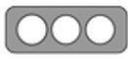


Nro. Alerta:	AL-2025-32	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	 TLP:BLANCO		
Fecha:	11-jul-2025	<b>Suplantación de Identidad “Cooperativa de Ahorro y Crédito 9 de Octubre”</b>	V 1.1

## I. DATOS GENERALES:

<b>Clase de alerta:</b>	Fraude – Scam
<b>Tipo de incidente:</b>	Falsificación de registros o identidad.
<b>Nivel de riesgo:</b>	Alto

## II. INTRODUCCIÓN

La técnica de Scam es una forma de fraude a través de internet o cualquier medio digital, que pretende engañar a las víctimas para obtener dinero o información personal confidencial tales como credenciales de cuentas de correo, banca electrónica, etc.

## III. VECTOR DE ATAQUE:

A través de páginas falsas de Facebook los atacantes emplearon el logotipo de la “Cooperativa de Ahorro y Crédito 9 de Octubre” y son contactados para ofrecerles créditos.

Para agilizar este falso trámite, quienes utilizan la imagen o el nombre de la Cooperativa solicitan distintas cantidades de dinero que deben ser depositadas en cuentas bancarias de otras instituciones financieras, provocando fraude y estafa.

## IV. INDICADORES DE COMPROMISO:

El indicador de compromiso reportado y asociado a la campaña maliciosa es el enlace que dirige a la página de Facebook fraudulenta:

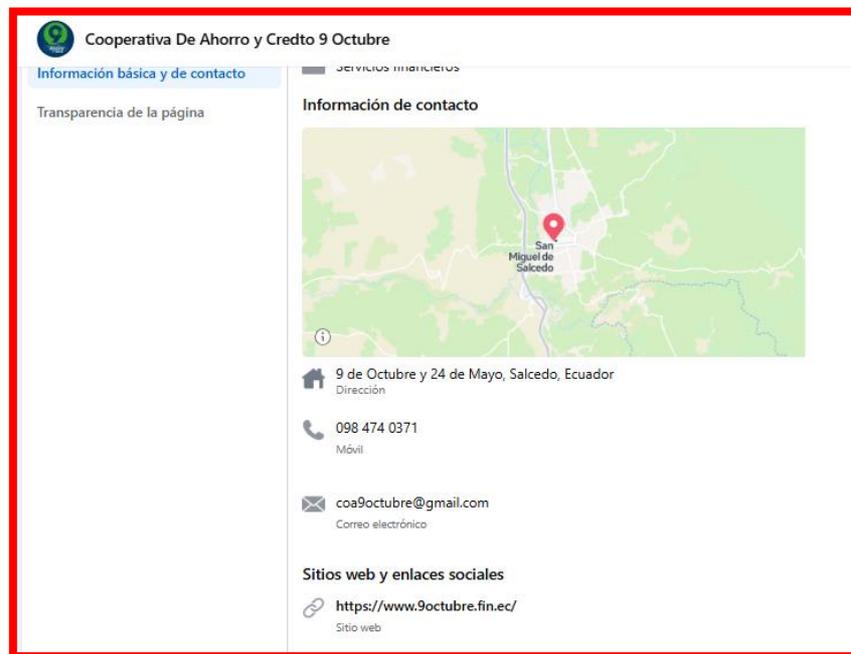
[https://www.facebook.com/profile.php?id=61574075673104&rdid=IW3tCqHlejgDkKXn&share\\_url=https%3A%2F%2Fwww.facebook.com%2Fshare%2F16qou31Ciz%2F#](https://www.facebook.com/profile.php?id=61574075673104&rdid=IW3tCqHlejgDkKXn&share_url=https%3A%2F%2Fwww.facebook.com%2Fshare%2F16qou31Ciz%2F#)

Nro. Alerta:	AL-2025-32	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	11-jul-2025	<b>Suplantación de Identidad “Cooperativa de Ahorro y Crédito 9 de Octubre”</b>	V 1.1

## V. IMÁGENES DE LA CAMPAÑA DE SUPLANTACIÓN DE IDENTIDAD



Gráfica 1.- Página en Facebook que suplanta a la Cooperativa de Ahorro y Crédito 9 de Octubre



Gráfica 2.- Información en Página en Facebook que suplanta a la Cooperativa de Ahorro y Crédito 9 de Octubre

Nro. Alerta:	AL-2025-32	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	11-jul-2025	<b>Suplantación de Identidad “Cooperativa de Ahorro y Crédito 9 de Octubre”</b>	V 1.1

**VI. SITIO WEB Y FACEBOOK REAL DE LA COOPERATIVA DE AHORRO Y CRÉDITO 9 DE OCTUBRE**

<https://www.9octubre.fin.ec/>

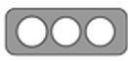


Gráfica 3.- Información en Página WEB real de la Cooperativa de Ahorro y Crédito 9 de Octubre.

<https://www.facebook.com/coac9deoctubre>



Gráfica 3.- Información real en Facebook de la Cooperativa de Ahorro y Crédito 9 de Octubre

Nro. Alerta:	AL-2025-32	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	 <b>TLP:BLANCO</b>		
Fecha:	11-jul-2025	<b>Suplantación de Identidad “Cooperativa de Ahorro y Crédito 9 de Octubre”</b>	V 1.1

## VII. RECOMENDACIONES:

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

- Validar si los sitios web en los que se navega son seguros (se utiliza el puerto https) y oficiales (el dominio corresponde al nombre de la empresa, no tiene errores ortográficos).
- Hacer caso omiso a correos, links o mensajes de dudosa procedencia y márcalos como spam o bloquearlos y comunicar a su departamento técnico.
- Ante cualquier duda contactarse directamente con la persona o empresa suplantada para su comprobación y/o denuncia.
- En caso de haber ingresado los datos personales en el sitio web fraudulento, cambiar la contraseña de las cuentas y comunicarse inmediatamente con la empresa suplantada para la toma de acciones de remediación.
- Nunca entregue los usuarios y contraseñas solicitados a través de correos electrónicos, redes sociales o llamadas telefónicas.
- Instalar y mantener actualizado una solución Antivirus.
- Bloquear los sitios web o direcciones de correo electrónicos indicados en la sección indicadores de compromisos.
- Mantenerse informado continuamente sobre tipos de amenazas en el internet.