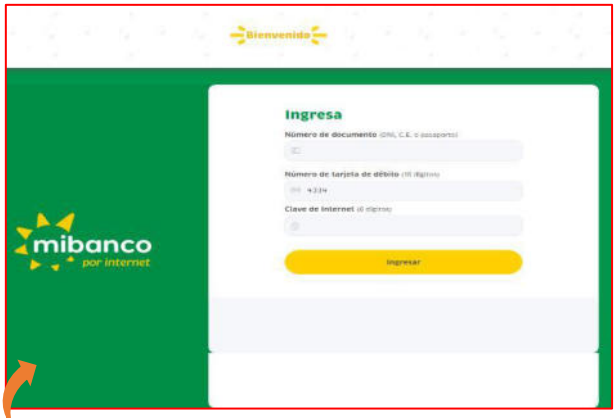
| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 111 | Fecha: 22-04-2022 |
|---|---|---|
| | | Página 7 de 9 |

| | | | |
|---|---|---|---|
| Componente que reporta | **DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ** | | |
| Nombre de la alerta | Phishing, suplantando la identidad de la entidad Bancaria Mi Banco | | |
| 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

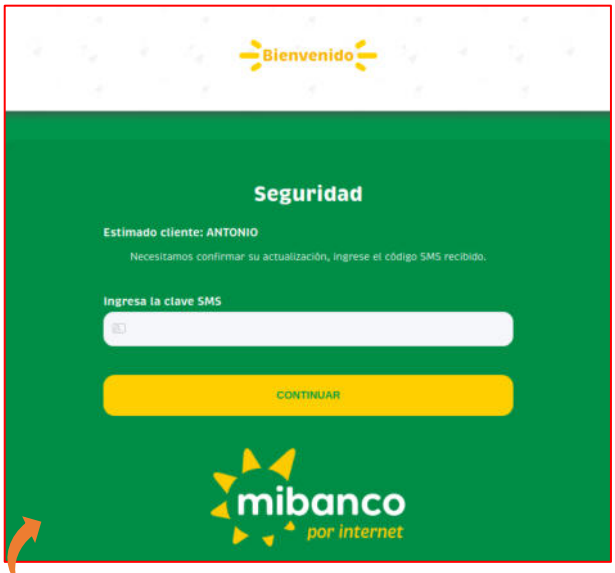
1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, por medio de los diferentes navegadores web, dirigido a los clientes y/o usuarios de la entidad bancaria Mi Banco; el cual, mediante la creación de un sitio web similar al original, solicitan a las posibles víctimas a ingresar las credenciales de inicio de sesión como DNI, número de tarjeta débito y clave de internet, para luego requerir una supuesta actualización de datos.

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




**Solicitan iniciar sesión ingresando DNI, N° de tarjeta débito y contraseña.**

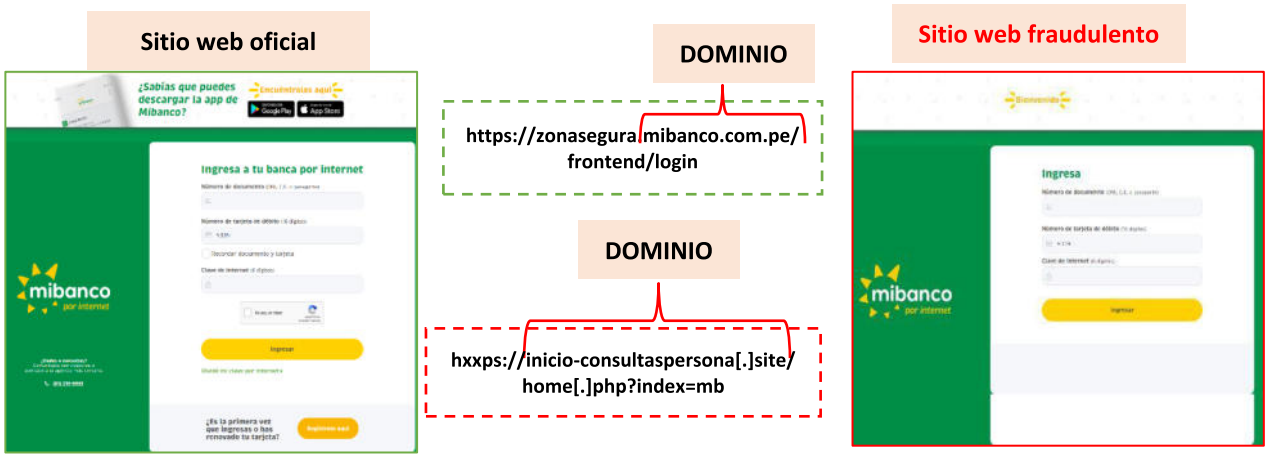

**Luego, indican que la entidad necesita realizar una actualización de datos por medida de seguridad.**




**A continuación, requieren ingresar el código de seguridad enviado al número de teléfono.**


**Finalmente, informan que la clave SMS a vencido, indicando que se enviará un nuevo código.**

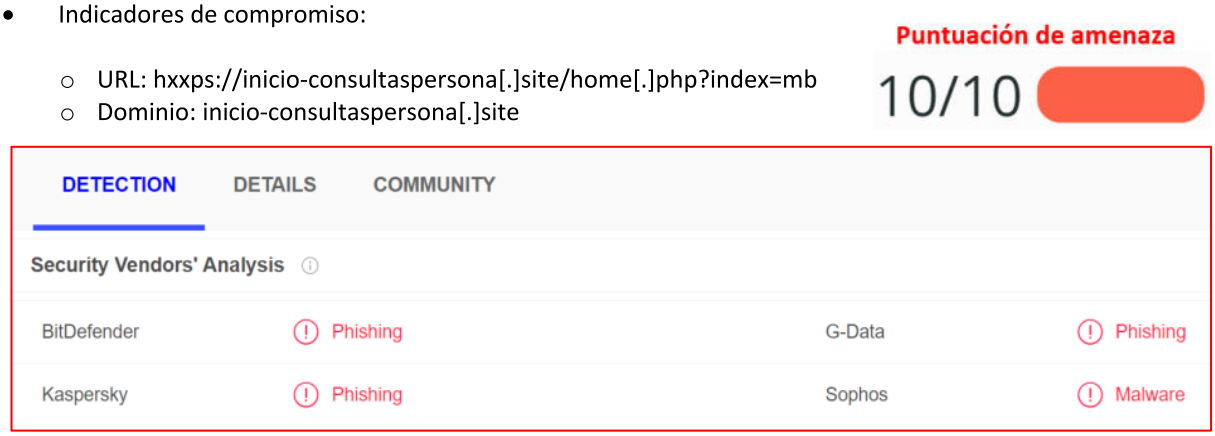
3. Comparación del sitio web oficial y fraudulento.




- 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, toda vez 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: hxxps://inicio-consultaspersona[.]site/home[.]php?index=mb
  - Dominio: inicio-consultaspersona[.]site




5. Apreciación de la información:

- La presente campaña de Phishing, permite a los actores de amenazas obtener información bancaria de los usuarios de Mi Banco.

- 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, dicho enlace malicioso, es enviado a través de las plataformas digitales como el WhatsApp, Telegram, Messenger y mensajes de textos SMS.

6. 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.
- 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 |