Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°184	Fecha: 10-08-2024 Página: 4 de 5

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Alertan de la nueva estafa del papel en el parabrisas		
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 ladrones cada vez son más inventivos a la hora de intentar robar, y WhatsApp se ha convertido en una herramienta cada vez más utilizada por los estafadores. Cada vez son más los que utilizan este mecanismo para enviar mensajes fraudulentos con los que intentan obtener información o datos de las personas estafadas.

Se está gestando esta nueva modalidad de estafa que consiste en dejar un papel en el auto, el cual ha sufrido un accidente menor, para que los ilusos conductores caigan en la trampa y los ciberdelincuentes puedan acceder a los datos del teléfono móvil.

2. DETALLES:

Este nuevo fraude tiene un funcionamiento extremadamente simple, pero no por ello deja de ser muy efectivo.

Al volver al lugar en el que habías dejado estacionado tu vehículo, te encuentras con un papel en el parabrisas en el que dice que te han abollado el coche sin querer o te han roto el espejo retrovisor, y en esa nota el estafador te dejará su número de teléfono para que le llames y así se pueda solucionar el inconveniente con la compañía de seguros.

Una vez llamas al número de teléfono apuntado en el papel, los estafadores te dirán que para poder contactar con la aseguradora y, de esta manera, arreglar todos los papeles y cobrar todo el dinero, debes ingresar a un enlace que te enviarán a través de WhatsApp. La víctima, pensando que es lo que debe hacer, hace clic, pero en realidad es una estafa.

Al clicar en ese link, los estafadores pueden introducirse y revisar todos los datos de tu teléfono, e incluso puede que te pidan alguna contraseña, los nombres y apellidos e incluso el DNI. Por lo tanto, ya estás a la merced de los ladrones, que aprovecharán para utilizar la tarjeta de crédito que tienes guardada en el móvil y así realizar cuantiosos cargos directamente a tu cuenta bancaria.

3. RECOMENDACIONES:

- Evitar hacer clic en enlaces o anuncios sospechosos, que provengan de correos electrónicos, mensajes de texto o mensajes de redes sociales que soliciten información personal.
- Revisar con atención los permisos solicitados por cualquier aplicación antes de instalarla. Desconfiar de las extensiones que solicitan un acceso excesivo a sus datos.
- Mantener el software actualizado. Actualizar periódicamente el sistema operativo, navegador y software antivirus para protegerse contra las últimas amenazas.
- Utilizar una solución antivirus confiable que pueda ayudar a detectar y bloquear software malicioso.
- Considerar utilizar un administrador de contraseñas dedicado para proteger su información confidencial.
- Realizar copias de seguridad de sus datos importantes periódicamente.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://www.20minutos.es/motor/actualidad/adios-estafas-timo-nota-parabrisas-coche-5536249/ • hxxps://www.farodevigo.es/sociedad/2024/08/15/maxima-alerta-estafa-papel-parabrisas-dv-107027060.html • Reporte De Seguridad Digital – CNSD