Nro. Alerta:	EC-2026-012	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	26-feb-2025	**Campaña de información de Suplantación de Identidad del Ministro del Interior**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Fraude – Deepfakes

Tipo de incidente: Suplantación de identidad.

Nivel de riesgo: Alto

II. INTRODUCCIÓN

Los deepfakes son contenidos digitales manipulados mediante técnicas avanzadas de inteligencia artificial que permiten alterar o generar imágenes, audios y videos con un alto nivel de realismo. A través de algoritmos de aprendizaje profundo (deep learning), es posible simular la apariencia y la voz de una persona, creando material falso que puede resultar difícil de distinguir del contenido auténtico.

Si bien esta tecnología puede tener aplicaciones legítimas en ámbitos como el entretenimiento o la educación, su uso malicioso representa un riesgo significativo, especialmente en escenarios de suplantación de identidad, fraude, desinformación e ingeniería social.

III. VECTOR DE ATAQUE:

Los ciberdelincuentes utilizan la imagen del Ministro del Interior en un video manipulado para promocionar supuestas plataformas de inversión que ofrecen ganancias fáciles y elevadas, indicando que con una inversión inicial de USD 100 se pueden obtener beneficios diarios entre USD 300 y USD 1.000.

El video redirige a una página web fraudulenta que suplanta la identidad del medio de comunicación El Comercio, con el objetivo de otorgar mayor credibilidad a la oferta y generar confianza en las potenciales víctimas.

Para acceder al supuesto programa, se solicita registrar una cuenta ingresando información básica como nombre, apellido, correo electrónico y número de teléfono. Posteriormente, se muestra un mensaje indicando que un “asesor” se comunicará

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

EL NUEVO ECUADOR

vía telefónica y se redirige a una nueva pantalla donde se requiere información adicional, incluyendo dirección domiciliaria, país, ciudad, código postal, nacionalidad, fecha de nacimiento y número de identificación.
Finalmente, se solicita el ingreso de datos de tarjeta de crédito o débito para realizar un depósito inicial. En esta etapa se materializa la estafa, ya que los atacantes obtienen información personal y financiera de las víctimas para su uso fraudulento.

La materialización de esta amenaza puede generar pérdidas económicas directas a las víctimas, derivadas de cargos no autorizados en tarjetas de crédito o débito, así como transferencias fraudulentas.

Asimismo, la recolección de datos personales y financieros expone a los afectados a riesgos adicionales como suplantación de identidad, apertura de cuentas bancarias o créditos no autorizados, campañas de phishing dirigidas y otras modalidades de fraude.

A nivel institucional, el uso indebido de la imagen de autoridades públicas puede afectar la reputación y credibilidad de las entidades involucradas, además de generar desinformación y pérdida de confianza ciudadana.

IV. INDICADORES DE COMPROMISO:

- **Sitios web:**

https://fearfuuafh.com/?utm_campaign=727427403301661&pixel=894008546832133&ad_id=120246152135070399&placement=an&adset_name=1&ad_name=1+%E2%80%94+%D0%9A%D0%BE%D0%BF%D0%B8%D1%8F&campaign_name=%7B%7Bcampaign.name%7D&creo=1&utm_medium=paid&utm_source=an&utm_id=120246152135020399&utm_content=120246152135070399&utm_term=120246152135040399&fbclid=IwY2xjawQL1xlleHRuA2FlbQEwAGFkaWQBqzM9AP7NH3Vzcm0AAAAAAAAAF3NydGMGYXBwX2lkDzI0NTc5MDgxODk1NTg2OAABHkg802NEt8u9k1rkem7YIlfCADF0P_tLo6Af1OrxtVuAgu1AARRMhwI6wsVP9_aem_qUdUCMOkshxVondSRkgHkA

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

EL NUEVO ECUADOR

https://fearfuuafh.com/

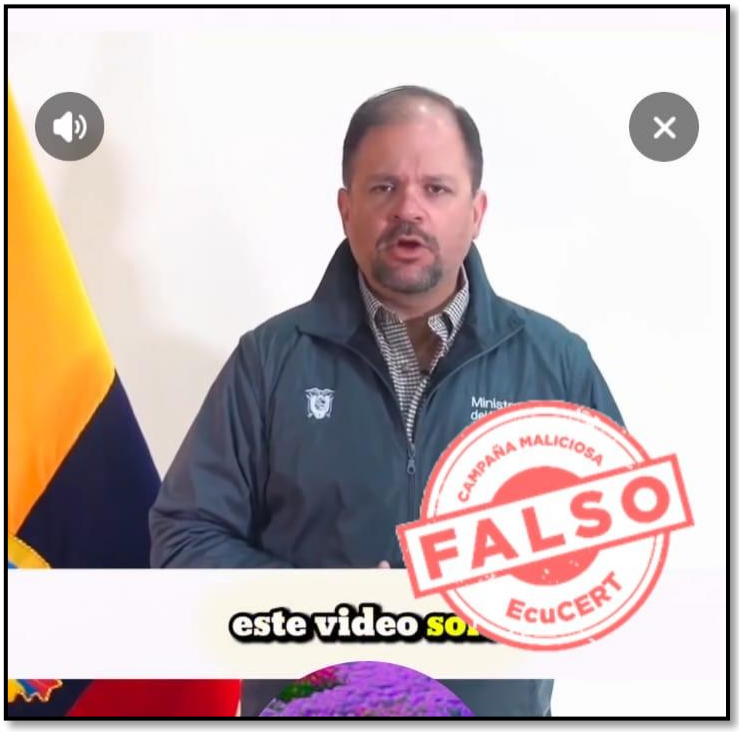
https://www.algobi.com/onboarding/personal-details-extended

https://www.algobi.com/onboarding/deposit

- **Direcciones Ip:** *(fuente: virustotal.com)*

172.67.140.106
52.55.39.221
172.66.40.73
172.66.43.183

V. IMÁGENES DE LA CAMPAÑA DE DEEPFAKES



Gráfica 1.- Captura de pantalla del video que suplanta al Ministro del Interior.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

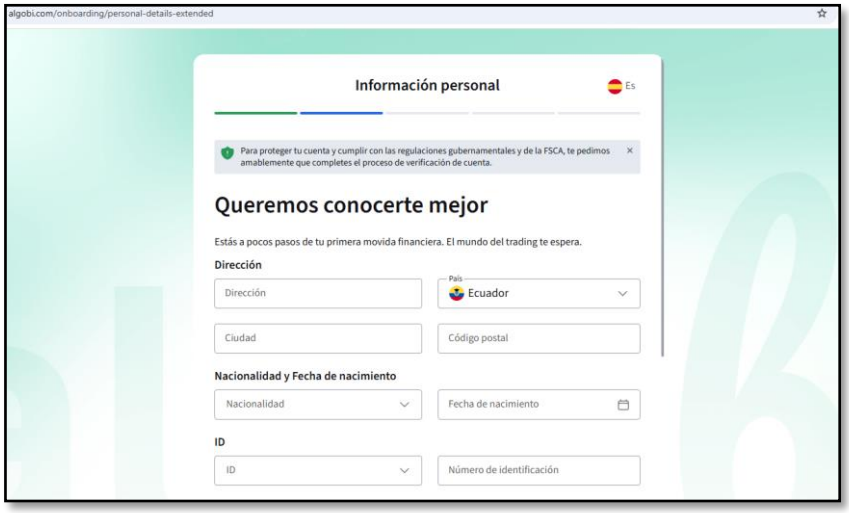
EL NUEVO ECUADOR

Nro. Alerta:	EC-2026-012	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	26-feb-2025	**Campaña de información de Suplantación de Identidad del Ministro del Interior**	V 1.1

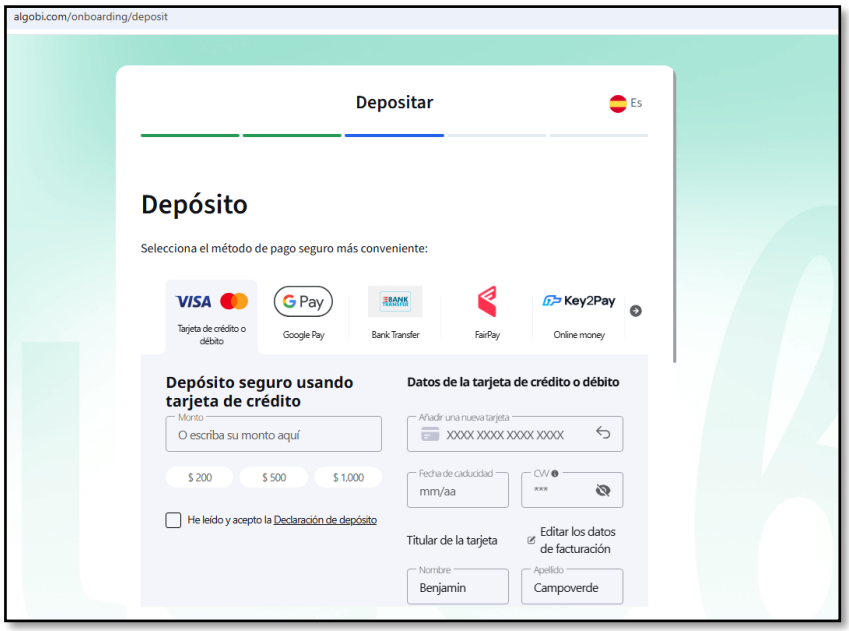
Gráfica 2.- Sitios web que suplanta el nombre de "El Comercio"

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	EC-2026-012	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	26-feb-2025	**Campaña de información de Suplantación de Identidad del Ministro del Interior**	V 1.1



Gráfica 3.- Sitio web en donde se solicita información personal



Gráfica 4.- Sitio web en la cual se solicita realizar el depósito inicial

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	EC-2026-012	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	26-feb-2025	**Campaña de información de Suplantación de Identidad del Ministro del Interior**	V 1.1

VI. RECOMENDACIONES:

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

- No confiar en publicaciones o videos que ofrezcan ganancias rápidas y desproporcionadas con inversiones mínimas. Este tipo de promesas constituye un indicador común de fraude.
- Verificar que la información provenga de fuentes oficiales y acceder directamente a los sitios web escribiendo la dirección en el navegador, evitando ingresar mediante enlaces patrocinados o compartidos en redes sociales.
- Confirmar la autenticidad de noticias o comunicados a través de los canales oficiales del medio de comunicación El Comercio u otras fuentes verificadas.
- No proporcionar datos personales, financieros o credenciales bancarias en sitios web no verificados.
- Activar mecanismos de seguridad adicionales en cuentas bancarias, tales como notificaciones de transacciones y autenticación multifactor.
- En caso de haber proporcionado información bancaria, contactar inmediatamente a la entidad financiera para bloquear tarjetas y reportar posibles cargos no autorizados.
- Hacer caso omiso a correos, links o mensajes de dudosa procedencia y márcalos como spam o bloquearlos y comunicar a su departamento técnico.
- Si proporcionó claves o PIN: Cambiar inmediatamente (banco, correo, cuentas importantes).
- Reporte el caso al Ministerio involucrado (canales oficiales) y a la Policía Nacional
- Si compartió documentos de identidad: presente la denuncia en la Fiscalía General del Estado y proceda a solicitar a la entidad emisora un nuevo documento de identidad.
- Guarde evidencias: capturas de pantalla del sitio, URLs, correos y números.
- Revise su estado de cuenta y reporte cargos sospechosos.
- Considere presentar una denuncia formal en la unidad de delitos informáticos de la Fiscalía General del Estado.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec