

	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°219</b>		<b>Fecha: 17-09-2023</b>
Componente que reporta	<b>DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ</b>		
Nombre de la alerta	Phishing, suplantado la identidad de la compañía multinacional Amazon		
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, los ciberdelincuentes se encuentran desarrollando una nueva campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad de la compañía multinacional de comercio electrónico Amazon, con el objetivo de acceder u obtener credenciales de acceso, datos personales y bancarios de las posibles víctimas.

**2. DETALLES:**



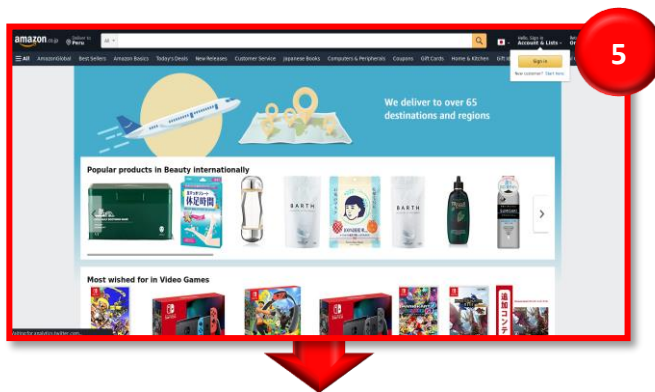
**Imagen 1:** Solicita dirección de correo electrónico y contraseña.

**Imagen 2:** Solicita datos bancarios como el número de tarjeta, fecha de caducidad y el CVC de la tarjeta.

**Imagen 3:** Solicita datos personales fecha de nacimiento, número telefónico, ciudad y más.



**Imagen 4:** Solicita ingresar las credenciales de acceso de la página (usuario y contraseña).



**Imagen 5:** Por último, es redirigido automáticamente a un supuesto sitio web de Amazon, donde la víctima puede verificar una serie de consultas como se aprecia en la imagen.

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

**a) Indicadores de compromisos:**

**I. URL:** `https://amazonsicurezzaweb.[81-161-229-136].[cprapid].[com/`



Nombre del envío:	https://amazonsicurezzaweb.81-161-229-136.cprapid.com/
Tamaño:	78B
Tipo:	<b>URL</b>
Mimica:	Texto sin formato
Sistema operativo:	ventanas
Último análisis antivirus:	17/09/2023 18:40:00 (UTC)
Último informe de:	17/09/2023 18:39:29 (UTC)
Sandbox:	

**II. SHA-256:** `480c0607deec0d8ad43620bc29f7626fd4aa176ce355113f1d53d3edd6e642f6`



RecoveryStore_88B090CO-D917-11E7-B67B-080027A49DD6_dat	sospechoso
307684c91551d40cc01dceaa17b0bed7ed47187d24bbdb55e540b1724cd0a8	
_56451212-5573-11EE-A4DC-0800279AD7D9_dat	sospechoso
ba3e29aaeb580c635c35af3057e95389724bf3e4814606b7fde29ce5499964e	
_4C67E9A7-5573-11EE-A4DC-0800279AD7D9_dat	sospechoso
506cac8ebc30083c31ad3aa63f53b61653e83c50c6844fe3ef5bc9d1371a874	
RecoveryStore_19C6f1BB-5579-11EE-AADA-080027A2D030_dat	sospechoso
0d3bala72105b323c9f2d932a2b074179209d8d9a011f6d3bad411536f497b55	
RecoveryStore_4C67E9A5-5573-11EE-A4DC-0800279AD7D9_dat	sospechoso
09058bd9753be2ce0a45371e307aced3e18f1da80bd3e82b95a61f488909161	
RecoveryStore_88B090CO-D917-11E7-B67B-080027A49DD6_dat	sospechoso
80af8337f72cf01c1b6a6d073bfab45e39b9f6c78ae739132b049e7eb8f95013	
_2389E04A-5579-11EE-AADA-080027A2D030_dat	sospechoso
c1275392aa77434340c9834fc3ee885ea0f0dabc17e9e036c602b426dfdb7f31	

**III. IP:** `81.[.]161.[.]229[.]136`



Conexión		Detección	
Dominio representativo	N / A	IP Proxy	FALSO
Certificado SSL	FALSO	IP VPN	FALSO
Propietario de la dirección IP	Delis LLC	Rasgar	FALSO
Nombre de host	81-161-229-136.cloud-search.org	IP de alojamiento	FALSO
Domínios conectados	1	IP móvil	FALSO
País	Estados Unidos	IP CDN	FALSO
		IP del escáner	<b>Verdadero</b>
		Problema especial	0

**IV. TIPOLOGÍA:**



**Se puede apreciar como la URL, esta alojada en un servidor ubicado en PAÍSES BAJOS.**

**B. Se hallaron 16 proveedores de seguridad que marcaron este dominio como malicioso.**

AlfaSOC	⚠ Suplantación de identidad	Avira	⚠ Suplantación de identidad
BitDefender	⚠ Suplantación de identidad	Clúster25	⚠ Suplantación de identidad
CRDF	⚠ Malicioso	Emsisoft	⚠ Suplantación de identidad
ESET	⚠ Suplantación de identidad	Fortinet	⚠ Suplantación de identidad
Datos G	⚠ Suplantación de identidad	Kaspersky	⚠ Suplantación de identidad
Netcraft	⚠ Malicioso	OpenPhish	⚠ Suplantación de identidad
Base de datos de phishing	⚠ Suplantación de identidad	búsqueda en seco	⚠ Malicioso
Sofos	⚠ Suplantación de identidad	VIPRE	⚠ Malicioso

**C. Otras detecciones:**

urlscan.io



100%

Análisis de escaneo de URL

Última actualización: 17/09/2023 18:40:00 (UTC)

Ver detalles: [🔗](#)

Visitar proveedor: [🔗](#)

Asesor de estafas



100%

Puntuación de estafa de dominio

Última actualización: 17/09/2023 18:40:00 (UTC)

Ver detalles: [🔗](#)

Visitar proveedor: [🔗](#)



malicioso

Puntuación de amenaza: 100/100  
Detección AV: 67%

#suplantación de identidad

MALICIOSO

https://amazonsicurezaweb.81-...

Analizado en: 17/09/2023 17:57:53 (...)

Ambiente: Windows 7 de 32 bits

Puntuación de amenaza: 100/100

Detección AV: 17% Sitio de phishing

Indicadores: 2 2 10

Red: 

**D. 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.)

**E. 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:**

- Mantener instalado un servicio de antivirus en el dispositivo.
- Verificar la información del sitio web correspondiente.
- Acceder al sitio web a través de fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No compartir la información con terceras personas, amigos o familiares.

Fuente de Información:

Análisis propio de redes sociales y fuente abierta.

	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°219</b>		<b>Fecha: 16-09-2023</b>
			<b>Página: 8 de 11</b>
Componente que reporta	<b>DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ</b>		
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:**

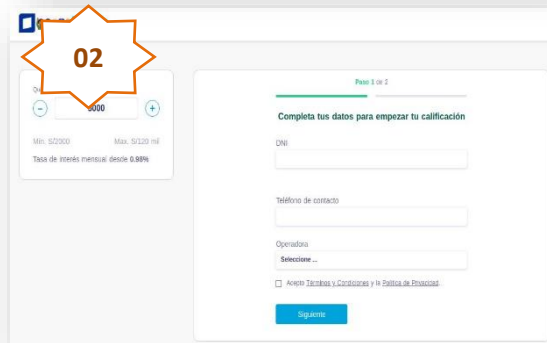


**Paso N°01**

Solicitan a la víctima registrar lo siguiente:

- El monto del préstamo solicitado.

Para luego dar clic en <Calificar ahora>.

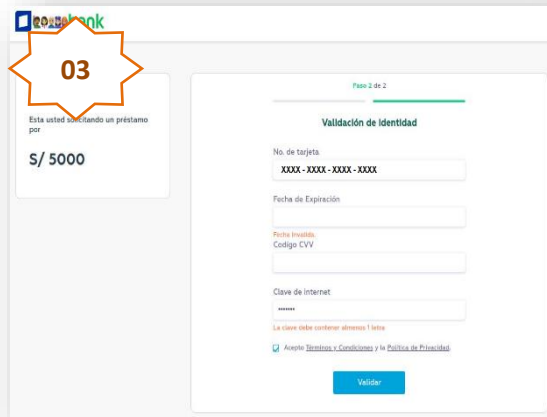


**Paso N°02**

Solicita a la víctima datos como:

- El número del Documento Nacional de Identidad (DNI).
- Número de celular
- Operador telefónico

Para luego dar clic en <Siguiente>.



**Paso N°03**

Una vez brindado los datos solicitados en el paso N.º 02, aparece una pantalla requiriendo información como el numero 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`



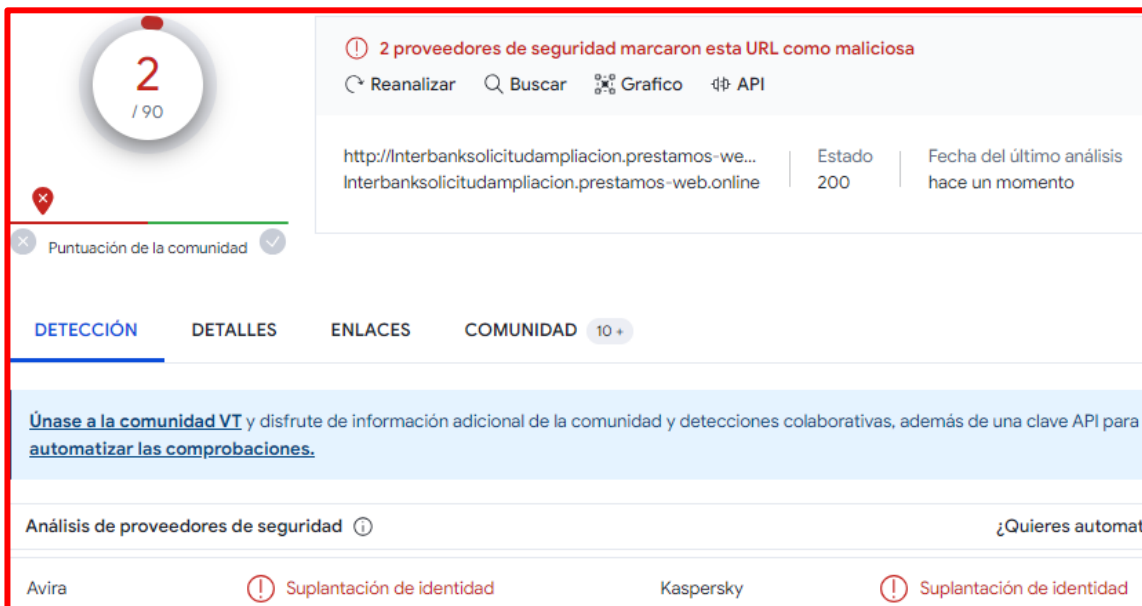
**SITIO WEB FRAUDULENTA**

`http://Interbanksolicitudampliacion.prestamos-web.online/`



- 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.**



2 / 90  
 2 proveedores de seguridad marcaron esta URL como maliciosa  
 Reanalizar | Buscar | Grafico | API  
 http://Interbanksolicitudampliacion.prestamos-we... Estado: 200 | Fecha del último análisis: hace un momento  
 Interbanksolicitudampliacion.prestamos-web.online  
 Puntuación de la comunidad  
 DETECCIÓN | DETALLES | ENLACES | COMUNIDAD 10+  
 Únase a la comunidad VT y disfrute de información adicional de la comunidad y detecciones colaborativas, además de una clave API para automatizar las comprobaciones.  
 Análisis de proveedores de seguridad | ¿Quieres automatizar?  
 Avira: Suplantación de identidad | Kaspersky: Suplantación de identidad

**C. Indicadores de compromiso (IoC)**

- Dominio : prestamos-web[.]online
- IP : 47[.]251[.]51[.]148
- Servidor : Apache
- SHA-256 : 912bb640cf3f2efca7beebe830ab4428c248fd640450a17ce01dda54e610a3e5
- Tipo Cont : Texto/Html
- Codigo : 200

#### D. Comparación de DOMINIOS

Domain Name: interbank.pe  
Sponsoring Registrar: NIC.PE  
Domain Status: ok  
Registrant Name: jaime arroyo vilcara  
Admin Name: BANCO INTERNACIONAL DEL PERU-INTERBANK  
Admin Email: dominiosibk@intercorp.com.pe  
Name Server: ns1-08.azure-dns.com  
Name Server: ns2-08.azure-dns.net  
Name Server: ns3-08.azure-dns.org  
Name Server: ns4-08.azure-dns.info  
>>> Last update of WHOIS database: 2023-08-21T23:58:04.815Z <<<

Domain Name: PRESTAMOS-WEB.ONLINE  
Registry Domain ID: D396209478-CNIC  
Registrar WHOIS Server: whois.hostinger.com  
Registrar URL: https://www.hostinger.com/  
Updated Date: 2023-09-13T07:05:22.0Z  
Creation Date: 2023-09-13T07:05:19.0Z  
Registry Expiry Date: 2024-09-13T23:59:59.0Z  
Registrar: HOSTINGER operations, UAB

#### E. Apreciación de la información:

- La presente campaña de Phishing permite a los actores de amenazas obtener información bancaria 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.

#### 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.
------------------------	---