Fundación Adultos Mayores
Chile

Manual Básico de Ciberseguridad

Área Informática

Septiembre, 2024.

Introducción

El uso de internet y la tecnología se ha vuelto una parte fundamental de nuestra vida diaria, ofreciendo comodidades como la posibilidad de acceder a información, realizar trámites bancarios, comprar en línea y mantenernos en contacto con familiares y amigos. Sin embargo, a medida que nos volvemos más dependientes de estas tecnologías, también aumenta el riesgo de encontrarnos con fraudes y estafas en línea.

Este manual ha sido creado con el objetivo de ayudar y a reconocer las estafas más comunes que circulan por internet, como los correos fraudulentos (phishing), los fraudes telefónicos y los enlaces maliciosos, entre otros. Aquí encontrarán consejos prácticos y fáciles de seguir para protegerse mientras navegan en internet, tanto en computadoras como en teléfonos móviles.

Estafas más comunes en internet

Phishing

- **¿Qué es?:** Es un engaño en el que te envian un correo electrónico, mensaje de texto o mensaje de whatsapp que parece ser de una empresa legítima (como un banco o una tienda)

- **Cómo funciona:** Te piden que hagas click o ingreses en un enlace para verificar tu cuenta o proporcionar información personal, como tu contraseña o números de tarjetas.

Ejemplo

- Recibes un mensaje de texto que aparenta ser de una tienda en línea en la que realizaste una compra reciente. El mensaje te informa que tu pedido ha tenido un problema y que necesitas confirmar tus datos de pago a través de un enlace para completar la transacción.

Consejo: No hagas clic en enlaces recibidos por mensaje de texto para verificar información de pagos. En lugar de eso, contacta a la tienda directamente usando el número de teléfono que aparece en su sitio web oficial y si estás seguro de que no ordenaste nada hacer caso omiso al mensaje preferiblemente bloquear el número.

Enlaces maliciosos

- **¿Qué son?:** Enlaces que parecen legítimos, pero te llevan a sitios falsos o descargan virus a tu computadora o dispositivo celular.

- **Cómo funcionan:** Los delincuentes te envían un enlace en un correo, mensaje de texto o WhatsApp, que al abrirlo puede robar tu información personal o infectar tu dispositivo.

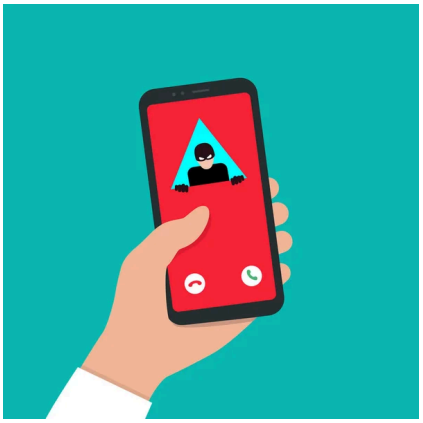
Ejemplo:

- Un mensaje en WhatsApp te ofrece un premio increíble por hacer clic en un enlace.

.

Consejo: Si no esperas recibir algo o te parece muy bueno para ser cierto, probablemente sea falso. No hagas clic y borra el mensaje.

Fraudes telefónicos de suplantación de identidad



- **¿Qué es?:** Los estafadores manipulan el identificador de llamadas para que parezca que la llamada proviene de una fuente confiable, como una institución bancaria, el gobierno o una empresa legítima.

- **Cómo funciona:** Recibes una llamada que parece venir de tu banco o un número oficial, en la que te informan sobre un problema con tu cuenta o tarjeta de crédito, y te piden información personal o detalles de tu tarjeta para "solucionarlo".

Ejemplo:

- Recibes una llamada del "banco" diciendo que se ha detectado actividad sospechosa en tu cuenta y te solicitan tu número de tarjeta o el código de seguridad para verificar.

Consejo: Nunca proporciones información personal por teléfono si no has iniciado tú la llamada. Si tienes dudas, cuelga y contacta directamente a la institución utilizando el número oficial. Recuerda que ningún banco o entidad legítima te pedirá tus claves de acceso o información confidencial por teléfono.

Consejos fáciles para evitar fraudes online tanto en computador como celular

Analiza el enlace antes de hacer clic

- **En Computador:** Antes de hacer clic en un enlace en un correo o mensaje, pasa el ratón sobre el enlace para ver la dirección completa en la esquina inferior izquierda de tu navegador. Si ves algo extraño o que no coincide con el sitio que esperabas, no hagas clic.

- **En celular:** Mantén presionado el enlace para ver la dirección completa. Si te parece sospechosa o no coincide con el sitio oficial, no hagas clic.

Teclea la URL directamente

- **En computador y celular:** Si recibes un mensaje pidiéndote que ingreses a un enlace, no lo hagas. En lugar de eso, abre tu navegador y escribe la dirección del sitio web manualmente para asegurarte de que estás visitando la página correcta.

Instala un buen antivirus

- **En computador:** Asegúrate de tener un antivirus actualizado, como **Windows Defender**, para proteger tu computadora de virus y ataques generalmente los computadores bien con este antivirus ya instalado

  .

- **En celular:** Considera instalar una aplicación de seguridad móvil confiable, la cual estará al final de este manual junto con una guía de como instalarla que te ayude a proteger tu teléfono de amenazas.

Usa páginas para verificar enlaces sospechosos

- **En computador y celular:** Si tienes dudas sobre un enlace, a continuación se mostrará una guía de un sitio el cual analiza el enlace de manera automática si es segura o si contiene alguna amenaza.

Confía en tu instinto

- Si un mensaje parece raro o demasiado bueno para ser verdad, confía en tu intuición. Si no estás esperando una llamada o mensaje, lo mejor es ignorarlo o consultarlo con un familiar antes de actuar.

Herramientas útiles para protegerte

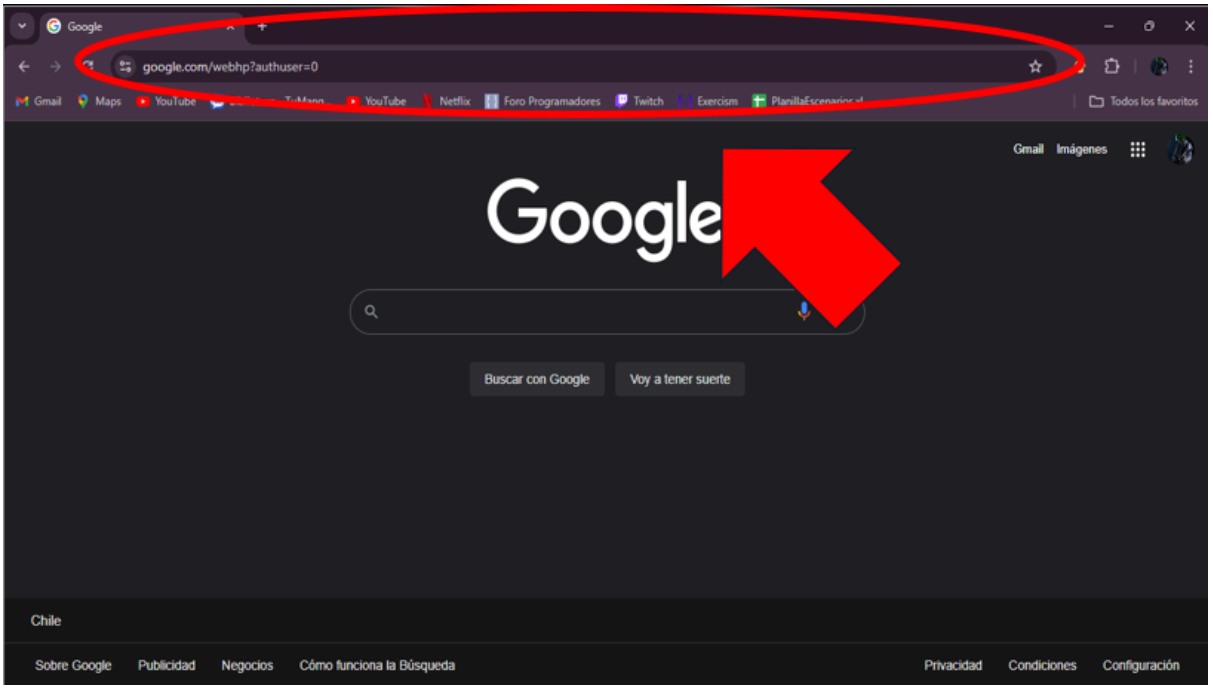
VirusTotal

¿Qué es?

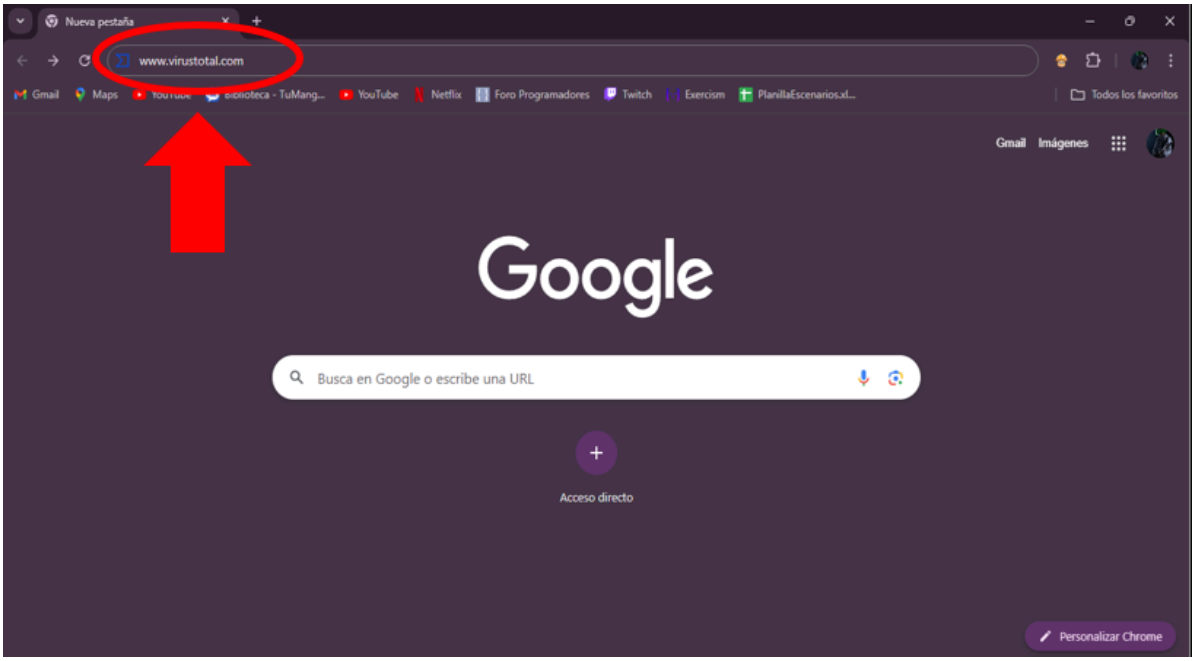
Es una herramienta en línea gratuita que permite analizar archivos y enlaces sospechosos en busca de virus, malware y otras amenazas. Funciona escaneando el contenido con múltiples motores antivirus y servicios de seguridad. Los usuarios pueden subir archivos o copiar y pegar enlaces para obtener un informe detallado sobre si el contenido es seguro o malicioso. Es una excelente opción para verificar la seguridad de archivos y sitios web antes de interactuar con ellos.

Instrucciones de cómo utilizar

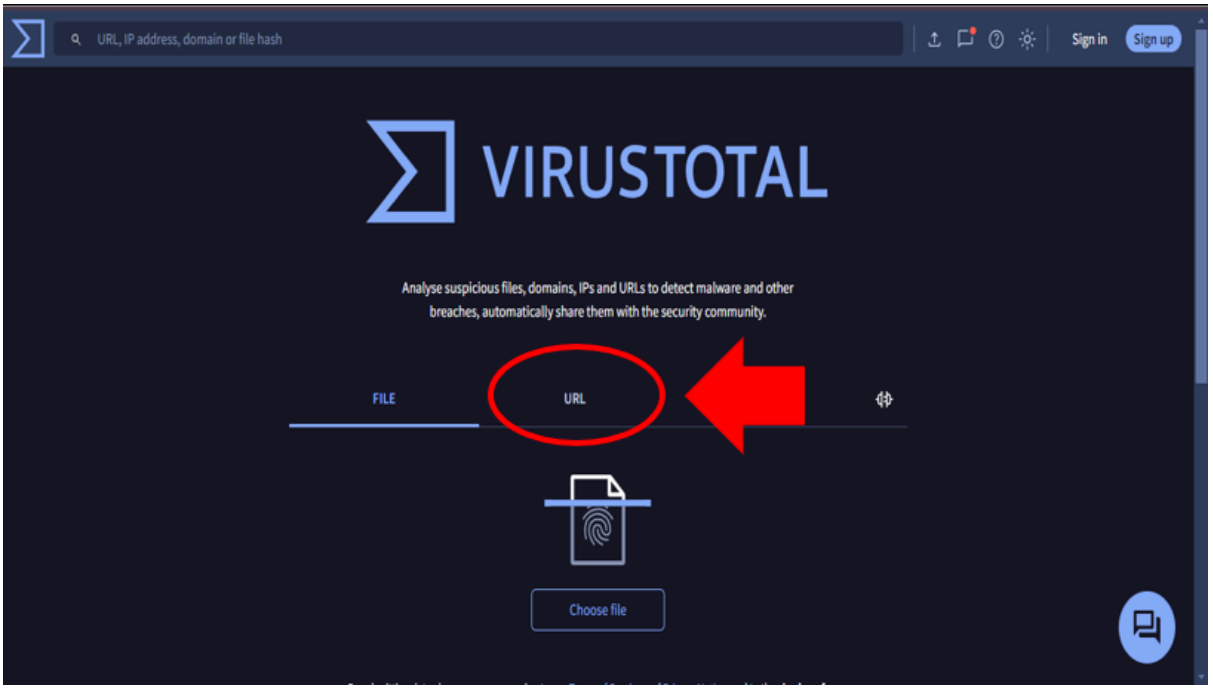
Paso 1-Nos posicionamos en la parte superior donde se ubica la barra de búsqueda y le damos click.



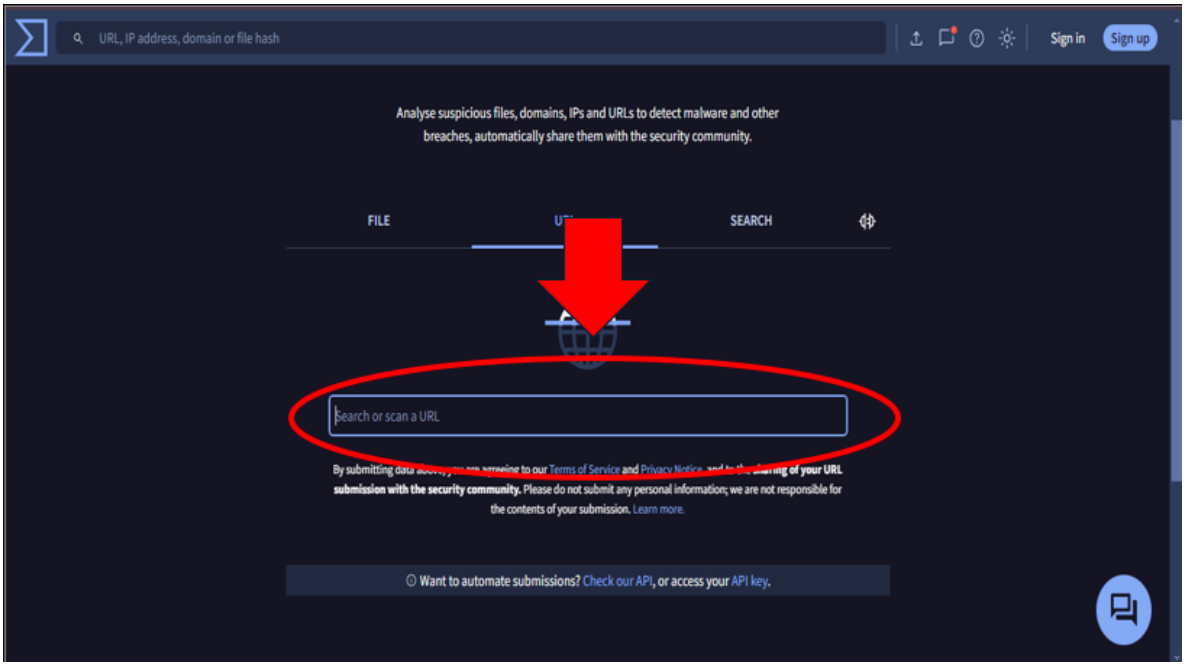
Paso 2-Una vez ubicados en la barra de búsqueda ingresamos la url de VirusTotal la cual es www.virustotal.com y presionamos la tecla "Enter"



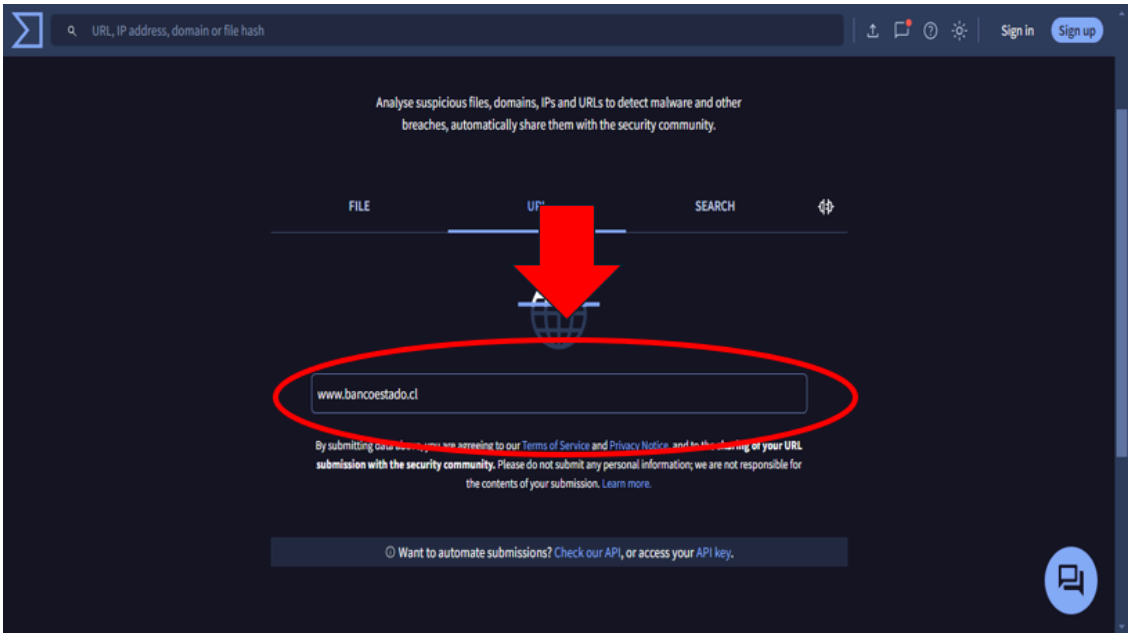
Paso 3-Esto nos redirigirá a la página en la cual damos click en la parte que dice “URL”



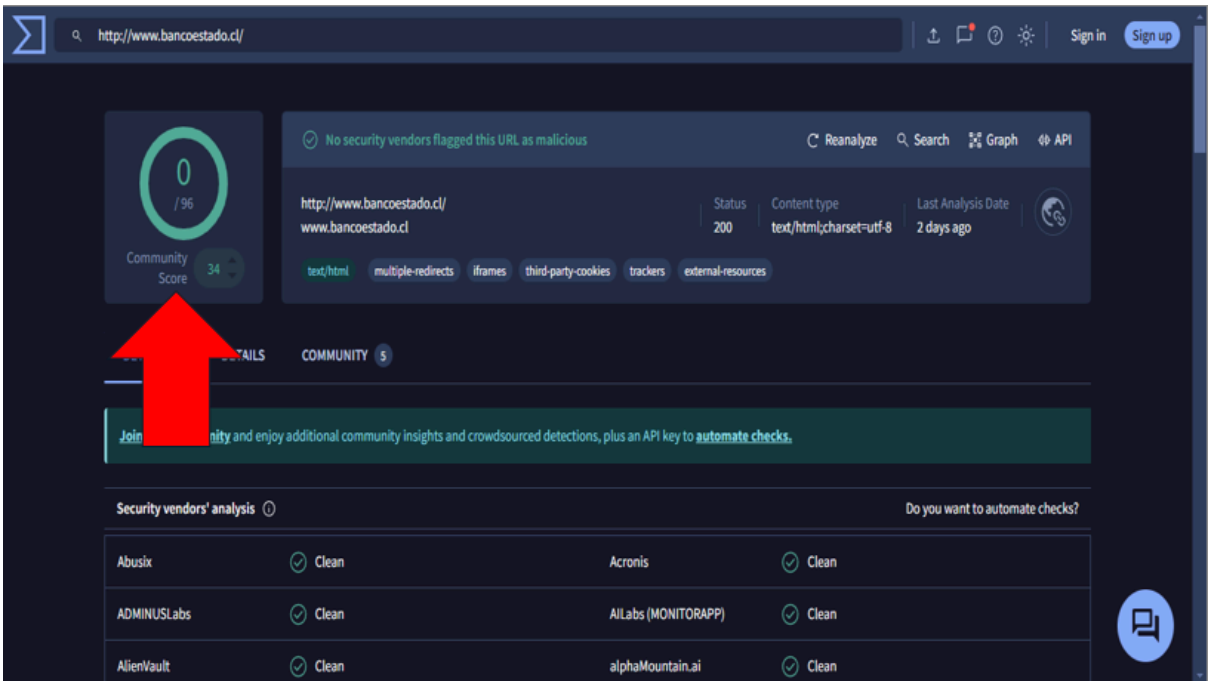
Paso 4-Una vez que clickeamos donde dice “URL” podremos ver una pequeña barra de búsqueda en la parte inferior en la cual ingresamos el enlace del cual no estamos seguros si es malicioso o no y presionamos la tecla “Enter”.



Como ejemplo podemos ingresar el enlace del Banco Estado el cual es www.bancoestado.cl para verificar si es seguro.

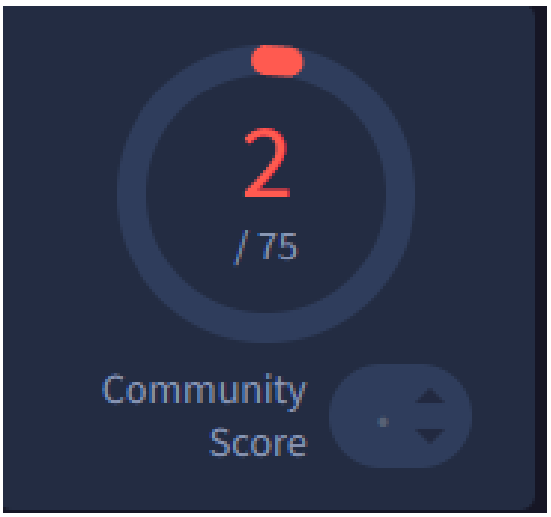


Paso 5-Por último para asegurarnos de que la página es segura debemos fijarnos en el círculo que aparece en la parte izquierda, si el círculo nos marca un "0" significa que la página está segura de cualquier amenaza.



En cambio si vemos que el círculo presenta un número mayor a "1", quiere decir que la página probablemente contenga alguna amenaza para nosotros ya sea robar contraseñas, página falsa o que posea algún virus para nuestro dispositivo.

Esto se mostraría de esta forma.



Truecaller

¿Qué es?

Truecaller es una aplicación móvil que ayuda a identificar y bloquear llamadas no deseadas, como las de estafadores o telemercadeo. La app permite ver quién está llamando, incluso si el número no está guardado en tu lista de contactos, utilizando una base de datos de números reportados por otros usuarios. Además, bloquea automáticamente números de spam y estafas conocidos, y también te permite buscar información sobre números desconocidos. Es una herramienta útil para evitar fraudes telefónicos y protegerse de llamadas molestas.

El cómo instalar y utilizar esta aplicación

Por suerte esta aplicación cuenta con diversas guías que explican su funcionamiento e instalación, a continuación adjuntamos un video al que pueden ingresar para aprender sobre cómo funciona y cómo instalar la aplicación en sus dispositivos móviles.

Enlace al video

https://www.youtube.com/watch?v=Md_XBiw9MuM&list=LL&index=1

Conclusión del manual básico de Ciberseguridad

La seguridad en línea no tiene que ser complicada. Siguiendo estos sencillos pasos y manteniéndote alerta, puedes protegerte contra las ciberestafas más comunes. Recuerda que la prevención es la mejor defensa: antes de hacer clic, piensa.