	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 113	Fecha: 15-05-2023
		Página 6 de 12

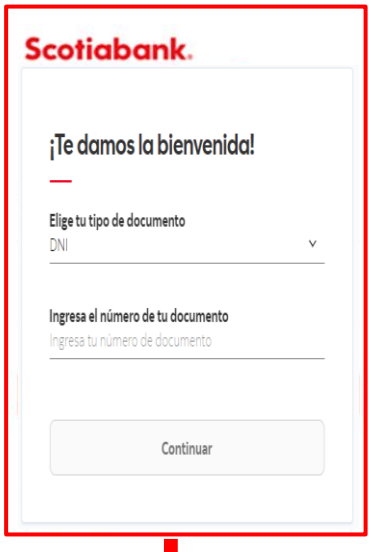
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Smishing, Campaña de envió de SMS fraudulentos, suplantando la identidad del banco Scotiabank.		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de subfamilia	G03
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 diferentes delitos informáticos empleando la modalidad de "Smishing" (SMS), quienes suplantan la identidad del Banco Scotiabank, indicando que el cliente cuenta con un bono de S/. 700.00, otorgado por el gobierno, para ello se quiere ingresar a un link adjuntado en el mensaje enviado, con la finalidad de robar información confidencial de las víctimas como, dirección de correo electrónico, contraseña, nombres, dirección de domicilio, datos de tarjeta bancaria, número de teléfono, entre otros.

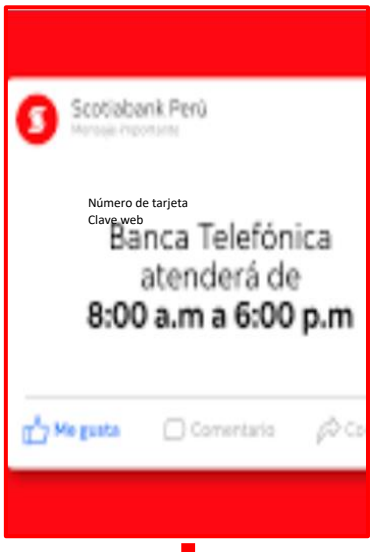
2. Detalles del proceso de estafa del Smishing:

Paso 01:
Mensaje enviado a la víctima.



Paso 02:
Una vez hecho clic, en el enlace del mensaje, es redirigido a un sitio falso que suplanta la identidad del Banco scotiabank, con el fondo de Yanapay Perú, donde se debe ingresar número de DNI.

Paso 03:
El sitio web falso requiere el ingreso de un número de <celular> para recibir un <código de verificación por SMS>, al ingresar el supuesto cogido de verificación y hacer clic en continuar.

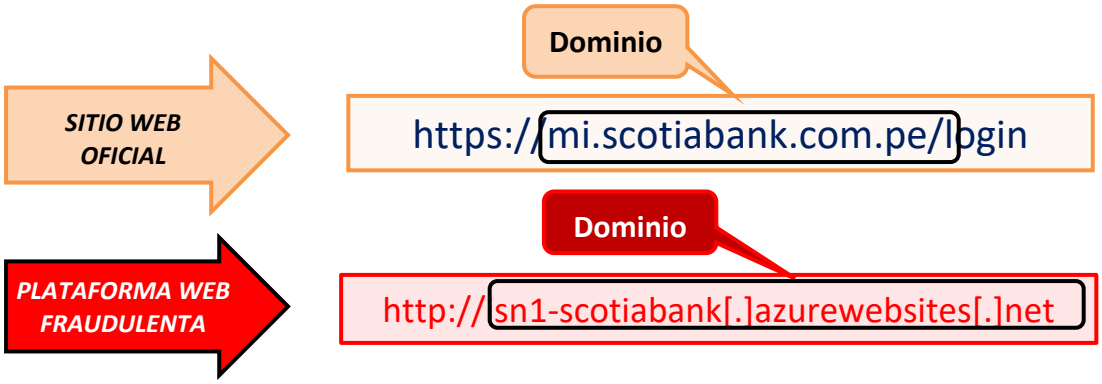


Paso 04:
Pasado unos segundos, carga una ventana donde requiere el ingreso de credenciales de acceso <número de tarjeta, clave web> y un mensaje indicando la "banca telefónica atenderá de 08:00 a.m. a 6:00 p.m., Sin embargo, los ciberdelincuentes obtuvieron los datos brindados por la víctima.

3. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

alphaMountain.ai	Suplantación de identidad	AlphaSOC	Suplantación de identidad
Anti-AVL	Malicioso	Avira	Suplantación de identidad
BitDefender	Suplantación de identidad	CRDF	Malicioso
CyRadar	Malicioso	ESET	Suplantación de identidad
Fortinet	Suplantación de identidad	kaspersky	Suplantación de identidad
Sophos	Suplantación de identidad	Onda de confianza	Suplantación de identidad
Inteligencia de amenazas de Viettel	Suplantación de identidad	VIPRE	Malicioso
raíz web	Malicioso	Abusix	Limpio

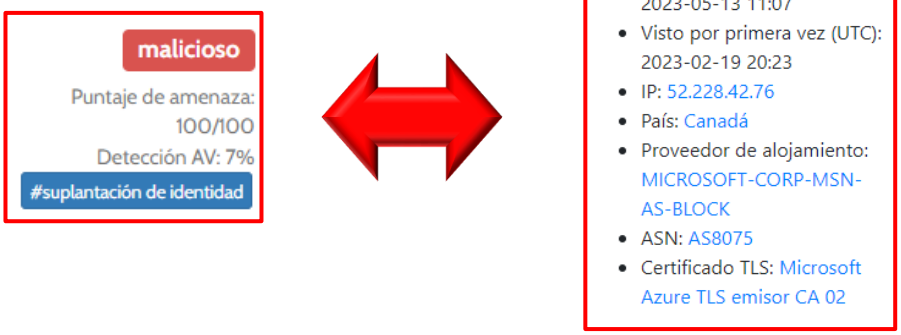
4. Comparación del sitio web oficial y sitio web fraudulento de Scotiabank:



- Existe una similitud entre el fondo y forma de cada sitio web (oficial y fraudulento).
- El sitio web fraudulento no poseen el ***PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS)***.

5. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

- **INDICADORES DE COMPROMISO:**
  - ✓ **URL** : hxxp:// isn1-scotiabank[.]azurewebsites[.]net
  - ✓ **Dominio :** isn1-scotiabank[.]azurewebsites
  - ✓ **IP** : 52[.]228[.]42[.]76
  - ✓ **Proveedor de alojamiento** : MICROSOFT-CORP-MSN-AS-BLOCK
- **OTRAS DETECCIONES:**



6. Cómo funciona el Smishing:

- Los correos electrónicos incluyen enlaces de sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- Medios de propagación del Smishing: WhatsApp, telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público o privado, entidad financiera, servicio técnico, etc.)

7. ALGUNAS RECOMENDACIONES:

- Verificar la información en la entidad correspondiente.
- Acceder al sitio web a través de fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No compartir la información con terceras personas, amigos o familiares.
- Mantener instalado un servicio de antivirus en el dispositivo.

Fuentes de información	▪ Análisis propio de redes sociales y fuente abierta