



Nro. Alerta:	EC-2022-89	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	 TLP:BLANCO		
Fecha:	03-ocubre-2022	EcuCERT advierte campaña Phishing “Cooperativa CREA”	V 1.2

I. DATOS GENERALES:

Clase de alerta:	Fraude – Scam
Tipo de incidente:	Phishing
Nivel de riesgo:	Alto

II. INTRODUCCIÓN

La técnica de Phishing es una forma de fraude a través de medios digitales que pretende engañar a las víctimas para obtener información personal confidencial tales como credenciales de cuentas de correo, banca electrónica, etc. En este sentido, los ciberdelincuentes emplean diferentes técnicas y artimañas para obtener información; por ejemplo:

- Contactarse telefónicamente simulando pertenecer a una institución financiera y brindar ciertos productos/servicios o un presunto mal uso de la tarjeta de crédito. Esta actividad se conoce como **VISHING**.
- Otra manera de obtener información personal es mediante ingeniería social mediante mensajes de texto o más comúnmente; a través de WhatsApp; esta técnica se denomina **SIMSHING** o SMS fraudulentos.

III. VECTOR DE ATAQUE:



A través de la aplicación de mensajería WhatsApp, se realiza una campaña de suplantación de identidad; haciéndose pasar por funcionarios de la Cooperativa de Ahorro y Crédito Crea Ltda.

IV. INDICADORES DE COMPROMISO:

El indicador de compromiso reportado y asociados a la campaña maliciosa es:

- +593 99 260 6175
- [https://www.\[.facebook\[.\]com/Coop-Crea-111028161489708](https://www.[.facebook[.]com/Coop-Crea-111028161489708)



Nro. Alerta:	EC-2022-89	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	 TLP:BLANCO		
Fecha:	03-ocubre-2022	EcuCERT advierte campaña Pishing “Cooperativa CREA”	V 1.2

V. IMAGEN DE LA CAMPAÑA

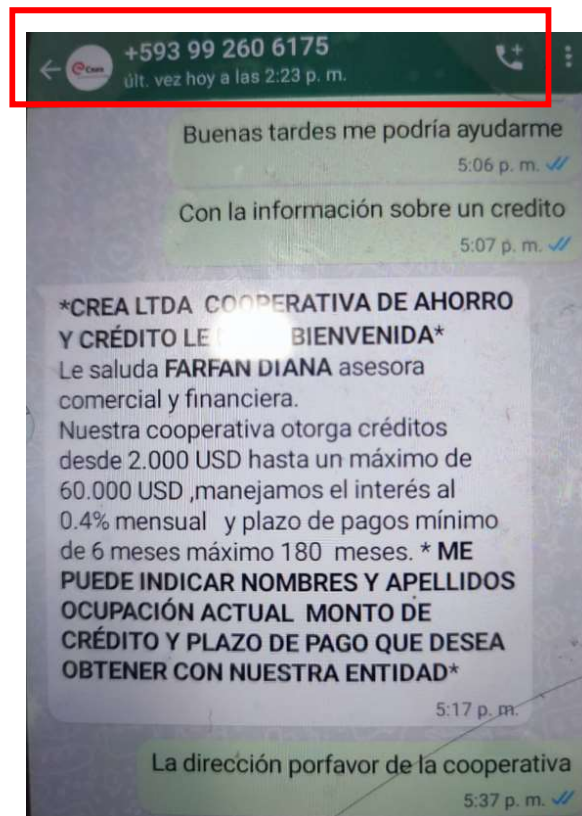




Figura 1.- Número telefónico que suplanta a Cooperativa CREA

Nro. Alerta:	EC-2022-89	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	 TLP:BLANCO		
Fecha:	03-ocubre-2022	EcuCERT advierte campaña Pishing “Cooperativa CREA”	V 1.2

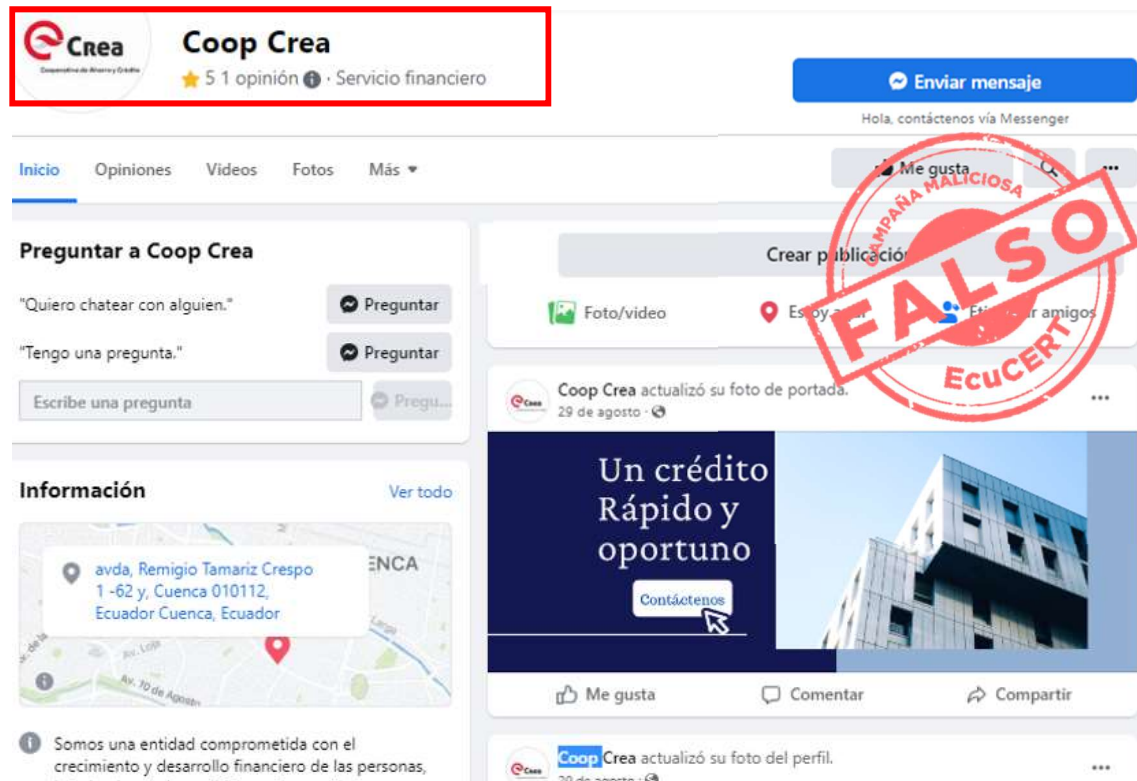




Figura 2.- Sitio que suplanta a Cooperativa CREA

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Hacer caso omiso a correos, links o mensajes de dudosa procedencia y márcalos como spam o bloquearlos.
- Ante cualquier duda contactarse directamente con la empresa suplantada para su comprobación y/o denuncia.
- Nunca entregue los usuarios y contraseñas solicitados a través de correos electrónicos, redes sociales o llamadas telefónicas, sitios web desconocidos
- Instalar y mantener actualizado una solución antivirus / antimalware.
- Bloquear los sitios web indicados en la sección indicadores de compromisos
- Informarse continuamente sobre tipos de amenazas en internet.



Nro. Alerta:	EC-2022-89	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	 TLP:BLANCO		
Fecha:	03-ocubre-2022	EcuCERT advierte campaña Pishing “Cooperativa CREA”	V 1.2

VII. Descargo de responsabilidad

- La información en la presente alerta; se proporciona "tal cual" solo con fines informativos. EcuCERT no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

