×

O

m

G

Facebook

×

×

I SEARCH FOR YOU.

twitter

Who are you?

×

google+

Social Networks & Privacy

Tips for teenagers

×

×

XING

twitter

lol

Whatsapp

×

×

Do you also have a profile in

a social network

like Instagram, SnapChat,

WhatsApp or Facebook?

What do we learn about you?

Which information

do you give price

… do people find out about your hobbies, favorite films and books?

... your political attitude? ... did you publish photos of yourself

public? ... do you write a blog? ... and you might find it

even your contact details, where you are or what you are doing

do?

You give in the virtual and seemingly anonymous (online) world

Price information that you might even own in real life

would hide from your best friends?

What risks and dangers for your personal rights with it

may be connected, you may not even know.

We want our information from a data protection point of view

inform about possible risks of social networks, so that

you won't get in trouble and your privacy is as good as possible

protects.

×

×

The Internet

don't forget anything!

What you find funny today might be really embarrassing tomorrow

or uncomfortable. Information that you have put on the web is

accessible to all and they can be uncontrolled copied and transferred to others

connections are made. And even if you think about it

prefer to delete or change your data on the web,

there are special service providers that change your data

Can be detected.

A separation of school or work and private life or also

You can only “forget” “sins of youth” on the Internet

then successfully prevail if you have nicknames on the internet

(Pseudonyms) uses only a few

initiates (e.g. your friends)

are known.

×

You should follow this basic rule with the

Note the use of social networks

ten since you have no control over who

looks at your posted profile.

The Internet Archive (www.archive.org)

has undertaken to

te Internet to archive. Of each

captured website are on a

Timeline also earlier versions

available, so maybe also per-

to read personal data that

should have been deleted long ago.

If you still have problems

have and don't want to

content of yours in the network of search engines like Google

or Bing are found and displayed, then the “Right

to be forgotten". This fundamental right applies to everyone and applies to everyone

on the search results for individual people. For this must

a corresponding application to the operators of the search engines

be asked. The best thing you can do is support yourself

are looking for experienced experts.

In which network

are you correct

There are social networks for different needs. While

you use one for private purposes (e.g. Instagram), you can

Make professional contacts (e.g. Xing) in other networks.

If you just want to keep in touch with friends, messengers are

like Threema, Signal, WhatsApp and SnapChat are more suitable. she

are more of a replacement for SMS than social networks, though too

since personal data is published (e.g. profile picture, status).

Pay attention to end-to-end encryption and who

service operates. Europe usually has a higher level of data protection.

Interesting are also services that send messages after some time

delete automatically - but don't rely on it 100%!

It is best to clarify the following questions before you join a social

network on the internet:

What do you want to achieve with your profile?

- Keep in touch with friends

- restore lost contacts

- establish new contacts

- Draw employers' attention to you

- Make professional contacts

What do you want to use your profile for?

- Self-presentation

- flirt profile

- Application profile

Is it absolutely necessary to enter your real name?

×

×

Why should you with your

data be careful?

Although it's easier to use your real name

find, you should consider the risks involved

know that the "community" has this information. which

Risks that can arise as a result are illustrated by the following examples

the press:

Who could also inter-

eat on your dates?

- Insurance companies that B. Special risks before the conclusion of

Life, disability, health or car insurance

want to determine.

- Credit bureaus, creditworthiness, purchasing power and sales

want to determine relevant behavior (frequent / infrequent calls).

- Applicants were rejected because of posts or photos on social networks that

do not fit the company's attitude or due to a lack of work

morally close, rejected.

×

- Landlords who question the behavior of applicants (often

parties, loud music, pets, other unwanted preferences)

want to determine.

- Employees were charged for nega-

tive statements about their work

giver terminated.

- Politically incorrect statements lead to

party exclusion or man-

data loss.

- Pupils were

the because of insulting external

ments about her teacher from the

expelled from school.

Phishing mails lure with tricky

Justifications on a website that

looks the same as the home page

your bank, your e-mail provider

or your social network and

try so confidential data of

to get you If the sender

such mails has information about you

(such as place of residence, music preferences)

or even under the name of one

friend writes, the deception falls

much easier.

- Employers who want a more comprehensive picture of the work

employees want to do or want to prove that the employees

time was used privately.

or

- Police and secret services that could use image data to

Identify people on surveillance video. Maybe

there will also soon be an app that will show the profiles of people who have been photographed

determined. In addition, you could through random network contacts

Accused come under suspicion - unpleasant consequences

would be e.g. B. Interviews or house searches.

- Data from social networks was used to

Phishing emails or email viruses as real messages from

to appear to friends.

- People were victims of targeted hate attacks, insults

and slander.

×

1. You use social

Networks private:

Use a pointed

name (pseudonym)!

Some social networks offer their users

explicitly, publicly under a nickname

to perform. Use this privacy-friendly option

so as not to have to reveal your identity. But also

if the network provider does not provide it: provisions

in the "General Terms and Conditions", which

Prohibit use of nicknames are i. i.e. R. ineffective,

since the operators according to Art. 5 Para. 1 General Data Protection Regulation

Regulation (DS-GVO) are obliged to data economy and

only necessary data may be processed.

×

2. You want to be in the social

network can be found:

Put an extra one for that

profile!

Is it exceptionally necessary that you under your real

names are found, you should create an additional profile for this

Create only those that are absolutely necessary to find them

contains data (e.g. city or university). Although you can

many networks limit the visibility of profile content

ken, but unfortunately these functions are often not error-free.

Enter your "real" name only when registering yours

profile if necessary, and remember that the

operator of the network has access to all data of your profile.

So be careful who you trust with your data.

×

3. You want your pri-

Publish father's photos:

Don't put photos on the web

on which you or others

people are recognizable!

Consider carefully whether the photos are really for the public

or whether they B. should only be intended for your friends. Can

the publication might harm you? Switch to everyone

Lost features that automatically recognize you in photos.

Otherwise you might easily look at other photos on the net or even on

Surveillance videos - with your consent - identified

will. Ideally, photos should only be in the network

be hired if you

or other people on it

recognized only by friends

can become.

×

Biometric photos allow com-

putern, you particularly well and quickly

on other, different photos

because of your unmistakable

male (eye distance, nose size etc.)

to recognize again.

eye area

(Pupils open

same height)

nose on the

centerline

×

4. You put your profile in the

social network to:

Publish only those

data that are necessary

and no more!

It is important that you determine the specific purpose that your

Profile should fulfill and then think carefully about which data

you want to publish about yourself.

You also have different roles in everyday life (at school, on

at work, privately or with friends, in the family etc.) and

decide who you give what information to. In social

Networks can only be differentiated to a limited extent. You can

Although entries are only accessible to certain "friends".

do, but happen in the process

easy mistake.

×

Therefore you should

different social roles too

different profiles with

Create relevant data.

Think about which sensor data

smartphone apps social network

works preserved or even published

allowed to.

Sensor data: smartphones and wearab

les (e.g. smart watches, bracelets, glasses

len) come with a lot of sensors

equipped, the fitness values and

health values (steps taken,

heart rate, skin resistance) and your

abode and thus your daily allowance

run can determine. Consider that e.g. B.

skin resistance and heart rate readings

are lie detectors.

×

5. Stay in control:

Give your contact details

not on!

Providing contact details (e.g. telephone number,

postal address) is not necessary, as each network is internal

provides contact options. Sure it's practical

to use social networks as an address book, however

the contact details are then publicly available – at least

for all online friends, not all of whom are real ones

Friends are. In addition, the data is stored on servers in

Saved out for criminal hackers because of the internet

large amounts of data are very lucrative. some networks

also use the contact details for sending

Advertising. This is for telephone, fax and email advertising

only allowed if the operator (voluntarily!) expressly

was allowed.

Even some messengers (Threema, Wire) come without it

phone number and without uploading the entire cell phone

address book.

×

Criminal hackers exploit gaps or

Errors in programs to

works to access data that

not supposed to be accessible to them

should - such as B. your passwords.

×

6. Decide who your pro-

fi l can see: Restrict

the data access!

Most networks allow you to choose which ones

Data public, d. H. for all users of the network or

even accessible to all Internet users or only to friends

meant to be. You can usually find this setting under

"Privacy" or "My profile". you always should

choose the most restrictive settings. It is particularly important

that your "friend list" is not public, otherwise

also got a lot of information about you from your friends

can become. You shouldn't enable that either

Photos or videos of others uncontrolled with your pro-

fi l links or messages to you in a publicly readable

Forum or guest book can be written. in one

Profile should really only be the information made public

be given to any stranger without hesitation

can be shared.

×

×

×

Sensor data: smartphones and wearab

Sensor data: smartphones and wearab

les (e.g. smart watches, bracelets, glasses

les (e.g. smart watches, bracelets, glasses

len) come with a lot of sensors

len) come with a lot of sensors

equipped, the fitness values and

equipped, the fitness values and

health values (steps taken,

health values (steps taken,

heart rate, skin resistance) and your

heart rate, skin resistance) and your

abode and thus your daily allowance

abode and thus your daily allowance

run can determine. Consider that e.g. B.

run can determine. Consider that e.g. B.

skin resistance and heart rate readings

skin resistance and heart rate readings

are lie detectors.

are lie detectors.

"Restrictive" means restricted.

Your interests, your date of birth

tum, your photo albums and also yours

real name should be maximum for

real friends be accessible. It

not every field in the program

fi l be filled in: data that is not

accessible, cannot miss

be needed.

×

7. Decide who is your profile

can fi nd in the network:

Restrict data access

on members and close it

for search engines!

In some networks, profile data can basically only be used by others

members are read, others offer the exclusion of search engines

chines or restricting access to members at least as

Option. If this option is not selected, the profile will be found later

not only on Google or Bing, but also in the result lists

ten specialized people search engines like yasni.de. Hence

you should always exclude Internet search engines.

The major search engines offer outdated search results, ie

e.g. B. deleted, changed or blocked for search engines entries,

to update or remove in the result lists. look at you

the help pages of the search engines.

In May 2014, the European Court of Justice also ruled

that search engines also remove links to existing websites

must be called if they violate personal rights and that

The public's right to information does not prevail. Also to fi n-

the hints at the search engine operators. However, should

you always try to get the data on the original web page first

remove.

criminal hackers use loopholes

criminal hackers use loopholes

or bugs in programs to over

or bugs in programs to over

Networks to access data that

Networks to access data that

actually not accessible to them

actually not accessible to them

should - such as B. your passwords.

should - such as B. your passwords.

×

×

×

8. What do you need

really: enable

Third Party Applications

no access to yours

profile data!

Some network operators allow others to

genes with more or less useful or funny additional

functions (e.g. sending hearts to friends or the

display of the current weather report). In addition

it is often necessary to access your profile data.

It is possible that these applications further

(undesirable) purposes, similar to spyware or adware,

pursue. This could e.g. B. scouting your

User data for targeted advertising or political

be manipulation. You should think carefully about whether and

to what extent you have access rights to your profile data

concede

×

×

×

Spyware is called sniffer programs,

who, in addition to their offi cial task

have other functions, e.g. B. Files

to spy on your computer and without

to pass on your knowledge or yours

understand online behavior.

"Restrictive" means restricted.

"Restrictive" means restricted.

means restricted.

Your interests, your date of birth

Your interests, your date of birth

tum, your photo albums and also yours

tum, your photo albums and also yours

real name should be maximum for

real name should be maximum for

real friends be accessible. It

real friends be accessible.

real friends be accessible. It

not every field in the program

not every field in the program

fi l be filled in: data that is not

fi l be filled in: data that is not

accessible, cannot miss

accessible, cannot miss

accessible, cannot miss

be needed.

be needed.

×

9. You want your data

protect: beware of

cross-network

Connections!

Social networks or additional service providers offer you

sometimes the possibility that profile data in several

Maintained jointly in networks or in other

hanging – e.g. B. on cooperating websites or apps

- be used. Better set up your profile so that the

Data usage outside of the actual platform

is additionally prevented. The login data should always only

entered on the platform itself. do you want one

still use such a link, you should

inform exactly who has access to which of your files

receives. Be especially wary of services that a

Type "Home" to all profiles in social networks

offer, since the login data of all profiles are also transferred here

will. Data thieves would have access to it in one fell swoop

all your accounts.

×

×

×

With Facebook “Connect” you need e.g. B. on

a game website do not register a new account

place, but play under your Facebook

criminal hackers use loopholes or

criminal hackers use loopholes or

names and you can easily add your friends

Errors in programs to

Errors in programs to

load and play against them. The problem is

works to access data that

works to access data that

now that the game website both on your

not supposed to be accessible to them

not supposed to be accessible to them

profile data as well as those of your friends

should – such as your passwords.

should – such as your passwords.

can access − and Facebook learns how

often you play there

×

10. You don't want one

Trouble with others:

Respect the rights of third parties!

A carelessly posted photo or comment in

a guest book you and others can quickly

bring comfortable situation.

Therefore, you should always ask permission before posting a photo,

Video or text published by or about someone else

most. This applies in particular if the material with information

tion to those (e.g. with photos) is linked.

If you don't have a nice, suitable photo for a post yourself

then you will fi nd a large selection in free image portals,

such as B. pixabay.com or jugendfotos.de. Here were almost all

Photos from the authors for free use

dation under a CC-0 or CC-BY 4.0 license.

×

×

×

are called sniffing programs,

Spyware is called sniffer programs,

spyware

Spyware is called sniffer programs,

"CC" stands for Creative Commons Licenses

who, in addition to their offi cial task

who, in addition to their offi cial task

and is a worldwide license system

have other functions, e.g. files on

have other functions, e.g. files on

with different legal gradations

to spy on your computer and without

to spy on your computer and without

to spy on your computer and without

gen. The free use and processing

to pass on your knowledge or yours

to pass on your knowledge

to pass on your knowledge or yours

processing of z. B. images or texts

understand online behavior.

understand online behavior.

. You can fi nd more information e.g. at:

www.creativecommons.org.

"Restrictive" means restricted.

means restricted.

means restricted.

Your interests, your date of birth

Your interests, your date of birth

tum, your photo albums and also yours

tum, your photo albums and also yours

real name should be maximum for

should at most for

real friends be accessible. It

real friends be accessible.

real friends be accessible. It

not every field in the program

not every field in the program

fi l be filled in: data that is not

data that is not

accessible, cannot miss

accessible, cannot miss

accessible, cannot miss

be needed.

be needed.

×

Why is she interested?

economy for your data?

Social networks record the connections of their users

and users, their acquaintances and friendships

among themselves.

Databases can be created from this, which can be used as a “social graph”

be designated.

The economic evaluation of these databases are increasingly

many companies for the development of new business areas.

×

Big data is the buzzword for the

lysis of large amounts of data. With techniques

how artificial intelligence is

is looking for, from the data mountain of the operator

social networks useful information

to win. It is Z. B. possible

Targeted advertising

Show people selected by

hundreds of features.

×

×

Hackers exploit gaps or bugs in

Hackers exploit gaps or bugs in

Programs to access via networks

Programs to access via networks

data access that actually does not

data access that actually does not

should be accessible to them – how

should be accessible to them – how

e.g. B. your passwords.

e.g. B. your passwords.

Conclusion

×

×

×

Spyware is called sniffer programs,

spyware

Spyware is called sniffer programs,

are called sniffing programs,

who, in addition to their offi cial task

who, in addition to their offi cial task

have other functions, e.g. B. Files

have other functions, e.g. B. Files

spy on your computer and

spy on your computer and

spy on your computer and

without passing on your knowledge or even

without sharing your knowledge

without passing on your knowledge or even

understand your behavior online.

understand your behavior online.

×

×

With Facebook “Connect” you need e.g. B. on a

With Facebook “Connect” you need e.g. B. on a

Game website do not create a new account, but

Game website do not create a new account, but

play under your Facebook name and can

play under your Facebook name and can

just invite your friends and play against them.

just invite your friends and play against them.

The problem now is that the game website both

The problem now is that the game website both

on your profile data as well as on those of your friends

on your profile data as well as on those of your friends

can access.

can access.

Social networks are one

great form of communication

and if you read our 10 tips

note, you protect with

your pri-

home sphere without

to give up parts.

"Restrictive" means restricted.

"Restrictive" means restricted.

means restricted.

Your interests, your date of birth

Your interests, your date of birth

tum, your photo albums and also yours

tum, your photo albums and also yours

real name should be maximum for

real name should be maximum for

real friends be accessible. It

real friends be accessible.

real friends be accessible. It

not every field in the program

not every field in the program

fi l be filled in: data that is not

fi l be filled in: data that is not

accessible, cannot miss

accessible, cannot miss

accessible, cannot miss

be needed.

be needed.

With Facebook “Connect” you need e.g. B.

With Facebook “Connect” you need e.g. B.

on a game website no new one

on a game website no new one

Create an account, but play under

Create an account, but play under

your Facebook name and you can

your Facebook name and you can

fold invite your friends and against them

fold invite your friends and against them

to play.

to play.

The problem now is that the game website

The problem now is that the game website

Problem now is that the game website

both on your profile data and on

both on your profile data and on

that your friends can access.

that your friends can access.

that your friends can access.

×

×

×

×

You can find more here

Information:

www.datenschutz.de

Joint portal of the data protection institutions of the federal states and

of the federal government as well as the churches in Germany and some institutes

tutions from abroad. Here you will find, among other things, information

Information about which contact person you can contact in which cases

need to contact data abuse.

www.datenschutz-berlin.de

The website of the Berlin Commissioner for Data Protection and Information

mation freedom.

www.bfdi.bund.de

The website of the Federal Commissioner for Data Protection and Information

freedom of operation.

www.bfdi.bund.de/bfdi_forum

The Privacy Forum. Here you can ask questions about the topic

Privacy ask by other forum members with a lot

expertise are answered. In addition, the Federal Data

protection officer here her blog.

www.klicksafe.de

The EU initiative for more security on the internet. In the category

"Topics" explains klicksafe the differences between forums,

social networks and Web 2.0 portals such as YouTube. Flyers for

Parents and teaching materials for teachers can be created as a PDF

be downloaded or ordered.

www.irights.info

The iRights.info initiative has been providing information from a legal point of view for years

point of view and in plain language about copyrights in the digital

World. In cooperation with klicksafe, an easy to read was created

comprehensible basic article on "copyright and personality

rights in social networks”.

www.youngdata.de

An information page from the State Commissioner for Data Protection

and the freedom of information in Rhineland-Palatinate contribute to self-protection

current Internet services, especially for young people.

www.handysector.de

Mobile phone sector is an independent contact point for the digital

Everyday life – with lots of tips, information and also creative ideas

en about the use of smartphones, tablets and apps. the

Page is commissioned by the State Media Authority of North Rhine-Westphalia and the

Media Education Research Association Southwest operated.

www.netzdurchblick.de

Netzdurchblick is an independent and ad-free Internet advice

for young people, by students at HAW Hamburg

is cared for.

imprint

Editor:

Berlin Commissioner for Data

protection and freedom of information

Address:

Friedrichstr. 219

10969 Berlin

Office hours:

Mon - Fri, 10 a.m. - 3 p.m

Thursday, 10 a.m. – 6 p.m

Visitor entrance:

Puttkamer Str. 16 – 18

Contact:

Telephone: 030 138890

Fax: 030 2155050

mailbox@datenschutz-berlin.de

Editorial staff:

Oliver Bertold

Speaker at the

Berlin representative

for privacy and

Freedom of Information

Astrid Dinges

Uta Voigt

music media park e.V.

×

×

State program youth network Berlin

Address:

Youth and Family Foundation

of the State of Berlin - Project Office

Obentrautstr. 55

10963 Berlin

Contact:

Telephone: 030 2847019-30

go@jugendnetz-berlin.de

Layout:

Gabriel Brown

Print:

Penguin Druck GmbH, Berlin

12th edition

Total circulation: 40,000

Status: July 2018, Berlin

Anyone can contact the Berliner

Data protection officer and

Contact freedom of information if

she/he believes that at

the processing of personal

gener data against data protection

regulations have been violated.

×

The aim of the Berlin state program jugendnetz-berlin is funding

of children and young people for a self-determined, creative

and responsible use of media, as a prerequisite for

Participation and participation in the digital society.

Develop, network and support in all 12 Berlin districts

Media competence centers a variety of media education

offers and model projects. Cooperation partners include the

Initiative comp@ss - computer driver's license, Bits 21 in fjs e.V. and

WeTeK Berlin gGmbH for the further training of socio-pedagogical

professionals and the network of Berlin youth culture centers. annual

lich organize the media competence centers with other partners

the youth media culture days, for trying out and creative design

of digital media in different genres.

With the Berlin skilled labor portal - jugendnetz-berlin.de - informed

the state program on topics, issues, projects and

Offers for contemporary media education in Berlin and beyond

out. The youth portal jup! Berlin offers a lot of information

for young people also a cross-media designed by young people

Media magazine and opportunities for digital participation.

The Berlin state program jugendnetz-berlin is run by the Senate

Administration for Education, Youth and Family and the Youth and Family

lienstiftung of the State of Berlin and jointly in cooperation

implemented with the Berlin districts.