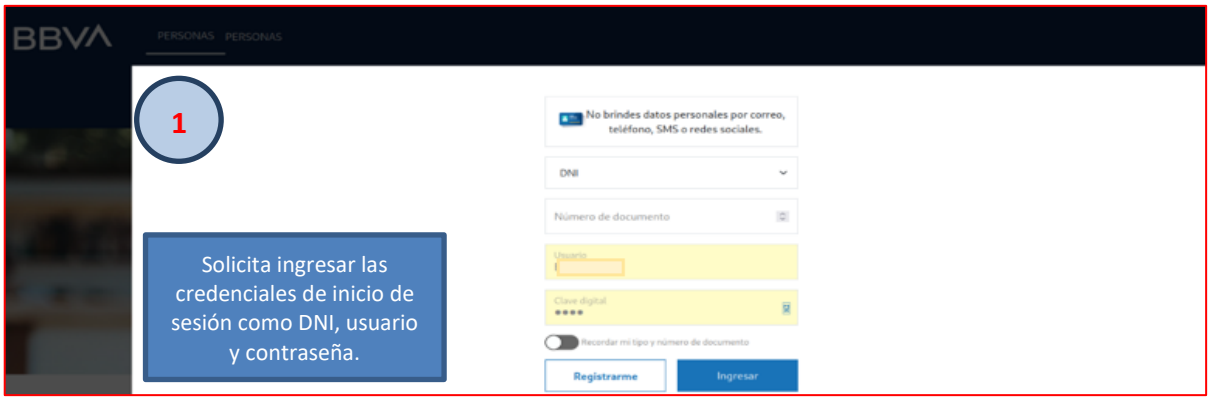
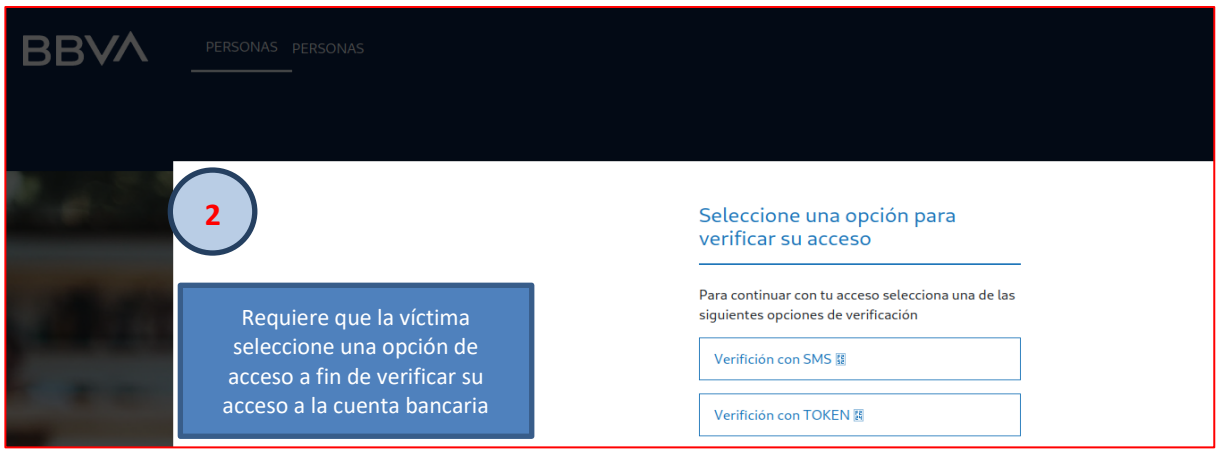
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 100	Fecha: 28-04-2023
		Página 11 de 13

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		

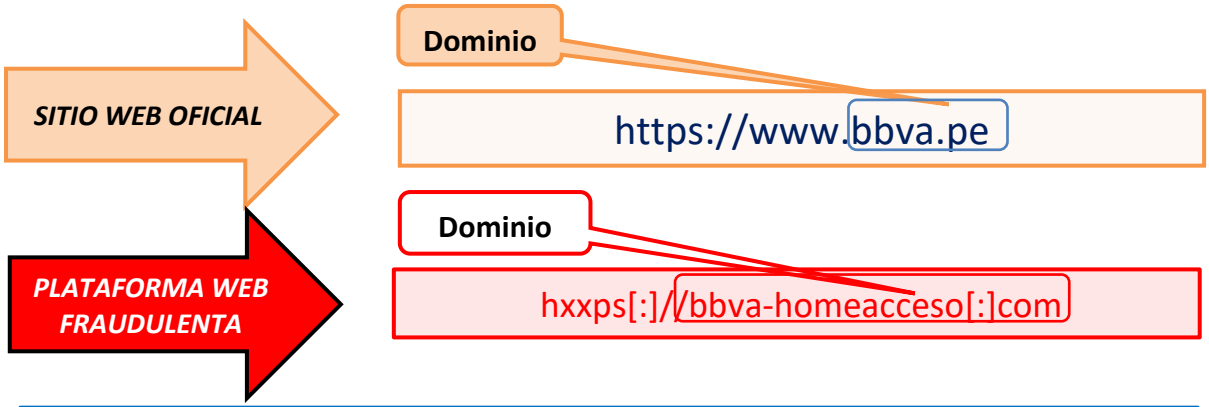
Descripción

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, a través de envíos masivos de correos electrónicos fraudulentos, simulando ser la página oficial de la entidad Bancaria BBVA, requiriendo a las víctimas ingresar las credenciales de inicio de sesión como número de DNI, usuario y clave digital de la cuenta, a fin de realizar una verificación de acceso a la misma.
2. Detalles del proceso de Phishing:





3. Comparación del sitio web oficial y sitio web fraudulento del banco BBVA:



- Existe diferencia entre los dominios del sitio web oficial y fraudulento.
- Ambos sitios web poseen el **PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS),** lo cual hace más convincente a que las víctimas ingresen a dicho sitio web.

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

alphaMountain.ai	Phishing	AlphaSOC	Phishing
Antiy-AVL	Malicious	Avira	Phishing
CyRadar	Malicious	ESET	Phishing
Forcepoint ThreatSeeker	Phishing	Fortinet	Phishing
Google Safebrowsing	Phishing	Heimdal Security	Phishing
Sophos	Malware	Trustwave	Phishing

- Indicadores de compromiso:
  - URL: https[:]//bbva-homeacceso[.]com
  - Dominio: bbva-homeacceso[.]com
  - SHA-256: 9a50136a82e60c31374c9e33aa75b51a291d26b5c0a4f118063b801ff11da9c0
  - Dirección IP: 104[.]21[.]7[.]47
  - Tamaño: 3.84 KB

5. Recomendaciones:

- Comunicarse con la entidad, a fin de corroborar la información solicitada.
- Verificar detalladamente la URL, que corresponda al sitio web oficial.
- 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