Guía anti-doxing definitiva

Cómo proteger tus datos online

kaspersky BRING ON THE FUTURE

kaspersky.es

Guía anti-doxing definitiva: cómo proteger tus datos online

Fotos, documentos, datos de aplicaciones instaladas en el smartphone: la gestión de datos es una actividad continua y diaria, seamos o no conscientes de ello. Pero ¿sabemos dónde acaban estos datos? ¿Podrían caer en las manos equivocadas? Tenemos que aprender a compartir datos personales de forma responsable; ya sean datos personales sobre los que tenemos el control, datos controlados por terceras partes, o incluso información sobre otras personas a la que tenemos acceso. Esta guía te mostrará cómo tomar el control de tus datos.

Información propia sobre la que tenemos el control

1.

Sé consciente de los datos personales que compartes y con quién, así como el grado de confianza que tienes en ellos

Al compartir información que permite identificarte (pasaporte, documento de identidad, número de la seguridad social), asegúrate de saber a qué servicio o persona se lo envías y en qué medida confías en ese servicio o persona en particular. En el caso de las empresas, comprueba si han sufrido una brecha de datos previa. Piensa siempre antes de entregar a alguien tus documentos.

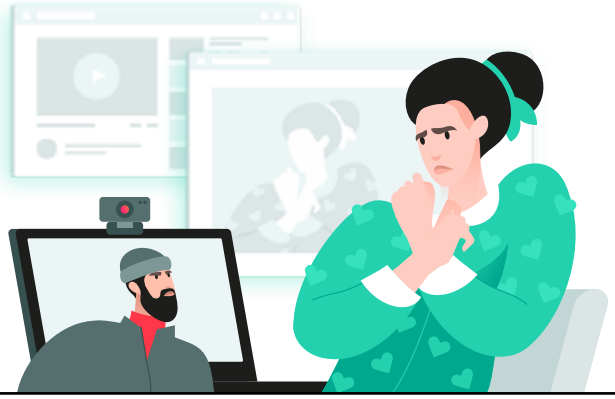
Esto es especialmente importante cuando se trata de compartir datos relacionados con la salud.

2.

Ten en cuenta con quién y cuándo compartes tus datos

Es una buena práctica llevar un registro de con quién has compartido tus datos. De este modo, si se produce una filtración de bases de datos de un determinado servicio que has utilizado, puedes comprobar si tus datos se han visto comprometidos. Una forma de hacerlo es utilizar un gestor de contraseñas a modo de listado de todos los servicios en los que te has registrado. Llevar un control de con quién compartes tus datos personales, te hará pensar dos veces si es necesario compartir algo

Más información: **Cómo mejorar la seguridad en Discord**
Qué datos recopilan las aplicaciones



3.

Piensa antes de publicar. Sé responsable con lo que compartes. Siempre. Incluso si tu cuenta está cerrada.

Aparte de los datos sensibles, es posible construir un "retrato social" a partir de tus publicaciones y utilizarlo en tu contra. Asegúrate de que estás preparado para rendir cuentas de lo que has dicho y publicado en Internet. Considera la posibilidad de hacer privada tu cuenta, pero ten en cuenta que esto no significa que esté totalmente oculta, y que todavía hay formas de exponer lo que has publicado (por ejemplo, que tus seguidores sean hackeados).

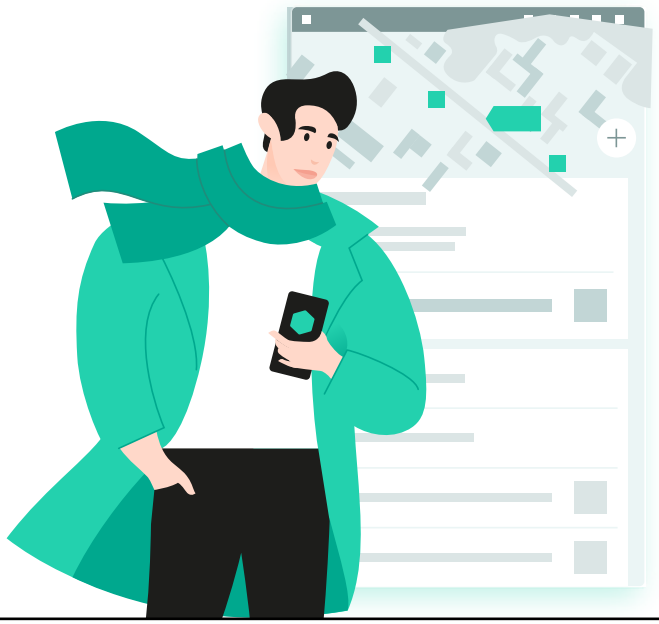
Más información: **Protege tu privacidad online**
Toma el control de tus datos personales

4.

Usa geoetiquetas abstractas. No etiquetes las fotos de lugares específicos que visites regularmente

La geolocalización es uno de los tipos de datos más sensibles que pueden comprometerte: siguiendo las geoetiquetas, es posible identificar dónde vives, dónde pasan el tiempo tus hijos, qué rutas utilizas, cuándo estás en casa y cuándo no...

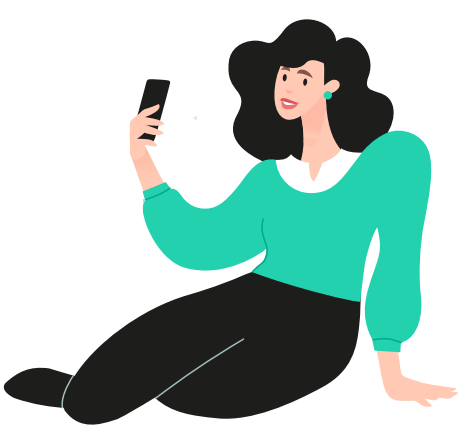
Configura tu privacidad en las redes sociales con la ayuda de Privacy Checker



5.

Asegúrate de no mostrar tus datos personales en las fotos que compartes

Esto debería ser fácil, sin embargo, mirando los hashtags #tickets o #vuelos podemos ver que mucha gente sigue compartiendo sus datos personales en las fotos: por ejemplo, los números de la reserva del vuelo en una tarjeta de embarque. Siempre que este tipo de datos se hacen públicos existe el riesgo de que alguien haga un mal uso.



De hecho, una vez un bromista canceló la reserva de un usuario simplemente llamando a la aerolínea con el número de reserva publicado en Internet y el nombre del usuario. Si piensas compartir algo sobre tus viajes, asegúrate de que las fotos no contengan datos personales, comparte sólo el destino.

Más información: Cómo mantener a los espías alejados de tu teléfono - en la vida real, no en las películas

6.

Entiende qué programas de mensajería son seguros y cuáles tienen cifrado de extremo a extremo

Las conversaciones personales, que generalmente tienen lugar en las aplicaciones de mensajería, son los datos más sensibles de todos. Utilizamos estas aplicaciones para discutir temas muy privados e importantes, que pueden identificar nuestras vulnerabilidades. Por lo tanto, es crucial entender qué nivel de seguridad tiene el programa de mensajería que estás usando, y qué tipo de datos -texto o fotos - pueden ser compartidos con bajo riesgo. También es importante saber si tu aplicación de mensajería favorita almacena los mensajes sólo en tu dispositivo o en una nube o servidor, desde donde pueden filtrarse. Considera otras opciones de privacidad, por ejemplo, si la aplicación te informa cuando el participante de una conversación hace una captura de pantalla de tu mensaje, o si intenta enviar mensajes inapropiados.

Más información: **Consejos de seguridad y privacidad de Telegram**

Qué es el cifrado de extremo a extremo y por qué lo necesitas

---

7.

Invierte con cabeza en tus dispositivos. Un desarrollo barato suele significar mayor riesgo de fuga de datos

Las pulseras de fitness y los smartwatches que llevamos 24 horas al día están ligados a aplicaciones específicas que recogen tus datos biométricos. Aunque hay muchos dispositivos, ten en cuenta que cuanto menos se haya invertido en el dispositivo y la aplicación, la seguridad será menor. La regla básica es considerar el precio, la popularidad y la facilidad de uso de la aplicación a la que está vinculado. Busca información sobre la aplicación, revisa cualquier historial de fugas de datos y lee las opiniones de los usuarios antes de comprarlo. Lo mismo ocurre para los teléfonos inteligentes, las cámaras de vídeo y los monitores de bebés.

8.

Compra online en tiendas de confianza. Y cuantas menos, mejor.

La miríada de tiendas online que ofrecen más o menos lo mismo puede confundirnos. Pero todas las tiendas tienen políticas de privacidad diferentes, y algunas, ninguna. Cuantas menos tiendas online utilices, menos información compartes.

Información sobre la que no tienes control

Actividad del navegador

Cada acción en tu navegador es rastreada por las cookies y las URLs de seguimiento. Y no sólo se trata de las cookies: existen innumerables mecanismos que se utilizan para identificar personalmente a un usuario online. Estos datos permiten a las organizaciones crear un perfil detallado de cada persona, adaptar la publicidad y mejorar la experiencia del usuario. Pero eso tiene un coste: la vulnerabilidad de los datos. Por lo tanto, depende de ti encontrar el equilibrio adecuado entre tu privacidad y la mejora de la experiencia de usuario - con la ayuda de nuestros consejos.

1.

Opta por un navegador que haya tenido en cuenta la privacidad en su desarrollo

Las URL de seguimiento para publicidad se cargan junto a las páginas web para rastrear tu actividad, además del seguimiento que realiza la propia página web. Instala complementos de seguridad y privacidad de confianza, tales como bloqueadores de rastreadores, bloqueadores de anuncios y de seguridad, y utiliza plug-ins que corten los enlaces de seguimiento. Por ejemplo, los productos de Kaspersky tienen un componente *Do Not Track* que impide la carga de elementos de seguimiento que monitorizan las acciones del usuario en los sitios web.

Más información: **¿Están recopilando la huella digital de tu navegador?**

2.

Elimina las cookies después de cada sesión en tu navegador

Configura los ajustes de navegación para limitar las cookies. De esta manera no permitirás que las cookies rastreen tu actividad en la web e impedirás que creen un perfil definido. Ten en cuenta la diferencia entre las cookies de origen y las de terceros: las de origen tienen como objetivo mejorar la experiencia del usuario, haciendo más cómoda la navegación y creando recomendaciones personalizadas. Por lo general, son seguras.

Por su parte, las cookies de terceros rastrean la misma actividad o las actividades más interesantes para crear un perfil tuyo y dirigirte publicidad; también pueden rastrear tu historial de navegación. Ten en cuenta que algunos navegadores, como Safari, han desarrollado una política de privacidad más sólida en relación con las cookies por defecto.

Más información: ¿Por qué deberías intentar escuchar a tus cookies?

3.

Funciones adicionales en los navegadores para mayor privacidad

Si estás dispuesto a esforzarte por proteger tus datos tanto desde el punto de vista de la privacidad como de la seguridad, considera tomar medidas adicionales. Por ejemplo, Firefox Containers es una buena opción que permite a los usuarios segmentar cuidadosamente partes de su actividad online en cajas separadas que mantienen los datos relevantes para esos segmentos separados unos de otros. Otra opción sería restringir qué sitios tienen acceso a tus datos de localización, micrófono y webcam, e incluso qué sitios tienen activado JavaScript.

Los usuarios más avanzados pueden considerar la posibilidad de desactivar las API de WebRTC si les preocupa la posibilidad de filtrar tu dirección IP. Otra opción que suele estar activada automáticamente en la mayoría de los navegadores y que muchos usuarios podrían querer desactivar para aumentar la seguridad es el autoguardado y el relleno automático de contraseñas. Si el navegador lo soporta, considera habilitar el "Modo solo HTTPS" que automáticamente intenta encriptar todo el tráfico HTTP de los sitios (la mayor parte de la web utiliza HTTPS, pero todavía hay sitios atípicos y es mejor asegurarse, que arrepentirse).

Muchas de estas tareas pueden hacerse automáticamente con la ayuda de extensiones del navegador como Privacy Badger.

4.

Modo incógnito

Si quieres buscar algo, pero no quieres que quede en tu historial, utiliza la navegación de incógnito. Esto impide que el navegador pueda rastrear tu historial de navegación y borrará todas las cookies, haciendo que tu búsqueda sea privada. Esto es especialmente útil si compartes ordenador con otras personas.

Más información: **Preguntas y respuestas sobre el modo incógnito**

Rastreo por aplicaciones

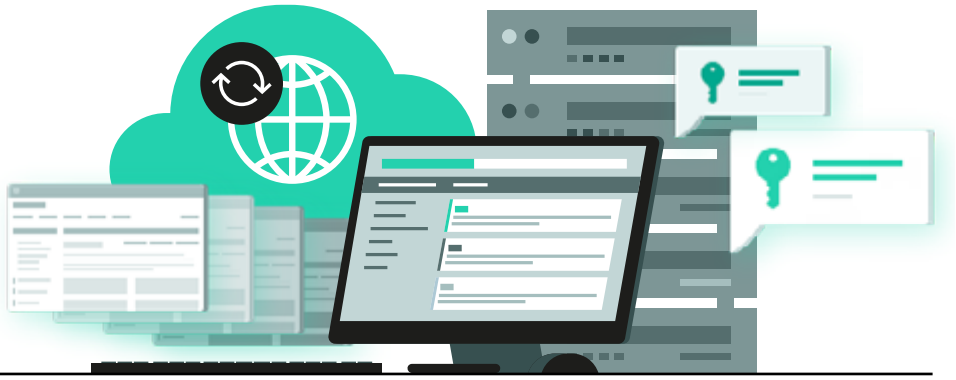
Las aplicaciones móviles rastrean y recopilan tus datos del mismo modo que los navegadores web. Peor aún: llevamos los smartphones a todas partes, así que saben mucho más sobre nosotros de lo que podríamos sospechar. Hay dos formas principales de limitar la recopilación de tu información en los dispositivos móviles: minimizar el rastreo y mezclar los datos con ruido. He aquí cómo hacerlo:

5.

Utiliza una VPN

Una VPN cifra completamente el tráfico del dispositivo, manteniéndolo seguro y oculto a todo el mundo, incluido tu proveedor e incluso si te conectas a redes Wi-Fi públicas. Puede cambiar cierta información sobre ti y tu dispositivo (por ejemplo, tu IP) y dificultar que las organizaciones te rastreen. Es importante tener en cuenta que una VPN también recopila datos del usuario y, por lo tanto, es importante seleccionar un servicio en el que realmente pueda confiar. Aunque la versión gratuita de una VPN será suficiente para ocultar el tráfico a un proveedor, éste también puede venderlo a terceros. Selecciona un servicio de un proveedor serio con una declaración de procesamiento de datos en vigor, por ejemplo, Kaspersky VPN.

Más información: **Cómo proteger tu Wi-Fi de los vecinos**
Cómo elegir una VPN



6.

Cambia la región de tu dispositivo

Informar mal a los rastreadores sobre tu ubicación ayudará a confundirlos y dificultará la creación de un perfil correcto sobre ti. Elige una región diferente en tu sistema operativo y elige un tercer país para tu conexión VPN. Por ejemplo, selecciona la versión alemana de iOS y una conexión VPN finlandesa. Con este tipo de configuración, puedes tener algún problema al querer utilizar un servicio de pago no disponible en el país que hayas seleccionado. En estos casos, basta con cambiar de nuevo a tu región, hacer el pago, y luego cambiar de nuevo al país de tu elección.

7.

Configura los ajustes de acceso para cada aplicación

Utiliza los instrumentos que los desarrolladores del sistema operativo han creado para que las aplicaciones sólo accedan a la información que necesitan. Las mejores prácticas incluyen permitir el acceso a tu ubicación sólo mientras usas una aplicación y limitar el acceso al micrófono y a las fotografías. Desconfía de las aplicaciones que solicitan datos que no deberían necesitar para realizar sus funciones.

Más información: **Mantén (casi) toda la información fuera de Facebook**

Configuración de seguridad en Instagram

8.

Nunca instales aplicaciones no verificadas

Las aplicaciones no verificadas (aplicaciones que no han pasado por el proceso de verificación de una tienda de aplicaciones) a menudo terminan siendo adware - un tipo de software que inunda el teléfono de publicidad y recopila metadatos. Y lo que es peor, la aplicación que se descarga puede ser maliciosa. Por ejemplo, puede contener un programa espía que recopila información sobre tu ubicación, tus conversaciones en los programas de mensajería o el registro de llamadas.

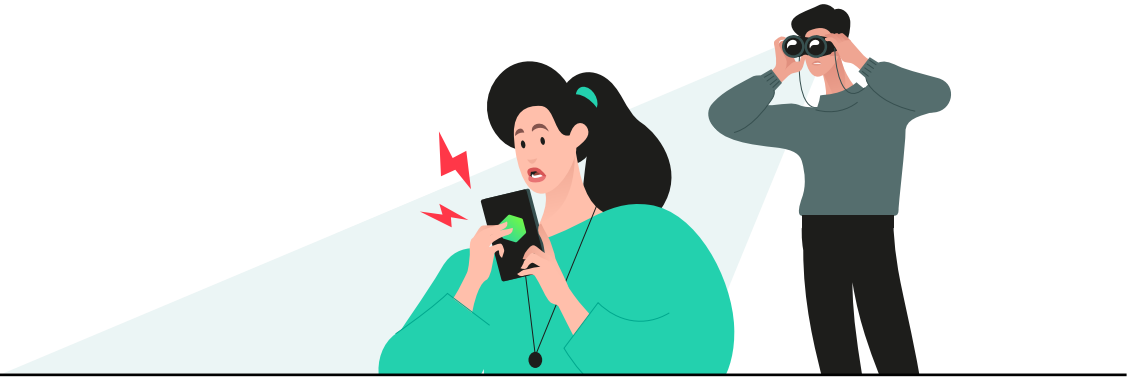
Información de otras personas sobre la que tienes el control

Fotos de otras personas, conversaciones, chats, números de teléfono y direcciones... a menudo se accede a la información personal de otras personas. Esto también requiere cuidado, y es tu responsabilidad mantenerla a salvo. He aquí cómo hacerlo:

1.

Comparte información personal sólo si tienes el consentimiento de las personas implicadas

Puede que hayas tomado una foto de alguien que para ti sea totalmente inofensiva, pero quizá puede perjudicar a otros. Lo mismo ocurre con capturas de pantalla de conversaciones, billetes de avión que hayas comprado junto con otra persona - prácticamente cualquier cosa que incluya una tercera persona y la información que pueda identificarla. Recuerda que eres responsable no sólo de tus datos, sino de los datos de otros que han pasado a ser tuyos.



2.

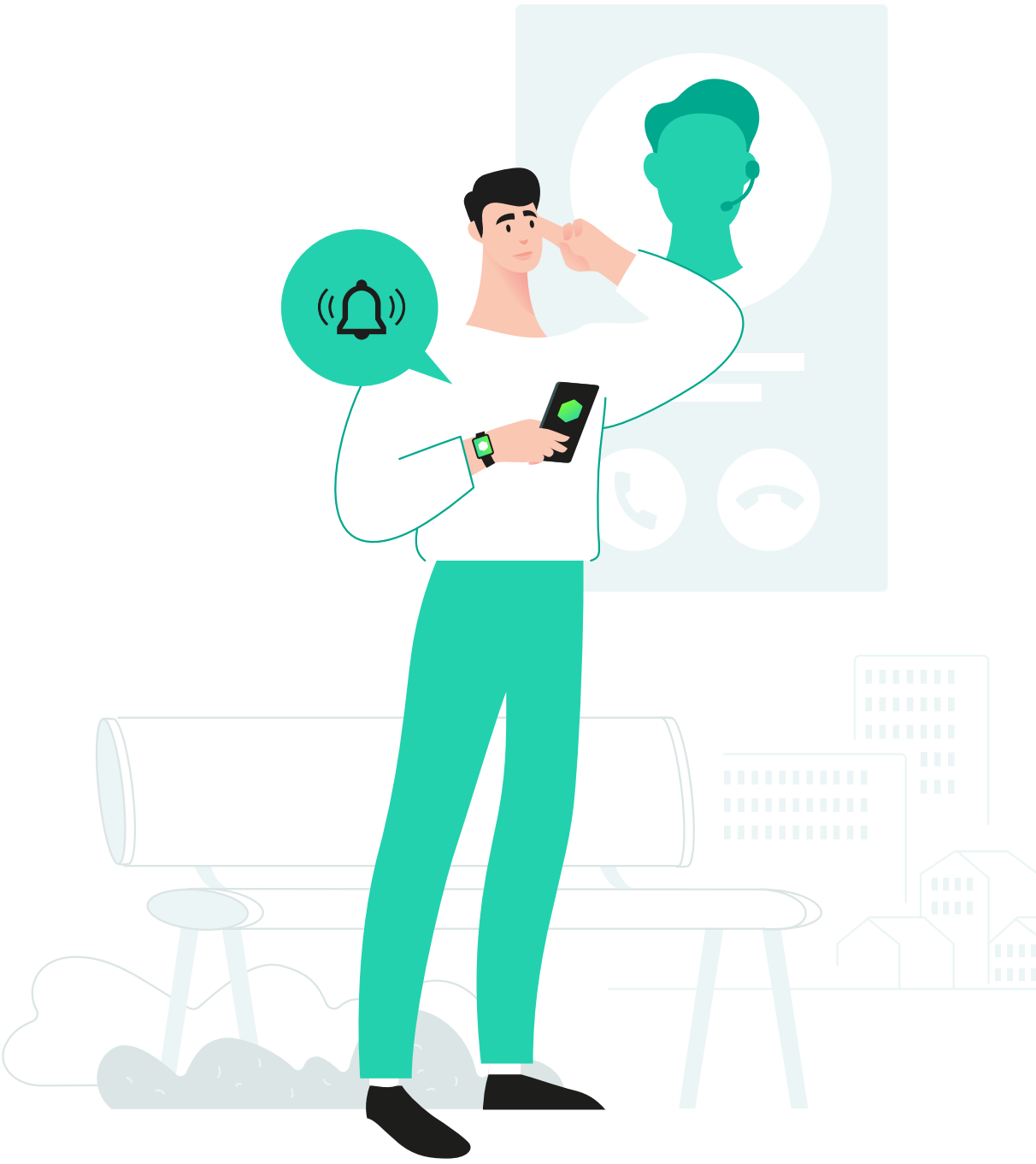
Trata los datos personales de los demás como tratarías los tuyos: con cuidado

Sigue las mismas normas con los datos de otras personas que sigues con tus datos personales que puedes controlar. Sube datos personales de terceros únicamente a recursos de confianza, no los muestres a otras personas y ten en cuenta el uso que pueden hacer de esos datos.

3.

Advierte siempre a los demás si se está grabando una conversación

Además de que las grabaciones no consentidas son poco éticas e irrespetuosas para los participantes en la conversación, en algunos países también son ilegales.



4.

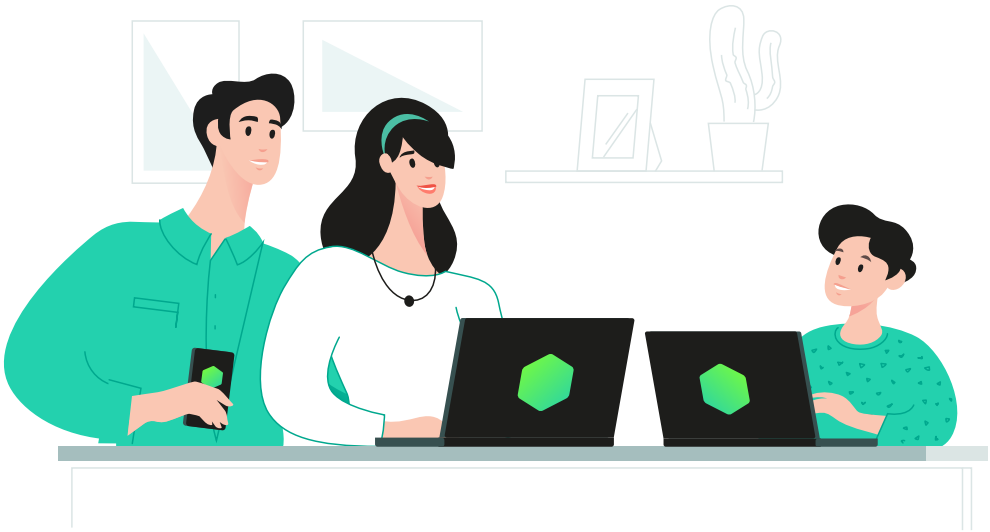
No compartas información sobre tus familiares o contactos estrechos en redes sociales

Los contactos personales revelan más de lo que crees: muestran qué personas significan mucho para ti y, por tanto, te hacen vulnerable. Esta información puede ser utilizada no sólo contra ti, sino también contra tus contactos cercanos.

5.

Habla con amigos y familiares sobre el tratamiento correcto de los datos

Habla con las personas de tu entorno para establecer normas de higiene de datos para cada uno, y recuerda que debes consultar con los demás cuando se produce una fuga de datos personales. Es importante disponer de un determinado nivel de confianza en el entorno cercano sobre cómo se comparten los datos con el exterior.



www.kaspersky.es

kaspersky

GBD-7837 Q1/21 V1