuente abierta