

Nro. Alerta:	EC-2022-85	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	 TLP:BLANCO		
Fecha:	03-octubre- 2022	EcuCERT advierte sobre campaña de suplantación de identidad “Cooperativa Andalucía Ltda.”	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.

III. VECTOR DE ATAQUE:

A través de redes sociales existen campañas en las que se comparten enlaces en referencias a suplantación de identidad; en este caso, durante agosto de 2022, existía un link de tipo malicioso, similar al de la Cooperativa Andalucía Ltda., y que buscaba recopilar datos de los usuarios que ingresen a este portal malicioso.

IV. INDICADORES DE COMPROMISO:

El indicador de compromiso reportado y asociados a la campaña maliciosa, y, que actualmente se encuentra dado de baja es:

- [https://dev-andalucia-avisos\[.\]pantheonsite\[.\]io/Andalucia/andalucia\[.\]html](https://dev-andalucia-avisos[.]pantheonsite[.]io/Andalucia/andalucia[.]html)



Nro. Alerta:	EC-2022-85	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	 TLP:BLANCO		
Fecha:	03-octubre-2022	EcuCERT advierte sobre campaña de suplantación de identidad “Cooperativa Andalucía Ltda.”	V 1.2

V. IMAGEN DE LA CAMPAÑA

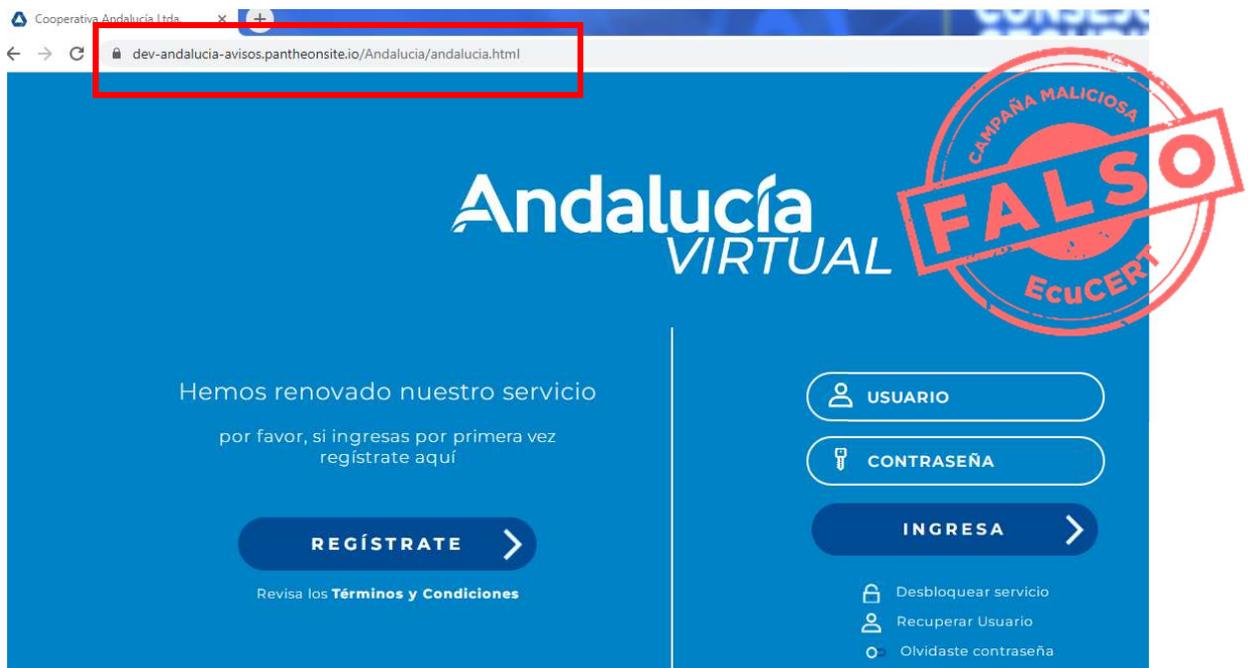


Figura 1.- Sitio que suplanta a la Cooperativa Andalucía.

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 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.
- Ante cualquier duda contactarse directamente con la persona o 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



Nro. Alerta:	EC-2022-85	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:			
Fecha:	03-octubre- 2022	EcuCERT advierte sobre campaña de suplantación de identidad “Cooperativa Andalucía Ltda.”	V 1.2

- 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 la internet.

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.

