Nro. Alerta:	EC-2025-45	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	25-ago-2025	**Campaña de información de Suplantación de Identidad a "DHL"**	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

La técnica de ciber ataque a través de email – phishing se refiere a un mensaje fraudulento que se hace pasar por una fuente confiable para engañar a las personas y robar información confidencial como contraseñas, datos financieros o información personal. Estos correos utilizan un lenguaje urgente, enlaces o archivos adjuntos maliciosos, y a menudo falsifican la identidad del remitente o la URL para hacer que parezcan legítimos.

III. VECTOR DE ATAQUE:

A través de correos electrónicos los atacantes emplearon el logotipo de la empresa DHL con el objetivo de solicitar a la ciudadanía actualizar información para la entrega de paquetería.

Para agilizar este falso trámite, quienes utilizan la imagen o el nombre de la empresa, solicitan validar datos personales con el fin de entregar un paquete en un tiempo determinado, haciéndose pasar por una fuente confiable para robar información confidencial, como contraseñas, números de tarjeta de crédito o datos bancarios.

IV. INDICADORES DE COMPROMISO:

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

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-2025-45	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	25-ago-2025	**Campaña de información de Suplantación de Identidad a "DHL"**	V 1.1

Links:

- https://deliveiry-report.info/Envio_dhl/login.php
- infos_id-ef47@assectra.com.br
- https://deliveiry-report.info/Envio_dhl/Envio_fcc2b6359/?Token_id=1f9e17bee6d1

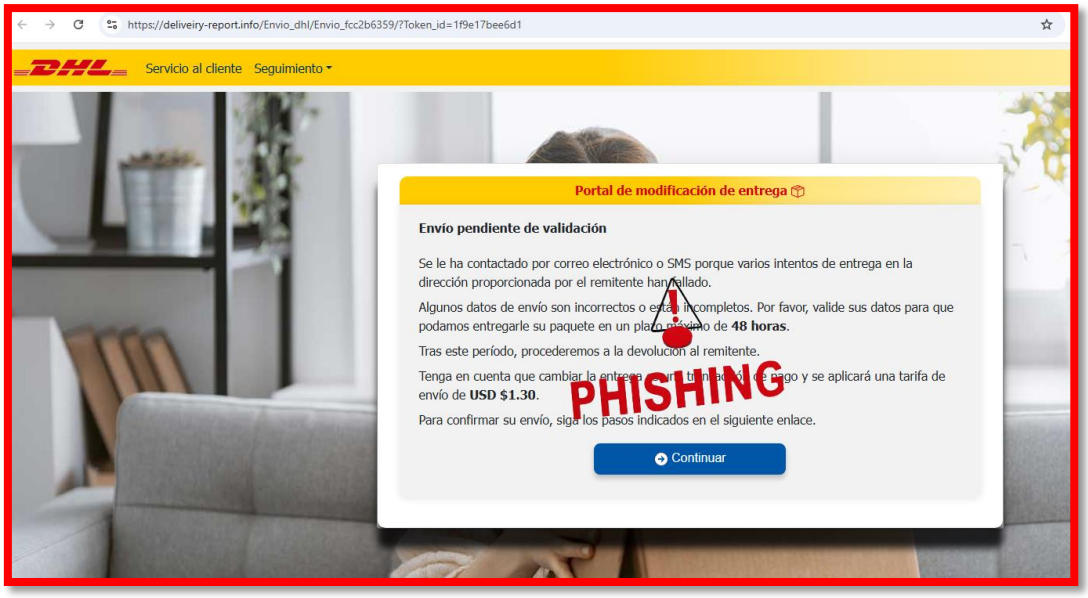
Serving IP Address (fuente: https://www.virustotal.com/)

- 104.21.20.93
- 44.242.88.230

Body SHA-256: (fuente: https://www.virustotal.com/)

- 84fe5b97052dfaf4c3f725f968b66e7861a26453e832dc4efd534edaa85fdd33

V. IMÁGENES DE LA CAMPAÑA DE SUPLANTACIÓN DE IDENTIDAD.



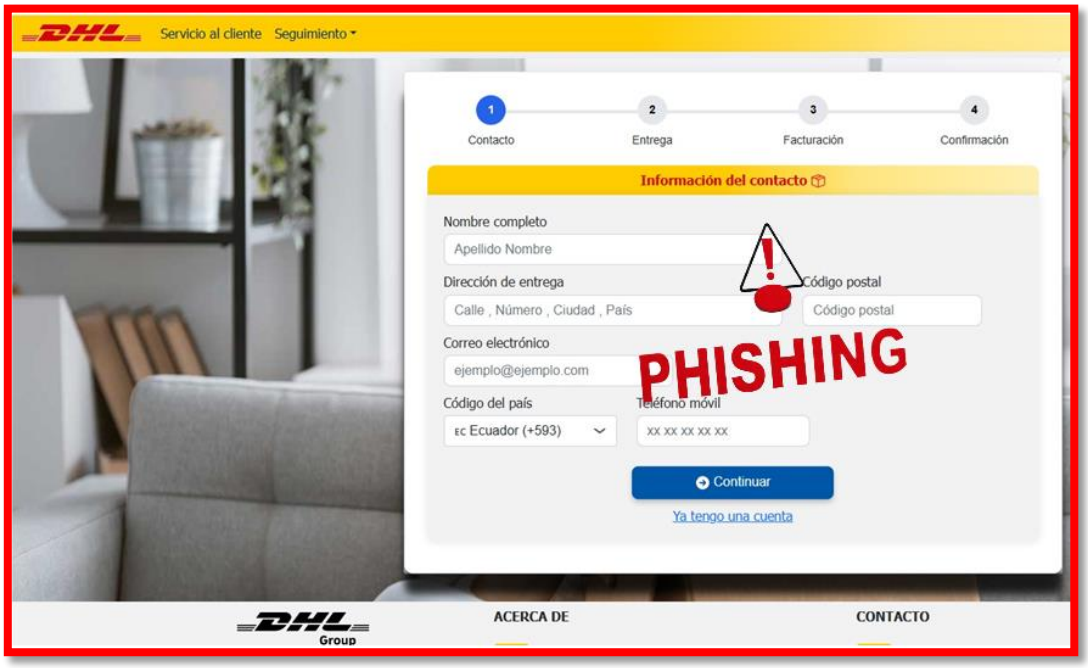
Gráfica 1.- Link malicioso que lleva a un sitio web que suplanta a DHL

Nro. Alerta:	EC-2025-45	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	25-ago-2025	**Campaña de información de Suplantación de Identidad a "DHL"**	V 1.1

Gráfica 2.- Correo electrónico que suplanta a DHL

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

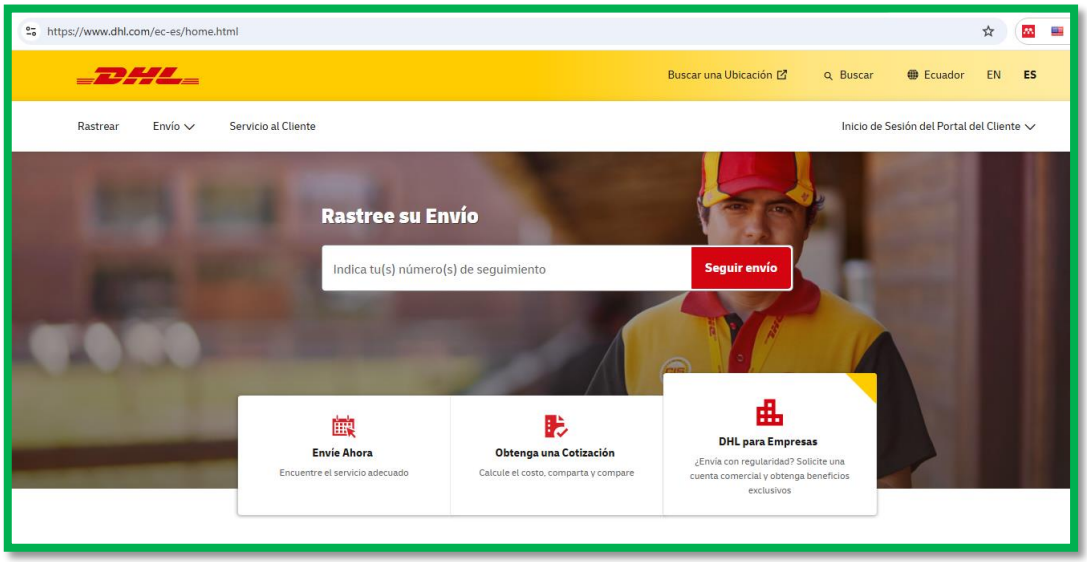
Nro. Alerta:	EC-2025-45	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	25-ago-2025	**Campaña de información de Suplantación de Identidad a "DHL"**	V 1.1



Gráfica 3.- Link malicioso que lleva a un sitio web que solicita datos personales

VI. SITIO WEB REAL DE LA EMPRESA DHL.

https://www.dhl.com/ec-es/home.html



Gráfica 4.- Información en Página WEB real de la empresa DHL

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-2025-45	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	25-ago-2025	**Campaña de información de Suplantación de Identidad a "DHL"**	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