Nro. Alerta:	EC-2022-41	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	25-feb-2022	**EcuCERT advierte nueva campaña de suplantación de identidad "Banco del Pichincha"**	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 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 correo electrónico circula una campaña maliciosa que invita al usuario a ingresar a ciertos enlaces que suplantan la identidad de la página web del Banco del Pichincha con el objetivo de captar las credenciales de la banca electrónica.

IV. INDICADORES DE COMPROMISO:

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

- https://mybank.toc[.]com[.]ec/login

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-41	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	25-feb-2022	**EcuCERT advierte nueva campaña de suplantación de identidad "Banco del Pichincha"**	V 1.1

V. IMAGEN DE LA CAMPAÑA

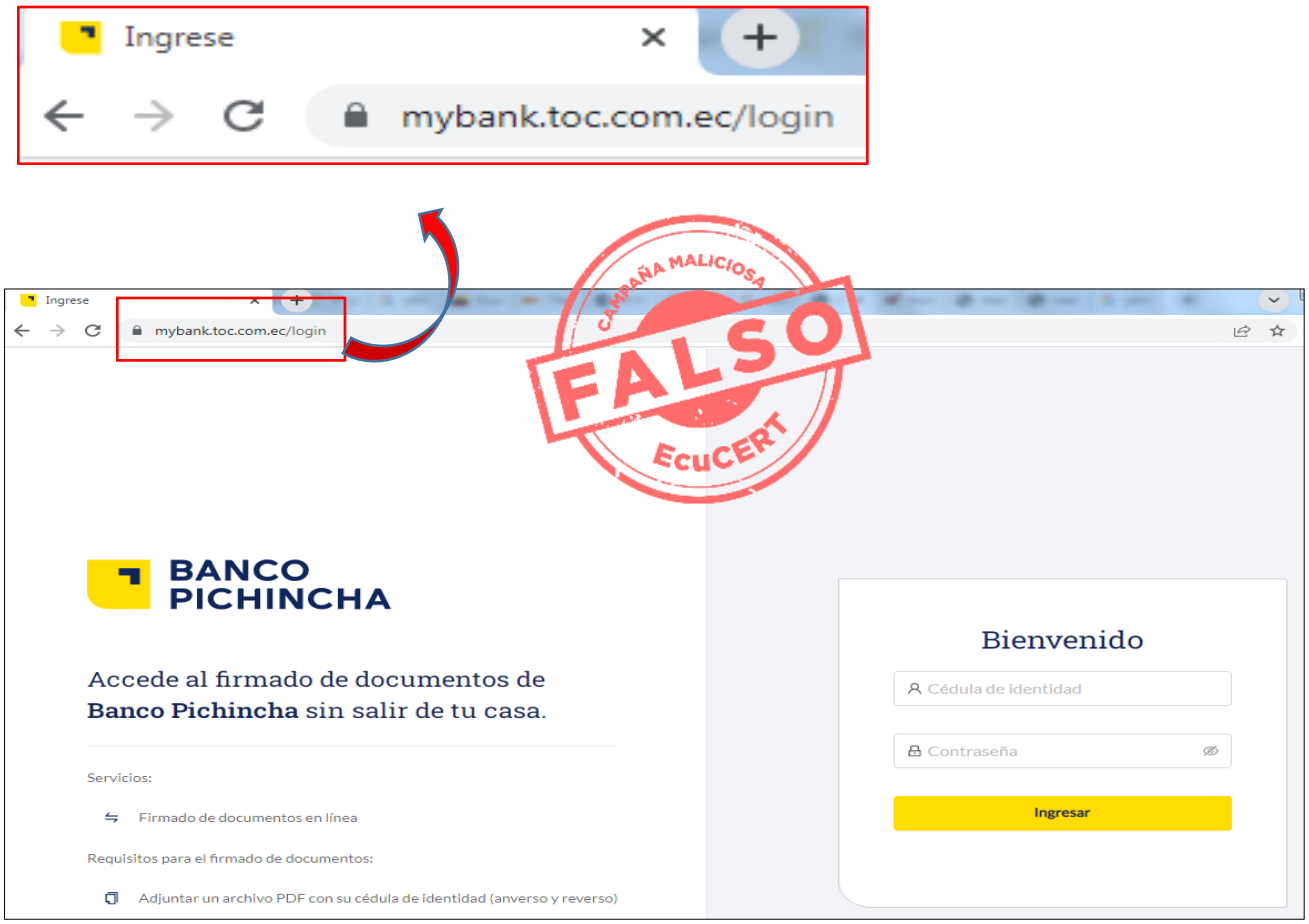

Figura 1.- ***Campaña maliciosa a nombre de Banco Pichincha***

VI. RECOMENDACIONES:

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

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-41	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	25-feb-2022	**EcuCERT advierte nueva campaña de suplantación de identidad "Banco del Pichincha"**	V 1.1

- 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.
- 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 indicados en la sección indicadores de compromisos
- Informarse continuamente sobre tipos de amenazas en la internet.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec