Nro. Alerta:	EC-2024-05	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	09-may-2024	**Campaña de suplantación de identidad "Cooperativa de Ahorro y Crédito el Sagrario"**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Fraude – Scam

Tipo de incidente: Falsificación de registros o identidad.

Nivel de riesgo: 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 y cuentas de WhatsApp los atacantes emplearon el logotipo de la Cooperativa de Ahorro y Crédito el Sagrario 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.

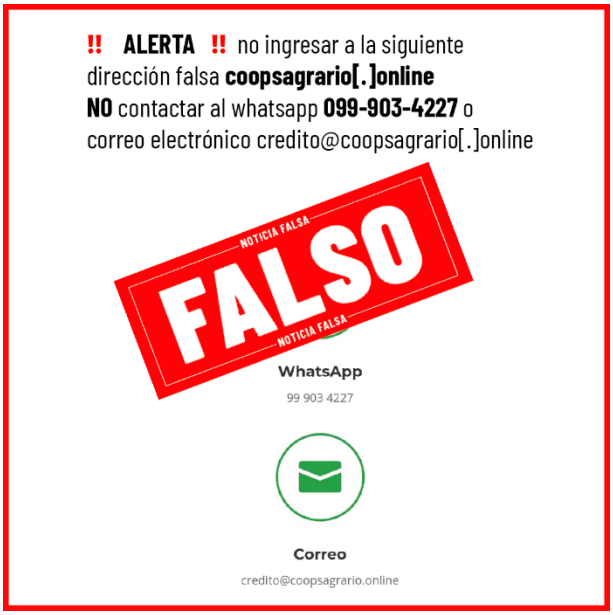
IV. INDICADORES DE COMPROMISO:

El indicador de compromiso reportado y asociado a la campaña maliciosa es la dirección **https[:]//coopsagrario[.]online/**

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código postal: 170513 / Quito - Ecuador
Teléfono: +593-2 2946 400
www.arcotel.gob.ec

Nro. Alerta:	EC-2024-05	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	09-may-2024	**Campaña de suplantación de identidad “Cooperativa de Ahorro y Crédito el Sagrario”**	V 1.1

V. IMÁGENES DE LA CAMPAÑA



Nro. Alerta:	EC-2024-05	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	09-may-2024	**Campaña de suplantación de identidad "Cooperativa de Ahorro y Crédito el Sagrario"**	V 1.1

VI. 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.

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código postal: 170513 / Quito - Ecuador
Teléfono: +593-2 2946 400
www.arcotel.gob.ec

EL NUEVO ECUADOR