

Alerta de seguridad cibernética	8FFR20-00832-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de Noviembre de 2020
Última revisión	18 de Noviembre de 2020

## NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los loC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los loC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de fraude no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado fraude, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado la activación de una pagina fraudulenta asociada a un dominio .cl que intenta suplantar al Banco TD Bank, el que podría servir para robar credenciales de usuarios.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad aludida.

## Indicadores de compromiso

### URL sitio falso

http[:]//www.fugas[.]cl/td/e.htm

### Body SHA-256

ee8b6d83c7d5000eb1684938596f604dcce4dd6b583c17cd0c777dd7ca281522

### Certificado Digital

Fecha Válido	2020/09/22
Fecha Término	2020/09/23
Emitido	RapidSSL TLS DV RSA Mixed SHA256 2020 CA-1

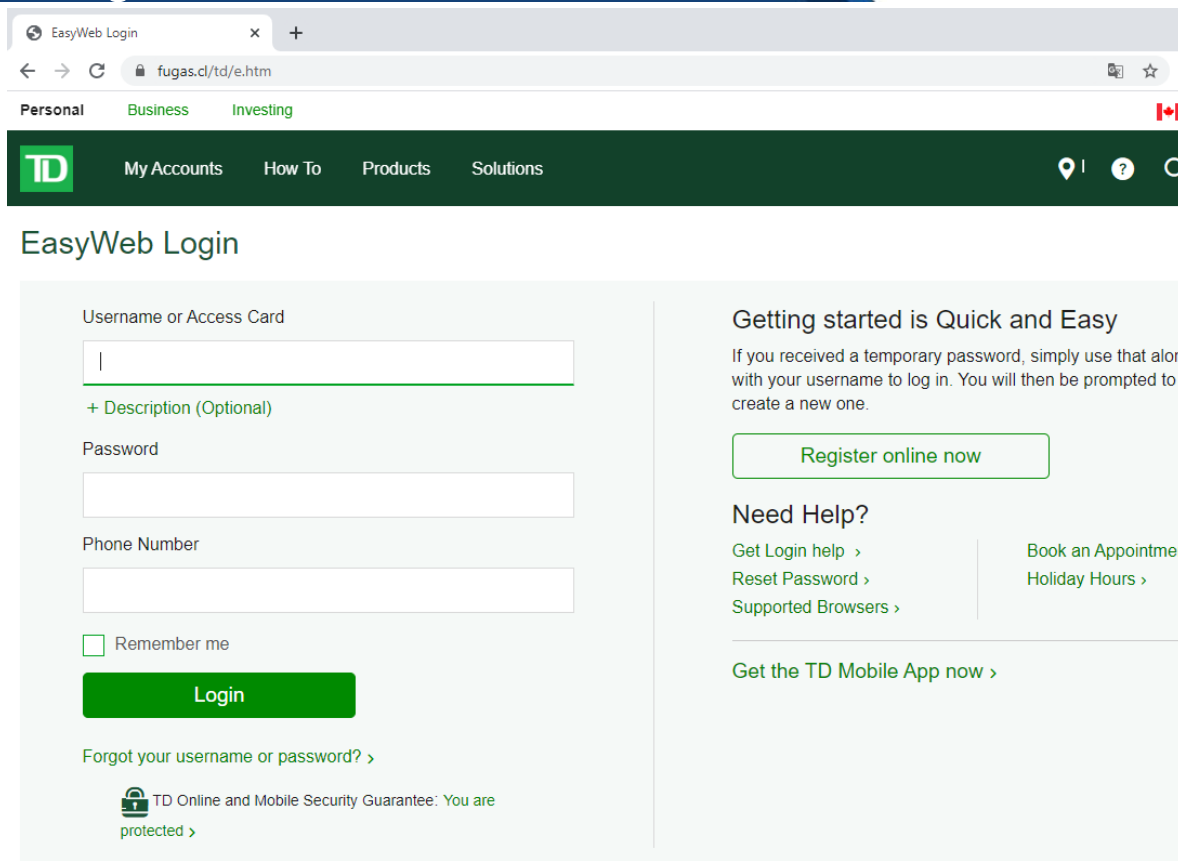
### Datos Alojamiento

IP	[201.148.107.69]
Número de Sistema Autónomo (AS)	265839
Etiqueta del Sistema Autónomo	HOSTING.
País	CL
Registrador	LANIC

### Datos del Dominio

Nombre de Dominio	fugas[.]cl
Creado	2008-10-28
Expira	2026-11-25
Información del Registrador	NIC Chile
ID IANA	No disponible
Correo Electrónico	No disponible
Name Server	dns1.hosting.cl dns2.hosting.cl dns3.hosting.cl dns4.hosting.cl

## Imagen del sitio



The screenshot shows a web browser window with the URL `fugas.cl/td/e.htm`. The page title is "EasyWeb Login". The navigation bar includes "Personal", "Business", and "Investing" tabs, along with a Canadian flag. The main navigation menu features "TD", "My Accounts", "How To", "Products", and "Solutions". The login form on the left includes fields for "Username or Access Card", "+ Description (Optional)", "Password", and "Phone Number", a "Remember me" checkbox, and a green "Login" button. Below the form is a link for "Forgot your username or password?". On the right, a section titled "Getting started is Quick and Easy" explains that a temporary password can be used with the username. It includes a "Register online now" button and a "Need Help?" section with links for "Get Login help", "Reset Password", "Supported Browsers", "Book an Appointment", and "Holiday Hours". At the bottom of the form area, there is a security guarantee: "TD Online and Mobile Security Guarantee: You are protected".

By using EasyWeb, our secured financial services site, offered by TD Canada Trust and its affiliates, you agree to the terms and services of the [Financial Services Terms](#), [Cardholder and Electronic Financial Services Terms and Conditions](#) and/or, the [Business Access](#)

## Recomendaciones

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los AntiSpam y SandBoxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.