Nro. Alerta:	AL-2025-050	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	TLP:BLANCO	**ALERTAS DE SEGURIDAD**	ecucert
Fecha:	08-sept-2025	**Suplantación de Identidad "El Comercio"**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Fraude – Phishing

Tipo de incidente: Falsificación de registros o identidad.

Nivel de riesgo: Alto

II. INTRODUCCIÓN

El Phishing es una técnica de ciberataque basada en la ingeniería social que busca engañar a las personas para que revelen información confidencial, como usuarios, contraseñas, datos bancarios o información personal.

Generalmente se realiza mediante correos electrónicos, mensajes de texto, llamadas o **sitios web falsos** que simulan ser legítimos (por ejemplo, de un banco, una institución pública o una empresa conocida). Los atacantes suelen crear una sensación de urgencia o miedo, como: "Su cuenta será bloqueada" o "Confirme su identidad inmediatamente". Una vez que la víctima cae en el engaño, puede entregar sus credenciales, descargar malware o autorizar transacciones fraudulentas.

III. VECTOR DE ATAQUE:

A través de sitios web falsos los atacantes emplearon el logotipo del medio digital "EL COMERCIO" con el fin de engañar a los usuarios para que ingresen información confidencial como son las credenciales de acceso, datos personales o bancarios y posteriormente robarlos y almacenarlos en bases de datos fraudulentas.

IV. INDICADORES DE COMPROMISO:

El indicador de compromiso reportado y asociado a la campaña maliciosa son los enlaces que dirigen a los sitios web fraudulentos:

- https://wallgeauih.com/VXfPckfq?pixel=1668717523821340&utm_campaign=6892614807995596&ad_id=120229382523140464&placement=Facebook_Mobile_Reels&adset_name=5&ad_name=1&campaign_name=Ec+purchase+8&fbclid=IwZXh0bgNhZW0BMABhZGlkAasj_Iu3DaABHgMqGHDO3TnAIGt8yNzMH-g7KW4Lwjbbr_RrsrfCU8m1Ed-rklwuuWk1alF-_aem_nCmAAe46-

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:	AL-2025-050	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	TLP:BLANCO	**ALERTAS DE SEGURIDAD**	ecucert
Fecha:	08-sept-2025	**Suplantación de Identidad "El Comercio"**	V 1.1

n7O5CxHORGFbQ&utm_medium=paid&utm_source=fb&utm_id=120229382523450464&utm_content=120229382523140464&utm_term=120229382523280464

- IP: 104.21.41.156
- https://wallgeauih.com/?_lp=1&_token=uuid_2r0j6m23j7rji_2r0j6m23j7rji68b9b123eceeb4.43866149
- IP: 172.67.148.39

Body SHA-256

d7263933f8b4d4faaa9351331794e9551d6d02a832098ebebf10b9f12987d965

V. IMÁGENES DE LA CAMPAÑA DE SUPLANTACIÓN DE IDENTIDAD

Gráfica 1.- Sitio web que suplanta al "EL COMERCIO"

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:	AL-2025-050	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	08-sept-2025	**Suplantación de Identidad "El Comercio"**	V 1.1

Gráfica 2.- Sitio web que suplanta a "EL COMERCIO"

VI. SITIO WEB REAL DE "EL COMERCIO"

https://www.elcomercio.com/

Gráfica 2.- Información en Página WEB real de "El Comercio"

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:	AL-2025-050	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	TLP:BLANCO	**ALERTAS DE SEGURIDAD**	ecucert
Fecha:	08-sept-2025	**Suplantación de Identidad "El Comercio"**	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.

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