	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 284	Fecha: 19-10-2022
		Página 12 de 14

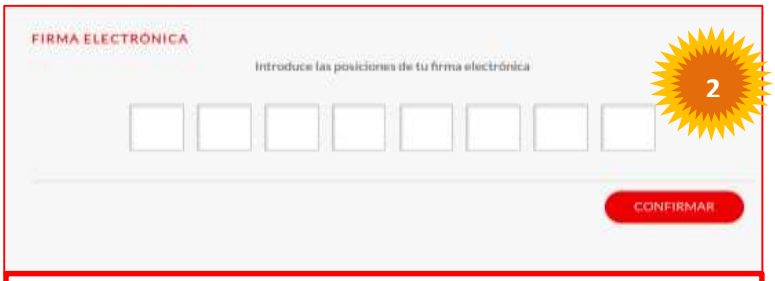
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Phishing suplantando la identidad del Banco Santander		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
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 del Banco Santander; 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, validando datos personas y bancarios como N° de tarjeta bancaria, clave web, fecha de vencimiento, clave de seguridad, entre otros.

2. Proceso del ataque phishing:

Solicita ingresar las credenciales de inicio de sesión

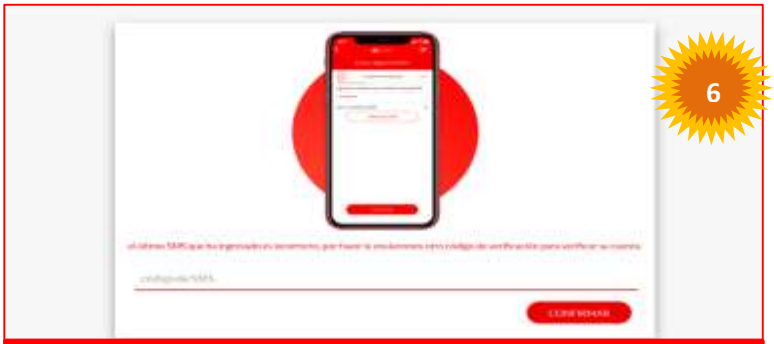


Pide, introducir la firma electrónica del titular de la cuenta

Requiere, ingresar datos de la tarjeta bancaria

A continuación, solicita ingresar el PIN o código de seguridad de la tarjeta

Luego, pide validar el código SMS, para confirmar la operación

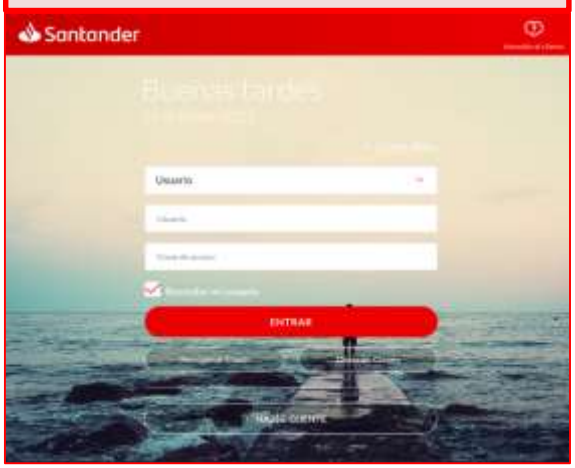


Por último, indica que el código SMS ingresado es incorrecto, informando que se enviara nuevamente otro código de verificación

3. Comparación del sitio web oficial y sitio web fraudulento:

sitio web oficial
https://particulares.bancosantander.es/login

sitio web fraudulento
hxxps://secure296.inmotionhosting[.]com/~ne75c85/tap/particulares[.]php



- 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, obteniendo la siguiente información:

- **URL:** hxxps://secure296.inmotionhosting[.]com/~ne75c85/tap/particulares[.]php
- **Dominio:** inmotionhosting.com
- **Direcciones IP:** 192.145.239.211
- **Tamaño:** 12.06 KB
- **SHA-256:** df1a642f642834aa7176f2c3272daa5eda5e130befb32f411cd8bb62b1ba34d2

alphaMountain.ai	Malicious	Avira	Phishing
BitDefender	Phishing	CyRadar	Malicious
Emsisoft	Phishing	Forcepoint ThreatSeeker	Phishing
G-Data	Phishing	Kaspersky	Phishing
Lionic	Malicious	Netcraft	Malicious
Phishing Database	Phishing	Segasec	Phishing
Sophos	Malware	Trustwave	Phishing
Webroot	Malicious	Abusix	Clean

5. Recomendaciones:

- No abrir correos ni mensajes de dudosa procedencia
- Desconfiar de los enlaces y archivos enviados a través de mensajes o correos electrónicos
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Prestar atención en los detalles de los mensajes o redes sociales
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

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