

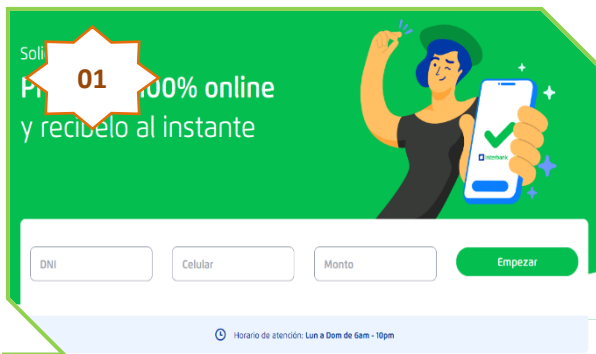
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°232		Fecha: 02-10-2023
			Página: 10 de 13
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Detección de sitio web fraudulento del Banco Interbank		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

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 de solicitud de préstamos del Banco Interbank, con la finalidad de robar información sensible de los usuarios de la entidad financiera como números de documento de identidad, tarjetas bancarias, etc.

2. DETALLES:



Paso N°01

Solicitan a la víctima registrar lo siguiente:

- El DNI de la víctima
- El monto del préstamo solicitado.
- El número de celular

Para luego dar clic en <EMPEZAR>.

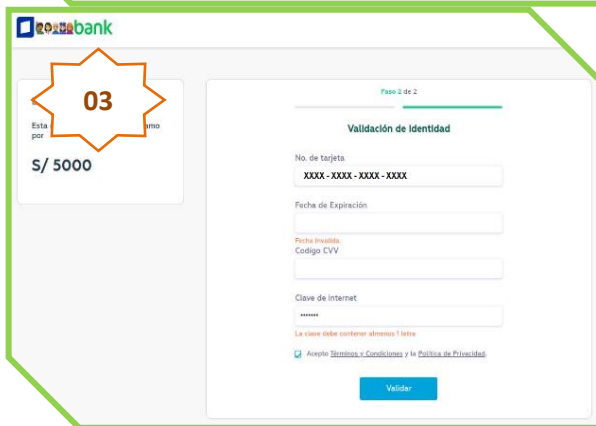


Paso N°02

Solicita a la víctima datos como:

- El número del Documento Nacional de Identidad (DNI).
- Número de tarjeta
- Clave de Internet

Para luego dar clic en <Continuar>.



Paso N°03

Una vez brindado los datos solicitados en el paso N.º 02, aparece una pantalla requiriendo información como el número de la tarjeta bancaria, la fecha de expiración, el código de seguridad (CVV) y la clave de seis dígitos del intranet, para luego dar clic en <Validar>. Pero, pasado unos segundos, redirige al sitio web oficial de la entidad bancaria; sin embargo, los ciberdelincuentes obtuvieron los datos proporcionados por la víctima.

A. Comparación del sitio web oficial y fraudulento.

SITIO WEB OFICIAL

<https://interbank.pe/inscripcion/prestamo-paso-1>



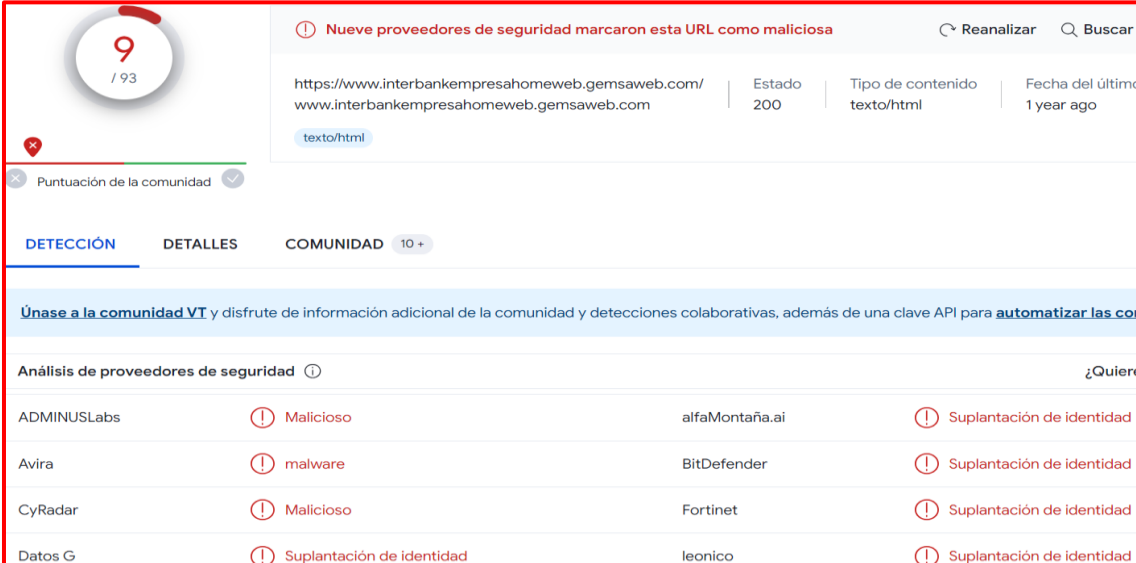
SITIO WEB FRAUDULENTA

[https://www.\[.\]interbankempresahomeweb\[.\]gemsaweb\[.\]com/](https://www.[.]interbankempresahomeweb[.]gemsaweb[.]com/)



- Existe una diferencia entre la URL original y la URL fraudulenta.
- La URL del sitio web fraudulento posee protocolo de seguridad de red (https)
- Existe una similitud entre ambas páginas en imagen, fondo y color.

B. Proveedor de seguridad informática no alerta como SUPLANTACIÓN DE IDENTIDAD - PHISHING.



Nueve proveedores de seguridad marcaron esta URL como maliciosa

URL	Estado	Tipo de contenido	Fecha del último
https://www.interbankempresahomeweb.gemsaweb.com/	200	texto/html	1 year ago

Proveedor de seguridad	Detección	Detalles	Acción
ADMINUSLabs	Malicioso	alfaMontaña.ai	Suplantación de identidad
Avira	malware	BitDefender	Suplantación de identidad
CyRadar	Malicioso	Fortinet	Suplantación de identidad
Datos G	Suplantación de identidad	leonico	Suplantación de identidad

C. Indicadores de compromiso (IoC)

- Dominio : gemsaweb[.]com

Dominio	gemsaweb.com
Nombre del servidor	ns144.neubox.net
registrar de dominio	Desconocido
Organización del servidor de nombres	whois.neubox.com

- IP : 47[.]251[.]51[.]48

Dirección IPv4 (65.99.252.10)			
rango de IP	País	Nombre	Descripción
::ffff:0.0.0.0/96	Estados Unidos	DIRECCIÓN-MAPEADA-IPV4-IPV4 DE IANA	Autoridad de asignación de números de Internet
↳ 65.0.0.0-65.255.255.255	Estados Unidos	NET65	Registro Americano de Números de Internet
↳ 65.99.192.0-65.99.255.255	Estados Unidos	COLO4-BLK5	TierPoint, LLC
↳ 65.99.252.10	Estados Unidos	COLO4-BLK5	TierPoint, LLC

- Servidor : Apache
- SHA-256 : c1e861a95ae9a50a39a3da921ae9e9d7250fe6e14bff390438ede2527c3b3cd8
- Tipo Cont : Texto/Html
- Código : 200

D. 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 Interbank.
- La propagación del sitio web fraudulento se realiza mediante envíos 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.

E. Referencia:

- El Phishing es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza, para manipularla y hacer que realice acciones que no debería realizar.

3. RECOMENDACIONES:

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No aceptar permisos de instalación de archivos desconocidos o dudosa procedencia.
- Mantener actualizado el sistema operativo y aplicaciones del equipo de cómputo.
- Mantener actualizado el sistema antivirus (el antivirus debe ser licenciado).
- Comunicar a la entidad financiera si ha realizado un registro de acceso en un sitio web sospechoso.

Fuente de Información:

Análisis propio de redes sociales y fuente abierta.