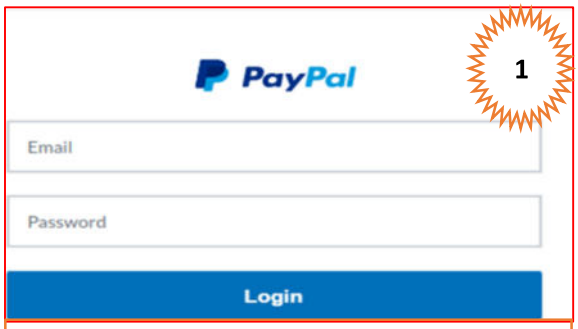
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 100	Fecha: 10-04-2022
		Página 3 de 5

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Phishing, suplantando la identidad de la compañía multinacional de pagos en línea 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		

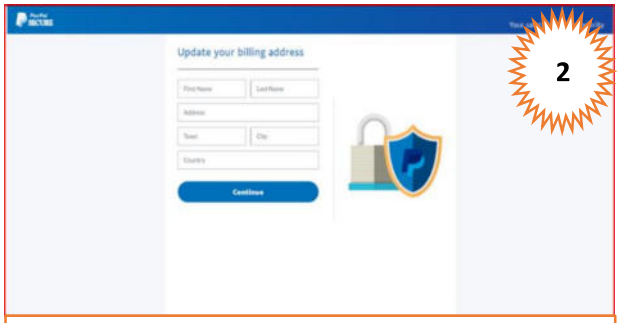
Descripción

1. A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes vienen llevando a cabo una campaña de Phishing, por medio de los diferentes navegadores web, dirigido a los clientes y/o usuarios de la compañía multinacional de pagos en línea PayPal; el cual, mediante la creación de un sitio web similar al original, solicitan a las posibles víctimas a realizar acciones indebidas que no son requeridas por dicha compañía, como supuestas actualizaciones de cuenta ingresado datos personales y/o bancarios.

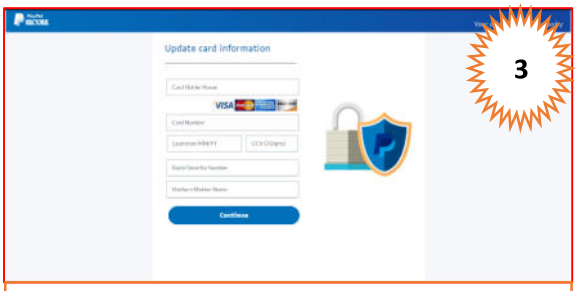
2. **Imagen**: Detalle del proceso del Phishing:



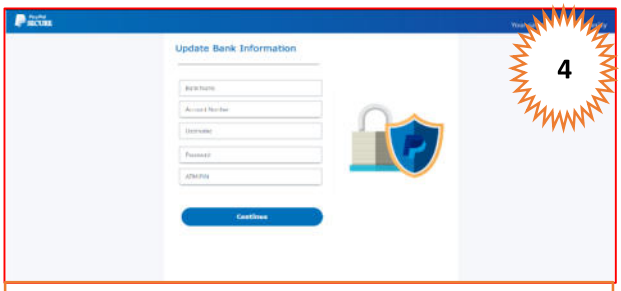
Solicita ingresar dirección de correo electrónico y contraseña de la cuenta.



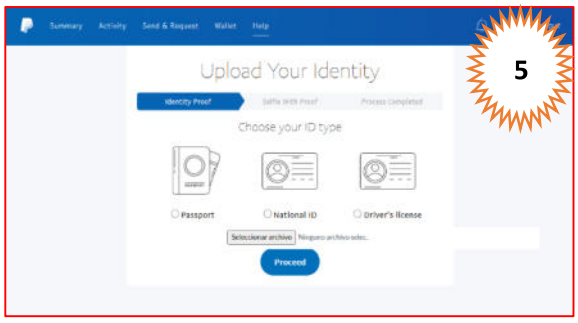
Luego, requiere actualizar la dirección de facturación.



Después, pide actualizar información de la tarjeta de crédito, visa, MasterCard, etc.

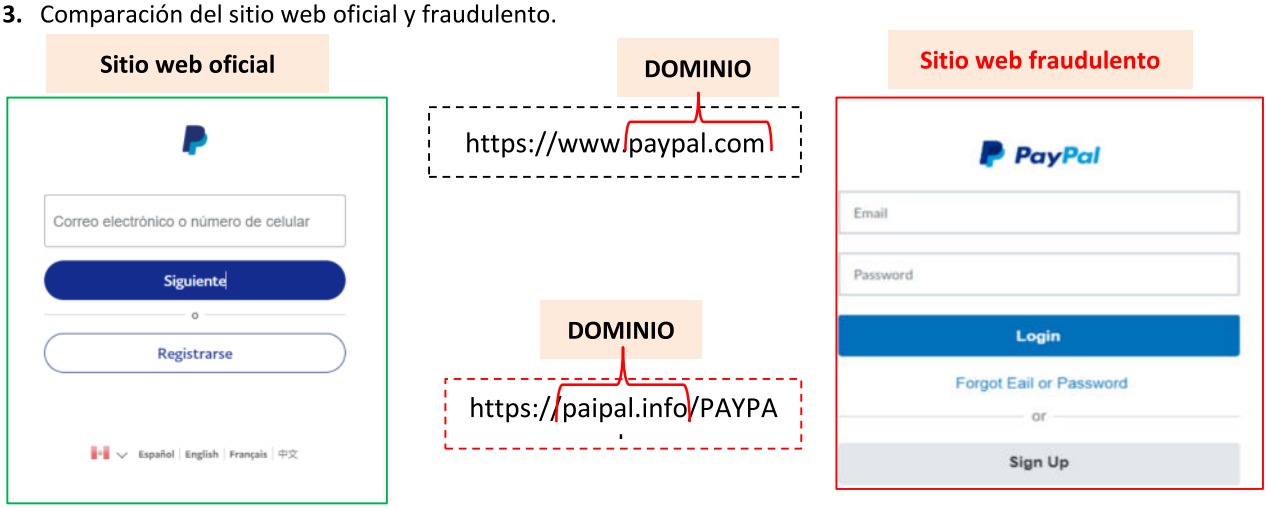


A continuación, debe ingresar datos bancarios, como nombre del banco, N° de cuenta, etc.



Por último, Solicita agregar la identidad del titular a través de un archivo.

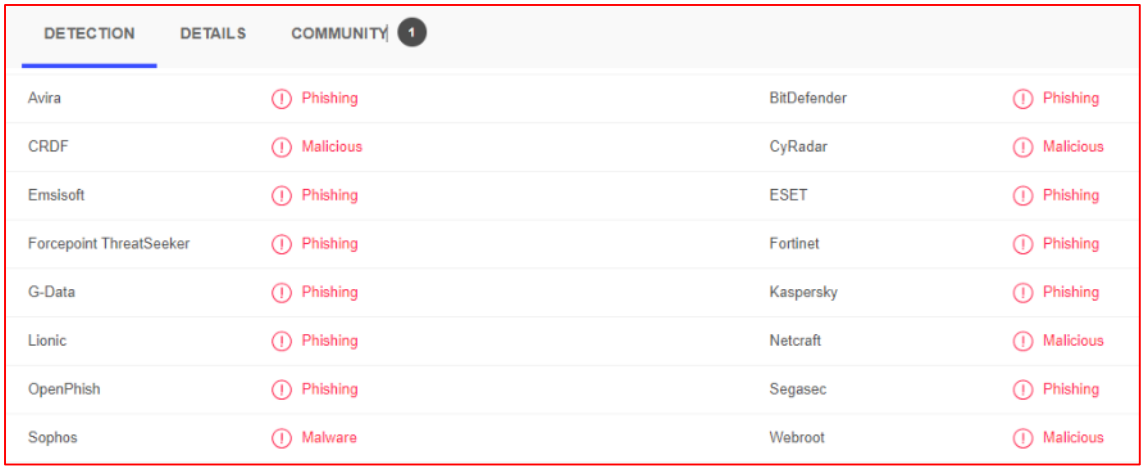
3. Comparación del sitio web oficial y fraudulento.



- Existe una similitud entre el fondo y forma de cada sitio web.
- Ambas URL´s utilizan el protocolo https, lo que hace más convincente a que las víctimas accedan al sitio web.
- La diferencia está en la URL, toda vez que el dominio del sitio web fraudulento, no coincide con el oficial.

4. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como Phishing (suplantación de identidad):

- Indicadores de compromiso:
  - URL: hxxps://paipal[.]info/PAYPAL
  - Dominio: paipal[.]info
  - IP: 185.176.221.79
  - Tamaño: 2.30 KB
  - SHA-256: a36419d9b4b9c596320ce246c29e29910fa10a1ab73e5a8c509b6f01e90e70be



5. Recomendaciones:

- No brindar información personal y/o bancaria en sitios web de dudosa procedencia.
- Ingresar de forma manual la URL de la entidad correspondiente.
- Verificar la información en la entidad oficial.
- No compartir la información con familiares o amigos.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener instalado un software antivirus.

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