	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 104		Fecha: 04-05-2023
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Campaña de Phishing suplantando la identidad de la compañía de comercio electrónico 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, por medio de los diferentes navegadores web, dirigido a los clientes y/o usuarios de la compañía de comercio electrónico Amazon; el cual, mediante la creación de un sitio web similar al original, solicitan a las posibles víctimas a ingresar información personal y bancaria como credenciales de inicio de sesión, contraseña, dirección de correo electrónico, clave, N° de tarjeta, fecha de expiración, etc.

2. Detalles del proceso de Phishing:



amazon 1

acceso

Correo electrónico (teléfono para cuentas móviles)

contraseña [¿Olvidaste tu contraseña?](#)

acceso

Permanecer conectado [detalle](#)

[¿Nuevo en Amazon?](#)

crear una cuenta de amazon

Al iniciar sesión, acepta nuestros [Términos de uso](#) y [venta](#) y nuestro [Aviso de privacidad](#).

FOTOCAPTURA N°01

Solicita ingresar las credenciales de inicio de sesión como dirección de Gmail y contraseña

FOTOCAPTURA N°02

Pide dirección de domicilio, país, región, provincia, a fin de realizar una verificación de

FOTOCAPTURA N°03

Requiere, datos de tarjeta bancaria, a fin de realizar una verificación de identidad



amazon 2

Verificación de dirección

Por favor ingrese su dirección de facturación (Paso 1 de 3)

nombre completo

Dirección Línea 1

Dirección 2

ciudad

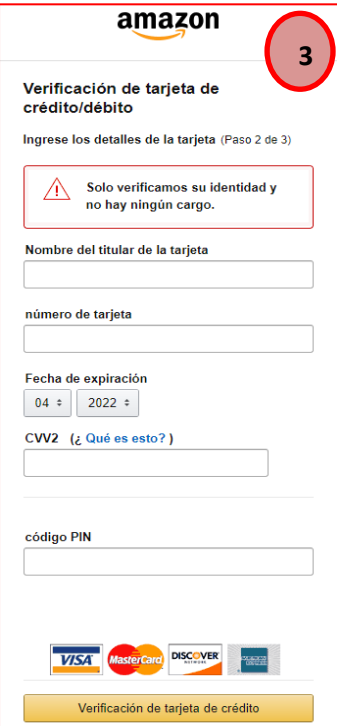
Estado / Provincia / Región

codigo postal

número de teléfono

País

Confirmar dirección de facturación



amazon 3

Verificación de tarjeta de crédito/débito

Ingrese los detalles de la tarjeta (Paso 2 de 3)

! Solo verificamos su identidad y no hay ningún cargo.

Nombre del titular de la tarjeta


número de tarjeta

Fecha de expiración

04 : 2022 :

CVV2 (¿Qué es esto?)

código PIN



Verificación de tarjeta de crédito



amazon 4

autenticación por mensaje de texto

Ingrese el código enviado a su número de teléfono (Paso 3 de 3)

codigo sms

confirmación

FOTOCAPTURA N°04

Después, indica que ingrese el código de autenticación enviado a través de mensaje de texto



amazon 5

Iniciar sesión

Número de celular o correo electrónico

Contraseña [¿Olvidaste tu contraseña?](#)

Iniciar sesión

Al continuar, aceptas las [Condiciones de uso](#) y el [Aviso de privacidad](#) de Amazon.

Recuérdame. [Detalles](#)

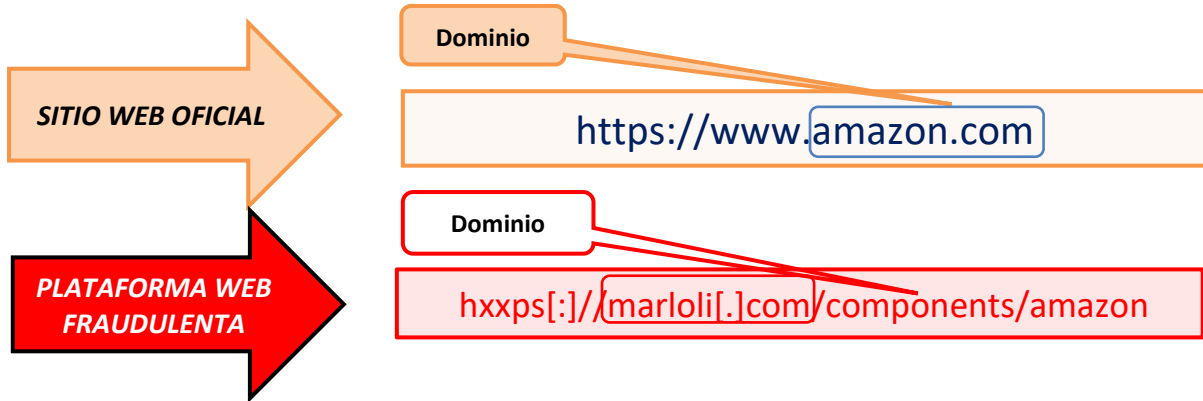
[¿Eres nuevo en Amazon?](#)

Crea tu cuenta de Amazon

FOTOCAPTURA N°05

Una vez ingresa los datos solicitados, redirige de forma automática al sitio web oficial de Amazon; toda vez que los autores de la amenaza ya se apoderaron de los datos brindados

3. Comparación del sitio web oficial y sitio web fraudulento de Amazon:



- Existe una similitud entre el fondo y forma de cada sitio web (oficial y fraudulento).
- Ambos sitios webs poseen el **PROTOCOLO SEGURO DE TRANSFERENCIA DE HIPERTEXTO (HTTPS)**, lo que hace mas convincente a que las víctimas ingresen a sitio web fraudulento

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

alphaMountain.ai	⚠ Malicious	BitDefender	⚠ Malware
CyRadar	⚠ Malicious	Emsisoft	⚠ Phishing
Fortinet	⚠ Phishing	G-Data	⚠ Malware
Lionic	⚠ Malicious	Netcraft	⚠ Malicious
Trustwave	⚠ Phishing	Abusix	✅ Clean

- Indicadores de compromiso:
 - URL: hxxps[:]//marloli[.]com/components/amazon
 - Dominio: marloli[.]com
 - SHA-256: 05193241298ec54241b307d8379da6953244404d7878f72ba797fa8776ab2cc1
 - Dirección IP: 45[.]79[.]148[.]55
 - Tamaño: 26.15 KB

5. Recomendaciones:

- Verificar la información en la entidad correspondiente.
- No seguir las instrucciones de sitio web sospechoso.
- Mantener el antivirus actualizado.
- No ingresar información confidencial a enlaces de dudosa procedencia.

Fuentes de información

- Análisis propio de redes sociales y fuente abierta