	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 102	Fecha: 02-05-2023
		Página 7 de 11

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de Phishing 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	G02
Clasificación temática familia	Fraude		

Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que actores de amenazas vienen llevando a cabo una campaña de Phishing, suplantando el sitio web del Banco Scotiabank (Banca por internet), por medio de la creación de un sitio web falso que simula el oficial, con el objetivo de robar credenciales de acceso, datos personales y/o bancarios.

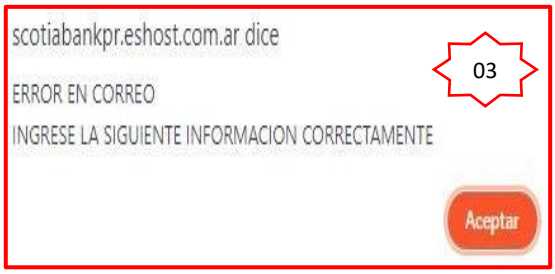
2. **Imagen**: Detalle del proceso del Phishing:

Paso N.º 01

El atacante mediante la creación de un sitio web similar al original del banco Scotiabank, solicita a las posibles víctimas a ingresar el tipo de documento, numero de documento y contraseña.

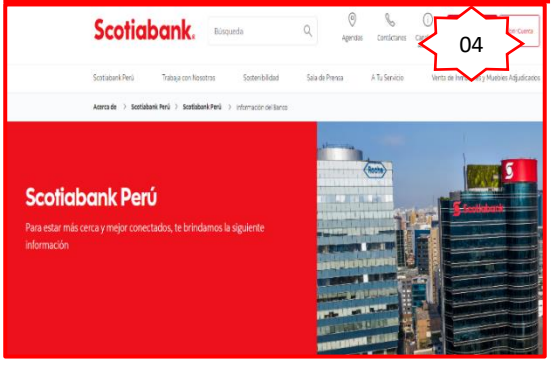
Paso N.º 02

Luego de continuar, solicita a la víctima ingresar el correo electrónico y la contraseña.



Paso N.º 03

Después de continuar, sale una ventana emergente, en la cual informa a la victima que ha ocurrido error al colocar el correo.



Paso N.º 04

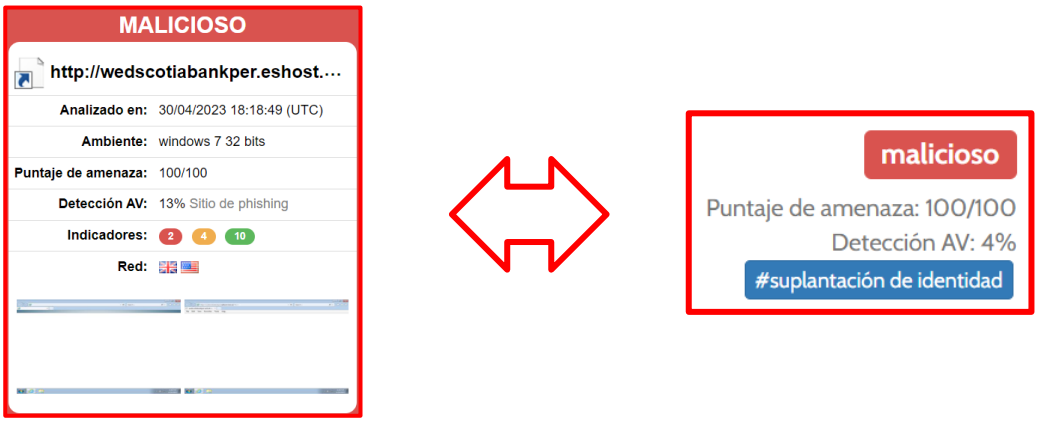
Finalmente, al completar lo requerido por el atacante, es redirigido al sitio oficial del sitio web de Scotiabank, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los cibercriminales.

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

- **INDICADORES DE COMPROMISO (IoC)**

  - **Url** : hxxp://wedscotiabankper[.]eshost[.]com[.]ar/
  - **Dominio** : eshost[.]com[.]ar
  - **IP** : 185[.]27[.]134[.]98
  - **Servidor** : Nginx
  - **Tipo** : Text/Html
  - **SHA-256** : 51f833943648e0c670791299433a378c3a552683dac6fed1cfdd18c2ff0b1ca6

4. Otras detenciones:



5. Apreciación de la información:

- La presente campaña de Phishing, permite a los actores de amenazas obtener las credenciales de acceso a la banca por internet de los usuarios del Banco Scotiabank.

- La propagación del sitio web fraudulento se realiza mediante envió masivos de email, adjuntando enlaces de sitios web fraudulentos con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram, Messenger, etc. y mensajes de textos SMS.

6. Algunas Recomendaciones:

- Verificar detalladamente las URL de los sitios web
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.
- Descargar aplicaciones de fuentes confiables.
- Realizar las actualizaciones correspondientes desde fuentes originales.
- Comunicar a la entidad financiera si ha realizado un registro de acceso en un sitio web sospechoso.

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

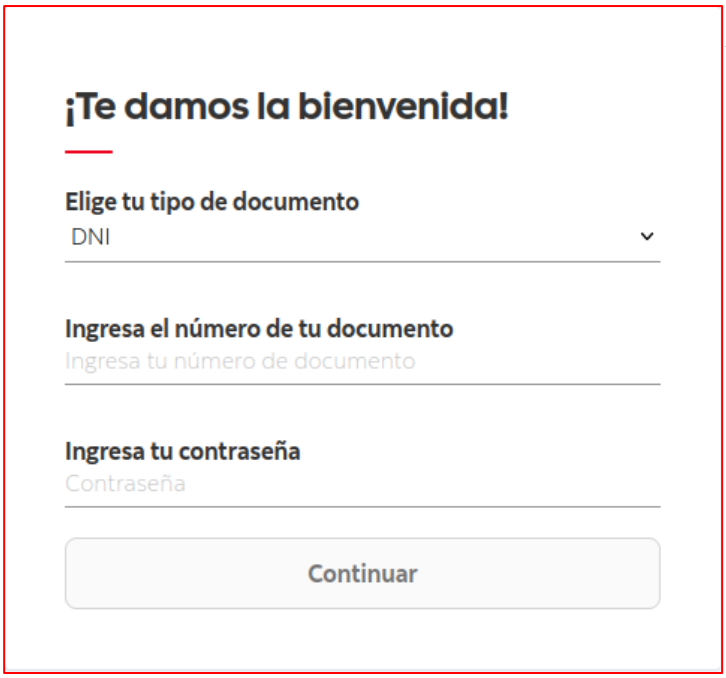
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 102	Fecha: 02-05-2023
		Página 9 de 11

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de Phishing 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	G02
Clasificación temática familia	Fraude		

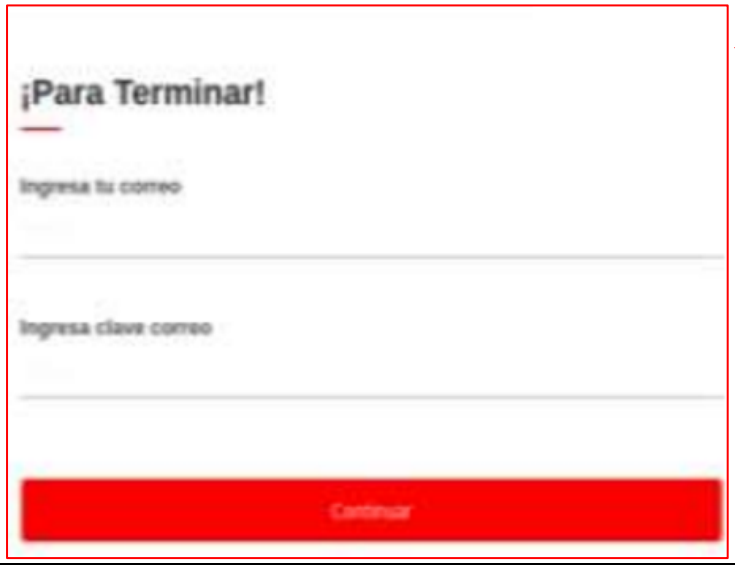
Descripción

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, por medio de los diferentes navegadores web, dirigido a los clientes y/o usuarios de la entidad bancaria Scotiabank; el cual, mediante la creación de un sitio web similar al original, solicitan a las posibles víctimas a ingresar las credenciales de inicio de sesión como DNI, contraseña, dirección de correo electrónico, clave de Gmail, entre otros.

2. Detalles del proceso de Phishing:

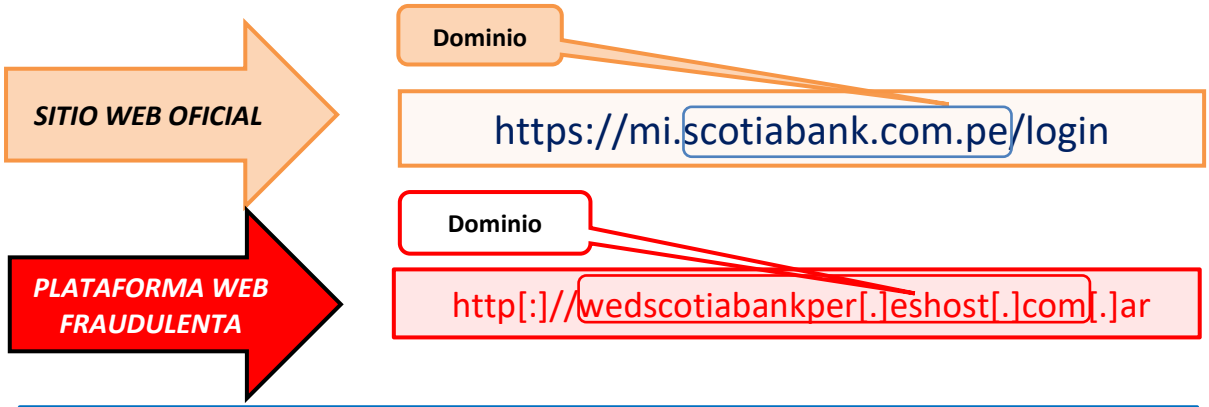


El supuesto sitio web fraudulento solita a las víctimas a ingresar las credenciales de inicio de sesión como DNI y contraseña



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

3. 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)***.

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

Avira	Phishing	CRDF	Malicious
CyRadar	Malicious	Emsisoft	Phishing
ESET	Phishing	Fortinet	Phishing
Kaspersky	Phishing	Lionic	Phishing
Netcraft	Malicious	PhishLabs	Phishing
Sophos	Phishing	Trustwave	Phishing

- Indicadores de compromiso:
  - URL: http[:]//wedscotiabankper[.]eshost[.]com[.]ar
  - Dominio: wedscotiabankper[.]eshost[.]com[.]ar
  - SHA-256: 3e66836688a11f282ed85c943010aad23c6fb77f4ba1f0e17a98a6d14a5e5ae8
  - Dirección IP: 185[.]27[.]134[.]98
  - Tamaño: 841 B

5. Recomendaciones:

- Verificar la información en la entidad correspondiente.
- Las entidades bancarias no solicitan realizar actualización de datos de manera online o virtual.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.

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