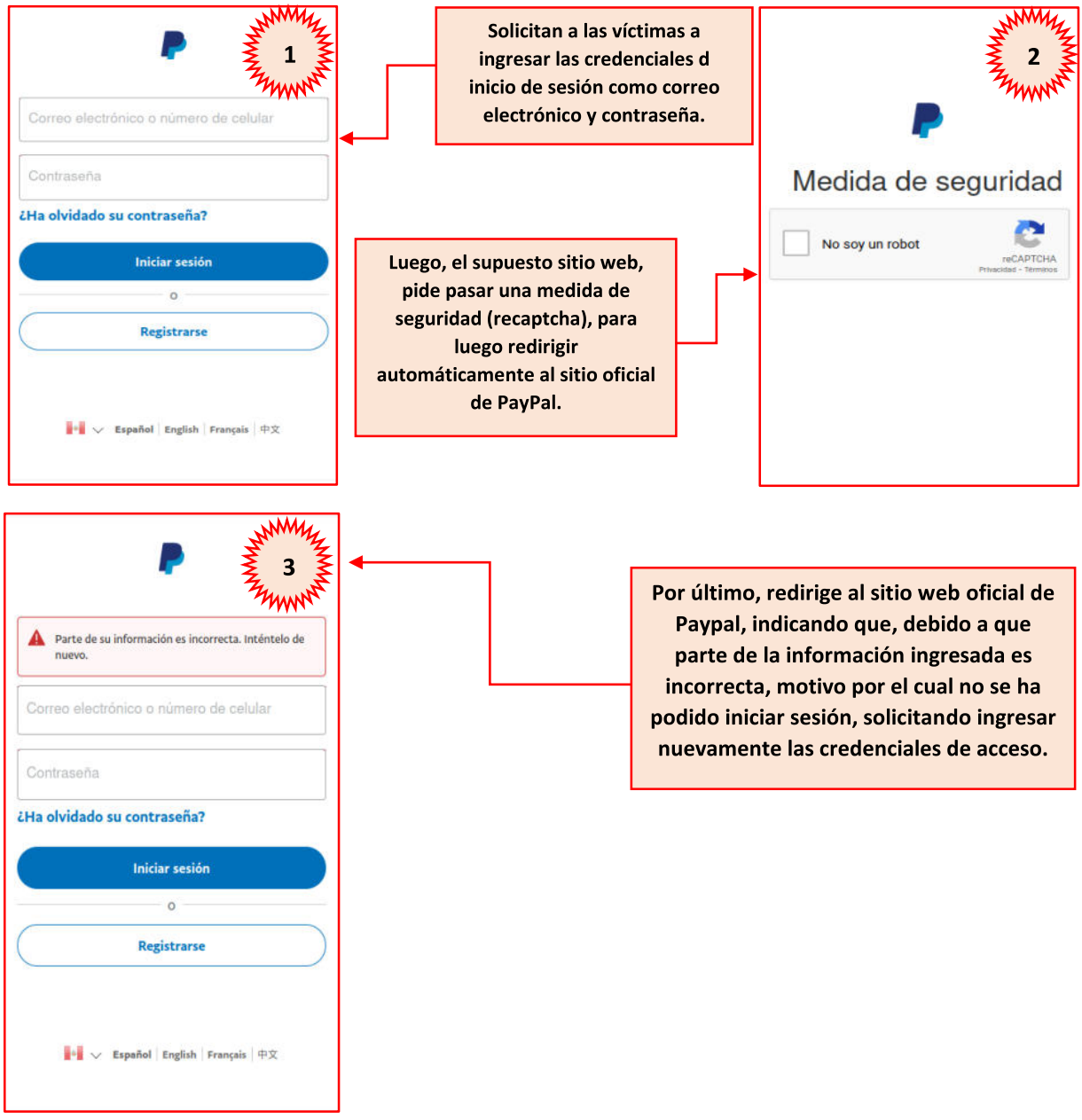
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 058	Fecha: 27-02-2022
		Página 5 de 7

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**			
Nombre de la alerta	Phishing, suplantando la identidad de la empresa 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, suplantando la identidad de la empresa de pagos en línea "PayPal", el cual tiene como finalidad apoderarse de manera ilícita de las credenciales de inicio de sesión de las posibles víctimas, como dirección de correo electrónico, contraseña.

2. Imagen: Detalles del proceso de estafa del Phishing.



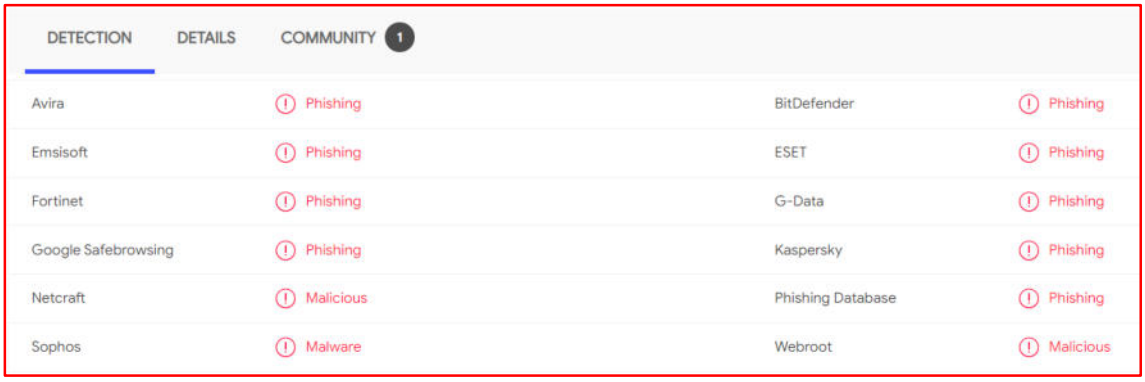
3. Comparación del sitio web oficial y fraudulento.

	Dominio
Sitio web Oficial	https://www.paypal.com/pe/signin
	Dominio
Sitio web fraudulento	hxxps[:]//inbound[.]paypal[.]interacgateway[.]com

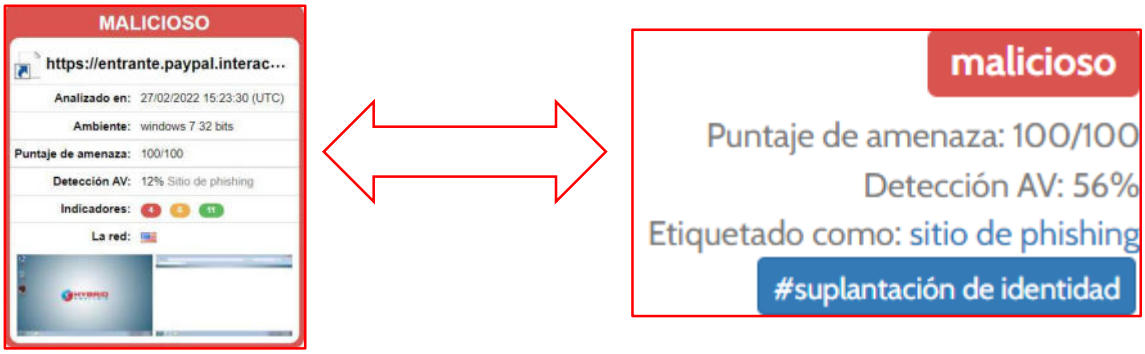
- El sitio web fraudulento utiliza protocolo HTTPS, lo que hace más convincente a que las víctimas accedan al sitio web de pagos en línea; sin embargo, la diferencia está en el dominio toda vez que, no coincide con el dominio oficial de PayPal.

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

- Indicadores de compromiso.
  - **URL Malicioso:** hxxps[:]//inbound[.]paypal[.]interacgateway[.]com
  - **Dominio:** interacgateway.com
  - **IP:** 192.254.190.210
  - **Tamaño:** 1.06 MB
  - **SHA-256:** 7a02d94b156360b8f864ef451aec710212981380a392bb60baa7b479df000358



- Otras detecciones.



5. Algunas Recomendaciones:

- Verificar detalladamente la URL de los sitios web a ingresar.
- No seguir instrucciones de sitios web fraudulentos.
- No ingresar a sitios webs, desde enlaces adjuntados a un mensaje o correo.
- Mantener instalado un software antivirus.
- No ingreses datos confidenciales en sitios web de dudosa procedencia.

Fuentes de información	Análisis propio de redes sociales y fuente abierta