



Unidad de Contenido

Protección de Teléfonos Inteligentes

Nombre del autor: bit Schulungcenter

Última fecha de procesamiento: [04.03.2020]

Funded by the
Erasmus+ Programme
of the European Union



"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein."

El tema

Introducción

Redes sociales, mensajería instantánea, compras, juegos, aplicaciones, tomar una foto rápida o buscar en Google: muchas personas apenas pueden imaginar la vida cotidiana sin su teléfono inteligente. Sin embargo, para hacer llamadas telefónicas, se usa cada vez menos. La clara tendencia es hacia escribir en lugar de hacer llamadas telefónicas. Esto también se muestra al observar la cantidad de usuarios de servicios de mensajería instantánea: alrededor de 1.600 millones de personas en todo el mundo usan WhatsApp, y alrededor de 1.300 millones se comunican con sus amigos a través de Facebook Messenger. Usar estos servicios es un juego de niños. Pero, ¿qué peligros acechan al usar los servicios de mensajería instantánea u otras aplicaciones de teléfonos inteligentes con respecto a la privacidad de los datos? No sin razón, los proteccionistas de datos critican repetidamente a Facebook u otros proveedores de aplicaciones gratuitas para teléfonos inteligentes. ¡Descubre cómo puedes proteger mejor tu teléfono inteligente, tus datos y tu privacidad!

Relevancia práctica: estos son los conocimientos y habilidades que adquirirá

Después de completar esta unidad de contenido, podrás evaluar mejor los riesgos asociados al uso de servicios de mensajería instantánea u otras aplicaciones de teléfonos inteligentes y conocerás algunos pasos útiles para proteger tu teléfono y tu privacidad de riesgos no deseados.

1. Construye Conocimiento: Medidas de protección básicas para teléfonos inteligentes

Para muchas personas, su teléfono inteligente es su compañero constante en la vida cotidiana. ¿También perteneces a quienes llevan su teléfono inteligente a todas partes y no pueden prescindir de él por un día? Si es así, probablemente también tengas **datos muy privados o confidenciales en tu teléfono** inteligente, como fotos, mensajes de texto confidenciales o información comercial. Para proteger tu teléfono inteligente y los datos potencialmente muy privados que almacenas, debes tomar las medidas adecuadas en caso de pérdida o robo.

Esto incluye, por ejemplo, proteger el teléfono inteligente contra el acceso no autorizado a través del **PIN** (número de identificación personal) y el **bloqueo de pantalla**.

Importante

Asegúrate de **no utilizar combinaciones de números comunes** como "1234", "1111" o similar. Estos son muy fáciles de hackear por personas no autorizadas.

Si te roban o pierdes tu teléfono inteligente, tu proveedor de red debe **bloquear** la tarjeta **SIM** (módulo de identidad del suscriptor) del dispositivo para que nadie pueda usarla para hacer llamadas telefónicas o incurrir en altos costos.

¿Conoce el número de serie de su teléfono inteligente? Se encuentra debajo de la batería, en el embalaje original o en la factura de compra del teléfono móvil. Debe anotar este número para poder denunciarlo a la policía en caso de robo.

Todos los sistemas operativos comunes ofrecen también **varios servicios** que pueden ser muy útiles en caso de robo o pérdida.

Ejemplos

¿No puedes encontrar tu teléfono móvil? Con el **Administrador de dispositivos Android**, puedes dejar que tu teléfono inteligente suene al máximo volumen, incluso si estaba silenciado. De esta manera, puedes localizar rápidamente un teléfono perdido en tu casa. Si está en otro lugar, puedes localizarlo en tiempo real y dejar un mensaje para el buscador.

Si pierdes o te roban tu iPhone, generalmente puedes buscarlo a través de **iCloud**, a condición de que el dispositivo esté encendido y tenga recepción de datos.

Probablemente ya hayas escuchado sobre la posibilidad de instalar un tipo de **aplicación antirrobo** en tu teléfono inteligente. Por ejemplo, te permite localizar y bloquear el teléfono inteligente perdido o robado y eliminar los datos almacenados en él. Los comandos necesarios para esto pueden ser emitidos por otro teléfono inteligente cuyo número haya sido almacenado o enviado al dispositivo a través de un portal en línea.

Consejo

En caso de robo o pérdida, debes bloquear la tarjeta SIM de inmediato si no tienes **una aplicación antirrobo instalada en tu teléfono**. Sin embargo, si se instala una aplicación, la tarjeta SIM no debe bloquearse hasta que los datos hayan sido localizados y eliminados de forma remota. De lo contrario, esto ya no será posible.

1. Aplica conocimiento

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_01_01

Situación: ¿Qué medidas puedes tomar para proteger tu teléfono inteligente del acceso no autorizado?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Puedo usar un PIN. Este PIN debe ser tan fácil de recordar como sea posible.
- Debería bloquear mi teléfono inteligente con un PIN y asegurarme de que no sea una combinación de números como 1234 o 1111.
- Puedo configurar un bloqueo de pantalla.
- Puedo instalar una aplicación de pago para configurar un número de identificación personal.

Exercise OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_01_02

Situación: Después de una tarde de compras en la ciudad, de repente te das cuenta en casa de que has perdido tu teléfono inteligente. ¿Qué medidas pueden ser útiles en tal situación?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Puedo usar el Administrador de dispositivos Android o iCloud para localizar mi teléfono inteligente
- Puedo instalar algún tipo de aplicación antirrobo para tales casos. Esto me permite localizar mi teléfono, bloquearlo o eliminar datos almacenados en el teléfono.
- Puedo bloquear mi tarjeta SIM para poder localizar mi teléfono.
- Puedo bloquear mi tarjeta SIM para evitar que alguien incurra en altos costes al usar mi teléfono.

2. Construye Conocimiento: Mensajería Instantánea (MI) y aplicaciones

The possibility of exchanging text messages via mobile phone is not new. However, in recent years, due to the widespread use of smartphones, communication via SMS has increasingly been replaced by the use of **instant messaging (IM)** services.

Definición

A diferencia de los servicios de SMS, la **MI** es una **comunicación basada en Internet** a través de **aplicaciones móviles**. Es un tipo de chat en línea que te permite intercambiar mensajes con otros usuarios casi en tiempo real. Para hacer esto, las aplicaciones de mensajería instantánea deben descargarse e instalarse.

Además de la transmisión de textos, la transmisión de archivos, secuencias de audio y video (y por lo tanto también video chat) también son posibles. La transmisión del mensaje se lleva a cabo en el llamado **procedimiento push**, que permite que los textos lleguen al destinatario inmediatamente después de haber sido enviados. A diferencia de los correos electrónicos, por ejemplo, los mensajes no tienen que recuperarse primero, sino que aparecen inmediatamente en la pantalla del interlocutor.

Ejemplo:

Ejemplos de servicios populares de mensajería instantánea:

- Windows life messenger
- Skype
- Facebook Messenger
- WhatsApp
- WeChat
- Telegram

Por ejemplo, alrededor de 1.300 millones de usuarios en todo el mundo ya usan Facebook Messenger para comunicarse.

El uso más común de los programas de mensajería instantánea es en dispositivos móviles como **teléfonos inteligentes** a través de aplicaciones de mensajería. Las **aplicaciones de Messenger** suelen ser gratuitas, prácticas, fáciles de usar y, por lo tanto, disfrutan de una popularidad cada vez mayor. Para usar WhatsApp, por ejemplo, todo lo que necesitas hacer es descargar la aplicación gratuita y registrarte a través de tu propio número de teléfono móvil.

Sin embargo, para cumplir el propósito deseado, una aplicación generalmente requiere una variedad de **autorizaciones**. Por lo tanto, la aplicación quiere acceder a ciertas funciones del dispositivo de tu teléfono inteligente, como calendario, cámara, contactos, micrófono, SMS, memoria, ubicación o función del teléfono.

Importante

¿Eres uno de los 1.600 millones de usuarios de WhatsApp en todo el mundo? Entonces debes tener en cuenta que WhatsApp accede al menos a todas **las direcciones de contacto almacenadas en su teléfono móvil**.

Esta es la única forma en que la aplicación puede determinar cuál de tus contactos también está usando WhatsApp y mostrarlos automáticamente en la aplicación. ¿Te gustaría enviar fotos o tu propia ubicación a través de WhatsApp o usarlo para video telefonía? Si es así, debes tener en cuenta que WhatsApp también necesita acceder a tus imágenes, cámara, micrófono y datos de ubicación.

Consejo

Debido a razones de protección de datos, vale la pena tener cuidado al asignar **autorizaciones a aplicaciones** y reducir las autorizaciones al nivel más necesario.

Si no estás seguro de qué permiso tiene cada aplicación en tu teléfono inteligente, debes verificar esto por razones de seguridad. ¿Te preguntas cómo hacerlo? Simplemente selecciona la aplicación apropiada en "configuración", mira qué accesos permites a la aplicación y ajústalos si es necesario.

Ejemplo

Supongamos que deseas utilizar Google Maps para encontrar una dirección específica. En este caso, tiene sentido permitir que **la aplicación acceda a tu ubicación mientras la usas**. Sin embargo, si no deseas compartir tu ubicación con sus contactos a través de WhatsApp, la aplicación no necesariamente necesita saber dónde se encuentra.



2. Aplica conocimiento

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_02_01

Situación: ¿Cuál de las siguientes afirmaciones sobre los servicios de mensajería instantánea (MI) son correctas?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Cada vez más personas utilizan los servicios de mensajería instantánea para intercambiar mensajes de texto, mientras que la comunicación por SMS ha perdido popularidad.
- La MI es comunicación basada en Internet.
- IM permite no solo el intercambio de mensajes de texto, sino también el intercambio de archivos, audios o comunicaciones a través de video chat.

- Si muchas personas usan servicios de mensajería instantánea populares al mismo tiempo, el destinatario suele tardar unos minutos en recibir los mensajes.
- Los servicios populares de mensajería instantánea son Facebook Messenger, WhatsApp o Windows life messenger.
- Los servicios populares de mensajería instantánea son Youtube, Twitter, WhatsApp y Google.

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_02_02

Situación: Te gustaría usar WhatsApp para comunicarse con sus amigos. ¿Qué debes tener en cuenta al instalar la aplicación?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Las aplicaciones de Messenger como WhatsApp generalmente requieren un pago único de una tarifa de uso por adelantado.
- Para usar WhatsApp, debes descargar la aplicación y registrarte con su nombre real.
- WhatsApp accede a todos los contactos almacenados en tu teléfono inteligente.
- Para usar ciertos servicios de WhatsApp, puede ser necesario permitir que la aplicación acceda a tus imágenes, cámara, micrófono o datos de ubicación.
- WhatsApp accede automáticamente a todos los contactos almacenados en tu teléfono inteligente, sus imágenes y sus datos de ubicación. Esta es la única forma en que la aplicación puede funcionar.

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_02_03

Situación: ¿Cuándo tiene sentido ajustar las autorizaciones de aplicaciones y cómo es esto básicamente posible?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Básicamente, puedes verificar fácilmente en "Configuración" cuáles de las aplicaciones instaladas poseen qué derechos de acceso y, si es necesario, reducirlos en la medida realmente necesaria.
 - Para saber qué derechos de acceso tiene una aplicación, es una buena idea llamar a su proveedor de telefonía móvil.
 - Si deseas utilizar Google Maps, por ejemplo, es una buena idea permitir que la aplicación acceda a sus datos de ubicación mientras la utiliza.
 - También es una buena idea permitir que WhatsApp acceda a los datos de tu ubicación, ya que esto ayudará a que tus mensajes se transfieran más rápido.
 - Dado que la mayoría de las aplicaciones son gratuitas, generalmente no es posible restringir los derechos de acceso de las aplicaciones individualmente.
-

3. Construye conocimiento: Riesgos de seguridad con la aplicación de teléfonos inteligentes

Si también almacenas y procesas una gran cantidad de datos en tu teléfono inteligente, en parte de una naturaleza muy privada y de terceros (por ejemplo, fotos), debes considerar en qué medida los **permisos de aplicaciones sin restricciones** podrían ser problemáticos.

No es ningún secreto que muchos productores de aplicaciones están interesados en tus datos personales. Después de todo, necesitan generar algún tipo de ingresos con las aplicaciones que a menudo se proporcionan de forma gratuita a los usuarios. **Si no pagas por un producto, entonces normalmente eres el producto**, se dice. Pero eso aún no es motivo de preocupación. En la mayoría de los casos, el uso de nuestros datos personales se hace anónimo en el marco de las regulaciones legales de protección de datos.

Sin embargo, **la adquisición de WhatsApp por Facebook**, por ejemplo, ha significado que los números de teléfono del directorio de contactos también se transmitan a Facebook. Además, el descubrimiento de varios incidentes de privacidad en el pasado también ha llevado a la conciencia de los peligros del monitoreo no autorizado. Los usuarios están cada vez más preocupados por la protección de datos.

¿Te estás preguntando qué problemas de seguridad y consecuencias no deseadas puede tener para ti el uso de servicios de mensajería instantánea y otras aplicaciones? Aquí están algunos ejemplos:

1. Al igual que con otros medios de comunicación en línea, los mensajeros también corren el riesgo de enviar **enlaces de phishing o transmitir malware** a través de hipervínculos clicables o archivos transferidos.
 1. Existe el peligro de que el **malware de todo tipo se oculte en las aplicaciones**, especialmente si las aplicaciones se han adquirido gratis en Internet de proveedores de aplicaciones menos confiables.
 2. Como ya sabe, las aplicaciones obtienen permisos para realizar funciones. Los permisos permiten que las aplicaciones lean datos. Por lo tanto, existe el **riesgo de acceso oculto a datos personales**, como datos de ubicación, hábitos de navegación móvil, datos de contacto almacenados o contraseñas. Además de la pérdida de privacidad, el **mal uso de tus datos de contacto** también puede ser una consecuencia desagradable.
 3. Pueden surgir **problemas con los derechos de autor**, por ejemplo, si las imágenes que no has creado tú y para las que no posees derechos de autor se utilizan como fotos de perfil.
 4. La **comunicación sin cifrar** representa un alto riesgo de seguridad. Por lo tanto, desde abril de 2016, el contenido enviado a través de WhatsApp, por ejemplo, se ha transmitido con un cifrado seguro de extremo a extremo. Esto se aplica a texto, imágenes, video y otros archivos. El cifrado de extremo a extremo significa que solo los socios de comunicación respectivos pueden recibir y leer el contenido.

Importante

Si usas la **aplicación de mensajes de Facebook**, debes tener en cuenta que su comunicación (a diferencia de WhatsApp) no está encriptada. Si deseas chatear encriptado de extremo a extremo, debes iniciar una "conversación secreta". Cómo funciona esto se explicará en la próxima sesión.

3. Aplica conocimiento

Ejercicio OPCIÓN ÚNICA

Objetivo específico asociado: OE_03_01

Situación: ¿Por qué los usuarios de aplicaciones están cada vez más preocupados por la privacidad de los datos?

Tarea: Elige las opciones correctas siguiendo el principio de opción única: solo una respuesta puede ser verdadera.

- Porque las aplicaciones son utilizadas por más y más personas.
- Debido a que las aplicaciones están desarrolladas principalmente por empresas ubicadas en países que no se preocupan por la protección de datos y, por lo tanto, no existen

reglas de protección de datos vinculantes para el manejo de datos de usuarios. Un ejemplo bien conocido es Facebook o WhatsApp.

- Porque las aplicaciones son cada vez más caras.
- Porque algunas violaciones de protección de datos se han conocido en los últimos años.
- Porque es imposible que los usuarios entiendan qué derechos de acceso se les otorgan a los distintos proveedores de aplicaciones.
- Debido a que los usuarios almacenan más y más fotos y otros archivos en sus teléfonos inteligentes y, por lo tanto, las capacidades de almacenamiento pronto se agotarán.

Ejercicio OPCIÓN MÚLTIPLE

Objetivo específico asociado: OE_03_02

Situación: ¿Qué riesgos de seguridad y consecuencias no deseadas pueden causar los servicios de mensajería instantánea y otras aplicaciones?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Los mensajeros corren el riesgo de enviar enlaces de phishing o transmitir malware a través de hipervínculos clicables o archivos transferidos.
- El malware puede estar presente especialmente en aplicaciones gratuitas de proveedores de aplicaciones menos conocidos.
- Un problema importante son los costes ocultos más que el acceso secreto a los datos personales.
- La comunicación no cifrada, como suele ser el caso a través de WhatsApp, por ejemplo, es un problema de seguridad importante.
- Los datos personales pueden perderse a través de la comunicación encriptada.

4. Construye conocimiento: Medidas y consejos para el uso seguro de las aplicaciones de teléfonos inteligentes

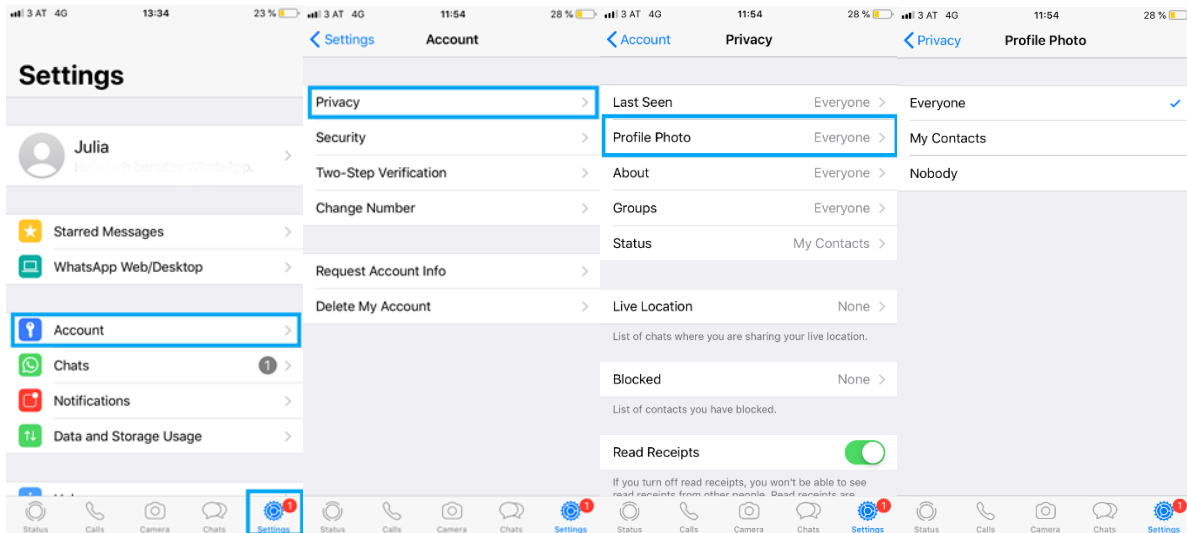
Dados los posibles riesgos de seguridad de usar aplicaciones en tu teléfono inteligente, probablemente te estés preguntando cómo puedes protegerte mejor a ti y a tu privacidad. Los siguientes son algunos consejos sobre **qué considerar al usar aplicaciones en su teléfono inteligente**:

En el pasado, se identificaron serias deficiencias de seguridad en varias aplicaciones. Posteriormente, se intentó remediar estas deficiencias haciendo los ajustes apropiados. Por esta razón, por ejemplo, es recomendable utilizar siempre **la última versión de WhatsApp Messenger**.

Para evitar problemas de derechos de autor, debes **abstenerte de usar imágenes que no sean de tu propiedad como imágenes de perfil**.

Consejo

También puedes usar la configuración de privacidad de WhatsApp para **limitar la visibilidad de su foto de perfil**: simplemente abre WhatsApp y toca "Configuración". Luego toca "Cuenta", selecciona "Privacidad" y cambia la configuración "Todos" a "Mis contactos" o "Nadie" para la foto de perfil.



Los proveedores de aplicaciones están obligados a proporcionar al usuario una **declaración de protección de datos** que contenga información sobre los permisos solicitados por la aplicación. Además, la mayoría de las aplicaciones actuales requieren que **aceses estos permisos cuando se instalan**. Debes **leer la política de privacidad y los términos y condiciones** de cada aplicación de manera crítica antes de instalarla. ¡También debes **controlar los derechos de acceso** de las aplicaciones! Los permisos otorgados se pueden ver y revocar en cualquier momento en la configuración de cada aplicación.

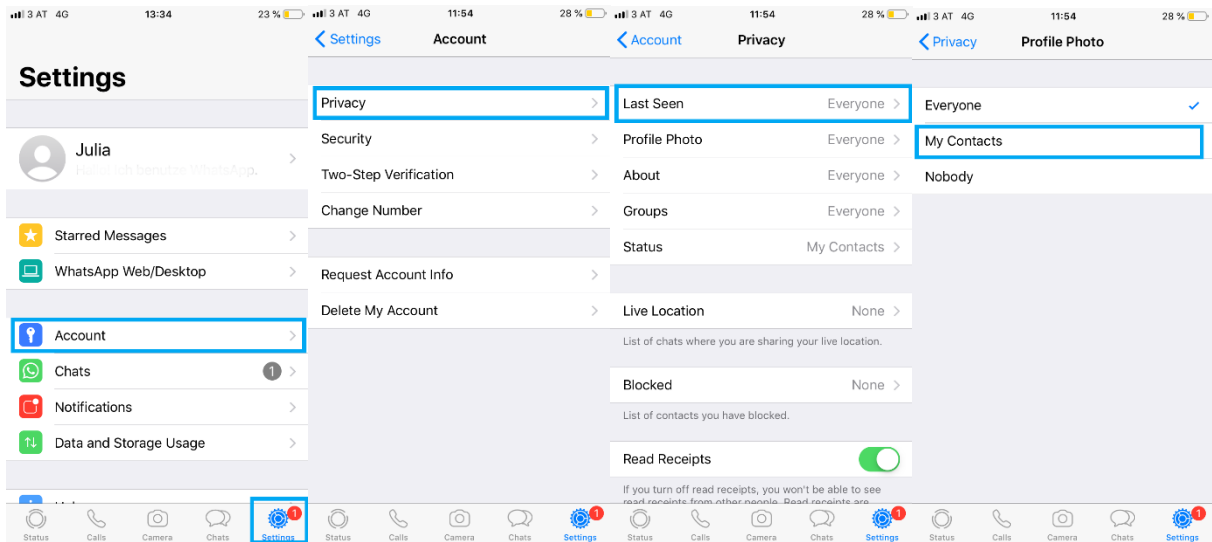
Ejemplo

Es fácil entender que, por ejemplo, una aplicación meteorológica para mostrar el pronóstico del tiempo debe poder consultar tu ubicación para proporcionar información de pronóstico más precisa. Sin embargo, por qué esta aplicación podría necesitar acceso a la cámara de tu teléfono inteligente ya no es tan obvio.

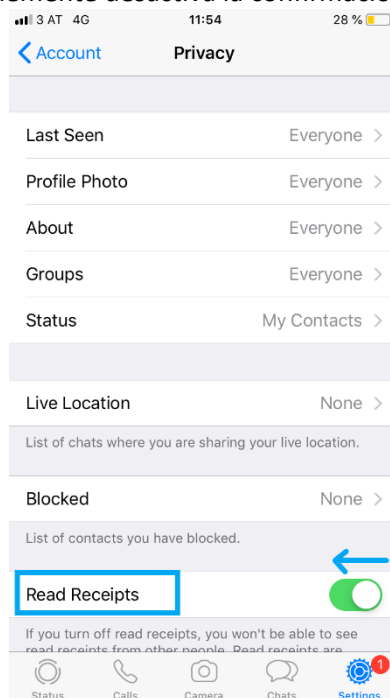
Solo debes ingresar los datos más necesarios. Usa una **dirección de correo electrónico adicional** que no revele mucho sobre ti y que no te moleste cuando llegue spam.

Una ventaja supuestamente grande de la mensajería instantánea es que siempre es obvio de inmediato cuando un contacto está en línea o cuando estuvo en línea por última vez. Sin embargo, la nueva configuración de privacidad de algunos mensajeros le ofrece la oportunidad de **evitar que otros sepan que estás en línea, la última vez que estuviste en línea o de desactivar las confirmaciones de lectura automáticas**. El siguiente ejemplo muestra cómo funciona WhatsApp:

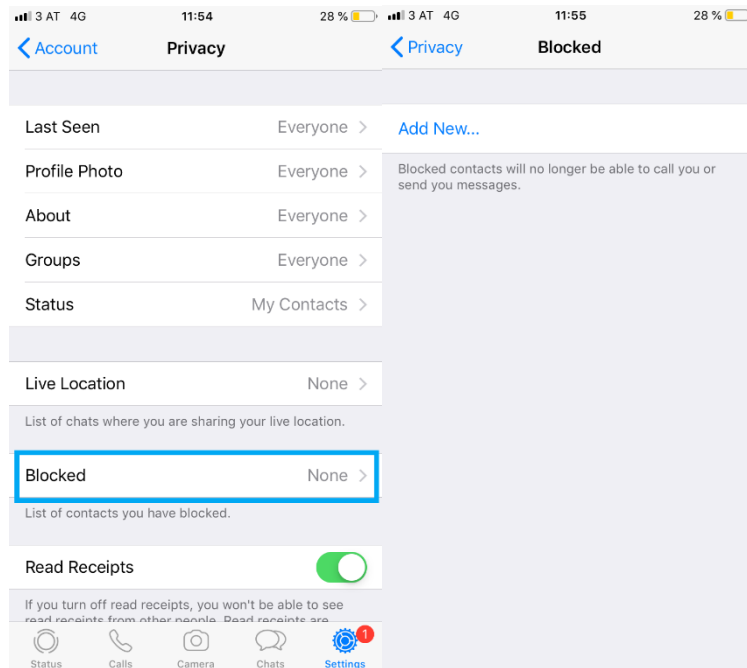
- **Cómo ocultar "Último visto"**: abre WhatsApp y toca "Cuenta". Luego toca "Privacidad", selecciona "Último visto" y elija quién o si alguien puede ver cuándo fue la última vez que estuviste en línea.



- **Cómo desactivar los recibos de lectura:** Vuelve a tocar "Configuración", "Cuenta" y "Privacidad". Luego, simplemente desactiva la confirmación de lectura.



Para evitar el contacto de extraños, siempre se debe **considerar cuidadosamente, en primer lugar, en qué casos se debe dar el número de teléfono móvil** y, sobre todo, a quién se debe comunicar. Si personas no deseadas intentan contactarte a través de WhatsApp, simplemente puedes bloquearlas. Para hacer esto, desplázate hacia abajo en "Privacidad" y toca los contactos bloqueados.

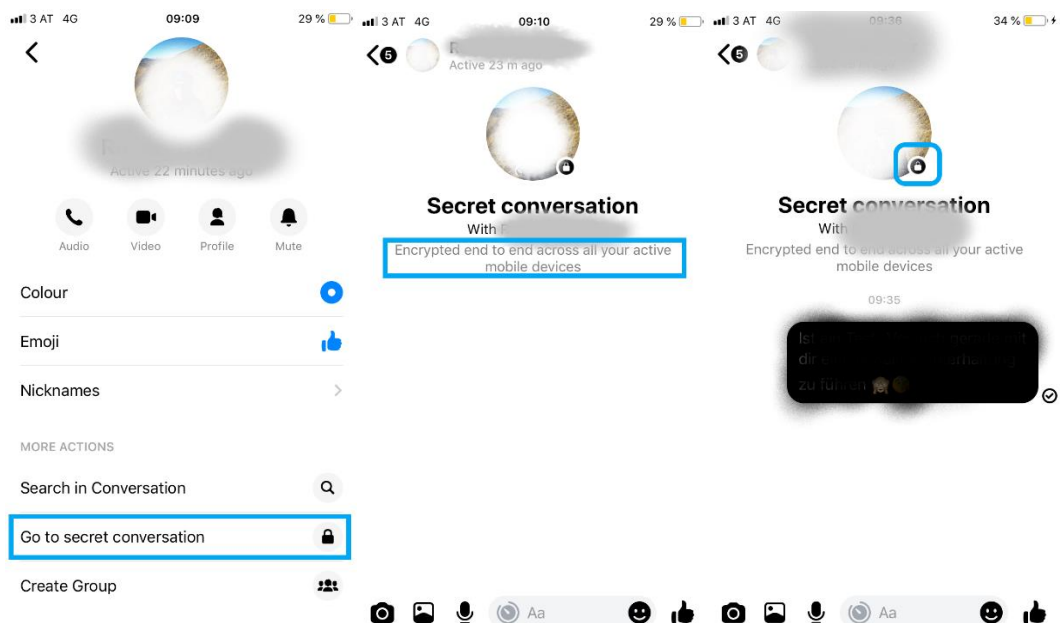


Importante

Bloquea los contactos si no estás seguro de quiénes son o si alguien te está acosando. Denuncia insultos, acoso sexual, chantaje o amenazas a la policía.

Algunas aplicaciones de mensajería, como Facebook Messenger, **no cifran automáticamente tus mensajes**. Debes cambiar la configuración manualmente si es posible.

Cómo comunicarte cifrado con Facebook Messenger: Ve al chat, toca el nombre de la persona y selecciona "Conversación secreta". Ahora el intercambio de mensajes con esta persona está encriptado de extremo a extremo. Nadie más que tú y tu compañero de chat verá tus mensajes, ni siquiera Facebook.



Consejo

Puedes reconocer un chat encriptado por el hecho de que la interfaz de usuario es **gris-negra**. También verás un **pequeño candado negro** en la foto de perfil de su compañero de chat.

4. Aplica conocimiento

Ejercicio ELECCIÓN MÚLTIPLE

Objetivo específico asociado: OE_04_01

Situación: ¿Qué se debe considerar al usar aplicaciones en teléfonos inteligentes para protegerse y proteger tu privacidad?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Debes leer la política de privacidad y los términos y condiciones de cada aplicación de manera crítica antes de instalarla.
- No debes aceptar ninguna actualización de aplicaciones si es posible.
- No es seguro usar imágenes de perfil de ti mismo. Es mejor usar imágenes que no tomaste, pero que encuentres en algún lugar de Internet.
- Debes controlar los derechos de acceso de las aplicaciones y ajustarlos adecuadamente.
- Debes usar una dirección de correo electrónico seria para registrarte (por ejemplo, que consista en tu nombre y apellido reales).
- Solo debes proporcionar tanta información sobre ti como sea absolutamente necesaria.

Ejercicio ELECCIÓN MÚLTIPLE

Objetivo específico asociado: OE_04_02

Situación: ¿Qué puedes hacer con respecto a la configuración de privacidad en aplicaciones populares como WhatsApp o Facebook Messenger para mejorar tu privacidad?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Por ejemplo, cuando uso WhatsApp, puedo deshabilitar en Configuración y Privacidad que otros usuarios pueden ver cuando estuve en línea por última vez.
 - Por ejemplo, puedo desactivar WhatsApp para acceder a mis contactos en Configuración y Privacidad.
 - Cuando uso WhatsApp, también puedo desactivar la confirmación de lectura o bloquear contactos no deseados haciendo clic en Configuración, Cuenta y Privacidad.
 - También puedo usar Facebook Messenger para comunicarme encriptado con mis amigos: para hacer esto, voy al respectivo chat, selecciono el nombre de la persona y simplemente comienzo una conversación secreta.
 - Para comunicarme con los contactos que están bloqueados en WhatsApp, selecciono el nombre de la persona y comienzo una "conversación secreta".
-

1. Afianza el conocimiento

Resumen

Para la mayoría de nosotros, nuestro **teléfono inteligente** es una parte integral de la vida cotidiana. Por lo tanto, no debemos olvidar proteger la información privada y los datos almacenados en consecuencia. Por ejemplo, en caso de pérdida o robo de tu teléfono inteligente, tiene sentido usar un **PIN seguro** (no una combinación de números como 1234) y un **bloqueo de pantalla**. También debes considerar instalar algún tipo de **aplicación antirrobo**.

Los proveedores de mensajería instantánea como **WhatsApp** se están volviendo cada vez más populares. Sin embargo, al usar estas u otras aplicaciones, siempre debe considerar **qué derechos de acceso le otorga a la aplicación** y mantenerlos al mínimo. ¿Alguna vez te has preguntado por qué usar WhatsApp es gratis? Al usar aplicaciones gratuitas, siempre debes tener en cuenta el hecho de que: si no tienes que pagar por el producto, **tú o tus datos generalmente sois el producto**. Además, existe el peligro de que varios **programas maliciosos** estén ocultos en las aplicaciones, especialmente si estas aplicaciones se distribuyen de forma gratuita en Internet y por proveedores de aplicaciones poco conocidos. Otro riesgo de seguridad es el hecho de que algunos proveedores de comunicación en línea **no cifran la comunicación** (por ejemplo, Facebook Messenger).

La adquisición de WhatsApp por Facebook ha hecho que muchos usuarios sean más críticos sobre las políticas de privacidad de estos servicios. Por lo tanto, las aplicaciones se optimizan constantemente con respecto a sus disposiciones de protección de datos. Por esta razón, por ejemplo, tiene sentido usar siempre la **última versión de WhatsApp Messenger**. Además, antes de usar aplicaciones, debes **leer la política de privacidad de la aplicación** que estás usando, verificar los derechos de acceso de la aplicación y ajustarlos si es necesario. También puedes **ajustar fácilmente la configuración de privacidad** de las aplicaciones, como la visibilidad de la imagen de perfil en WhatsApp o el bloqueo de contactos no deseados.

Las respuestas correctas aparecen marcadas en negrita

Situación: ¿Qué medidas puedes tomar para proteger tu teléfono inteligente del acceso no autorizado?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Puedo usar un PIN. Este PIN debe ser tan fácil de recordar como sea posible.
- **Debería bloquear mi teléfono inteligente con un PIN y asegurarme de que no sea una combinación de números como 1234 o 1111.**
- **Puedo configurar un bloqueo de pantalla.**
- Puedo instalar una aplicación de pago para configurar un número de identificación personal.

Situación: Después de una tarde de compras en la ciudad, de repente te das cuenta en casa de que has perdido tu teléfono inteligente. ¿Qué medidas pueden ser útiles en tal situación?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- **Puedo usar el Administrador de dispositivos Android o iCloud para localizar mi teléfono inteligente**
- **Puedo instalar algún tipo de aplicación antirrobo para tales casos. Esto me permite localizar mi teléfono, bloquearlo o eliminar datos almacenados en el teléfono.**
- Puedo bloquear mi tarjeta SIM para poder localizar mi teléfono.
- **Puedo bloquear mi tarjeta SIM para evitar que alguien incurra en altos costes usando mi teléfono.**

Situación: ¿Cuál de las siguientes afirmaciones sobre los servicios de mensajería instantánea (MI) son correctas?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- **Cada vez más personas utilizan los servicios de mensajería instantánea para intercambiar mensajes de texto, mientras que la comunicación por SMS ha perdido popularidad.**

- **La MI es comunicación basada en Internet.**
- **IM permite no solo el intercambio de mensajes de texto, sino también el intercambio de archivos, audios o comunicaciones a través de video chat.**
- Si muchas personas usan servicios de mensajería instantánea populares al mismo tiempo, el destinatario suele tardar unos minutos en recibir los mensajes.
- **Los servicios populares de mensajería instantánea son Facebook Messenger, WhatsApp o Windows life messenger.**
- Los servicios populares de mensajería instantánea son Youtube, Twitter, WhatsApp y Google.

Situación: Te gustaría usar WhatsApp para comunicarse con sus amigos. ¿Qué debes tener en cuenta al instalar la aplicación?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Las aplicaciones de Messenger como WhatsApp generalmente requieren un pago único de una tarifa de uso por adelantado.
- Para usar WhatsApp, debes descargar la aplicación y registrarte con su nombre real.
- **WhatsApp accede a todos los contactos almacenados en tu teléfono inteligente.**
- **Para usar ciertos servicios de WhatsApp, puede ser necesario permitir que la aplicación acceda a tus imágenes, cámara, micrófono o datos de ubicación.**
- WhatsApp accede automáticamente a todos los contactos almacenados en tu teléfono inteligente, sus imágenes y sus datos de ubicación. Esta es la única forma en que la aplicación puede funcionar.

Situación: ¿Cuándo tiene sentido ajustar las autorizaciones de aplicaciones y cómo es esto básicamente posible?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- **Básicamente, puedes verificar fácilmente en "Configuración" cuáles de las aplicaciones instaladas poseen qué derechos de acceso y, si es necesario, reducirlos en la medida realmente necesaria.**
- Para saber qué derechos de acceso tiene una aplicación, es una buena idea llamar a su proveedor de telefonía móvil.
- **Si deseas utilizar Google Maps, por ejemplo, es una buena idea permitir que la aplicación acceda a sus datos de ubicación mientras la utiliza.**
- También es una buena idea permitir que WhatsApp acceda a los datos de tu ubicación, ya que esto ayudará a que tus mensajes se transfieran más rápido.
- Dado que la mayoría de las aplicaciones son gratuitas, generalmente no es posible restringir los derechos de acceso de las aplicaciones individualmente.

Situación: ¿Por qué los usuarios de aplicaciones están cada vez más preocupados por la privacidad de los datos?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- Porque las aplicaciones son utilizadas por más y más personas.
- Debido a que las aplicaciones están desarrolladas principalmente por empresas ubicadas en países que no se preocupan por la protección de datos y, por lo tanto, no existen reglas de protección de datos vinculantes para el manejo de datos de usuarios. Un ejemplo bien conocido es Facebook o WhatsApp.
- Porque las aplicaciones son cada vez más caras.
- **Porque algunas violaciones de protección de datos se han conocido en los últimos años.**

- Porque es imposible que los usuarios entiendan qué derechos de acceso se les otorgan a los distintos proveedores de aplicaciones.
- Debido a que los usuarios almacenan más y más fotos y otros archivos en sus teléfonos inteligentes y, por lo tanto, las capacidades de almacenamiento pronto se agotarán.

Situación: ¿Qué riesgos de seguridad y consecuencias no deseadas pueden causar los servicios de mensajería instantánea y otras aplicaciones?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- **Los mensajeros corren el riesgo de enviar enlaces de phishing o transmitir malware a través de hipervínculos clicables o archivos transferidos.**
- **El malware puede estar presente especialmente en aplicaciones gratuitas de proveedores de aplicaciones menos conocidos.**
- Un problema importante son los costes ocultos más que el acceso secreto a los datos personales.
- La comunicación no cifrada, como suele ser el caso a través de WhatsApp, por ejemplo, es un problema de seguridad importante.
- Los datos personales pueden perderse a través de la comunicación encriptada.

Situación: ¿Qué se debe considerar al usar aplicaciones en teléfonos inteligentes para protegerse y proteger tu privacidad?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- **Debes leer la política de privacidad y los términos y condiciones de cada aplicación de manera crítica antes de instalarla.**
- No debes aceptar ninguna actualización de aplicaciones si es posible.
- No es seguro usar imágenes de perfil de ti mismo. Es mejor usar imágenes que no tomaste, pero que encuentres en algún lugar de Internet.
- **Debes controlar los derechos de acceso de las aplicaciones y ajustarlos adecuadamente.**
- Debes usar una dirección de correo electrónico seria para registrarte (por ejemplo, que consista en tu nombre y apellido reales).
- **Solo debes proporcionar tanta información sobre ti como sea absolutamente necesaria.**

Situación: ¿Qué puedes hacer con respecto a la configuración de privacidad en aplicaciones populares como WhatsApp o Facebook Messenger para mejorar tu privacidad?

Tarea: Elige las opciones correctas siguiendo el principio de opción múltiple: Ninguna, una, más de una o todas las opciones pueden ser verdaderas.

- **Por ejemplo, cuando uso WhatsApp, puedo deshabilitar en Configuración y Privacidad que otros usuarios pueden ver cuando estuve en línea por última vez.**
- Por ejemplo, puedo desactivar WhatsApp para acceder a mis contactos en Configuración y Privacidad.
- **Cuando uso WhatsApp, también puedo desactivar la confirmación de lectura o bloquear contactos no deseados haciendo clic en Configuración, Cuenta y Privacidad.**
- **También puedo usar Facebook Messenger para comunicarme encriptado con mis amigos: para hacer esto, voy al respectivo chat, selecciono el nombre de la persona y simplemente comienzo una conversación secreta.**
- Para comunicarme con los contactos que están bloqueados en WhatsApp, selecciono el nombre de la persona y comienzo una “conversación secreta”.