how safe is yours

smart phone?

Advice on data protection

How secure is your smartphone?

Advice on data protection

Editor:

Berlin representative for

Privacy and Freedom of Information

Friedrichstr. 219

Visitor entrance: Puttkamerstr. 16-18

10969 Berlin

Telephone: 030 13889-0

Fax: 030 2155050

Email: mailbox@datenschutz-berlin.de

Design: april agency GbR

Printing: ARNOLD group.

Status: March 2020

Contents

7. Localization (movement profiles)

8. Eavesdropping

9. Unencrypted Wi-Fi hotspots

10. Photos on social networks

11. Mobile Apps and Fake Apps

12. App Access Rights

13. Platform Provider AppStore

14. Unlock Code/PIN

15. Updates

3

4

5

7

8th

9

10

11

12

13

14

15

16

17

18

19

Introduction

your conversation!

Your messages!

your address book!

Your photos! Your music!

Your data!

Of course, you always have your smartphone with you. Are you doing

photos, play your favorite songs, stream mu-

sik, share your experiences, use them to manage your appointments

and contacts, surf the internet and use apps.

But this also applies: the more functions your smartphone has

has, the more vulnerable it is to various dangers. And

Of course, in the event of damage ultimately not

to regret your smartphone.

On the contrary: it is you who, through an exploited security

vulnerability may result in serious disadvantages

the has.

The German Basic Law grants you the right to “inform-

mental self-determination". After that you basically

lich the right itself over the disclosure and use

determine your personal data. You need to

but also pay attention to the protection of your data. In the

Dealing with smartphones e.g. B. There are a number of useful ones

Tips to keep in mind if you want to prevent

that the wrong people are looking at your call logs, your music,

your messages, your photos, just your personal ones

Smartphone data can come.

PERSONAL DATA: This is

to all possible identifiable details of a

concrete person. So in addition to obviously personal

related data such as your name, your birth

tag or your residential address etc. are e.g. B. also yours

Eating habits, your taste in music or the content

meant by phone calls. As sensitive (especially

sensitive) personal data apply

about your health, your ethnic origins and

such as your religious, political or sexual orientation.

This brochure will give you these tips: First,

do you drive where possible dangers to your personal

data in dealing with smartphones. Afterward

we will show you how best to counteract these dangers.

1. Viruses and Other Malicious Software

What has been well known from the PC for a long time does

has also been increasing in smartphones for some time.

VIRUSES, WORMS AND TROJANS: These are small ones

malicious programs that spread through different ways

spread independently from smartphone to smartphone

can. If such a program reaches your smart

phone, it can significantly impair its function

gen, spy on or delete your data and even

high costs (e.g. by sending so-called

premium SMS).

With the increasing range of functions of the devices, the

Danger of infection by smartphone viruses increased

men. It is therefore important that you take certain precautions

gen meet to protect your smartphone against the new dangers

to make immune. Possible gateways for viruses into your

smartphone are the download of ring tones, logos,

Games, apps and unprotected radio interfaces such as

Bluetooth and open WLAN connections (unencrypted

te, wireless internet connections).

4

So make sure that you have sent pictures, songs or

only accept files if you actually accept them

requested or the sender and his/her

really know. The receipt of unsolicited data

You can prevent this by using the Bluetooth function

of your smartphone to "invisible". Do you use

the radio interfaces of your smartphone only occasionally

then it is best to turn this off completely in the menu

switched on and only to be activated again when required. That's how you keep

you are always in control and dangerous programs

no access. There are now antivirus programs

for smartphones with Android operating systems.

Tip: Never use executable files

which are unsolicited in your smart

want to sneak in phone.

2. Mobile data storage

Many mobile phones and smartphones have a relative

big memory. They replace u. a. the conventional ones

USB sticks as mobile data storage. So of course apply

all safety instructions for USB sticks in connection with

computers equally for your smartphone.

The transmission of com-

computer viruses from one pc to another via an infected one

smart phone. Unfortunately, it also happens again and again that

mobile data storage devices are lost or stolen.

This means that your personal data can easily fall into the wrong hands

reach. It is therefore important that you take your smartphone with you

password that is as secure as possible or at least six

digit PIN entered when activating the device

must be practiced so that you can use your smartphone.

5

Be prepared for virus risks even when working on the PC.

not. Eighth e.g. B. always make sure that the computer to which

you connect your smartphone, have an up-to-date anti-virus

ren software features. Should there ever be a PC virus

have wormed their way into your smartphone, so make sure

that this is removed first before you connect the device to the

"healthy" computer at home or with your friends

and join friends.

SIM LOCK: In case you lose your smartphone

lost it or it was stolen from you, you should immediately

block the SIM card in your smartphone. There-

with is prevented that the thief (or finder)

can continue calling at your expense. To the lockdown

your smartphone dial the central blocking emergency call

116 116 and keep the phone number and customer number

mer of your mobile phone contract ready.

It is clear that you always protect your smartphone from loss

or protect against theft. However, since one can never

You should be careful not to send any sensitive data

stored unencrypted on your mobile memory.

Sensitive data is data with an increased need for protection,

such as B. your grades, your bank balance, your photos.

Tip: Always make sure you have an up-to-date anti-virus

Protect and store as little sensitive as possible

Data unprotected on the smartphone.

3. Espionage & data theft

Even without someone holding your smartphone

occurs, non-observance of certain safety

possible to access the data stored on it

long. Not only can you use the Bluetooth function

unsolicited files are sent to your smartphone

the. It can also be used on smartphones with security gaps

be possible for outsiders who are on it

Read out data and in extreme cases even every conceivable one

type of commands to execute.

To protect you from such Bluetooth attacks,

always test the latest version of the operating system

installed on your smartphone. Furthermore,

what has already been said about protection against smartphone viruses

was: Turn off Bluetooth function permanently and only

reactivate if necessary.

BLUETOOTH: Bluetooth is a radio transmission

technology for digital data. In smartphones it is used e.g.

B. to stream music to your headset or photos to an

to send their smartphone. The range of Blue

tooth connections is between 10 and 100 meters.

Because of the wireless connection, this technique

particularly vulnerable to attacks, e.g. B. of viruses. But also

the advertising industry is increasingly using Bluetooth.

There are Bluetooth-enabled billboards that you

demanded product information on your in passing

want to send smartphone. To use the Bluetooth interface

make your smartphone secure against attacks,

you should always set the function to “invisible” or

switched".

A particularly secure variant of data exchange

via Bluetooth represents the so-called pairing procedure.

In this case, communication is carried out on the two

the entry of the same password.

enough. Only if they match are the desired ones

Transfer data encrypted.

And one more thing: Your smartphone has a name! The-

You can find this in the "Settings" of your smartphone.

Other Bluetooth-enabled devices are given this name

displayed in the transmission area of your smartphone. To poten-

not presenting an overly obvious target to attackers,

think of a fantasy name for your smartphone,

which as far as possible does not suggest that the telephone

belongs to you

Tip: To prevent data theft attacks, de-

activate the bluetooth function of your smart

phones and stop the operating system software

up to date.

4. Backup

You have to decide for yourself how important regular

backing up the data on your smartphone. If you

actually only the phone numbers of your friends and

saved friends, then it is certainly enough to

to update the address book at home.

But there are also programs that save the data from your smart

phones with the appointment calendar and the address book

synchronize with the PC and update automatically. Look

Check the smartphone manufacturer's website.

There are also backup services for smart

phones. Note, however, that the Internet service all

gets your smartphone data.

Tip: Only use online backup services if they

are trustworthy.

8th

5. Deletion of Data upon Disclosure

& Disposal

If you want to sell your old smartphone, give it away

or just throw away? Then you should

always make sure that your saved personal

data does not fall into the hands of anyone else.

To protect your smartphone from all personal data

must clean the SIM card and any existing ones

memory cards are removed. Also, you should about

the menu (if available) delete the following private data:

• Phone Book, Address Book or Contacts

• Calendar data, notes, to-do lists

• Video and sound files

• Connection data such as dialed or

answered calls

• Messages (SMS, MMS, emails)

• Internet data (cache memory, cookies,

Bookmark)

• Communication data (such as e-mail provider,

Bluetooth connection settings)

• Apps and their data

To do this, use the “Reset to factory settings” option

set". The function performs a "hard reset" at

the entire memory to the delivery state

is reset. Contains particularly sensitive data

on your smartphone, you should use a special delete

deploy software.

ATTENTION ENVIRONMENTAL PROTECTION: Old smartphones are allowed

not just be thrown in the dustbin, but

must be disposed of properly. bring your smart

phone to one of the designated ones for this purpose

public collection points or ask in your mobile

telephone shop or an electronics store, whether this

to take care of you.

Tip: Make sure that when passing on or disposing of

no personal data on your old smartphone

more on it.

6. Lure calls

Again and again it happens that fraudsters with

called "lure calls" by mobile phone owners

want to pull the money out of their pockets. There will be one

SMS sent to your smartphone (usually with a

contained question) or briefly on your smartphone

rang so that you could not manage to time the call

to accept. The scammer is now hoping that you have a

text back or the unknown caller

call back Is it then the recalled one?

You are the number one for a so-called “value-added service”.

a lot poorer and the scammer makes a living

the large number of callbacks a golden nose.

If the sender number begins with the digits "0137" or

"0900", or "+49137" or "+49900" or has the number

only 5-6 digits, there is definitely a value-added service

behind that can cost you dearly. So not

call back! Be careful with foreign phone numbers

me. They also start with a “+” or “00”, followed by

but a different number than the 49 (the 49 is the international one

Telephone area code for Germany).

Tip: It is best to never reply to SMS or

calls from unknown numbers,

to avoid unwanted costs from the outset

avoid.

7. Localization (movement profiles)

In order for you to be able to make calls at all on the go, you have to

your smartphone at the nearest mo-

Register a bilfunk transmission antenna. So your network knows

provider basically always where you are located.

If you summarize this information over a certain period of

together, it is also possible to use so-called "movements"

to create "supply profiles" of you, e.g. B. to learn where

you've been banging around all day long.

Creating such profiles of strangers is indeed

legally forbidden. However, there are providers who allow parents

their child's (or their child's phone) location

locate. Parents who resort to such measures do so in all

usually only out of concern for their children. Still belong

in a free society also the preparation for

a self-determined life and trust in maturity

and responsibility for educating adolescents to do so.

Also, an abuse of such location applications

cannot be ruled out outside of parent-child controls.

Your parents should consider this type of surveillance

pull or actually already do it, then talk to us

them about their reasons and your attitude towards this

take. The location of a switched-on smartphone

can be reduced to less than 100 meters by the mobile network operator

be determined precisely. Permission to such

Localization is, however, severely restricted by law.

With smartphones, on the other hand, there is much more of a risk that

highly accurate positioning techniques available in the device, such as GPS

be abused by some apps. You should

of the app, whether this really has the location function

needed. With every smartphone you can use individual apps

prohibit using the location functions. consider

apps for social networks beforehand whether you want to use such location

functions you really want to use and who you tell

want where you are right now. Because even through such programs

me (e.g. Facebook Places, Foursquare or through the live

Location on WhatsApp) a movement profile is created, which may

from the provider of the network or from some "friends"

dinnen" and "friends" can be abused.

Tip: Turn off your smartphone when you

don't carry it with you, or use at least

least a PIN-protected locking function. May be

careful with strange text messages

with content that seems strange to you,

such as reports on localizations carried out,

Registration confirmations or activation codes.

Only allow apps to access the location

feature you trust and this off

understandable reasons.

8. Eavesdropping

Cell phone conversation tapping is just like that

In principle, wiretapping of landline calls is possible. One

such a measure violates your fundamental rights.

About phone tapping by the mobile operator

it usually only comes up in the context of investigations

the police or other state security agencies

Suspicion of a particularly serious crime.

Smartphones can also be manipulated in such a way that

they can be bugged in rooms in which they are

condition. However, something like this requires complex changes

changes on the phone or installing a "sniffing

software". With such software, yours could too

Tapped into smartphone conversations and your messages

be read along. So pay attention to the instructions here as well

to protect against viruses and other malware.

12

You are also not allowed to make any secret sound or image recordings yourself.

take, e.g. B. from classmates and

teachers in class or during breaks. She

are not allowed because they violate the fundamental rights of those affected

affect.

PRIVACY: Of course you have to be careful that

your data stay with you as much as possible - pay attention e.g. B.

on who's listening when you're on the phone. Vice versa follows

but also that you yourself are your fellow human beings

not allowed to spy without permission. Also secret

sound recordings, e.g. B. in the classroom, are prohibited.

9. Unencrypted WiFi hotspots

Anyone can record and read your data traffic

sen, unless it is separately encrypted. a

encryption is e.g. B. recognizable by "https://".

However, even then, curious third parties can at least

read along to which servers (wikipedia.org., face-

book.com etc.) you connect (metadata).

Here are a few more tips that will help you deal with WLAN

Facilitate Hotspots:

• The operating system usually indicates which

WLANs are encrypted and which are unencrypted.

• Many chat apps, such as B. Threema and Signal,

encrypt all messages themselves.

• If you can connect to the WiFi and

then be redirected to a website where you

Accept the terms of use and possibly user

Entering your name and/or password is that

WiFi usually not encrypted.

Tip: Set the e-mail app so that e-mails are only sent via

encrypted connections can be retrieved and sent.

10. Photos on social networks

Think carefully about whether your private photos are really for the

should be intended for the general public. Above all, you should never-

times publish photos of friends

or tag them on photos without asking first.

Especially not if the photos are publicly visible and not

are only accessible to a certain group of people.

Because it is not allowed to single with a smartphone

Photographing, filming or filming people without their consent

men or these photos without the consent of the photographed

to publish.

Before posting photos of friends on social

networks, you should talk to your parents

wonder if that is allowed. your friends

should talk to their parents first, if

before they give you permission.

Tip: If you don't get tagged in photos

want, you should go into the settings of the social

len network to see if you can set

can that one is not marked. given-

if you can also restrict by whom

can be marked.

14

11. Mobile Apps and Fake Apps

Mobile apps (usually called apps for short) are available for different

those areas. Most of it is free, a small-

The other part, for mostly small amounts, has to be paid in the respective app

Store or Play Store can be purchased.

Make sure you install the correct app. Some-

sometimes there are counterfeit apps that have unwanted functions

include. These are apps that have no functions,

but cost money or secretly spy on users

(fake apps).

In recent years, dangers are self-installed

Smartphone apps have become more relevant. Please consider before

the installation of a new app, that these are usually not dated

manufacturer of the smartphone, but from sometimes dubious

liable sources. There are now countless

games for apps that send personal data to the manufacturer of the

Share app. For example, very often the stay

stop location determined or the phone book entries

passed on (e.g. on the Facebook smartphone app).

Before installing an app, you should therefore find out

agree who the manufacturer is, whether the app is from the shop operator

or smartphone manufacturer has been checked or whether

the ratings by other users

find a dubious provider. At the installation

you should think carefully about whether an app is really all

Data required to be queried or referenced by the app

requests access.

Tip: Do not agree to the installation of apps whose origin

future and purpose you don't know for sure - even if they

sent or recommended by a friend.

Check beforehand how many downloads the app already has

and how it is evaluated.

12. App Access Rights

The permissions that an app claims are often

figure ignored. Many applications access data from

mobile device that they are not entitled to – especially

Sensitive data worth protecting. Before installing

Apps you should change the app permissions in the App Store/Play

control stores.

Does the new game actually need access to the address

a book? Does a fitness app really need access to the ca-

mera? Does the manufacturer explain somewhere (e.g. on their web

page), what access rights the app needs for what?

How encroaching an app can be, you as a smart

phone user think twice before installing. You

you can also take a look at the data protection

throw statement. It should be explained there which data

the provider of the app processes and what he does with it.

In most cases, you can also set individual access rights after the

withdraw installation.

Tip: If necessary, you should

settings” of your smartphone go and

disable unwanted features.

13. Platform Provider AppStore

The apps are usually activated via a central, dated

Platform operators controlled service, the so-called

App Store installed. The AppStore enables the platform

form operator has control over the data entered on the platform

set applications. This can be beneficial as the

Apps checked before publication and so at least in principle

potentially dangerous and particularly data-hungry applications

be kept away from the platform.

However, the platform operator also experiences this in a special way

much about the users.

A possibility to use the knowledge of the platform provider

limit, the registration would be under an imaginary

names. In the meantime, however, i. i.e. R. the indication of

Mobile phone number required for higher security

security against account theft.

Tip: For purchasing apps or music, you should

you do not use a credit card, but on the

Prepaid cards from the providers that

you can buy anywhere anonymously.

17

14. Unlock Code/PIN

Every smartphone has a lock function that protects it from

unauthorized access. You should get an unlock code for

set your smartphone. That's how strangers come

not immediately to your data when you use your smartphone

lose or it is stolen.

It is advisable to use a PIN or password for this

to set. However, simple PINs like “1111” help

not much. A more complicated number combination should-

te it already be. If it's possible, so can you

set a “backup PIN” that will be needed if you

entered the wrong PIN ten times. The "reserve"

PIN” should be longer if possible. In which case

you can write them down and keep them safe at home

(but not in your wallet).

Tip: "Swipe codes" are not secure.

You can often see them on screen

recognize when looking at the smartphone

holds against the light.

18

15. Updates

New vulnerabilities are discovered every day. The

Smartphone manufacturers release updates that

to close security gaps. So that your smart

phone is protected, you should check updates from apps and from

Always install the operating system as soon as possible.

Tip: If possible, you should download the updates

as long as you are connected to a WiFi network. That's how you save

mobile data volume.

More information on the internet

www.datenschutz-berlin.de

www.data-kids.de

www.datenschutz.de

www.handy-sector.de

www.stiftung-warentest.de