



PERÚ

Presidencia
del Consejo de Ministros

Secretaría de Gobierno
y Transformación Digital



Siempre
con el pueblo



ALERTA INTEGRADA DE SEGURIDAD DIGITAL



Lima, 20 de noviembre de 2022

ALERTA INTEGRADA DE SEGURIDAD DIGITAL



315-2022-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

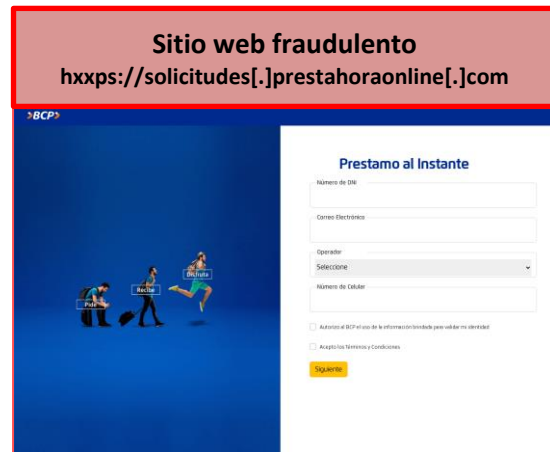
Phishing, suplantando la identidad del Banco de Crédito del Perú - BCP	4
Índice alfabético	6

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 315		Fecha: 20-11-2022
			Página 4 de 6
Componente que reporta	DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ		
Nombre de la alerta	Phishing, suplantando la identidad del Banco de Crédito del Perú - BCP		
Tipo de ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Enlaces de internet		
Código de familia	C	Código de subfamilia	C07
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 del Banco de Crédito del Perú - BCP; el cual, mediante la creación de un sitio web similar al original, requiere a las posibles víctimas a solicitar la aprobación de un préstamo inmediato, ingresando datos personales y/o bancarios, como DNI, N° de tarjeta bancaria, clave web, fecha de vencimiento, clave de seguridad, número de contacto, entre otros.
2. Proceso del ataque Phishing:



3. Comparación del sitio web oficial y fraudulento:



- La diferencia está en la URL, toda vez que el dominio del sitio web fraudulento, no coincide con el oficial.
- Ambos sitios webs utilizan el protocolo https, lo que hace más convincente para que las víctimas ingresen a dicho sitio web.

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

- **URL:** hxxps://solicitudes[.]prestahoraonline[.]com
- **Dominio:** solicitudes[.]prestahoraonline[.]com
- **Direcciones IP:** 20.25.21.155
- **Tamaño:** 6.43 KB
- **SHA-256:** d2e66969f0c0df91a326d8367995a9de17cfbfa097dba24012e69f76cd096d3b

Antiy-AVL	⚠ Malicious	BitDefender	⚠ Phishing
ESET	⚠ Malware	Forcepoint ThreatSeeker	⚠ Malicious
Fortinet	⚠ Phishing	G-Data	⚠ Phishing
Kaspersky	⚠ Malware	Netcraft	⚠ Malicious
Seclookup	⚠ Malicious	Sophos	⚠ Phishing

5. Recomendaciones:

- No abrir correos ni mensajes de dudosa procedencia
- Desconfiar de los enlaces y archivos enviados a través de mensajes o correos electrónicos
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Prestar atención en los detalles de los mensajes o redes sociales
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales

Fuentes de información

- Análisis propio de redes sociales y fuente abierta

Índice alfabético

BCP	4
fraudulento	5
Phishing	4
víctimas	4