

	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°043</b>		<b>Fecha: 19-02-2024</b>
			<b>Página: 11 de 17</b>
Componente que reporta	<b>DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ</b>		
Nombre de la alerta	Nueva campaña de Phishing que suplanta la identidad 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 ha detectado una nueva campaña de "Phishing" en la que ciberdelincuentes están suplantando la identidad del Banco Interbank, bajo la modalidad de participar en el sorteo de las "20 entradas dobles para el concierto de Justin Bieber", instando a los usuarios a registrarse y participar, con el objetivo de obtener información personal de las víctimas.

**2. DETALLES:**

**Paso 1**

La victima proporciona los siguientes datos:

- Nombres
- DNI
- Teléfono
- Correo electrónico

Acepta condiciones y hace clic en "**¡Quiero Ganar!**"

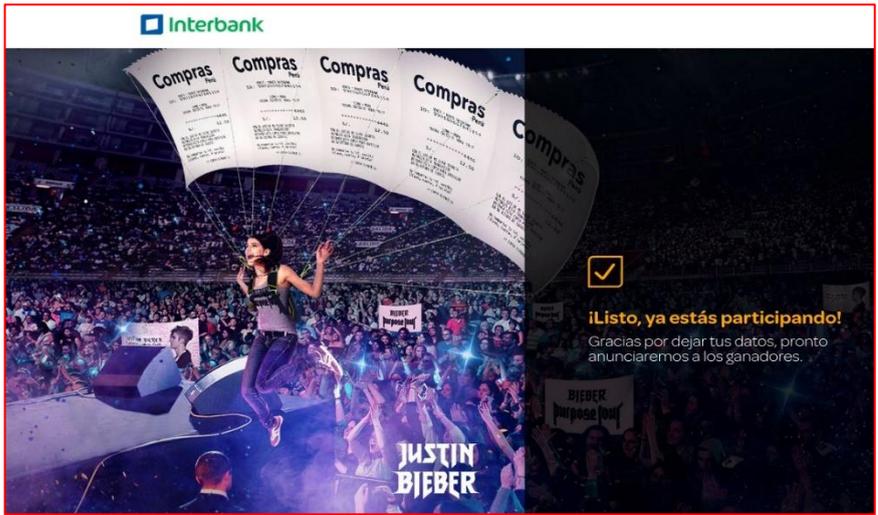


**Paso 2**

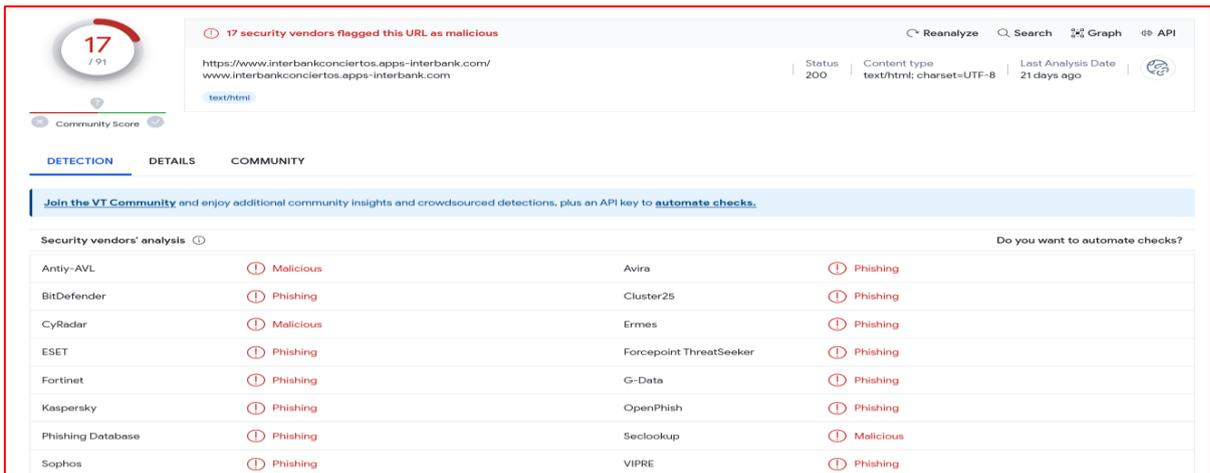
Culminado el registro, aparece en la pantalla lo siguiente:

**"Listo, ya participas. Los ganadores se anunciarán próximamente."**

Dando fin al proceso.



A. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD-PHISHING**:



17 security vendors flagged this URL as malicious

https://www.interbankconciertos.apps-interbank.com/

Status: 200 | Content type: text/html; charset=UTF-8 | Last Analysis Date: 21 days ago

Security vendors' analysis	Do you want to automate checks?
Antiy-AVL	Malicious
Avira	Phishing
BitDefender	Phishing
Cluster25	Phishing
CyRadar	Malicious
Ermes	Phishing
ESET	Phishing
Forcepoint ThreatSeeker	Phishing
Fortinet	Phishing
G-Data	Phishing
Kaspersky	Phishing
OpenPhish	Phishing
Phishing Database	Phishing
Seclookup	Malicious
Sophos	Phishing
VIPRE	Phishing

a) **Indicadores de compromisos:**

I. **URL:**

https[:]//www[.]interbankconciertos[.]apps[-]interbank[.]com



Site	<a href="https://www.interbankconciertos.apps-interbank.com">https://www.interbankconciertos.apps-interbank.com</a>
Netblock Owner	GoDaddy.com, LLC
Hosting company	GoDaddy
Hosting country	US

II. **DOMINIO:**

apps[-]interbank[.]com



Domain	<a href="https://apps-interbank.com">apps-interbank.com</a>
Nameserver	ns1.secureserver.net
Domain registrar	godaddy.com
Nameserver organisation	whois.wildwestdomains.com

III. **IP:**

166[.]62[.]85[.]139



IPv4 address (166.62.85.139)	
IP range	Country
::ffff:0.0.0.0/96	United States
↳ 166.0.0.0-166.255.255.255	United States
↳ 166.62.0.0-166.62.127.255	United States
↳ 166.62.85.139	United States

**IV. SHA-256:**

1a4bc6d53534cda07547ed22a61198ae100e55bdc4a498af5ccfb7f46ec7ac14

**V. Servidor:**

Apache

**B. Cómo funciona el Phishing:**

- Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- Medios de propagación del Phishing: WhatsApp, Telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legítima (organismo público o privado, entidad financiera, servicio técnico, etc.)

**C. Referencia:**

- Phishing o suplantación de identidad: Es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

**3. RECOMENDACIONES:**

- Evitar acceder a enlaces que llegan inesperadamente por correo electrónico u otros medios.
- No proporcionar datos personales (contraseñas, tarjetas, cuentas bancarias, etc.) por correo, teléfono o SMS.
- No introducir datos confidenciales en sitios web sospechosos o de dudosa procedencia.
- Verificar la fuente de información de tus correos entrantes.
- Introducir tus datos únicamente en webs seguras.
- Tener siempre actualizado el sistema operativo y el antivirus. En el caso del antivirus, comprobar que está activo.

Fuente de Información:

Análisis propio de redes sociales y fuente abierta.