	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°161	Fecha: 08-07-2023
		Página: 8 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	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 Sub familia	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 ingrese a su plataforma, 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:**
El proceso de estafa del Phishing:

Paso 01:

El ciberdelincuente envía a la víctima, una vez hecho clic, en el enlace del mensaje, es redirigido a un sitio falso que suplanta la identidad del Banco scotiabank, donde se debe ingresar número de DNI.

Paso 02:

Luego, requiere ingresar dirección de correo electrónico y clave, con el fin de terminar con el proceso de identidad de la cuenta bancaria

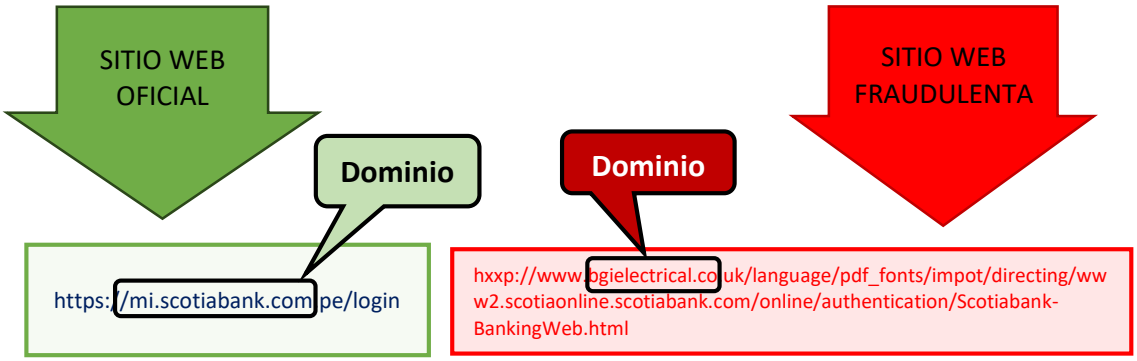
Paso 03:

Pasado unos segundos, carga una ventana donde requiere el ingreso de credenciales de acceso <número de tarjeta, clave web>, Sin embargo, los ciberdelincuentes obtuvieron los datos brindados por la víctima.

A. 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
Avira	Suplantación de identidad	BitDefender	Suplantación de identidad
CyRadar	Malicioso	Emsisoft	Suplantación de identidad
ESET	Suplantación de identidad	Fortinet	Suplantación de identidad
G-datos	Suplantación de identidad	Navegación segura de Google	Suplantación de identidad
Leonico	Suplantación de identidad	netcraft	Malicioso
Búsqueda segura	Malicioso	Sophos	Suplantación de identidad
VIPRE	Malicioso	raíz web	Malicioso

B. Comparación del sitio web oficial y sitio web fraudulento de Netflix:



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

C. INDICADORES DE COMPROMISO:

- **URL** : hxxp://www[.]bgielectrical[.]co[.]uk/language/pdf_fonts/impot/directing/www2.scotiaonline[.]scotiabank[.]com/online/authentication/Scotiabank-BankingWeb[.]html
- **Dominio :** bgielectrical[.]es
- **IP** : 209[.]235[.]144[.]9
- **Nombre de servidor:** dns115[.]a[.]register[.]com
- **Otras detecciones:**

3. 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.

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