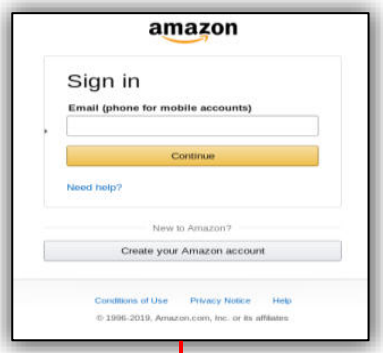
	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 077	Fecha: 18-03-2022
		Página 8 de 10

Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**			
Nombre de la alerta	Phishing, suplantando la identidad de la aplicación de “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 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, a través de los diferentes navegadores web, quienes vienen suplantando la identidad del servicio digital de Amazon (Compañía de comercio electrónico), con la finalidad de obtener información confidencial de las víctimas como, dirección de correo electrónico, contraseña, fecha de nacimiento, país, número telefónico, datos bancarios, entre otros.

2. ***Imagen: detalles del proceso de la estafa del Phishing***.

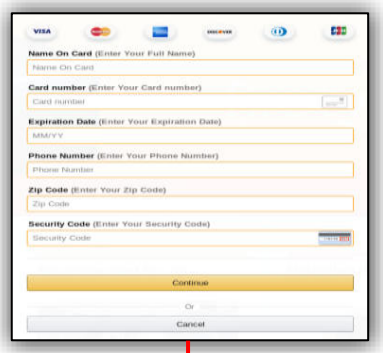


Paso Nº 01

El sitio web, solicita ingresar la dirección de correo electrónico y dar clic en CONTINUAR.

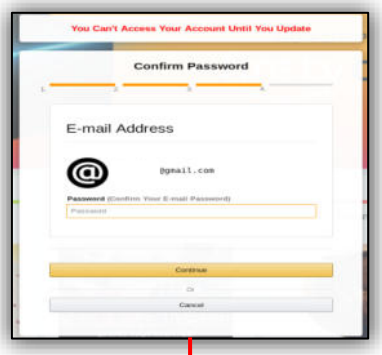
Paso Nº 02

Luego de haber ingresado el correo electrónico, requiere la contraseña, para iniciar sesión.



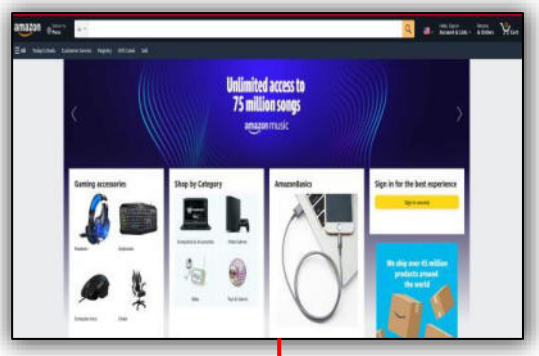
Paso Nº 03

Al introducir las credenciales y hacer clic en <Iniciar sesión>, se cargará otro formulario en el cual solicitará ingresar los datos personales del usuario.



Paso Nº 04

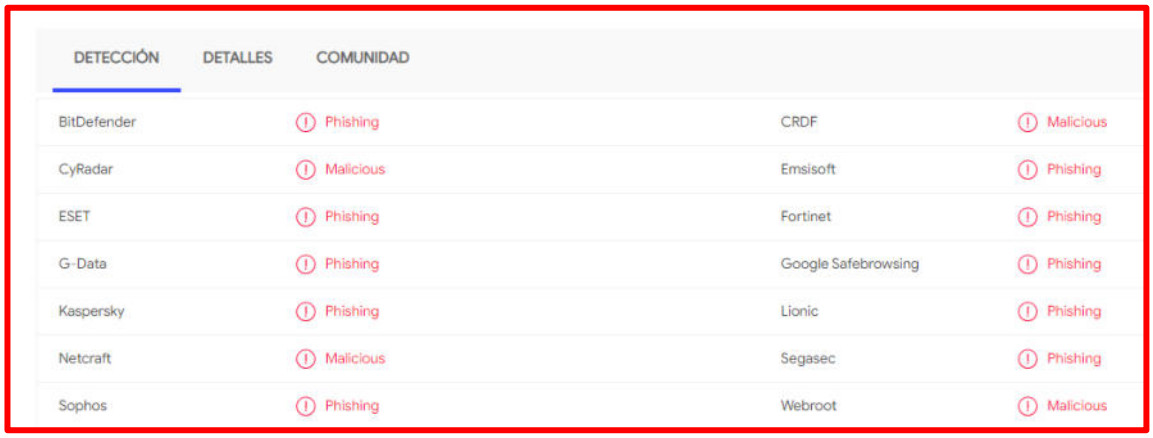
Después de haber completado toda la información personal y/o bancario, requiere enlazar el correo electrónico ingresando la contraseña.



Paso Nº 05

Finalmente, es redirigido al sitio web oficial de Amazon, aludiendo un aparente error de autenticación; sin embargo, los datos fueron capturados por los ciberdelincuentes.

3. ***Se procedió a analizar la URL fraudulenta, obteniendo como resultado que DIEZ (10) proveedores de seguridad informática alertan como SUPLANTACIÓN DE IDENTIDAD – PHISHING y CUATRO (04) como MALICIOSO.***



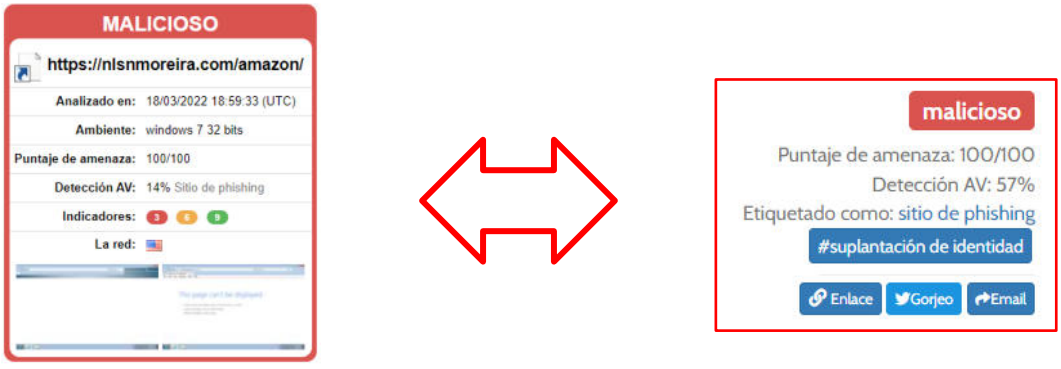
DETECCIÓN | DETALLES | COMUNIDAD

BitDefender	Phishing	CRDF	Malicious
CyRadar	Malicious	Emsisoft	Phishing
ESET	Phishing	Fortinet	Phishing
G-Data	Phishing	Google Safebrowsing	Phishing
Kaspersky	Phishing	Lionic	Phishing
Netcraft	Malicious	Segasec	Phishing
Sophos	Phishing	Webroot	Malicious

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

- ✓ **SHA-256** : 60fe71638e67427ea3d7714021cdbbc3bd67f503641d9f1b2fa6d4c2d7ea3787
- ✓ **URL** : hxxps://nlsnmoreira[.]com/amazon/
- ✓ **Dominio** : nlsnmoreira[.]com
- ✓ **Tamaño** : 7.94KB

5. ***Otras detecciones:***



6. ***Apreciación de la información*:**

- La presente campaña de Phishing, permite a los actores de amenazas obtener información personal, del correo electrónico y cuentas bancarias.

- La propagación del sitio web fraudulento se realiza mediante envió masivos de email (SPAM), con la finalidad de obtener información sensible de las víctimas; asimismo, a través de las aplicaciones de mensajería instantánea entre ellos WhatsApp, Telegram y Messenger.

7. ***Algunas recomendaciones:***

- Verificar detalladamente las URL de los sitios web.
- No abrir o descargar archivos sospechosos.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.
- Tener precaución al abrir enlaces de dudosa procedencia.

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