Milpa Digital

Tails: Conectándonos a internet de manera segura y anónima

Cuando encendemos nuestra computadora o nos conectamos a internet, todos nuestros datos y navegaciones quedan expuestas a la vigilancia y control de todo tipo de compañías, la censura, la publicidad, y los virus haciendo de nuestra experiencia en línea insegura. Dichosamente se han creado sistemas operativos como **Tails** (*The Amnesic Incognito Live System*) una distribución Linux diseñada para preservar la privacidad y el anonimato cuando navegas por la web desde tu computadora.

¿Cómo funciona?

La forma de funcionamiento de Tails es bastante peculiar pues lo hace desde una memoria USB que permite que cualquier persona pueda arrancar la computadora con ella, y no dejar ningún rastro en los discos duros sin importar la computadora que utilices.

Una vez que se apaga la computadora, los datos de la memoria RAM se borran y es imposible saber que se ha usado Tails en esa computadora o tener acceso a los datos de navegación o uso que hayas hecho.

Antes de usar Tails aseguremos que:

- Tenemos un procesador fabricado después de 2005
- Tenemos al menos 2 GB de RAM
- Tenemos una memoria USB de al menos 8 GB.
- Descargamos desde el navegador Firefox o desde BitTorrent, para confirmar que nadie lo ha modificado

¿Quiénes pueden usar Tails?

Activistas: con el fin de proteger sus identidades, evitar la censura y comunicarse de manera segura.

Periodistas: para publicar información confidencial, acceder a Internet desde lugares inseguros y proteger sus fuentes.

Tú: cuando necesites privacidad adicional en el mundo digital.

Pasos para usar Tails

1. Descarga Tails desde el sitio **https://tails.boum.org/install/index.es.html**
2. Grábalo en una memoria USB.
3. Una vez instalada enciende la computadora que estés utilizando e inicia en tu memoria USB presionando **F11**.
4. Pulsa la tecla **"Enter"** para iniciar Tails. Aparecerá una ventana de inicio. Asegúrate de **cambiar el idioma** a español en la barra inferior, y pulsa en **"Entrar"**.

Información importante

- Ten en cuenta que al usar Tails no se tiene acceso al disco duro de la computadora, por lo que si quieres almacenar deberás usar otra memoria USB o un disco duro externo.
- Toda la información en la memoria USB se perderá cuando se instale Tails, por ello utiliza una nueva o sin documentos importantes.
- Tails no funciona en ninguna tablet o teléfono.

Ventajas de Tails

- Encripta carpetas correos, mensajería instantánea, documentos, contraseñas, redes wifi y cualquier otro dato que comúnmente se guarda en el disco duro de tu computadora, para que nadie pueda espiarlos ni copiarlos.
- Todas las conexiones a Internet están encriptadas y anonimizadas a través de la red, nadie podrá accesar a tus datos de navegación, identidad o ubicación.
- Como al usar Tails los datos no se alojan en el disco duro o en la memoria de intercambio (SWAP) se minimiza el riesgo de infección por virus informáticos y troyanos
- Después de utilizarlo se puede comenzar de nuevo en otro sistema operativo después de apagar Tails.
- Tails utiliza diversos programas seguros como *Aircrack-ng, Gimp, Keepass, LibreOffice, Audacity*, entre otros.

Dato curioso

Tails fue utilizado y es recomendado por Edward Snowden para mantener sus comunicaciones fuera del espionaje de la Agencia Central de Inteligencia (CIA) y de la Agencia de Seguridad Nacional (NSA) de los Estados Unidos.

Suscríbete a ResistenciaDigital en Telegram @CanalResistenciaDigital

¡No olvides que puedes imprimir tu propia MilpaDigital y compartirla!

CódigoSur EDICIONES