Content Unit

[Smartphone Protection]

Project: B-SAFE
Number: 2018-1CZ01-KA204-048148
Name of author: bit schulungscenter
Last processing date: 14.08.2020

Funded by the
Erasmus+ Programme
of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

Smartphone Protection

First Introduction

Social media, instant messenger, shopping, games, apps, taking a quick photo or do some googling - many people can hardly imagine everyday life without their smartphone. For making phone calls, however, it is used less and less. The clear trend is towards typing instead of making phone calls. This is also shown by a look at the number of users of instant messenger services: About 1.6 billion people worldwide are using WhatsApp, and around 1.3 billion communicate with their friends via Facebook Messenger. Using these services is child's play. But what dangers do lurk when using instant messenger services or other smartphone applications with regard to data privacy? It is not without reason that Facebook or other providers of free smartphone applications are repeatedly criticized by data protectionists. Find out how you can better protect your smartphone, your data and your privacy!

Practical relevance – This is what you will need the knowledge and skills for

After completing this content unit you will be able to better assess the risks associated with the use of instant messaging services or other smartphone apps, and you will get to know some useful steps to protect your phone and your privacy from unwanted risks.

Overview of learning objectives and competences

In LO_ Smartphone protection_01 you will receive information about some basic security measures in the event of loss or theft of your smartphone. In LO_ Smartphone protection _02 you will learn from the example of WhatsApp why apps require access rights and that you should keep them to a minimum. In LO_ Smartphone protection_03 you will learn about the weaknesses in the security of instant messaging and other apps. In LO_ Smartphone protection_04 you will learn about some measures and tips for secure use of smartphone applications and how to make privacy settings for frequently used apps.

Learning objectives	Fine objectives
LO_Smartphone protection_01: You know some basic protective measures for your smartphones.	FO_Smartphone protection_01_01: You can take measures to protect your smartphone from unauthorized access. FO_Smartphone protection_01_02: You can name some helpful measures in the event of loss or theft of your smartphone.
LO_Smartphone protection_02: You know that using apps like WhatsApp requires granting some access permissions to the app and you know that you should keep them to a minimum.	FO_Smartphone protection_02_01: You can explain what instant messaging means and give examples of popular instant messaging services. FO_Smartphone protection_02_02: You can explain using WhatsApp as an example which prerequisites must usually be fulfilled for using an app. FO_Smartphone protection_02_03: You can give examples when it makes sense to adjust App authorizations and understand how this is basically possible.
LO_Smartphone protection_03: You know the security problems and unwanted consequences of using instant messaging services or other smartphone applications.	FO_Smartphone protection_03_01: You can give reasons why app users are becoming increasingly concerned about data protection. FO_Smartphone protection_03_02: You can give examples of what security risks and unwanted consequences instant messaging services and other apps can cause.
LO_Smartphone protection_04: You know measures and tips for the safe use of smartphone applications.	FO_Smartphone protection_04_01: You can explain what should be considered when using apps on smartphones in order to protect yourself and your privacy. FO_Smartphone protection_04_02: You can adjust privacy settings for popular applications such as WhatsApp or Facebook Messenger.

1.Build knowledge - Basic protective measures for smartphones

For many people, their smartphone is their constant companion in everyday life. Do you also belong to those who take their smartphone everywhere and can't do without it for a day? If so, you probably also have **very private or sensitive data on your smartphone**, such as photos, confidential text messages or business information. In order to protect your smartphone and the potentially very private data it stores, you should take appropriate measures in the event of loss or theft.

Co-funded by the
Erasmus+ Programme
of the European Union

This includes, for example, protecting the smartphone against unauthorized access via **PIN** (Personal Identification Number) and **screen lock.**

Important
Make sure that you **do not use common number combinations** such as "1234", "1111" or similar. These are very easy to hack by unauthorized persons**.**

If your smartphone is stolen or lost, you should have **the SIM card** (subscriber identity module) of the device **blocked** by your network provider so that no one can use it to make phone calls or incur high costs.

Do you know the **serial number of your smartphone?** This is located under the battery, on the original packaging, or on the mobile phone purchase invoice. You should make **a note of this number** so that you can report it to the police in the event of theft.

All common operating systems also offer **various services** that can be very helpful in the event of theft or loss.

Examples
Can't you find your cell phone? With the **Android Device Manager** you can let your smartphone ring at maximum volume, even if it was muted. This way you can quickly locate a lost phone at home. If it's somewhere else, you can locate it in real time and leave a message for the finder. If your iPhone has been lost or stolen, you can usually search for it via **iCloud**, on condition that the device is switched on and has data reception.

You probably already heard about the possibility of installing a kind of **anti-theft application** on your smartphone. For example, it allows you to locate and lock the lost or stolen smartphone and delete the data stored on it. The commands required for this can be issued by another smartphone whose number has been stored or sent to the device via an online portal.

Tip
In the event of theft or loss, you should block the SIM card immediately if you do not have **an anti-theft app installed on your phone**. However, if an app is installed, the SIM card should not be blocked until the data has been located and remotely deleted. Otherwise this is no longer possible.

Co-funded by the
Erasmus+ Programme
of the European Union

1.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_01_01

Situation: What measures can you take to protect your smartphone from unauthorized access?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- I can use a PIN. This PIN should be as easy to remember as possible.
- **I should lock my smartphone with a PIN and make sure that it is not a combination of numbers like 1234 or 1111.**
- **I can set up a screen lock.**
- I can install a paid application to set up a personal identification number.

Exercise MULTIPLE CHOICE

Associated fine objective: FO_01_02

Situation: After an afternoon of shopping in the city, you suddenly realize at home that you have lost your smartphone. What measures can be useful in such a situation?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **I can use the Android Device Manager or iCloud to locate my smartphone**
- **I can install some kind of anti-theft app for such cases. This allows me to locate my phone, lock it or delete stored data on the phone.**
- I can have my SIM card blocked so that I can locate my phone.
- **I can block my SIM card to prevent someone from incurring high costs by using my phone.**

2.Build knowledge - Instant Messaging (IM) and Applications

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.

Definition
In contrast to SMS services, **IM** is an **internet-based communication** via **mobile apps.** It is a type of online chat that allows you to exchange messages with other users in near real time. To do this, instant messaging applications must be downloaded and installed.

In addition to the transmission of texts, the transmission of files, audio and video sequences (and thus also video chat) is usually also possible. The message transmission takes place in the so-called **push procedure**, which allows the texts to arrive at the recipient immediately after they have been sent. Unlike e-mails, for example, the messages do not have to be retrieved first, but appear immediately on the screen of the communication partner.

Example:
Examples of popular instant messaging services:

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

For example, around 1.3 billion users worldwide already use Facebook Messenger to communicate.

The most common use of instant messaging programs is on mobile devices such as **smartphones** via **messenger apps**. Messenger apps are usually for free, practical, easy to use and hence enjoy increasing popularity. To use WhatsApp, for example, all you need to do is download the free app and register via your own mobile phone number.

However, to fulfil the desired purpose, an app usually requires a variety of **authorizations**. Therefore, the app wants to access certain device functions of your smartphone, such as calendar, camera, contacts, microphone, SMS, memory, location or phone function.

Important
Are you one of the 1.6 billion WhatsApp users worldwide? Then you should be aware that WhatsApp accesses at least **all contact addresses stored on your mobile phone**.

This is the only way for the app to determine which of your contacts is also using WhatsApp and automatically display them in the app. Would you like to send pictures or your own location via WhatsApp or use it for video telephony? If so, you should be aware that WhatsApp also needs to access your pictures, camera, microphone and location data!

Tip
Due to data protection reasons it is worthwhile to be careful when assigning **authorizations to apps** and to reduce the authorizations to the most necessary level.

If you are not sure about what permission each app has on your smartphone, you should check this for security reasons. Are you wondering how to do that? Simply select the appropriate app in "settings", see which accesses you allow the app and adjust them if necessary.

Example

Suppose you would like to use Google Maps to find a specific address. In this case, it makes sense to allow the app to **access your location while using the app**. However, if you don't want to share your location with your contacts via WhatsApp, the app doesn't necessarily need to know where you are.

2.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_02_01

Situation: Which of the following statements about instant messaging (IM) services are correct?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- More and more people use IM services to exchange text messages, whereas communication via SMS has lost popularity.
- IM is Internet-based communication.
- IM allows not only the exchange of text messages, but also the exchange of files, audios or communication via video chat.
- If many people use popular IM services at the same time, it usually takes a few minutes for the recipient to receive the messages.
- Popular IM services are Facebook Messenger, WhatsApp or Windows life messenger.
- Popular IM services are Youtube, Twitter, WhatsApp and Google.

Exercise MULTIPLE CHOICE

Associated fine objective: FO_02_02

Situation: You would like to use WhatsApp to communicate with your friends. What should you be aware of when you install the app?

Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- Messenger apps like WhatsApp usually require a one-time payment of a usage fee in advance.
- To use WhatsApp, you need to download the app and register with your real name.
- **WhatsApp accesses all contacts stored in your smartphone.**
- **To use certain services of WhatsApp, it may be necessary to allow the app to access your pictures, camera, microphone or location data.**
- WhatsApp automatically accesses all contacts stored in your smartphone, your pictures and your location data. This is the only way the app can work.

Exercise MULTIPLE CHOICE

Associated fine objective: FO_02_03

Situation: When does it make sense to adjust app authorizations and how is this basically possible?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **Basically you can easily check under "Settings" which of the installed apps possess which access rights and if necessary reduce them to the really necessary extent.**
- To find out which access rights an app has, it' s a good idea to call your mobile phone provider.
- **If you want to use Google Maps, for example, it is a good idea to allow the app access to your location data while you are using the app.**
- It is also a good idea to allow WhatsApp to access your location data, as this will help your messages get transferred faster.
- Since most apps are free of charge, it is usually not possible to restrict the access rights of the apps individually.

3.Build knowledge - Security risks using smartphone application

If you also store and process a lot of data on your smartphone, partly of a very private nature and from third parties (e.g. photos), you should consider to what extent **unrestricted app permissions** could be problematic.

It is no secret that many app producers are interested in your personal data. After all, they need to generate some form of revenue with the apps that are often provided free of charge to users. **If you don't pay for a product, then you are usually the product,** it is said. But that is not yet a cause for concern. In most cases, the use of our personal data is made anonymous within the framework of the legal data protection regulations.

However, the **takeover of WhatsApp by Facebook**, for example, has meant that the telephone numbers from the contact directory are also passed on to Facebook. In addition, the discovery of various privacy incidents in the past has also led to awareness of the dangers of unauthorized monitoring. Users are increasingly concerned about data protection.

Are you now wondering what security issues and unwanted consequences the use of instant messaging services and other apps can have for you? Here are a few examples:

- As with other online communication media, messengers also run the risk of sending **phishing links or transmitting malware** via clickable hyperlinks or transferred files.
- There is a danger **that malware of all kinds will be hidden in the apps**, especially if apps have been purchased for free on the Internet from less reputable app providers.
- As you already are aware, apps get permissions to perform functions. The permissions allow apps to read data. Thus, there is a **risk of hidden access to personal data** such as location data, mobile surfing habits, stored contact data or passwords. In addition to the loss of privacy, the **misuse of your contact data** can also be an unpleasant consequence.
- **Problems with copyright** can arise, for example, if images that you have not created yourself and for which you do not own the copyright are used as profile photos.
- **Unencrypted communication** represents a high security risk. Therefore, since April 2016, content sent via WhatsApp, for example, has been transmitted with secure end-to-end encryption. This applies to text, images, video and other files. End-to-end encryption means that only the respective communication partners can receive and read the content.

Important
If you use the **Facebook Message app,** you should be aware that your communication (unlike WhatsApp) is principally not encrypted! If you want to chat end-to-end encrypted, you need to start a "secret conversation". How this works will be explained in the next session.

3.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_03_01

Situation: Why are app users increasingly concerned about data privacy?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- Because apps are used by more and more people.
- Because the apps are primarily developed by companies based in countries that do not care about data protection and therefore there are no binding data protection rules for handling user data. A well-known example is Facebook or WhatsApp.
- Because apps are becoming more and more expensive.
- **Because some data protection violations have become known in recent years.**
- Because it is impossible for users to understand what access rights they are granted to the various app providers.

- Because users are storing more and more photos and other files on their smartphones and therefore the storage capacities will soon be exhausted.

Exercise MULTIPLE CHOICE

Associated fine objective: FO_03_02

Situation: What security risks and unwanted consequences can instant messaging services and other applications cause?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **Messengers run the risk of sending phishing links or transmitting malware via clickable hyperlinks or transferred files.**
- **Malware can be present especially in free apps from less known app providers.**
- A major problem is rather high hidden costs than secret access to personal data.
- Unencrypted communication, as is usually the case via WhatsApp, for example, is a major security problem.
- Personal data can be lost through encrypted communication.

4. Build knowledge - Measures and tips for the safe use of smartphone applications

Given the potential security risks of using apps on your smartphone, you're probably wondering how you can better protect yourself and your privacy. The following are some tips on **what to consider when using apps on your smartphone**:

In the past, serious safety deficiencies have been identified in various apps. Subsequently, an attempt was made to remedy these deficiencies by making appropriate adjustments. For this reason, for example, it is advisable to always use the **latest version of WhatsApp Messenger.**

To prevent copyright problems, you should **refrain from using images that you do not own as profile images.**

Tip
You can also use WhatsApp's privacy settings to **limit the visibility of your profile picture:** Just open WhatsApp and tap “Settings”. Then tap “Account”, select “Privacy “and change the "Everyone" setting to "My Contacts" or "Nobody" for Profile Photo.

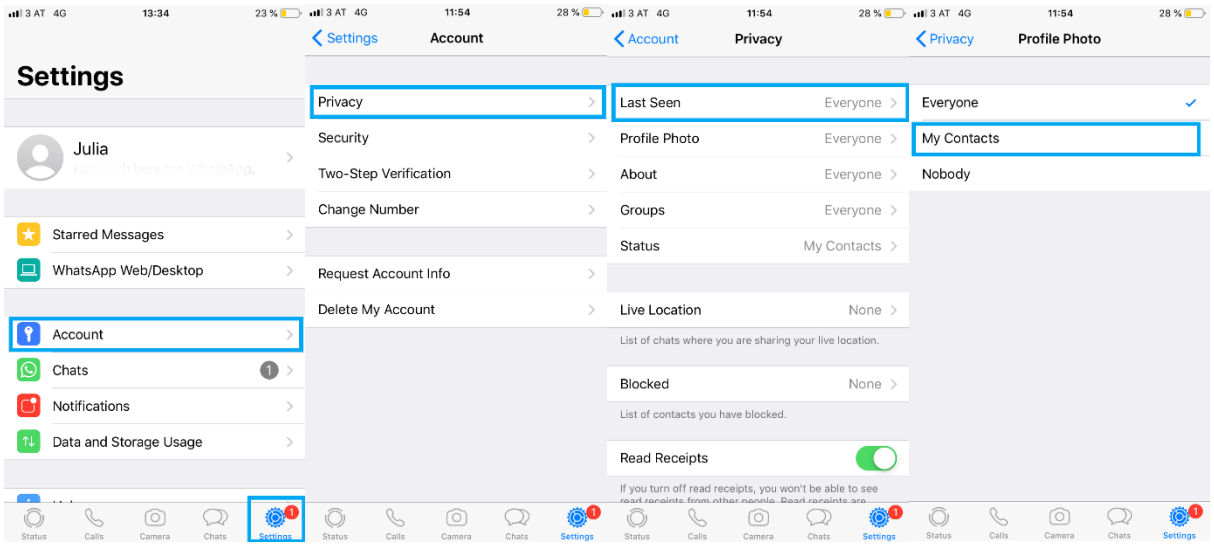
App providers are obliged to provide the user with a **data protection declaration** which contains information about the permissions requested by the app. In addition, most apps today require you to **agree to these permissions** when they are installed. You should **read the privacy policy** and the terms and conditions of each app critically before installing it. You should also **control the access rights of apps!** The granted permissions can be viewed and revoked at any time in the settings for each app.

Example
It's easy to understand that, for example, a weather app to display the weather forecast must be able to query your location to provide more accurate forecast information. Why this app might need access to your smartphone's camera, however, is no longer so obvious.

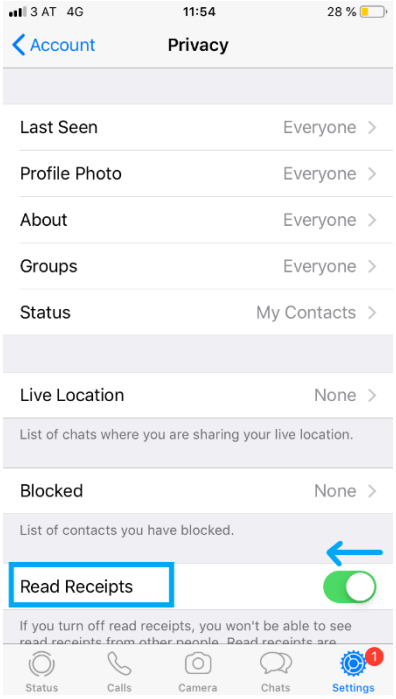
You should only enter the most necessary data. Use an **extra e-mail address** that doesn't reveal much about you and doesn't bother you when it comes to spam.

A supposedly big advantage of IM is that it is always immediately obvious when a contact is online or when it was last online. However, new privacy settings of some messengers offer you the opportunity **to keep others from knowing that you are online, when you were last online or to turn off automatic read confirmations.** How this works is demonstrated in the following by the example of WhatsApp:

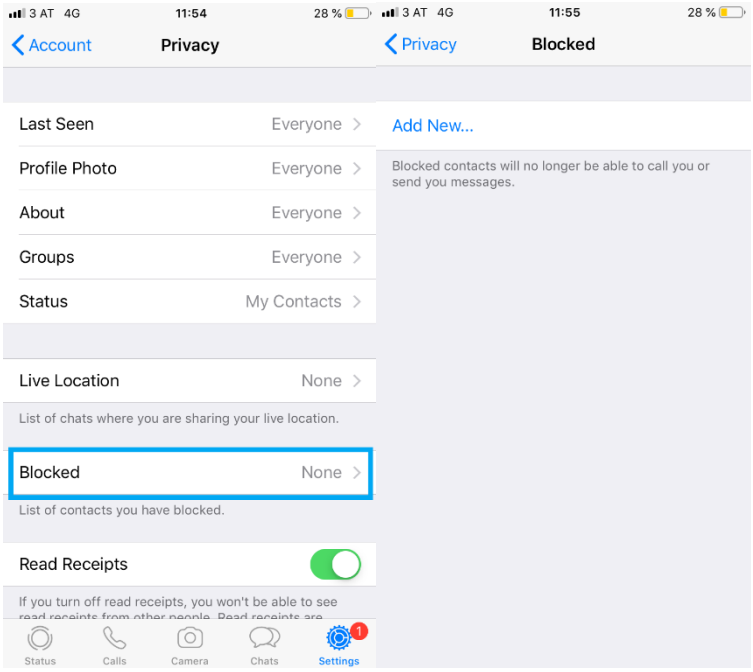
- **How to hide "Last Seen":** Open WhatsApp and tap on “Account”. Then tap on “Privacy”, select “Last Seen” and choose who or if someone can see when you were last online.



- **How to turn off read receipts**: Tap again on “Settings”, “Account” and ”Privacy”. Then simply deactivate the read confirmation.



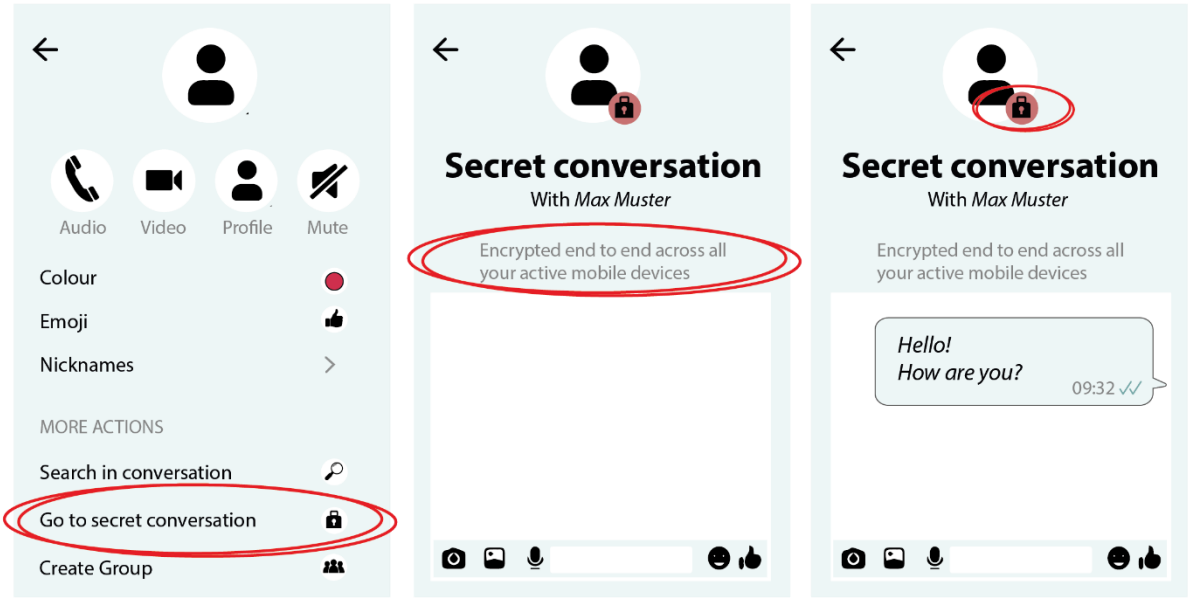
In order to avoid contact by strangers, one should always **consider carefully in the first place in which cases the mobile phone number should be given** and, above all, to whom it should be communicated! If unwanted persons try to contact you via WhatsApp, you can simply block them. To do this, scroll down in "Privacy" and tap on blocked contacts.



Important
Block contacts if you're unsure who they are or if someone is harassing you. Report insults, sexual harassment, blackmail or threats to the police.

Some messenger apps, such as Facebook Messenger, **do not automatically encrypt your messages.** You should change the settings manually if possible.

How to communicate encrypted with Facebook Messenger: Go to the chat, tap the person's name and select "Secret conversation". Now the message exchange with this person is end-to-end encrypted. Nobody but you and your chat partner will see your messages, not even Facebook.



Tip
You can recognize an encrypted chat by the fact that the user interface is **gray-black**. You will also see a **small black lock** on your chat partner's profile picture.

4.Apply knowledge

Exercise MULTIPLE CHOICE

Associated fine objective: FO_04_01

Situation: What should be considered when using apps on smartphones in order to protect yourself and your privacy?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- **You should read the privacy policy and the terms and conditions of each app critically before installing it**
- You should not agree to any updates of apps if possible.
- It is not safe to use profile pictures of yourself. It's better to use pictures that you didn't take yourself, but found somewhere on the internet
- **You should control the access rights of the apps and adjust them appropriately.**
- You should use a serious e-mail address to register (e.g. consisting of your real first and last name).
- **You should only provide as much information about yourself as absolutely necessary.**

Exercise MULTIPLE CHOICE

Associated fine objective: FO_04_02

Co-funded by the
Erasmus+ Programme
of the European Union

Situation: What can you do about privacy settings on popular apps like WhatsApp or Facebook Messenger to improve your privacy?
Task: Pick the right options following the multiple-choice principle: None, one, more than one or all options can be true.

- For example, when using WhatsApp, I can disable under Settings and Privacy that other users can see when I was last online.
- For example, I can disable WhatsApp from accessing my contacts under Settings and Privacy.
- When using WhatsApp, I can also deactivate reading confirmation or block unwanted contacts by clicking on Settings, Account and Privacy.
- I can also use Facebook Messenger to communicate encrypted with my friends: To do this, I go to the respective chat, select the person's name and simply start a secret conversation.
- To communicate with contacts that are blocked on WhatsApp, I select the person's name and start a "secret conversation".

Sources

klicksafe.de: https://www.klicksafe.de/smartphones/sicherheit-wie-schuetze-ich-das-smartphone/

klicksafe.de: https://www.klicksafe.de/themen/kommunizieren/whatsapp/was-ist-der-whatsapp-messenger/

klicksafe.de: https://www.klicksafe.de/themen/kommunizieren/whatsapp/probleme-mit-dem-whatsapp-messenger/

saferinternet.at: https://www.saferinternet.at/privatsphaere-leitfaeden/whatsapp/schritt-fuer-schritt/kontakte-blockieren/

saferinternet.at: https://www.saferinternet.at/privatsphaere-leitfaeden/facebook-messenger/faq/was-ist-eine-geheime-unterhaltung-im-messenger/

saferinternet.at:https://www.saferinternet.at/privatsphaere-leitfaeden/facebook-messenger/schritt-fuer-schritt/verschluesselt-chatten/

digitaltrends.com: https://www.digitaltrends.com/mobile/how-to-protect-your-smartphone-from-hackers-and-intruders/

techsafe.org: https://www.techsafety.org/12tipscellphones

avast.com: https://blog.avast.com/9-smartphone-tips-privacy-security

fraud-magazine.com: https://www.fraud-magazine.com/article.aspx?id=4294992799

Save Knowledge

Summary

For most of us, their **smartphone** is an integral part of everyday life. Therefore, we should not forget to protect the private information and data stored on it accordingly. For example, in case your smartphone is lost or stolen, it makes sense **to use a secure PIN** (not a combination of numbers like 1234) and **a screen lock**. You should also consider installing some kind of **anti-theft app.**

Instant messaging providers like **WhatsApp** are becoming more and more popular. However, when using these or other apps, you should always consider **what access rights you grant the app** and keep them to a minimum.
Have you ever been wondering why using WhatsApp is for free? When using gratis apps, you should always be aware of the fact that: If you don't have to pay for the product, **you or your data is usually the product**. Furthermore, there is the danger that **various malware** is hidden in applications, especially if these apps are distributed for free on the Internet and by little known application providers. Another security risk is the fact that some online communication providers **do not encrypt communication** (e.g. Facebook Messenger).

The takeover of WhatsApp by Facebook has made many users more critical about the privacy policies of these services. Applications are therefore constantly being optimized with regard to their data protection provisions. For this reason, for example, it makes sense to always use the **latest version of**

WhatsApp Messenger. In addition, before using apps, you should read the privacy policy of the app you are using, check the access rights of the app and adjust them if necessary. You can also easily adjust the privacy settings of apps, such as the visibility of the profile picture on WhatsApp or blocking unwanted contacts.