	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 009	Fecha: 09-01-2022
		Página: 4 de 6

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**			
Nombre de la alerta	Nueva campaña de phishing que suplanta 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 financiero			

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una nueva campaña de phishing que se distribuye a través de navegadores webs, en donde suplantan la identidad del Banco BBVA, con el objetivo robar credenciales de acceso e información bancaria de los usuarios.
2. Proceso del ataque phishing:

Figura N° 01: Sitio web fraudulento que suplanta la identidad del Banco BBVA, insta al usuario, ingresar sus credenciales de acceso (usuario y contraseña).

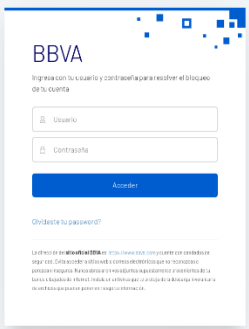
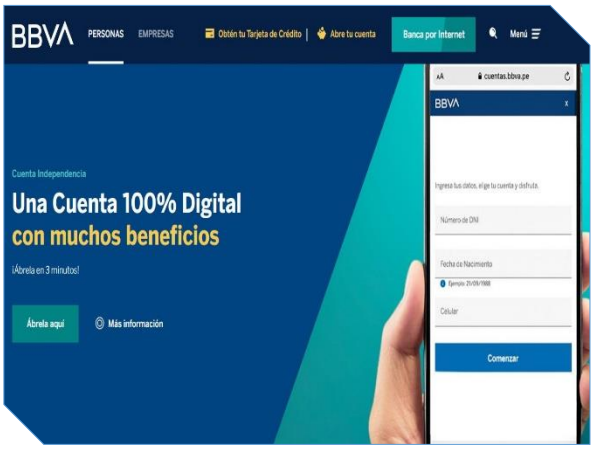


Figura N° 02: Pasado unos segundos, es redirigido al sitio web oficial del Banco BBVA, aludiendo un aparente error de autenticación, sin embargo, los datos fueron capturados por los ciberdelincuentes.



3. La URL maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo como resultados que, CATORCE (14) proveedores de seguridad informática alertan como **PHISHING.**
   - URL: hXXp://phishmetraining[.]co[.]uk/bbva/592cf4/425bdbd3-91cf-4e9f-9498-7a06b3ad75ec
   - Dominio: phishmetraining[.]co[.]uk
   - Dirección IP: 3[.]121[.]154[.]182
   - Código De Estado: 200
   - Longitud Corporal: 6,56 KB
   - Cuerpo SHA-256: 7e976ed50644ac6fe9aa73828faa1ba209ca1c2315583143bbcb2ad657a20b09

4. Otros resultados:
   - URL: hXXp://phishmetraining[.]co[.]uk/bbva/592cf4/425bdbd3-91cf-4e9f-9498-7a06b3ad75ec

5. Cómo funciona el phishing:
   - Los ciberdelincuentes a través de los correos electrónicos adjuntan enlaces que redirige a sitios webs fraudulentos en los que solicitan información personal.
   - Los ciberdelincuentes utilizan como medios de propagación del phishing: WhatsApp, telegram, redes sociales, SMS entre otros.
   - Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público, entidad financiera, servicio técnico, etc.).

6. Referencia:
   - Phishing o suplantación de identidad: Es una técnica fraudulenta consiste en engañar al usuario solicitando información personal, contraseñas, datos bancarios etc., a través del correo electrónico o redirigiendo a la víctima a una copia falsa de una página web donde se le solicita el ingreso de los datos que se quieren obtener.

7. Recomendaciones:
   - Visualizar los sitios web que se ingresen sean los oficiales.
   - No proporcionar información personal o bancaria en páginas web fraudulentas.
   - Revisar las cuentas periódicamente para tener controlados los movimientos bancarios.
   - No guardar información bancaria en el dispositivo móvil.
   - Mantén siempre un antivirus actualizado.

Fuentes de información	Análisis propio de redes sociales y fuente abierta