PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

Siempre con el pueblo

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 13 de junio de 2022

N° 158-2022-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 158	Fecha: 13-06-2022
		Página 4 de 6

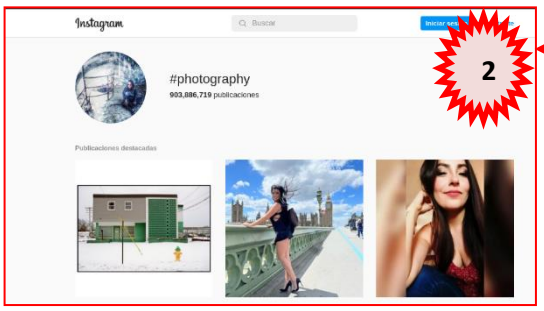
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Campaña de Phishing, suplantando la identidad de la red social Instagram		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, 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 que se difunde en los diferentes navegadores web, suplantando la identidad de la red social Instagram, con la finalidad de robar las credenciales de inicio de sesión de las posibles víctimas como número telefónico o dirección de correo electrónico y contraseña.

2. Proceso del ataque Phishing.

Solicita ingresar las credenciales de inicio de sesión, como número de teléfono o dirección de correo electrónico y contraseña de la cuenta.

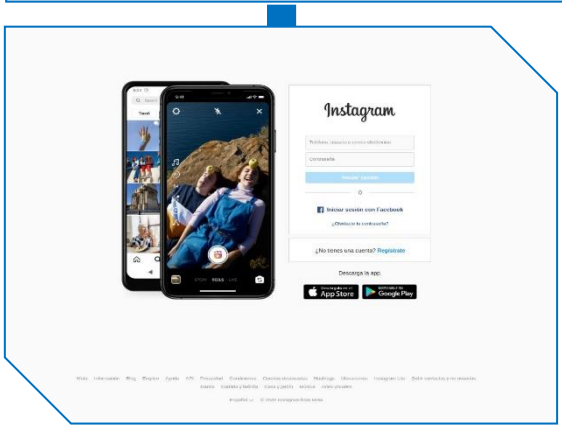


Al hacer clic en iniciar sesión redirige automáticamente a un supuesto perfil de Instagram, toda vez que los ciberdelincuentes ya se apoderaron de dicha información.

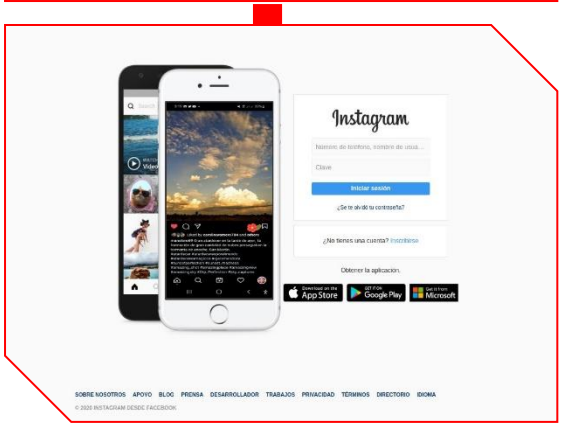
Por último, muestra el sitio web oficial de Instagram solicitando nuevamente ingresar las credenciales de inicio de sesión.

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

SITIO WEB OFICIAL
URL: https://www.instagram.com/



SITIO WEB FRAUDULENTO
URL: hxxp://instagramphotos-contests[.]netlify[.]app



- Existe una similitud entre el fondo y forma de cada sitio web.
- La URL hxxp://instagramphotos-contests[.]netlify[.]app del sitio web fraudulenta NO POSEE EL PROTOCOLO DE SEGURIDAD DE RED (https).

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

- **URL** : hxxp[:]//instagramphotos-contests[.]netlify[.]app
- **Dominio :** instagramphotos-contests[.]netlify[.]app
- **IP.** : 52[.]73[.]153[.]209
- **Tamaño** : 155.39 KB
- **SHA-256 :** b09ed700a85c2e798fcc78d6f7d4f27d10df17a3d9f853d7e6759e994cd791fa

DETECTION | DETAILS | LINKS | COMMUNITY

Security Vendors' Analysis

Avira	Phishing	BitDefender	Phishing
CRDF	Malicious	CyRadar	Malicious
Emsisoft	Phishing	ESET	Phishing
Forcepoint ThreatSeeker	Phishing	Fortinet	Phishing
G-Data	Phishing	Google Safebrowsing	Phishing

5. Algunas Recomendaciones:

- Verificar la información en la entidad correspondiente.
- Acceder al sitio web a través de sus fuentes oficiales.
- No abrir enlaces de dudosa procedencia.
- No seguir indicaciones de sitios web fraudulentos.
- No compartir la información con terceras personas, amigos o familiares y otros.
- Mantener instalado un servicio de antivirus en el dispositivo.

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

Índice alfabético