

Guía de seguridad del usuario

La privacidad y la seguridad de los usuarios de myPlan es lo más importante. Los supervivientes son increíblemente listos y creativos para dirigir su propia seguridad cada día; sin embargo, la actividad en línea puede ser difícil de esconder por completo y myPlan puede no ser un recurso al que todos puedan acceder en forma segura



Su seguridad empieza antes de entrar a la aplicación

- + Proporcionamos información en el sitio web y en las tiendas de aplicaciones acerca del riesgo de usarla si algún asociado monitorea la actividad de su dispositivo móvil
- + Proporcionamos enlaces para ver información de planificación de seguridad tecnológica en el sitio web de myPlan
- + myPlan ofrece opciones para tener acceso a la aplicación de una forma más segura: a través de la aplicación móvil o del navegador de la red

Mantenemos su actividad en privado



- + Establezca su propio código NIP seguro y específico para su dispositivo para mantener su información en privado



- + Proporcionamos un "código ficticio", por si alguna vez se ve obligado a abrir la aplicación, este código esconderá todo el contenido de la aplicación



- + Botón de salida rápida en cada página para bloquear la aplicación rápidamente

Le aseguramos que se mantendrá en el anonimato



- + No se requiere configurar ninguna cuenta y no recolectamos datos de identificación personal; su uso es **completamente anónimo**
- + Los datos del usuario **nunca se compartirán** con ninguna otra entidad

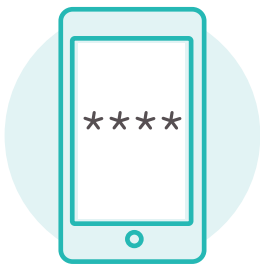
Estrategias de seguridad tecnológica



La forma más segura de tener acceso a myPlan es usando un dispositivo al que un compañero abusivo no tenga acceso

Proteja sus dispositivos y contraseñas

- + Vigile sus dispositivos. Nunca deje un dispositivo desbloqueado o desatendido
- + Proteja todos sus dispositivos con contraseña. Si es posible, utilice un control de acceso biométrico (como su huella digital)
- + Cree contraseñas fuertes
- + Configure una verificación de acceso de dos pasos
- + Use un administrador de contraseñas, como LastPass
- + Salga completamente de todo (salir de una aplicación o sitio no garantiza que haya salido de todos los sitios y la siguiente persona que use el dispositivo podría tener acceso a sus cuentas)



Tenga configuraciones de privacidad estrictas

- + Cambie sus configuraciones de privacidad
- + Use el modo privado o incógnito para visitar sitios que no quiere que queden registrados en su historial de búsqueda
- + Desactive el Bluetooth, el GPS y los servicios de ubicación si no son necesarios

Elimine todo lo que quiere que nadie más vea

- + Cierre las pestañas del navegador en su iPhone o Android
- + Elimine solo los sitios que no quiere que se vean de su historial de navegación. Si borra todo el historial, puede despertar sospechas si alguien más está vigilando su dispositivo
- + Borre myPlan cuando termine de usarlo (siempre puede volver a instalarlo) y elimine su historial de compras y descargas para iPhone (siempre puede "esconderlo", pero no borrarlo totalmente) o de Android

