	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°067	Fecha: 18-03-2024
		Página: 9 de 15

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de Phishing suplantando la identidad de “Plaza Vea”		
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 en el ciberespacio, se ha identificado una campaña de Phishing en la que ciberdelincuentes están suplantando la identidad del supermercado "Plaza Vea". En esta campaña maliciosa, utilizan una publicación en la red social Facebook, en la cual se ofrece una PlayStation 5 Slim por solo S/ 12, incitando a hacer clic en "Enviar solicitud" para aprovechar la supuesta oferta. El objetivo de esta actividad maliciosa es obtener credenciales de acceso, así como datos personales y bancarios de las posibles víctimas.

2. **DETALLES:**

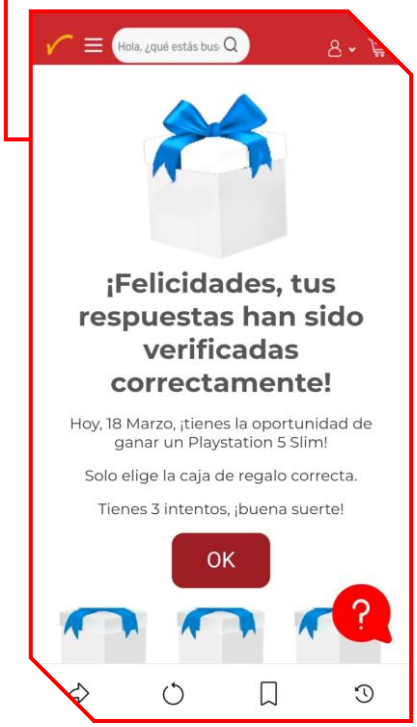
- Al hacer clic en "Enviar Solicitud", se redirige a un sitio web falso de "Plaza Vea", donde ofrecen ***“Una promoción especial con Sony. Se anuncia la posibilidad de adquirir una PlayStation 5 Slim por solo S/ 12.00 soles para 100 personas en Perú. Se invita a completar un formulario, indicando que los premios son limitados”.***

Paso 1. El formulario comienza con la pregunta **"¿Vive en Perú?".**

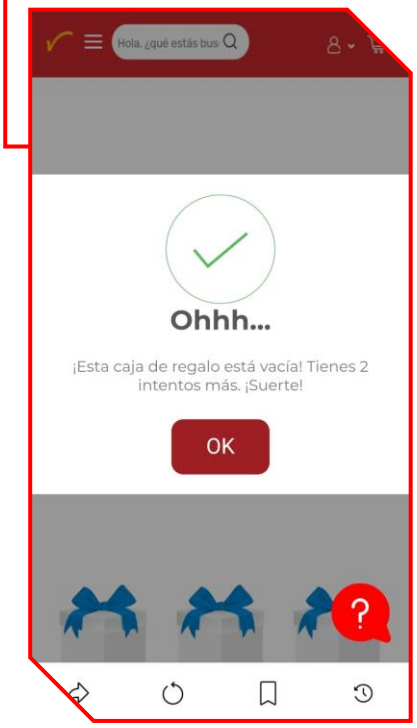
Paso 2. Continúa con la pregunta **"¿Ha utilizado productos Sony?".**

Paso 3. Prosigue con la pregunta **"¿Alguna vez ha comprado algo en Plaza Vea?".**

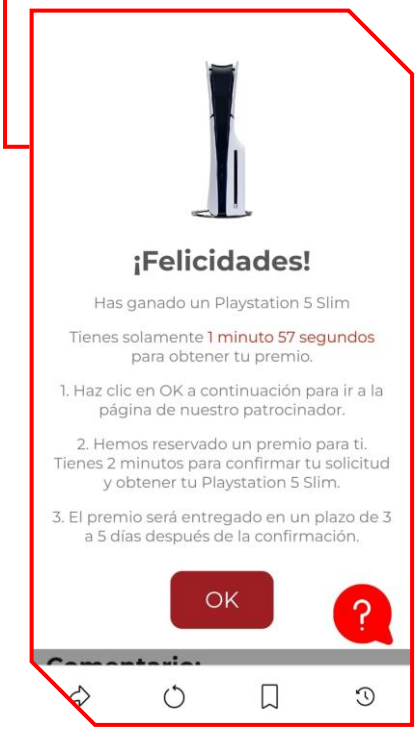
Paso 4. Después de completar el formulario, aparece el mensaje: "¡Felicidades! 3 intentos. ¡Buena suerte!".



Paso 5. Al seleccionar una caja, se muestra: "Caja vacía. 2 intentos restantes. ¡Buena suerte!".



Paso 6. Se anuncia "¡Felicidades! Ganaste un PlayStation 5 Slim", y se solicita hacer clic en "OK" para continuar.

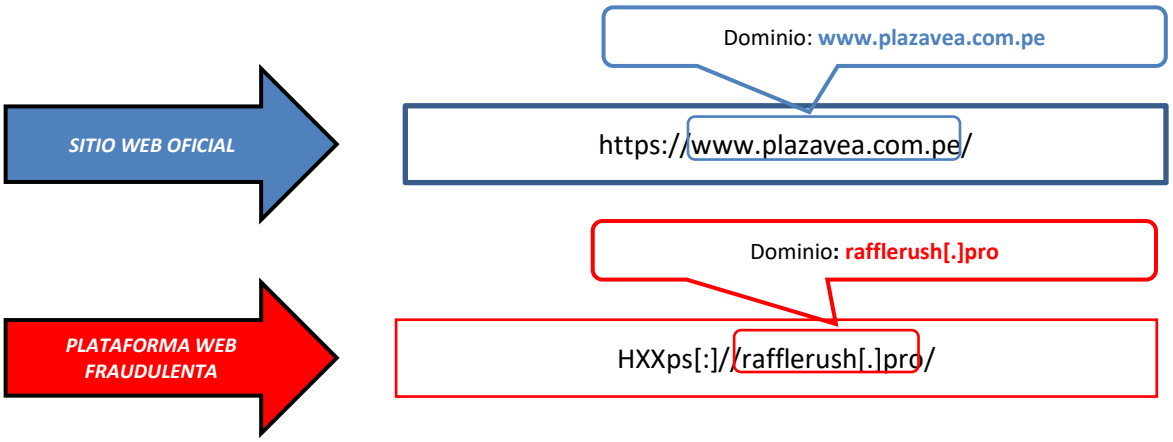


Paso 7. Luego, se solicita ingresar los datos personales de la víctima.

Paso 8. Seguidamente, se solicita ingresar los datos de la tarjeta de crédito para pagar el supuesto premio.

Paso 9. Finalmente, se reporta un error en el pago, pero los ciberdelincuentes capturaron los datos.

A. Comparación entre el sitio web oficial y el sitio web fraudulento de Plaza Vea:



- El sitio web fraudulento posee el **PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS), lo que hace más convincente a la víctima al momento de acceder.**

B. Proveedores de seguridad informática alertan como **SUPLANTACIÓN DE IDENTIDAD – PHISHING**:

Antiy-AVL	Malicioso	Avira	Suplantación de identidad
BitDefender	malware	ESET	Suplantación de identidad
Fortinet	Suplantación de identidad	Datos G	malware
Navegación segura de Google	Suplantación de identidad	búsqueda en seco	Malicioso

- Indicadores de compromiso:

  - URL: HXXps[:]//rafflerush[.]pro/
  - Dominio: rafflerush[.]pro/
  - SHA-256: 72a768c1f559654915d6270a1283815beb89f57f5f0f5dae45bb578df95163e0
  - Dirección IP: 172[.]67[.]176[.]79
  - Código: 200
  - Longitud: 33.52 KB

3. RECOMENDACIONES:

- Evitar hacer clic en enlaces sospechosos no vinculados al sitio oficial.
- Verificar cuidadosamente la URL para confirmar su correspondencia con el sitio web oficial.
- No seguir indicaciones de sitios web que generen desconfianza para preservar la seguridad de los datos personales y bancarios.
- Mantener el antivirus actualizado como primera defensa contra ataques cibernéticos.
- Evitar compartir la URL para prevenir riesgos en la seguridad en línea.
-

Fuente de Información:	Análisis propio de redes sociales y fuente abierta