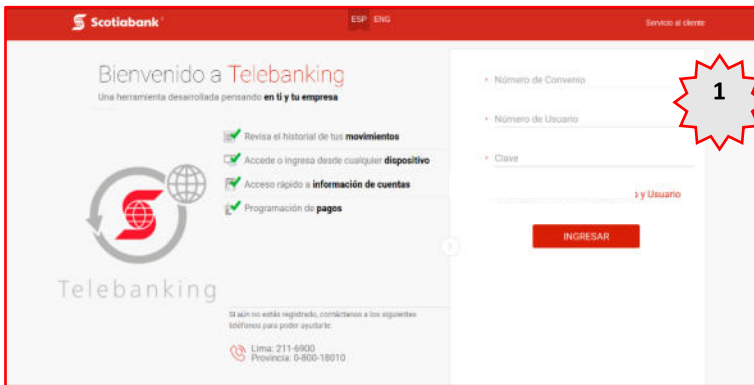


	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 062</b>	Fecha: 03-03-2022	
		Página 7 de 9	
Componente que reporta	<b>DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ</b>		
Nombre de la alerta	Campaña de Phishing, suplantando la identidad del Banco Scotiabank		
Tipo de ataque	Phishing	Abreviatura	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 del Banco **SCOTIABANK**; el cual, mediante la creación de un supuesto sitio “**Banca Por Internet**” de la entidad bancaria, solicitan a las posibles víctimas a ingresar las credenciales de inicio sesión, como usuario y clave web, con la finalidad de apoderarse de manera ilícita de la información bancaria.

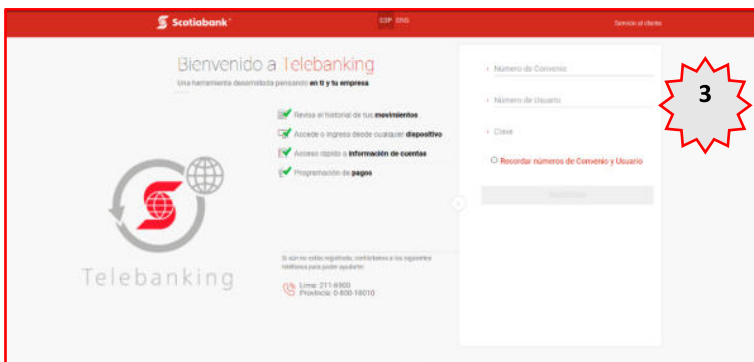
2. **Imagen:** Detalle del proceso del Phishing:



Solicitan a las posibles víctimas ingresar datos confidenciales, como Número de convenio, N° de usuario y clave web.



Al continuar con el proceso, requiere actualizar el número telefónico, a fin de ser afiliado a la banca por internet del Banco Scotiabank.



Por último, redirige automáticamente al sitio web oficial del Banco Scotiabank, aludiendo que las credenciales de acceso fueron erróneas, sin embargo, los datos ingresados fueron capturados por los ciberdelincuentes.

3. Comparación del sitio web oficial y fraudulento.

**Sitio web oficial**

URL: <https://bancainternetempresas.scotiabank.com.pe>

**Sitio web fraudulento**

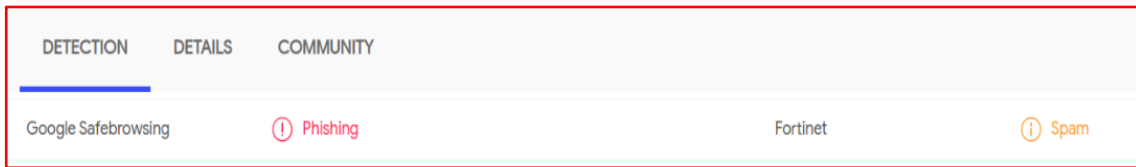
URL: [https://bancasinternetempresas\[.\]scotiabanak-pe\[.\]com](https://bancasinternetempresas[.]scotiabanak-pe[.]com)

**Dominio**

- Existe una similitud entre el fondo y forma de cada sitio web.
- Ambas URL's utilizan el protocolo **HTTPS**, lo que hace más convincente a que las víctimas accedan al sitio web.
- La **diferencia** está en la **URL**, debido a que el **dominio** del sitio web fraudulento **no coincide** con el oficial.

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

- Indicadores de compromiso:
  - URL: [https://bancasinternetempresas\[.\]scotiabanak-pe\[.\]com](https://bancasinternetempresas[.]scotiabanak-pe[.]com)
  - Dominio: [scotiabanak-pe\[.\]com](https://scotiabanak-pe[.]com)
  - IP: 162[.]144[.]15[.]87
  - Tamaño: 176.86 KB
  - SHA-256: 8921837f64b2f43000b77681bc23ee6d224bf797474eb1440d3c843a6bf0e667



Otras detecciones.

**MALICIOSO**

**https://bancasinternetempresa...**

Analizado en: 03/03/2022 14:14:43 (UTC)

Ambiente: windows 7 32 bits

Puntaje de amenaza: 10/10

Detección AV: 1% Sitio de phishing

Indicadores: 1 5 9

La red:

Puntuación de amenaza

10/10

5. Recomendaciones:

- No brindar información personal y/o bancaria en sitios web de dudosa procedencia.
- Ingresar de forma manual la URL de la entidad correspondiente.
- Verificar la información en la entidad correspondiente.
- No compartir la información con familiares o amigos.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener un software antivirus.

Fuentes de información

Análisis propio de redes sociales y fuente abierta