Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°118	Fecha: 21-05-2024
		Página: 4 de 6

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Phishing, suplantado la identidad del MTC		
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 Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. ANTECEDENTES:

Se está intentando suplantar identidad (phishing) para engañar a usuarios del sistema de trámite Documentario y de Casilla Electrónica del MTC, con el objetivo que compartan contraseñas y otra información confidencial.

2. DETALLES:

El MTC reportó el siguiente comunicado para informar a los usuarios sobre la necesidad de estar alerta ante estos ataques de suplantación, y evitar brindar información que luego pueda ser comercializada y usada en perjuicio de los mismos usuarios.

Los ataques de phishing son correos electrónicos fraudulentos, mensajes de texto, llamadas telefónicas o sitios web diseñados para engañar a los usuarios, para descargar malware, compartir información confidencial o datos personales (seguridad social y números de tarjetas de crédito, números de cuenta bancaria, credenciales de inicio de sesión) u otras acciones que expongan a sus organizaciones.

El éxito de los ataques de phishing suele dar lugar a robos de identidad, fraudes con tarjetas de crédito, ataques de ransomware, filtraciones de datos y enormes pérdidas económicas para particulares y empresas.

IoC:

https://pe.postcloth.trickip.net/message

3. RECOMENDACIONES:

- Verificar la información en la entidad correspondiente.
- Acceder al sitio web a través de fuentes oficiales.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Hacer uso del doble factor de autentificación.
- Revisar las cuentas existentes en su servidor y confirmar que no se hayan creado nuevas cuentas.
- Desactivar automáticamente las cuentas del empleado que haya cesado de la empresa.
- Practicar una higiene estricta de sus contraseñas. Utilizar contraseñas únicas y complejas, y distintas para cada una de las cuentas, y cambiarlas periódicamente.
- Verificar que no exista algún software sospechoso en sus sistemas.
- Realizar periódicamente un escaneo completo a su infraestructura con antivirus. Incluso, analizar el rendimiento de procesamiento y discos duros para asegurarse que no esté alterado.
- Revisar si hay algún tipo de variación en la información o fuga de datos de la empresa y sus bases de datos.
- Capacitar y concientizar a los usuarios sobre seguridad y mejores prácticas, para reconocer las estafas de phishing y saber tratar cualquier correo electrónico sospechoso y mensaje de texto.

Fuente de Información:	MTC y fuente abierta.