Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°105	Fecha: 06-05-2024
		Página: 4 de 6

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Cuidado con los Ataques de Phishing dirigidos a usuarios de Tarjetas AmericanExpress		
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:

Los ciberdelincuentes se dirigen a los titulares de tarjetas American Express a través de correos electrónicos engañosos que imitan las comunicaciones oficiales del gigante de los servicios financieros.

2. DETALLES:

Según un tweet reciente de Avast Threat Labs, el ataque de phishing comienza con un correo electrónico que parece ser de American Express instando a los destinatarios a participar en un proceso de configuración falso de una "Clave de seguridad personal de American Express".

Estos correos electrónicos pretenden alertar a los destinatarios sobre una supuesta "verificación de seguridad crítica", instándolos a actualizar los detalles de su cuenta American Express de inmediato. El objetivo principal de estos correos electrónicos de phishing es engañar a los destinatarios para que revelen sus credenciales de inicio de sesión.

El correo electrónico contiene un enlace que dirige a los usuarios a una página web fraudulenta alojada en plataformas como Google Forms.

A las víctimas se les pide que ingresen su número de seguro social, fecha de nacimiento, apellido de soltera de la madre, dirección de correo electrónico y detalles completos de su tarjeta American Express, incluidos los códigos de seguridad y la fecha de vencimiento.

El diseño y el lenguaje del correo electrónico y la página web imitan fielmente las comunicaciones legítimas de American Express, lo que hace que la estafa sea particularmente convincente.

American Express aconseja a los clientes que estén atentos e informen inmediatamente de actividades sospechosas.

3. RECOMENDACIONES:

- Verificar la dirección de correo electrónico del remitente.
- Buscar errores ortográficos sutiles o dominios incorrectos que puedan indicar un intento de phishing.
- Buscar saludos genéricos. Los correos electrónicos de phishing suelen utilizar saludos genéricos como "Estimado cliente" en lugar de su nombre.
- No hacer clic en enlaces sospechosos o no solicitados. En su lugar, visitar el sitio web escribiendo la dirección directamente en su navegador.
- Comunicarse directamente con la empresa, si recibe una solicitud inesperada de información personal, utilizando un número de teléfono o una dirección de correo electrónico desde su sitio web oficial.
- Utilizar software de seguridad. Proteger sus dispositivos con software antivirus actualizado, que puede ayudar a detectar y bloquear descargas y sitios maliciosos.
- Diseñar una estrategia de concientización y capacitación que incluya la responsabilidad en el manejo de la información. Realizar capacitaciones periódicas para dos grupos: los usuarios finales y su equipo de seguridad.

Fuente de Información:	• hxxps://gbhackers.com/beware-of-phishing-attacks/