	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 287	Fecha: 22-10-2022
		Página 07 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de phishing que tiene como objetivo robar credenciales de acceso, datos personales y/o bancarios de PayPal.		
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 actores de amenazas vienen llevando a cabo una campaña de phishing "tipo de robo de identidad en línea", que utilizando correos electrónicos falsos suplantando la identidad de "PayPal" para atraer la atención de la víctima, en el texto del mensaje se advierte que se ha detectado en la cuenta una actividad de acceso inusual, por lo que será cancelada a menos que se ingrese en el enlace que se adjunta, para actualizar la información, con el objetivo robar credenciales de acceso, datos personales y/o bancarios.

2. Proceso del ataque phishing:

Imagen 1: Sitio web falso preparado por los ciberdelincuentes solicita a la víctima, ingresar sus credenciales de acceso (correo electrónico y contraseña).

Imagen 2: Solicitud, para restaurar la cuenta y actividades, haga clic en <<continuar>>.

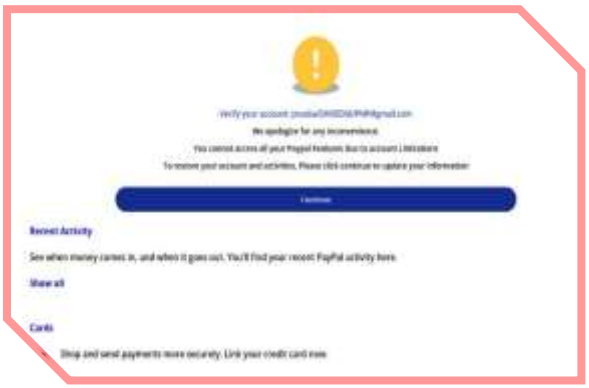


Imagen 3: Formulario, para vincular tarjeta y datos personales (clave, número de seguro, fecha de nacimiento, dirección de envió, código postal, número de tarjeta, caducidad, entre otros).

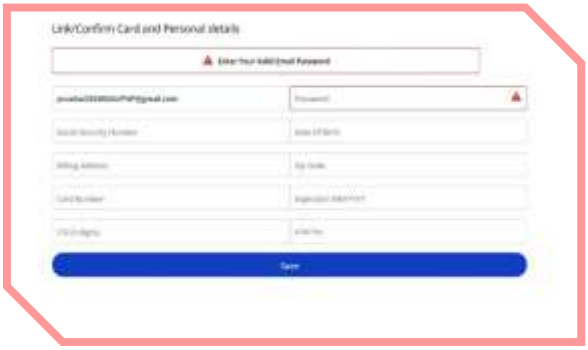


Imagen 4: Validación para vincular datos bancarios (clave, nombre del banco y número de cuenta).

Imagen 5: Engaño, solicitud para subir una foto del anverso y reverso de la identificación emitida por el estado para completar su verificación.

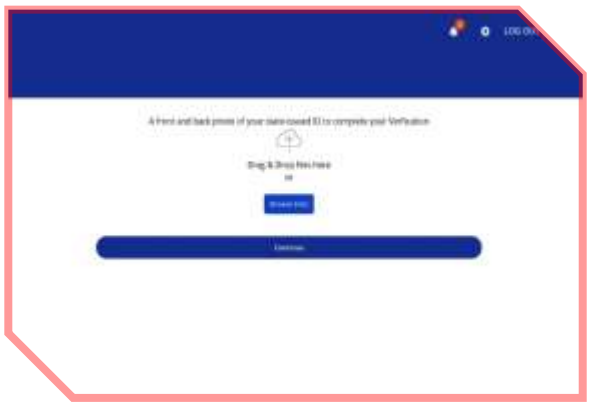
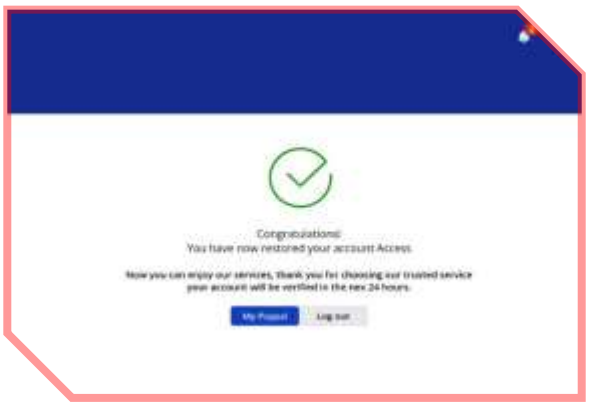


Imagen 6: Finalmente, indica que la cuenta se ha restaurado y puede acceder.



3. Comparación del sitio web oficial PayPal y sitio web falso:

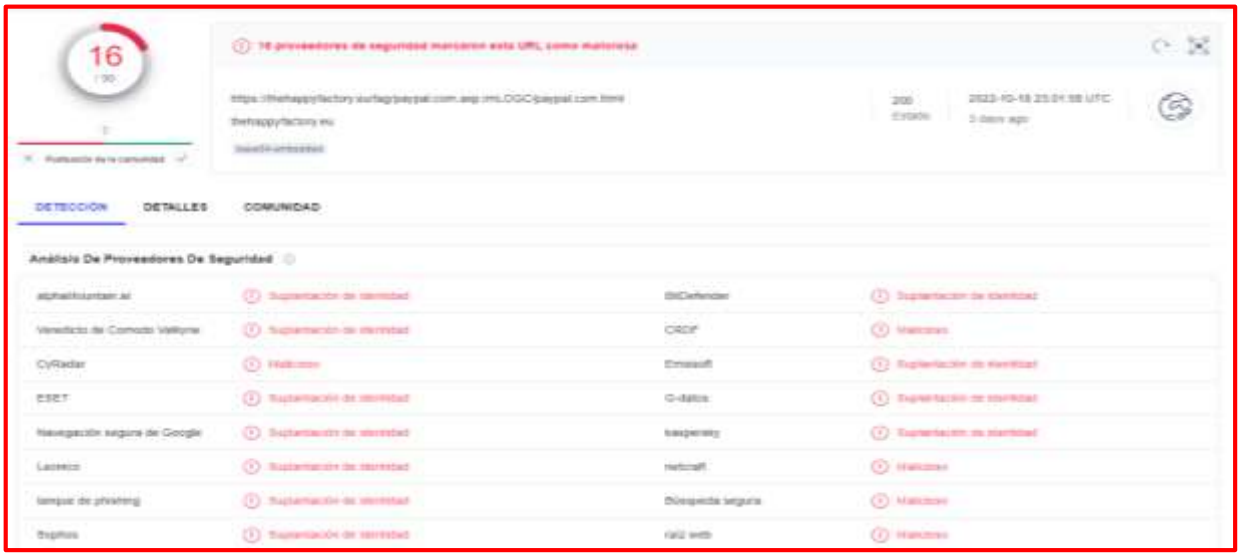
   - Sitio oficial : https://www.paypal.com
   - Sitio falso : hXXp[:]//thehappyfactory[.]eu/tag/paypal[.]com[.]axp[.]rmLOGC/paypal[.]com[.]html

   No tiene certificado de seguridad de protocolo HTTPS

   El dominio se hace pasar por el sitio oficial, pero no coincide

4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, obteniendo la siguiente información:

   - **URL:** hXXps[:]//thehappyfactory[.]eu/tag/paypal[.]com[.]axp[.]rmLOGC/paypal[.]com[.]html
   - **Dominio:** thehappyfactory[.]eu
   - **Direcciones IP:** 213[.]186[.]33[.]17
   - **Código De Estado:** 200
   - **Tamaño:** 57.94 KB
   - **SHA-256:** b9ecdc29b6312c07092a3fc91aa2f1f260f2d964f24c81af9b2cfce99d4a2598



5. **Otras detecciones del análisis**:

6. **Recomendaciones:**

- Acceder al sitio web a través de fuentes oficiales
- Evitar responder a mensajes enviados desde (correo electrónico, Whatsapp, SMS y otros), que contengan enlaces de dudosa procedencia.
- Verificar detenidamente la redacción y ortografía de la dirección URL, que coincidan con el sitio web oficial.
- Evitar proporcionar información personal y/o financiera a través de sitios webs de dudosa procedencia.
- Utilizar una firma de antivirus actualizado, ya que es la primera barrera ante posibles ataques cibernéticos.

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