

PRIVATE – no access?

personal data

sensitive data

identity theft

transparent individuals

privacy

locating of cell phones

spam text messages

malware

retention of data



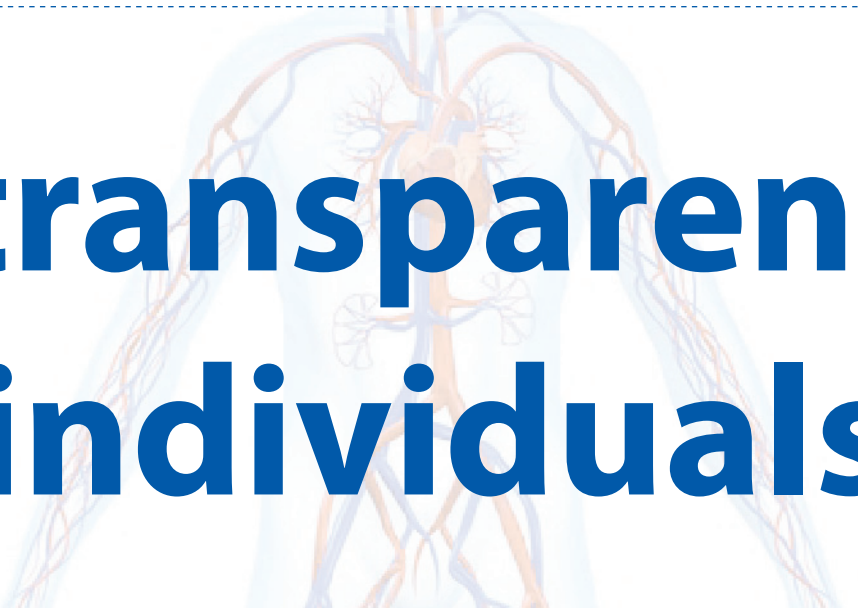
personal data



sensitive data



identity theft



transparent individuals



privacy



locating of cell phones



**spam text
messages**



malware



**retention
of data**

Have you heard?

Read through the descriptions and then try to summarise the described problem in one sentence.



An app with hidden possibilities

Paul S. was excited: thanks to a new app he was able to integrate his private photos into the film sets of recent blockbusters by pressing just one button! He had never ever sent as many multimedia messages like after he had installed this app. All his friends could admire themselves side by side with their movie heroes.

However, an unpleasant surprise was soon to come. What Paul S. did not know was that the app was far more powerful. And he himself had allowed the app and its operators to be so powerful. In order to be able to install the app Paul S. had to give

the app operators some authorisations, among other things access to his personal contacts and his call list. Data protectors now assume that such data was not only collected, but had also been passed on. And Paul S. now is afraid that he and his friends will in future receive loads of spam text messages and that his private photos may appear on any given websites.

.....

.....



Missed calls can be expensive ...

Sandra S. hardly could believe her eyes when she looked at her last mobile phone bill: she had been charged EUR 30 for calls to value-added service numbers which she just could not explain to herself! She calmed down and called the billing hotline of her mobile radio provider. Only when they asked for calls from unknown numbers she remembered the missed calls she had found on her mobile phone some time ago. She had always tried to call back but had only reached weird answering machine loops. Obviously she had called value-added services without noticing it! Her

contact at the hotline offered her to block her mobile phone for value-added service numbers.

.....

.....



Free app may be expensive ...

Last week Isabelle F., a student from Upper Austria, fell victim to a malicious attack of mobile phone hackers. Together with a free app she also received a free but unwanted Trojan which sent text messages to all her contacts without her noticing it. Only when her classmates asked her why she sent empty text messages she became suspicious. However, she found no empty text message in her outbox. Only when she called her mobile radio provider she learned that she had already exceeded the number of included free text messages and that approx. 300 text messages had been sent from her mobile phone per day.

.....

.....



Hello, here I am!

Luke, Matthew and Jacob, three students from Deutschlandsberg, had planned everything very well. They started off on time in the morning and instead of going to school then went to the train station. They took the 8.05 train and went to Graz: they had planned to go shopping instead of attending school. They had even thought of changing their Facebook status several times during their little trip, always using similar phrases like: „I feel sooo sick“. Thanks to their new smartphones this was no problem at all. However, they had overlooked the fact that on their Facebook sites

they had activated the function to automatically detect their location and state it on their profile together with every new status message. So their status messages read „I feel sooo sick“; however, Graz and not their home town was stated as their location on all three profiles. So the three truants got caught very quickly thanks to their digital lead.

.....

.....



Alter ego

Florian E. was very happy with his new smartphone. He was so happy that he did not even think about his old mobile phone any more, which he had sold with profit. Until last Friday, when his colleague left the office and said: „Don't go too far, Loverboy85!“ Mr. E first looked puzzled; then, after he had asked several times, his colleague felt pity for him and explained what this „Loverboy“ thing was all about. He showed Mr. E the profile of a single man with the username „Loverboy85“ on a well-known online dating portal. And this profile was actually loaded with private photos of Mr. E. Mr. E. made some research and found out that the buyer of his old smartphone had found the photos and had created a profile on the online portal „just for fun“!

.....

.....



Zeynep K. & the subscription trap

Zeynep K. always wanted a new ringtone. So she was thrilled when she found her favorite song for download as a ringtone in a new app. Was also quite easy: She only had to confirm „Buy“ and could download her new ringtone. The rude awakening came quickly, however. Because suddenly, the entire balance was used up on her prepaid card. With her click on „Buy“ she not only ordered one ringtone, but a full subscription.

.....

.....

My mobile phone and me



1. My gender: ☐ male ☐ female

2. Can you access the internet with your phone?

☐ Yes ☐ No

3. What do you do when going online with your mobile phone?

Rate the suggested options with 1 to 5: „1“ stands for „very often“, „5“ stands for „very rarely“:

☐ ...

surf the internet

☐ ...

send and receive e-mails

☐ ...

check the weather report

☐ ...

check my profile on Facebook/Twitter, etc.

☐ ...

I use route planners, e.g. „Qando“ of the Verkehrsverbund Ost-Region/VOR [public transport association for the Eastern region of Austria]

4. What do you do if you do not need your mobile phone any more?

☐ I throw it away.

☐ I give it to one of my relatives/friends.

☐ I donate it. (For example Ö3)

☐ I keep it at home.

☐ I sell it.

☐ I give it to recycling.

5. Do you check what data still is stored on your phone before you replace it?

☐ Yes

☐ No

6. Have you ever lost your mobile phone or has it been stolen?

☐ Yes

☐ No

If so, what did you worry about most when it was gone?

☐ That I was not able to make phone calls any more.

☐ That I had lost all my phone numbers.

☐ That I had lost all my photos.

☐ That I could not send text messages any more.

☐ That I did not know who might have found my phone.

7. Have you ever received any unwanted advertising text messages?

☐ Yes

☐ No


8. Do you have a smartphone?

☐ Yes

☐ No

9. Can you install apps on your mobile phone?

☐ Yes

☐ No

If so:

10. How many apps are installed on your phone?

☐ 0

☐ 1 - 5

☐ 6 - 10

☐ 11 - 15

☐ more than 15

☐ I don't know.

11. Which apps do you use most? List your top three apps:

1.

2.

3.

12. What happens to apps you no longer use?

☐ I keep them on my mobile phone.

☐ I delete them.

☐ I would like to delete them, but I don't know how to.

13. What security measures have you taken for the case of a mobile phone loss or theft?

☐ I back up my data periodically.

☐ I have activated my phone lock.

☐ I have noted the IMEI number.



My mobile phone and me

Evaluation

1. People asked:

- male: in percent: %
- female: in percent: %

2. Can you access the internet with your phone?

- Yes: in percent: %
- No: in percent: %
- Portion of all respondent women who can access internet with their mobile phones:
..... of total in percent: %
- Portion of all respondent men who can access internet with their mobile phones:
..... of total in percent: %

3. Most common online activities:

	number of votes	place
surf the internet		
e-mails		
weather report		
social networks		
route planners		

4. What do you do if you do not need your mobile phone any more?

- I throw it away. in percent: %
- I give it to one of my relatives. in percent: %
- I donate it. in percent: %
- I keep it at home. in percent: %
- I sell it. in percent: %
- I recycle it. in percent: %



5. Do you check what data still is stored on your phone before you replace it?

- Yes: in percent: %
- No: in percent: %

6. Have you ever lost your mobile phone or has it been stolen?

- Yes: in percent: %
- No: in percent: %

If so, what did you worry about most when it was gone?

- That I was not able to make phone calls any more. in percent: %
- That I had lost all my phone numbers. in percent: %
- That I had lost all my photos. in percent: %
- That I could not send text messages any more. in percent: %
- That I did not know who might have found my phone. in percent: %

7. Have you ever received any unwanted advertising text messages?

- Yes: in percent: %
- No: in percent: %

8. Do you have a smartphone?

- Yes: in percent: %
- No: in percent: %
- Portion of all respondent women who own a smartphone:
..... of total in percent: %
- Portion of all respondent men who own a smartphone:
..... of total in percent: %

9. Can you install apps on your mobile phone?

- Yes: in percent: %
- No: in percent: %
- Portion of all respondent women who are able to install apps on their mobile phone:
..... of total in percent: %
- Portion of all respondent men who are able to install apps on their mobile phone:
..... of total in percent: %



10. How many apps are installed on your phone?

- None: in percent: %
- 1-5: in percent: %
- 6-10: in percent: %
- 11-15: in percent: %
- More than 15: in percent: %
- I don't know: in percent: %

11. Top 3 der Apps:

app	number of votes	place

12. What happens to apps you no longer use?

- I keep them on my mobile phone. in percent: %
- I delete them. in percent: %
- I would like to delete them, but I don't know how to. in percent: %

13. What security measures have you taken for the case of a mobile phone loss or theft?

- I back up my data periodically. in percent: %
- I have activated my phone lock. in percent: %
- I have noted the IMEI number. in percent: %



My mobile phone and me

Unless stated otherwise, the following results are from the Austrian Internet Monitor-Consumer (AIM-C). INTEGRAL Markt- und Meinungsforschung questioned a representative group of Austrian people (12,000 persons – 3,000 a quarter). The respondents were at least fourteen years old. (www.integral.co.at/de/downloads/?f=AIM)

Do you have an web-enabled mobile phone?

- 24% of all Austrian women older than fourteen years owning a mobile phone have a web-enabled mobile phone.
- 19% of all respondent women use the internet on their mobile phones.
- 30% of all respondent men use the internet on their mobile phones.
- 50% of all respondents between fourteen and nineteen years use the internet on their mobile phones. 31% of the respondents between thirty and thirty-nine and 25% of the respondents between forty and forty-nine use the internet on their mobile phones.

Most common activities on the internet

activities	place
surf the internet	1
social network	2
weather report	3
e-mails	4
route planners	5

Disposal of mobile phones

A survey of the Aris polling firm carried out with 1,000 German respondents older than fourteen years in November 2011 showed that two out of three owners of mobile phones (66.67%) keep their old phone when they get a new one. Every third female respondent (33%) gives her phone away as a gift.

Lost mobile phones

Robbery of mobile phones is an offence committed more and more frequently in Austria according to the Federal Office of Criminal Investigations [Bundeskriminalamt]: in 2011 20% more mobile phones were robbed in Austria than in the year before; expressed in figures these are 444 mobile phones.



Owners of smartphones

32 % of all Austrian women older than fourteen years owning a mobile phone have a smartphone.

In the course of the German JIM survey 1,208 young people between twelve and nineteen years were questioned in 2010. The survey arrived at the following result: 14% of all respondents have a smartphone, 11% of the girls and 16% of the boys.

Apps on the mobile phone

20% of all Austrian women older than fourteen years owning a mobile phone have installed apps. 12% of female owners of mobile phones and 28% of male owners of mobile phones.

42% of all male and female mobile phone users between fourteen and nineteen years have installed apps. 28% of the respondents between thirty and thirty-nine years and only 16% of the respondents between forty and forty-nine years have installed apps.

Number of apps

The average Austrian app user older than fourteen years has installed ten apps on his/her phone, of which six are used regularly

Top three of apps

The apps most popular among Austrian app users come from the areas of:

- navigation: 72%
- weather: 64%
- games: 60%
- social networks: 57%

What happens to apps no longer used?

Most Austrian app users delete programmes they no longer use. On average, every app user has already deleted eight apps s/he no longer uses.





Free home delivery of data

Consumers handle their personal data carelessly

In view of sky-rocketing numbers of electronic services scientists warn of handling private data too carelessly. According to a research project of six European institutions on technological impact assessment, among them the Institute for technological impact assessment (ITA) of the Austrian Academy of Applied Sciences (ÖAW) the significance of privacy is underestimated by citizens and enterprises and by politicians. [...]

According to the experts the high speed of progress in electronic services bears both chances and risks. Users of the internet and/or mobile phones profit from the possibilities of technology but also leave data traces. The scientists request that politics should deal the issue of privacy. [...]

Unforeseeable consequences

Although many users are aware of how much personal information they disclose when using information and communication technologies, one cannot expect them to be able to estimate long-term consequences. Therefore, Walter Peissl of the ITA requests a higher degree of sensitivity of the users

of electronic services as regards the issue of privacy. In their project report the scientists found that the protection of privacy often is weighed against values such as comfort, security, economic advantages or social interaction.

The experts are convinced that many problems in connection with privacy could be avoided. For this purpose the requirements of data protection must be taken into account at an earlier point of time, i.e. already in the design and development of electronic offers. Obligatory privacy impact assessment could contribute thereto.

When collecting personal data the following principle should always be followed: „As little as possible and only as much as necessary.“ Monitoring institutions should be established for surveillance systems. Moreover, citizens should be given simple access to the data stored about them. Last but not least, data protection authorities should be given more competences and resources.

Source of the German version of the text:
www.wienerzeitung.at/nachrichten/panorama/chronik/106034_Daten-frei-Haus.html



In this text, there are many new words. Can you match the German translation to the right word?

abschätzen

Anliegen

Aufsichtsstelle

berücksichtigen

Datenschutzbehörde

Datenspur

einrichten

etwas abwägen

etwas beitragen

fordern

frei Haus

in sich bergen

rasant ansteigend

sich einer Sache bewusst sein

Stellenwert

Technikfolgenabschätzung

to be aware of

to bear

to contribute something

data protection authority

data trace

to establish

to estimate

free home

to request

requirement

significance

sky-rocketing

surveillance system

to take into account

technological impact assessment

to weigh something



Free home delivery of data

Consumers handle their personal data carelessly

In view of sky-rocketing numbers of electronic services scientists warn of handling private data too carelessly. According to a research project of six European institutions on technological impact assessment, among them the Institute for technological impact assessment (ITA) of the Austrian Academy of Applied Sciences (ÖAW) the significance of privacy is underestimated by citizens and enterprises and by politicians. [...]

According to the experts the high speed of progress in electronic services bears both chances and risks. Users of the internet and/or mobile phones profit from the possibilities of technology but also leave data traces. The scientists request that politics should deal the issue of privacy. [...]

Unforeseeable consequences

Although many users are aware of how much personal information they disclose when using information and communication technologies, one cannot expect them to be able to estimate long-term consequences. Therefore, Walter Peissl of the ITA requests a higher degree of sensitivity of the users

of electronic services as regards the issue of privacy. In their project report the scientists found that the protection of privacy often is weighed against values such as comfort, security, economic advantages or social interaction.

The experts are convinced that many problems in connection with privacy could be avoided. For this purpose the requirements of data protection must be taken into account at an earlier point of time, i.e. already in the design and development of electronic offers. Obligatory privacy impact assessment could contribute thereto.

When collecting personal data the following principle should always be followed: „As little as possible and only as much as necessary.“ Monitoring institutions should be established for surveillance systems. Moreover, citizens should be given simple access to the data stored about them. Last but not least, data protection authorities should be given more competences and resources.

Source of the German version of the text:

www.wienerzeitung.at/nachrichten/panorama/chronik/106034_Daten-frei-Haus.html

Words to help you:

- free home – *frei Haus*
- sky-rocketing – *explodierend, rasant ansteigend*
- technological impact assessment – *Technikfolgenabschätzung*
- significance – *Stellenwert, Bedeutung*
- to bear – *in sich bergen*
- data trace – *Datenspur*
- to be aware of – *sich einer Sache bewusst sein*
- to estimate – *abschätzen, ermessen*
- to request – *fordern*
- to weigh something – *etwas abwägen*
- requirement – *Anliegen*
- to take into account – *berücksichtigen*
- to contribute something – *etwas beitragen*
- to establish – *einrichten*
- surveillance system – *Aufsichtsstelle*
- data protection authority – *Datenschutzbehörde*



Questions for analysis

1. *What are the problems that the scientists mentioned in this article warn of?*

.....

.....

2. *In your opinion, which services and/or offers are covered by the term „electronic services“?*

.....

.....

3. *The article refers to personal data. In your opinion, what data is included?*

.....

.....

4. *The article states several reasons why users handle their data carelessly. What are those reasons?*

.....

.....

5. *Can you think of some other reasons which might be responsible therefor?*

.....

.....

6. *What possible solutions are stated in the article?*

1.
2.
3.
4.



7. *This article dates from the year 2007. Do you think that the problem described therein is still an issue?*

.....

.....

8. *How high do you think is the risk that your personal data is misused?*

.....

.....

.....

9. *What data on your mobile phone do you consider to be „private“ and should remain private?*

- ☐ text messages
- ☐ photos
- ☐ multimedia messages
- ☐ appointments
- ☐ phone numbers
- ☐ list of callers

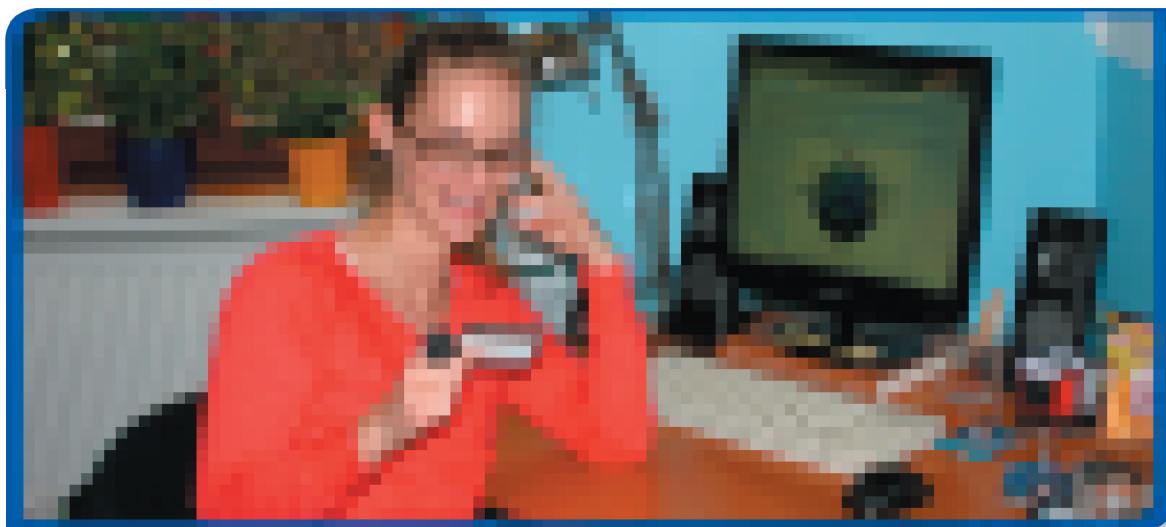
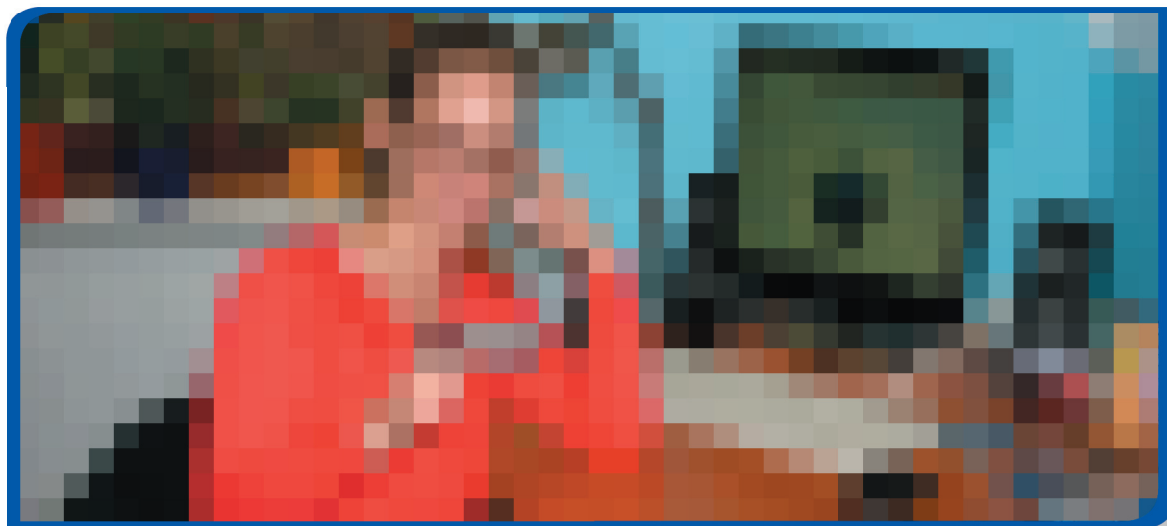


Many new words ...

- to be aware of – *sich einer Sache bewusst sein*
- to bear – *in sich bergen*
- to contribute something – *etwas beitragen*
- data protection authority – *Datenschutzbehörde*
- data trace – *Datenspur*
- to establish – *einrichten*
- to estimate – *abschätzen, ermessen*
- free home – *frei Haus*
- to request – *fordern*
- requirement – *Anliegen*
- significance – *Stellenwert*
- sky-rocketing – *rasant ansteigend*
- surveillance system – *Aufsichtsstelle*
- to take into account – *berücksichtigen*
- technological impact assessment – *Technikfolgenabschätzung*
- to weigh something – *etwas abwägen*



The modern human being – a walking database





Caution – sensitive!

All data related to us is considered sensitive data. In the Austrian Data Protection Act [Datenschutzgesetz] such data is described as „personal data“ [„personenbezogene Daten“]. Some personal data is considered to be particularly sensitive.



What do you think – which of the data listed below is sensitive data?

Data	Yes	No
Address		
Age		
Allergies		
Birthday		
Body height		
Colour of eyes		
Colour of hair		
Date of birth		
Education/occupation		
E-mail address		
Favourite colour		
Favourite dish		
International certificate of vaccination		
IP address of the computer		
Marital status		
Membership in a political party		
Membership in a sports association		
Membership in a trade union		
Membership in an association for the support of equal rights of homosexuals		
Mobile phone number		
Name		
Nationality		
Religion		
Shoe size		
Taste in music		
Vote at the last election for the Austrian Parliament		

Smart & Safe

Caution – sensitive!

Allergies

Vote at the last election for
the Austrian Parliament

Marital status

Membership in a
trade union

International certificate of
vaccination

Membership in an
association for the support
of equal rights of
homosexuals

Membership in a
political party

Religion

Nationality



Deserving special protection?

The Austrian Data Protection Act regulates who may use which data, which steps must be taken by Austrian enterprises to guarantee data security and which national institutions monitor data protection. Moreover, there is a separate part on video surveillance.

Answer the following questions using the Austrian Data Protection Act.

1. Article 1 of the Austrian Data Protection Act stipulates the right to secrecy of your data. To which data is such secrecy related? What restrictions are defined? What are your rights concerning your data?

.....

.....

.....

2. Which part and/or section defines data deserving special protection?

.....

What is the wording of this definition?

.....

.....

.....

.....

3. Article 2 defines exceptions from the duty to maintain secrecy. Which part and which section(s) contain(s) those exceptions?

.....

Name an example for such an exception!

.....

.....

4. What monitoring institutions are there in Austria to maintain data protection?

.....

.....

Words to help you:

to stipulate – festlegen | secrecy – Geheimhaltung | data deserving special protection – besonders schutzwürdige Daten | to maintain – erhalten, wahren

Who may do what?



80 at last!

Margit N. organises a birthday party for her grandmother's 80th birthday. She has invited all relatives to the party, even those with whom she otherwise is not so much in touch. Long before the party Margit calls all persons to be invited and asks them for their addresses and e-mail addresses to send them official invitations. In addition she asks them to give her their mobile phone numbers so that she can reach the invited persons as quickly as possible, if need be. In this manner a considerable contact list of her relatives is created. One week before the party Margit decides to

contact all guests on the phone once more as a precaution. To get this done more quickly she shares the list with her sister so that each of them only has to personally contact half of the list.

- ☐ Yes, this is allowed under the Austrian Data Protection Act.
☐ No, this is prohibited by the Austrian Data Protection Act.

Reason:

.....

.....

.....

.....



Top offer at a special price for friends

Bernd P. has been invited to a big birthday party. He gets the latest information on the programme of the party by e-mail, which was erroneously sent to a disclosed mailing list. As Bernd P. is an insurance agent, he takes the opportunity and uses these addresses to send all party guests an offer for a private pension fund.

- ☐ Yes, this is allowed under the Austrian Data Protection Act.
☐ No, this is prohibited by the Austrian Data Protection Act.

Reason:

.....

.....

.....

.....

.....



First-hand information

Nadine H. is a student at the University of Vienna. In the fourth term she writes her first term paper for which she also does some „field research“. She prepares a questionnaire on the topic „The radio and its social significance in the Sixties of the twentieth century“ and sends the same to various persons older than sixty years who agreed to take part in the survey. For Nadine to be able to evaluate the data according to various criteria the respondents also state data such as age, sex and marital status. However, the results are anonymised so that the term paper does not state

which persons were actually questioned and what answers they had given.

Two terms later Nadine uses the data of the „radio survey“ once again for a different paper which is about the percentage of divorces in the 60+ generation. Again, the evaluation is anonymised.

- ☐ Yes, this is allowed under the Austrian Data Protection Act.
- ☐ No, this is prohibited by the Austrian Data Protection Act.

Reason:



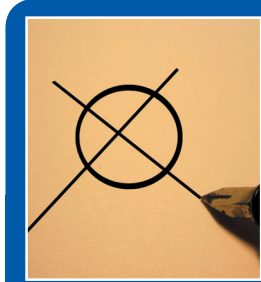
Research made easy!

Bernhard E. is a student at the University of Vienna and has to write a research paper on the life situation of men above the age of 65. As he knows that his fellow student Nadine H. has made interviews with many persons of that age group in a different context he asks her for the list of interview partners to call all men from the list and ask them whether he may interview them on his topic. Nadine knows how difficult it had been to find people willing to take part in her survey on a voluntary basis, so

she gives Bernhard E. the list.

- ☐ Yes, this is allowed under the Austrian Data Protection Act.
- ☐ No, this is prohibited by the Austrian Data Protection Act.

Reason:



Time to vote?

Two days before the Parliamentary Elections is Sandra S.'s sixteenth birthday. This means that she may go to an election for the first time. Three weeks before the election she receives a letter personally addressed to her which contains an information leaflet published by the President of the Nationalrat [National Council of the Austrian Parliament] which informs her about the tasks of the Nationalrat and reminds and asks Sandra to exercise her right to vote at the next election.

- ☐ Yes, this is allowed under the Austrian Data Protection Act.
- ☐ No, this is prohibited by the Austrian Data Protection Act.

Reason:



My data for bargain-sale?

I frequently take part in sweepstakes. It is obvious that I have to state some of my personal data; the organisers of the sweepstakes need to know how to contact the winner!



I sometimes take part in market surveys and opinion polls. Often you get goods for free, sometimes even some money. It is clear that I state not only my name and address but also some more personal details. Otherwise the whole thing would make no sense!

I love and collect store cards! The special offers where one can make a bargain with them are simply great! They make shopping much more fun!



I often take part in discussions in internet forums. Sometimes the topics are unimportant, but sometimes there are heated debates on really important issues! As I can see no reason why I should not stand by my opinion, I state my real name and my full contact data as a rule.

A rising number of bars and clubs send information about their events via text messages. I really like that, as this always keeps me up to date. I always carry my mobile phone with me; as it happens, I sometimes do not check my e-mails for a day or two. It would be a pity if I missed a top event for that reason!



Words to help you:

sweepstake – Gewinnspiel | store card – Kundenkarte | bargain – Schnäppchen



The mobile phone – producer of data

Traffic data



Master data



Location data



Content data





Mobile daily record

In Austria owners of mobile phones between the age of 14 and 27 send approx. 15 text messages and make phone calls for 37.5 minutes per day. This way quite a lot of traffic data and location data is created. What about you? Do you always carry your mobile phone with you, like 80% of all owners of mobile phones in Austria? Even more so, what traffic data and location data do you create on an average day?

Enter every call you make and every message you send in one day into the table below.

Explanation: „In“ means „incoming calls and/or messages“ you receive, „out“ means „outgoing calls and messages“ you make/send.

[illegible]

The right connection?

Connect the correct phrases!

If somebody knows whom you call

A person who knows the time when you use your mobile phone

The frequency and duration of your phone calls

Your whereabouts during the day

The traffic data and location data of your mobile phone

can be seen from the location data of your mobile phone.

he can get an idea of your contacts and friends.

do not tell anything about the contents of your calls or messages.

also knows about your daily routine.

shows how important that person is to you.

Free access? The legal situation

The Austrian Telecommunications Act [Telekommunikationsgesetz] regulates which data a telecommunications provider may store and how such data may be used.

Stammdaten

§ 97. (1) Stammdaten dürfen von Anbietern nur für folgende Zwecke ermittelt und verwendet werden:

1. Abschluss, Durchführung, Änderung oder Beendigung des Vertrages mit dem Teilnehmer;
2. Verrechnung der Entgelte;
3. Erstellung von Teilnehmerverzeichnissen und
4. Erteilung von Auskünften an Notrufträger.

(2) Stammdaten sind spätestens nach Beendigung der vertraglichen Beziehungen mit dem Teilnehmer vom Betreiber zu löschen. Ausnahmen sind nur soweit zulässig, als diese Daten noch benötigt werden, um Entgelte zu verrechnen oder einzubringen, Beschwerden zu bearbeiten oder sonstige gesetzliche Verpflichtungen zu erfüllen.

Auskünfte an Betreiber von Notrufdiensten

§ 98. (1) Betreiber eines Kommunikationsnetzes oder -dienstes haben Betreibern von Notrufdiensten auf deren Verlangen Auskünfte über Stammdaten sowie über Standortdaten zu erteilen. In beiden Fällen ist Voraussetzung für die Zulässigkeit der Übermittlung ein Notfall, der nur durch Bekanntgabe dieser Informationen abgewehrt werden kann. Die Notwendigkeit der Informationsübermittlung ist vom Betreiber des Notrufdienstes zu dokumentieren und dem Betreiber unverzüglich, spätestens jedoch innerhalb von 24 Stunden nachzureichen. Der Betreiber darf die Übermittlung nicht von der vorherigen Darlegung der Notwendigkeit abhängig machen. Den Betreiber des Notrufdienstes trifft die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegrens.

(2) Ist eine aktuelle Standortfeststellung nicht möglich, darf die Standortkennung (Cell-ID) zum letzten Kommunikationsvorgang der Endeinrichtung des gefährdeten Menschen verarbeitet werden, auch wenn hierfür ein Zugriff auf gemäß § 102a Abs. 3 Z 6 lit. d gespeicherte Vorratsdaten erforderlich ist. Der Anbieter hat den betroffenen Teilnehmer über eine Auskunft über Standortdaten nach dieser Ziffer frühestens nach 48 Stunden, jedoch spätestens nach 30 Tagen grundsätzlich durch Versand einer Kurzmitteilung (SMS), wenn dies nicht möglich ist schriftlich, zu informieren. Diese Information hat zu enthalten:

- a) die Rechtsgrundlage,
- b) die betroffenen Daten,
- c) das Datum und die Uhrzeit der Abfrage,
- d) Angabe der Stelle, von der die Standortfeststellung in Auftrag gegeben wurde, sowie eine entsprechende Kontaktinformation.

Verkehrsdaten

§ 99. (1) Verkehrsdaten dürfen außer in den in diesem Gesetz geregelten Fällen nicht gespeichert oder übermittelt werden und sind vom Anbieter nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren. [...]

(2) Sofern dies für Zwecke der Verrechnung von Endkunden- oder Vorleistungsentgelten erforderlich ist, hat der Betreiber eines öffentlichen Kommunikationsnetzes oder -dienstes Verkehrsdaten zu speichern. Die Verkehrsdaten sind zu löschen oder zu anonymisieren, sobald der Bezahlvorgang durchgeführt wurde und innerhalb einer Frist von drei Monaten die Entgelte nicht schriftlich beansprucht wurden. Die Daten sind jedoch nicht zu löschen, wenn

1. ein fristgerechter Einspruch erhoben wurde, bis zum Ablauf jener Frist, innerhalb derer die Abrechnung rechtlich angefochten werden kann.
2. die Rechnung nicht beglichen wurde, bis zum Ablauf jener Frist, bis zu der der Anspruch auf Zahlung geltend gemacht werden kann, oder
3. ein Verfahren über die Höhe der Entgelte eingeleitet wurde, bis zur endgültigen Entscheidung. [...]

(4) Dem Anbieter ist es außer in den in diesem Gesetz besonders geregelten Fällen untersagt, einen Teilnehmeranschluss über die Zwecke der Verrechnung hinaus nach den von diesem Anschluss aus angerufenen Teilnehmernummern auszuwerten. Mit Zustimmung des Teilnehmers darf der Anbieter die Daten zur Vermarktung für Zwecke der eigenen Telekommunikationsdienste oder für die Bereitstellung von Diensten mit Zusatznutzen verwenden.

Inhaltsdaten

§ 101. (1) Inhaltsdaten dürfen - sofern die Speicherung nicht einen wesentlichen Bestandteil des Kommunikationsdienstes darstellt - grundsätzlich nicht gespeichert werden. Sofern aus technischen Gründen eine kurzfristige Speicherung erforderlich ist, hat der Anbieter nach Wegfall dieser Gründe die gespeicherten Daten unverzüglich zu löschen.

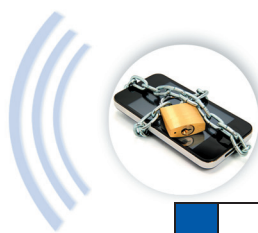
Free access?

Decide whether the statements are true or false. Add the correct statement if you decide that the statement is „false“.

	true	false	correct statement
If an emergency service receives an emergency call, the location data of the phone from which the call was made must be advised immediately thereafter.			
Content data may be stored for accounting purposes.			
Content data may be stored only if they are a material component of a communication service.			
If an accident can be prevented only because the location data of a certain person and/or of his/her phone are known, such data may be passed on to emergency services.			
Master data may be sold to other enterprises for advertising purposes.			
Master data may be used also after termination of a contract in order to send advertisements.			
In emergency cases master data may be passed on to emergency services.			
Master data may be used to prepare a bill.			
Telecommunications providers may pass on master data and location data only to emergency services after they have received a written documentation of the necessity of such a transfer.			
Traffic data may be stored for accounting purposes.			
Traffic data must be deleted after three months, even if bills are still outstanding.			
If an accident can be prevented only because the content data of a certain person and/or of a phone are known, such data may be passed on to emergency services.			

Words to help you:
accounting purposes – Rechnungszweck

Free access?



© babimu - Fotolia.com

Smart & Safe

	true	false	correct statement
If an emergency service receives an emergency call, the location data of the phone from which the call was made always must be advised immediately thereafter.		X	The location data must be advised if the caller can not tell and the data are necessary to ensure help.
Content data may be stored for accounting purposes.		X	Content data must not be saved.
Content data may be stored only if they are a material component of a communication service.	X		
If an accident can be prevented only because the location data of a certain person and/or of his/her phone are known, such data may be passed on to emergency services.	X		
Master data may be sold to other enterprises for advertising purposes.		X	Master data must not be sold to other enterprises.
Master data may be used also after termination of a contract in order to send advertisements.		X	Master data must not be used after termination of a contract in order to send advertisements.
In emergency cases master data may be passed on to emergency services.	X		
Master data may be used to prepare a bill.	X		
Telecommunications providers may pass on master data and location data only to emergency services after they have received a written documentation of the necessity of such a transfer.		X	Telecommunications providers may pass on master data and location data to emergency services. A written documentation of the necessity must be supplemented within twenty-four hours.
Traffic data may be stored for accounting purposes.	X		
Traffic data must be deleted after three months, even if bills are still outstanding.		X	If bills are outstanding, traffic data concerning these bills, can be stored.
If an accident can be prevented only because the content data of a certain person and/or of a phone are known, such data may be passed on to emergency services.		X	Even if an accident can be prevented only because the content data of a certain person and/or of a phone are known, such data must not be passed on to emergency services.

Big Brother?



On 1 April 2012 retention of data became the law in Austria. Providers of public communications services now have to store certain data generated when their customers use mobile phones, land-line phones, e-mail and the internet for a period of six months.

Storage of such data serves the exclusive purpose of investigating, ascertaining and prosecuting crimes that are subject to punishment by imprisonment for more than one year.

A reasoned request by the public prosecutor or by the criminal police is sufficient for an inquiry of master data; an independent public prosecutor must give his consent to such a request. Justice and the police in principle need the approval of a court to access traffic data. In cases of imminent danger such approval need not be obtained. Every inquiry of retained data must be reported to a person responsible for legal protection.

Since 1 April 2012 mobile radio providers must store the following data for six months:

- subscriber number or other ID of the calling terminal and of the called terminal.
- in the case of additional services such as call forwarding or call redirection the subscriber number to which the call is forwarded/redirected.
- name and address of the caller and of the person called.
- date, time of commencement and duration of a communication stating the underlying time zone.
- the nature of the service used (calls, additional services, messaging services and multimedia services).
- International Mobile Subscriber Identity (IMSI) of the calling terminal and of the called terminal.
- International Mobile Equipment Identity (IMEI) of the calling terminal and of the called terminal.
- date and time of first activation of the service and the location ID (cell ID) at which the service was activated, if pre-paid anonymous services are concerned.
- the location ID (cell ID) at the beginning of a connection.

The contents of calls and messages as well as data on addresses visited on the internet still must not be stored.

1. Which data is stored within the scope of retention of data?

☐ Content data

☐ Master data

☐ Location data

☐ Traffic data

2. For how long must such data be stored?

.....

3. For how long may such data be stored?

.....

4. Why is such data stored?

.....

5. How can it be ensured that retained data is not misused?

.....

.....

Words to help you:

retention of data – *Vorratsdatenspeicherung* | to ascertain – *ermitteln* | to prosecute – *gerichtlich verfolgen* | public prosecutor – *Staatsanwalt*
 consent – *Zustimmung* | approval of court – *richterliche Zustimmung* | legal protection – *Rechtsschutz* | subscriber number – *Teilnehmernummer*
 call forwarding – *Rufweiterleitung* | call redirection – *Rufumleitung* | commencement – *Beginn*





Pros & Cons



Collect arguments in favour of and against the retention of data: what are the advantages, what disadvantages may arise?

+	-



Know how!

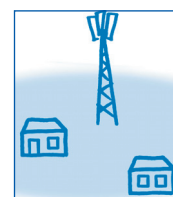


Locating mobile phones via radio cells

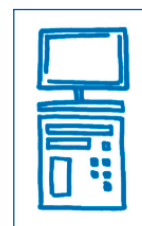
Many **individual mobile radio stations**, each of which is equipped with a mobile radio antenna, ensure that you can be reached everywhere on your mobile phone. For your mobile phone regularly contacts the nearest mobile radio antenna by means of **radio waves**. The phone „informs“ the radio station that it is still within its range. Even if you make no calls and send no text messages.



So every mobile radio station knows which mobile phones are turned on within its range. This area which provides every mobile radio station with reception is also called a **radio cell**.



The individual radio stations are connected with a central **radio switching station** via point-to-point radio or cable. This central switching computer knows the locations of all mobile phones that are turned on and forwards data from one radio cell to another and also to a different telephone network.



Thus your mobile phone and/or the radio cell in which your mobile phone is located can be found within a few seconds.

Radio cells differ in size. In urban areas with a high number of mobile radio subscribers and a high density of buildings there are many small radio cells. This guarantees a good quality of the network and mobile radio stations and the mobile phone can work with the lowest possible transmission power. In rural areas with a low number of mobile radio subscribers and many unbuilt areas there are larger radio cells.



*Does the size of a radio cell affect the result of locating mobile phones?
If so – why and in what form?*

.....

.....

.....

.....

.....

Words to help you:

mobile radio station – *Mobilfunkstation* | radio wave – *Funkwelle* | radio cell – *Funkzelle* | radio switching station – *Funkvermittlungsstation*
point-to-point radio – *Richtfunk* | subscriber – *Teilnehmer*



Calculation examples on the size of radio cells

Every dot on the map symbolises a mobile radio station which constitutes the centre of a radio cell.

Calculate for each map, ● how many sq.m and/or sq.km of area are shown on the relevant map section.

● how many sq.m and/or sq.km of area an average radio cell in that map section has.

Map 1 (○ = radio antenna, Scale 1:10.000)

The map section shows an area of sq.m,

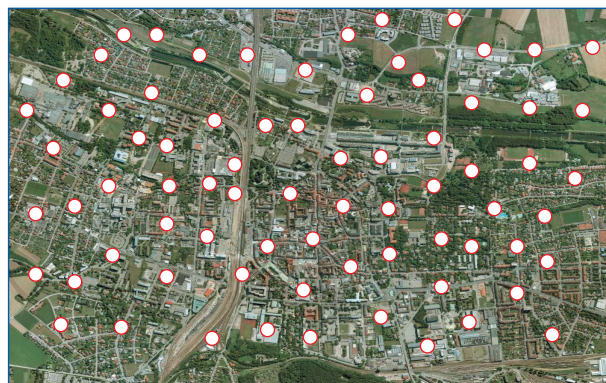
this corresponds to sq.km.

There are mobile radio stations in the area shown on the map.

One radio cell has an average area of sq.m,

this corresponds to sq.km..

The map shows ☐ rural area. ☐ urban area. ☐ metropolitan area.



Map 2 (○ = radio antenna, Scale 1:65.000)

The map section shows an area of sq.m,

this corresponds to sq.km.

There are mobile radio stations in the area shown on the map.

One radio cell has an average area of sq.m,

this corresponds to sq.km..

The map shows ☐ rural area. ☐ urban area. ☐ metropolitan area.



Map 3 (○ = radio antenna, Scale 1:240.000)

The map section shows an area of sq.m,

this corresponds to sq.km.

There are mobile radio stations in the area shown on the map.

One radio cell has an average area of sq.m,

this corresponds to sq.km..

The map shows ☐ rural area. ☐ urban area. ☐ metropolitan area.



Locating mobile phones via satellite

A **satellite system** consists of

- **satellites** which orbit the Earth and send electromagnetic signals at the speed of light, and
- **receiving stations** on the Earth which receive and evaluate those signals.

The systems can fulfil different tasks; for example, there are weather satellites that monitor the Earth and collect data that can be used for weather forecasts; television satellites broadcast television programmes. Every satellite system is sending on different radio frequencies.

How is navigation done?

Every **navigation satellite** regularly sends its coordinates down to the Earth: its name, position and the time the signal is sent.

The recipient of this signal can calculate its own **distance** to the satellite from the time it takes to transmit the signal, the so-called **signal transit time**.

If the receiver receives signals from several navigation satellites, it can not only determine its distance to those satellites but also its position on the Earth.



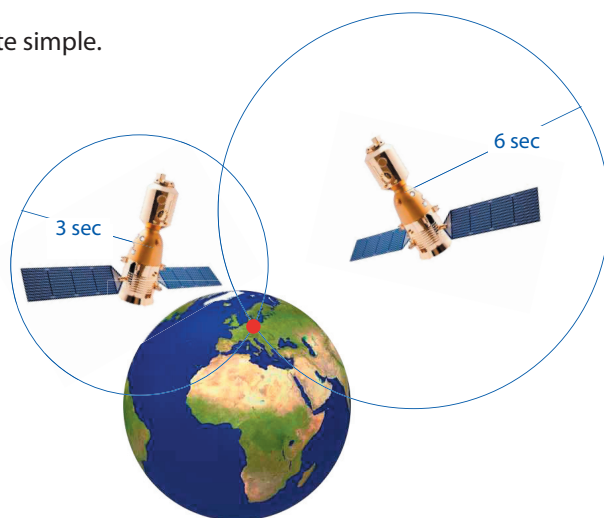
Max does not know where to go: he is lost and there is no one around whom he could ask where he actually is.

Sounds hopeless – thanks to help from space the solution is quite simple.

Max only needs to turn on his GPS mobile phone. This mobile phone sends on the same frequency like news satellites and therefore automatically receives their signals.

After a short period messages from two navigation satellites are received: One from satellite Brisk which is six seconds away from Max and one from satellite Swift with three seconds distance.

After Brisk and Swift have announced their exact position and after their distance to Max has become clear thanks to the signal transit time, Max's location can be determined easily. If you imagine a circle around each satellite the radius of which is the distance between the satellites and Max, Max is located at the intersection of those two circles on the Earth.



What is the advantage of locating mobile phones via satellite as compared to locating via radio cells?

.....

.....

Can the mobile phone transmit Max' location to third parties without mobile reception?

.....

.....

Words to help you:

signal transit time – Signallaufzeit | intersection – Schnittpunkt



Smart & Safe

Know how!

Lost and found



Navigation



Emergencies



Protective functions



Sightseeing & Shopping



Social networks



Prosecution of crimes



Once upon a time ...



Story 1: Nobody's perfect!

The plot: Luke and Matthew get caught by their parents when skipping school, because the locating function of their mobile phones has been activated.

The twins Luke and Matthew are real sports cracks. No matter whether in Summer or Winter - the two of them are absolutely unstoppable. They are very fond of snowboarding. Last Christmas they even got smartphones from their parents on which a safety programme is installed which allows to locate them at any time. The purpose

was not to monitor them but that they could have fun on the slopes alone and that, in case of an emergency, aid could be sent to them quickly.

At the moment, however, Luke and Matthew have anything but a case of emergency on their mind. Actually they think of a case of school-skipping due to Spring. Spring has finally arrived and the day is far too nice to spend it at school.



Story 2: Burglary made easy

The plot: While Elias is on holiday with his family, burglars enter their flat. Eventually it turns out that the burglars knew that the family would be on holiday due to Elias's social network profile.

Elias is very fond of Facebook and Twitter. He regularly posts new photos with his smartphone and informs his many friends, of whom he only knows a few personally, about everything they had always wanted to know about him. He uses all the possibilities that Facebook and Twitter offer, also Facebook Places: every time he changes his profile his location is posted beside his profile.

Of course, he does not leave his new cool smartphone at home during the family holiday. He documents every tiny detail of the activities of the Wallner family far down in the South.

All safe?

This text is about security risks that may lure when mobile phones are used too carelessly. Unfortunately a virus has sneaked in and has caused some chaos. Can you match the correct terms with the descriptions of risks?

apps

malware

Bluetooth and infrared interfaces

wifi networks

Thanks to the development of mobile phones our life has become far more easier and more amusing. We can do a lot more with a mobile phone than make phone calls! Unfortunately, this increase in possibilities of use has led to an increase in security risks. However, those who are familiar with those risks and know how to protect their data against misuse can use the full range of functionalities of modern mobile phones.

One potential security lapse are They enable not only an easy exchange of data but also are a door into your mobile phone. If you do not close this door after the guests you expected have arrived it may soon happen that unwanted intruders stand right in the middle of your flat, i.e. access your mobile phone. And this may happen without you knowing it at once. As we know, open doors usually do not creak...

However, free..... can be dangerous. You can use them to surf on the internet for free; however, clever criminals with some technical expertise can follow every step you take on the internet. Therefore you should rather be double careful in using passwords, going online shopping or making your banking transactions if you use this free possibility to access the internet. Otherwise the free web can be rather expensive.

Smartphones are about to take the lead. An increasing number of customers chooses one of the new clever mobile phones which in many areas already replace the PC or notebook. Therefore this „target group“ becomes more and more interesting for programmers who dedicate their work to the production of so-called Although there are still very little known viruses, worms and Trojans that attack mobile phones, experts expect this number to increase significantly in the next years. As the saying goes: „The bigger the market, the greater the variety of offers!“

Finally, one must also consider the highly acclaimed and popular as a security risk. You have got time for a quick game, are looking for the next bus or tram stop, quickly need a water level or want to make a quick price check before you proceed to the cashier's desk? No problem! Nowadays these small programmes offer a mobile solution for almost every question. However, those who act too carelessly when installing those mini programmes might place a little spy into their mobile phone themselves. For some programmes access areas of the phone which actually should be off limits for them and transmit data to the programme manufacturer that are and should continue to be private.

All safe?

This text is about security risks that may lure when mobile phones are used too carelessly. Unfortunately a virus has sneaked in and has caused some chaos. Can you match the correct terms with the descriptions of risks and complete the text with the right verbs?



apps

Bluetooth and infrared interfaces

malware

wifi networks

Thanks to the development of mobile phones our life has far more easier and more amusing. We can do a lot more with a mobile phone than make phone calls!

Unfortunately, this increase in possibilities of use has to an increase in security risks. However, those who familiar with those risks and know how to their data against misuse can the full range of functionalities of modern mobile phones.

One potential security lapse are

They not only an easy exchange of data but also are a door into your mobile phone. If you do not this door after the guests you expected have it may soon happen that unwanted intruders stand right in the middle of your flat, i.e. access your mobile phone. And this may happen without you knowing it at once. As we know, open doors usually do not

However, free can be dangerous. You can use them to surf on the internet for free; however, clever criminals with some technical expertise can every step you take on the internet. Therefore you should rather double careful in using passwords, going online shopping or your banking transactions if you use this free possibility to access the internet. Otherwise the free web can be rather expensive.

are
arrived
be
become
chooses
close
creak
dedicate
enable
follow
increase
installing
led
making
offer
protect
transmit
use



Smartphones are about to take the lead. An increasing number of customers one of the new clever mobile phones which in many areas already replace the PC or notebook. Therefore this „target group“ becomes more and more interesting for programmers who their work to the production of so-called Although there are still very little known viruses, worms and Trojans that attack mobile phones, experts expect this number to significantly in the next years. As the saying goes: „The bigger the market, the greater the variety of offers!“

Finally, one must also consider the highly acclaimed and popular as a security risk.

You have got time for a quick game, are looking for the next bus or tram stop, quickly need a water level or want to make a quick price check before you proceed to the cashier's desk?

No problem! Nowadays these small programmes
..... a mobile solution for almost every question. However, those who act too carelessly when those mini programmes might place a little spy into their mobile phone themselves. For some programmes access areas of the phone which actually should be off limits for them anddata to the programme manufacturer that are and should continue to be private.





Lots of verbs ...



Fill in the correct form of the verb and translate into German!

	infinitive	Perfect tense	Past tense	German translation
are	be	I have been	I was	sein
arrived		she	she	
be		they	they	
become		you	you	
chooses		he	he	
close		I	I	
creak		it	it	
dedicate		I	I	
enable		you	you	
follow		they	they	
increase		it	it	
installing		I	I	
led		it	it	
making		you	you	
offer		we	we	
protect		she	she	
transmit		you	you	
use		I	I	



Questions on understanding

What functions do modern mobile phones offer? What can you use them for?

What are Bluetooth and infrared interfaces in mobile phones used for?

Have you ever used one of those interfaces? If so, what for?

What possibilities do free wifi networks offer?

Have you ever used a free wifi network?

☐ Yes

☐ No

What should be considered when using free wifi networks?

What threats can be summarised under the term „malware“?

What should you consider when installing an app?



Lots of verbs ...

	infinitive	Perfect tense	Past tense	German translation
are	to be	I have been	I was	sein
arrived	to arrive	she has arrived	she arrived	ankommen
be	to be	they have been	they were	sein
become	to become	you have become	you become	werden
chooses	to choose	he has chosen	he chose	wählen
close	to close	I have closed	I closed	schließen
creak	to creak	it has creaked	it creaked	knarren
dedicate	to dedicate	I have dedicated	I dedicated	widmen
enable	to enable	you have enabled	you enabled	können
follow	to follow	they have followed	they followed	folgen
increase	to increase	it has increased	it increased	ansteigen
installing	to install	I have installed	I installed	installieren
led	to lead	it has led	it led	führen
making	to make	you have made	you made	machen
offer	to offer	we have offered	we offered	anbieten
protect	to protect	she has protected	she protected	schützen
transmit	to transmit	you have transmitted	you transmitted	übermitteln
use	to use	I have used	I used	gebrauchen



Mobile phone security: What are the risks?

June 17, 2011 | By Amy Gahran, Special to CNN

The more people rely on cell phones and tablets, the more attractive these devices become as targets to thieves and other nefarious types.

Fortunately, protecting yourself against mobile security risks doesn't require getting paranoid about your phone. Rather, it's about maintaining good habits, watching for red flags and deciding whether you need mobile security tools or services.

At a recent mobile security conference in San Francisco, staffers from digital security provider Norton outlined some common current mobile threats:

Malware

This is an app contaminated with malicious code that makes your phone do things it shouldn't -- such as steal your personal data. While no smartphone platform is immune from malware, so far Android apps appear to present the greatest malware risk. This is because of the openness of this platform and Google's Android market.

This week, The Register reported on the latest rash of Android malware and noted that Google has admitted that „more than 90 percent of Android users are running older versions of the mobile operating system that contain serious kernel vulnerabilities. That gives attackers an easy way to bypass Android's security sandbox, which is supposed to limit the data and

resources each app is allowed to access.”

At the Norton conference, a presenter demonstrated how quick and easy it is to „trojanize” an Android app. He downloaded an existing legitimate app from the Android Market, viewed the source code, copied in some malicious code, renamed the app and uploaded the now-malware to the market -- all in about three minutes.

Mobile security tools such as Lookout or Norton Mobile Security (in beta) can help guard against Android malware by scanning apps and other programs and data on your phone.

However, the best way to protect yourself against malware is to read the list of permissions that an Android app requests before you install it. Does that list make sense? For instance, does a game really need to be able to send premium text messages or access your contact list?

It helps to understand what each of the available Android permissions mean and to check the apps already on your phone to spot excessive permission requests. [...]

<http://edition.cnn.com/2011/TECH/mobile/06/17/mobile.security.gahran/index.html>



10 common mobile security problems to attack

By Michael Cooney, NetworkWorld

When it comes to security, most mobile devices are a target waiting to be attacked. That's pretty much the conclusion of a report to Congress on the status of the security of mobile devices this week by watchdogs at the Government Accountability Office. [...]

„Mobile devices face an array of threats that take advantage of numerous vulnerabilities commonly found in such devices. These vulnerabilities can be the result of inadequate technical controls, but they can also result from the poor security practices of consumers,” the GAO stated. „Private [companies] and relevant federal agencies have taken steps to improve the security of mobile devices, including making certain controls available for consumers to use if they wish and promulgating information about recommended mobile security practices. However, security controls are not always consistently implemented on mobile devices, and it is unclear whether consumers are aware of the importance of enabling security controls on their devices and adopting recommended practices.“ [...]

The GAO report came up with a list of mobile vulnerabilities it says are common to all mobile platforms and it offered a number of possible fixes for the weaknesses. From the report:

Mobile devices often do not have passwords enabled. Mobile devices often lack passwords to authenticate users and control access to data stored on the devices. Many devices have the technical capability to support passwords, personal identification numbers (PIN), or pattern screen locks for authentication. Some mobile devices also include a biometric reader to scan a fingerprint for authentication. However, anecdotal information indicates that consumers seldom employ these mechanisms. Additionally, if users do use a password or PIN they often choose passwords or PINs that can be easily determined or bypassed, such as 1234 or 0000. Without passwords or PINs to lock the device, there is increased risk that stolen or lost phones' information could be accessed by unauthorized users who could view sensitive information and misuse mobile devices. [...]

Wireless transmissions are not always encrypted. Information such as e-mails sent by a mobile device is usually not encrypted while in transit. In addition, many applications do not encrypt the data they transmit and receive over the network, making it easy for the data to be intercepted. For example, if an application is transmitting data over an unencrypted WiFi network using http (rather than secure http), the data can be easily intercepted. When a wireless transmission is not encrypted, data can be easily intercepted.

Mobile devices may contain malware. Consumers may download applications that contain malware. Consumers download malware unknowingly because it can be disguised as a game, security patch, utility, or other useful application. It is difficult for users to tell the difference between a legitimate application and one containing malware. For example, an application could be repackaged with malware and a consumer could inadvertently download it onto a mobile device. The data can be easily intercepted. When a wireless transmission is not encrypted, data can be easily intercepted by eavesdroppers, who may gain unauthorized access to sensitive information.

Mobile devices often do not use security software. Many mobile devices do not come preinstalled with security software to protect against malicious applications, spyware, and malware-based attacks. Further, users do not always install security software, in part because mobile devices often do not come preloaded with such software. While such software may slow operations and affect battery life on some mobile devices, without it, the risk may be increased that an attacker could successfully distribute malware such as viruses, Trojans, spyware, and spam to lure users into revealing passwords or other confidential information.

Operating systems may be out-of-date. Security patches or fixes for mobile devices' operating systems are not always installed on mobile devices in a timely manner. It can take weeks to months before security updates are provided to consumers' devices. Depending on the nature of the vulnerability, the patching process may be complex and involve many parties. [...]

The GAO report went on to state that connecting to an unsecured WiFi network could let an attacker access personal information from a device, putting users at risk for data and identity theft. One type of attack that exploits the WiFi network is known as man-in-the-middle, where an attacker inserts himself in the middle of the communication stream and steals information. Communication channels may be poorly secured. Having communication channels, such as Bluetooth communications, „open“ or in „discovery“ mode (which allows the device to be seen by other Bluetooth-enabled devices so that connections can be made) could allow an attacker to install malware through that connection, or surreptitiously activate a microphone or camera to eavesdrop on the user. In addition, using unsecured public wireless Internet networks or WiFi spots could allow an attacker to connect to the device and view sensitive information.

<http://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html>

Wireless LAN Security Risks

By Alan Hughes, eHow Contributor

Wireless networks are relatively easy and inexpensive to set up today. In addition to many businesses that have installed wireless LANs, many people have installed wireless LANs in their homes and enjoy the benefits of connecting without cables. Unfortunately, the ease of wireless LAN and the nature of wireless technology may leave many users in homes and businesses with a network that is not secured, exposing their personal and business information to a drive-by cyber criminal.

War Drivers

"War driving" is a term that describes driving around looking for wireless networks. These cyber crooks drive through neighborhoods or business areas using their laptops to look for wireless network signals. When they find a network that is not secured, they attempt to hop on the connection. Once on the network, they target vulnerable computers and hack into them if at all possible or just passively "sniff" the network traffic looking for valuable information. One solution to this problem is to enable one of the wireless security methods on the wireless access point. WEP (wired equivalency protocol) is the easiest to enable and should be activated and configured to achieve at least minimal security.

Rogue Access Points

A particular problem in businesses is the deployment of rogue access points. Someone in a department may want to set up a wireless network in the office similar to what they have at home. If they are unwilling to wait for the information technology (IT) department to set one up, or worse, if they are unwilling to contact the IT department at all, such an installation may open the

business up to network hacking. This is especially true if they do not activate any security protocols, such as WEP or WPA. Every business should have network monitoring tools in place to detect rogue access points

Man-in-the-Middle Attacks

Wireless hot spots are very popular and many restaurants offer free Internet access via their wireless network. Unfortunately cyber criminals also frequent these establishments. By setting up a wireless network ID that looks like what a customer might be expecting, they lure the unsuspecting victim into connecting to their "network." From that point the interceptor just forwards the network requests on to legitimate destinations while rummaging through the victim's laptop and stealing vital personal information. It is best to be alert when frequenting such a place, and be aware of any suspicious activity. Also be sure to connect to the business's valid network ID.

Jamming

Jamming occurs when a signal stronger than the signal produced by a wireless access point (WAP) is disrupted. This can be done deliberately by someone with bad intentions, or it can happen inadvertently if other wireless devices nearby interfere with the WAP's signal. Baby monitors, cordless phones and cell phones are all capable of "jamming" the signal of a wireless access point. Whether intentional or unintentional, jamming disrupts the wireless network and interferes with its proper operation.

www.ehow.com/list_6684310_wireless-lan-security-risks.html

Mobile phone security

Attacks on Bluetooth-enabled devices can take place within a distance of 10 metres or more. [...]

As many as three-quarters of mobile phone users are not aware of the internet security risks linked to Bluetooth-equipped devices. These risks come in four main guises:

- Bluejacking is when anonymous text messages are sent to mobile phones
- Bluespamming is when a phone's contacts are secretly sent text messages
- Bluesnarfing is when hackers gain access to a mobile phone's contacts
- Bluebugging is when hackers have access to a handset's commands

While each of these risks is a nuisance, bluesnarfing and bluebugging are particularly serious. With bluesnarfing, hackers can gain access to stored data, such as a phonebook, calendar or to clone a phone.

Bluebugging, on the other hand allows hackers to

make phone calls from the mobile phone they control. They can write messages and send them from the phone and they can even eavesdrop on private conversations. [...]

As with any mobile device, there are important precautions you can take to protect yourself against Bluetooth security breaches on a mobile phone:

- Always disable Bluetooth functionality on your phone when it's not in use
- Protect your phone with mobile antivirus software

By simply turning off Bluetooth, hackers are unable to mount your handset's commands or access the information on your Bluetooth-enabled mobile phone.

www.kaspersky.com/threats/bluetooth-risks



Hit the nail on the head?



Text

Rating according to the school grades system: 1 = very good, 5 = failed.

	apps	Bluetooth	wifi networks	malware
The title is meaningful.				
The introduction makes you read more.				
The description of risks - is correct. - is comprehensible. - is suitable for people older than 70.				
Security advice - is correct. - is comprehensible. - is suitable for people older than 70.				

Image

If graphical elements were used they are valued according to the school grades system.

	apps	Bluetooth	wifi networks	malware
How well do the graphical elements support the message(s) of the text?				
Are they suitable for the target group?				

The target group

Is the information leaflet suitable for aged people older than 70?

	very good	good	acceptable	sufficient	insufficient
apps					
Bluetooth					
wifi networks					
malware					



What was especially well done in the adaptation for the target group?

apps	
Bluetooth	
wifi networks	
malware	

What should be changed in order to better reach the target group?

apps	
Bluetooth	
wifi networks	
malware	

Overall valuation

How well is the information leaflet suited to make aged people older than 70 fit for using mobile phones?

	very good	good	accept- able	sufficient	insuffi- cient
apps					
Bluetooth					
wifi networks					
malware					

Did we manage not to raise fears but to convey competence and security in using mobile phones?

	very good	good	accept- able	sufficient	insuffi- cient
apps					
Bluetooth					
wifi networks					
malware					



Erased and deleted forever?

You got a new smartphone as a birthday present and now generously give your old phone to your little sister. However, you only want to give her your phone, but not your contacts, photos, texts and multimedia messages.



What to do? In what order do you take the following steps? Put the sentences in the correct order!



I remove the SIM card and any additional memory cards.



If a factory reset is not possible I use an app to finally delete the phone memory.



Now my little sister can be happy and can revive my old mobile phone with loads of fresh data!



If a factory reset is possible for my mobile phone, I choose this method. This way I can be sure that my personal data cannot be restored.



Then I check the user manual of my phone for how to finally delete my personal data.



Thereby must consider that there are three different memories: the SIM card, the internal phone memory and additional memory cards.



First I make a backup of all data I do not want to lose.





Erased and deleted forever?

1

First I make a backup of all data I do not want to lose.



2

Thereby must consider that there are three different memories: the SIM card, the internal phone memory and additional memory cards.



3

Then I check the user manual of my phone for how to finally delete my personal data.



4

If a factory reset is possible for my mobile phone, I choose this method. This way I can be sure that my personal data cannot be restored.



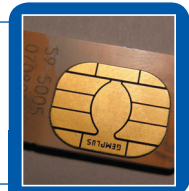
5

If a factory reset is not possible I use an app to finally delete the phone memory.



6

I remove the SIM card and any additional memory cards.



7

Now my little sister can be happy and can revive my old mobile phone with loads of fresh data!





Help! My mobile phone is gone!

You have looked for it everywhere, have tried to call yourself but it still has not turned up? This does not happen to you alone. Around 80 mobile phones are stolen in Austria every day, others are misplaced or simply lost.

Mobile phone is gone? Have the SIM card blocked!

No matter whether it was stolen or whether you just lost it: in order to keep the damage as low as possible you should have the SIM card blocked as soon as possible!

Why is it important to block the SIM card? What can you prevent by blocking it?

.....


.....

.....

All Austrian mobile radio providers offer hotlines for blocking mobile phones, in some cases you can enable blocking also via the internet.

Please note: non-registered pre-paid mobile phones cannot be blocked. Any remaining balance is lost together with the mobile phone. A remaining balance on registered pre-paid mobile phones will remain after the SIM card has been blocked and can be transferred to the new SIM card.

blocking hotlines



A1:	0800 / 664 100
Bob:	0900 / 680 680
Drei:	0800 / 30 30 30
eety:	0681 / 83083
Orange:	0699 / 70 699
tele.ring:	0820 / 650 650
Tele2mobil:	0800 / 240020
T-Mobile:	0676 / 2000
yesss!:	0820 / 810 810

May 2013

Stolen? Report the theft to the police!

If your mobile phone was stolen you should report the theft to the police in any case.

Every mobile phone has an **IMEI number**, i.e. a 15-digit serial number that is allocated only once and cannot be deleted. You can find it below the battery and on the original packaging of your mobile phone; moreover, you can retrieve it by entering the code *#06#. You should note down the IMEI number in any case and tell it to the police in the case of a theft. If the police find your mobile phone in the course of an investigation or if it is deposited at the lost and found office, it can be made clear whether it is your mobile phone or not thanks to the IMEI number, even if all your personal data has been deleted and your old SIM card has been removed.

A blessing in disguise: If you lose a mobile phone you lose not only lots of data – blocking and issue of a new SIM card as well as the purchase of a new mobile phone cost a lot of money. When you submit the theft report, some mobile radio providers charge you nothing for blocking the SIM card and issuing a new one.

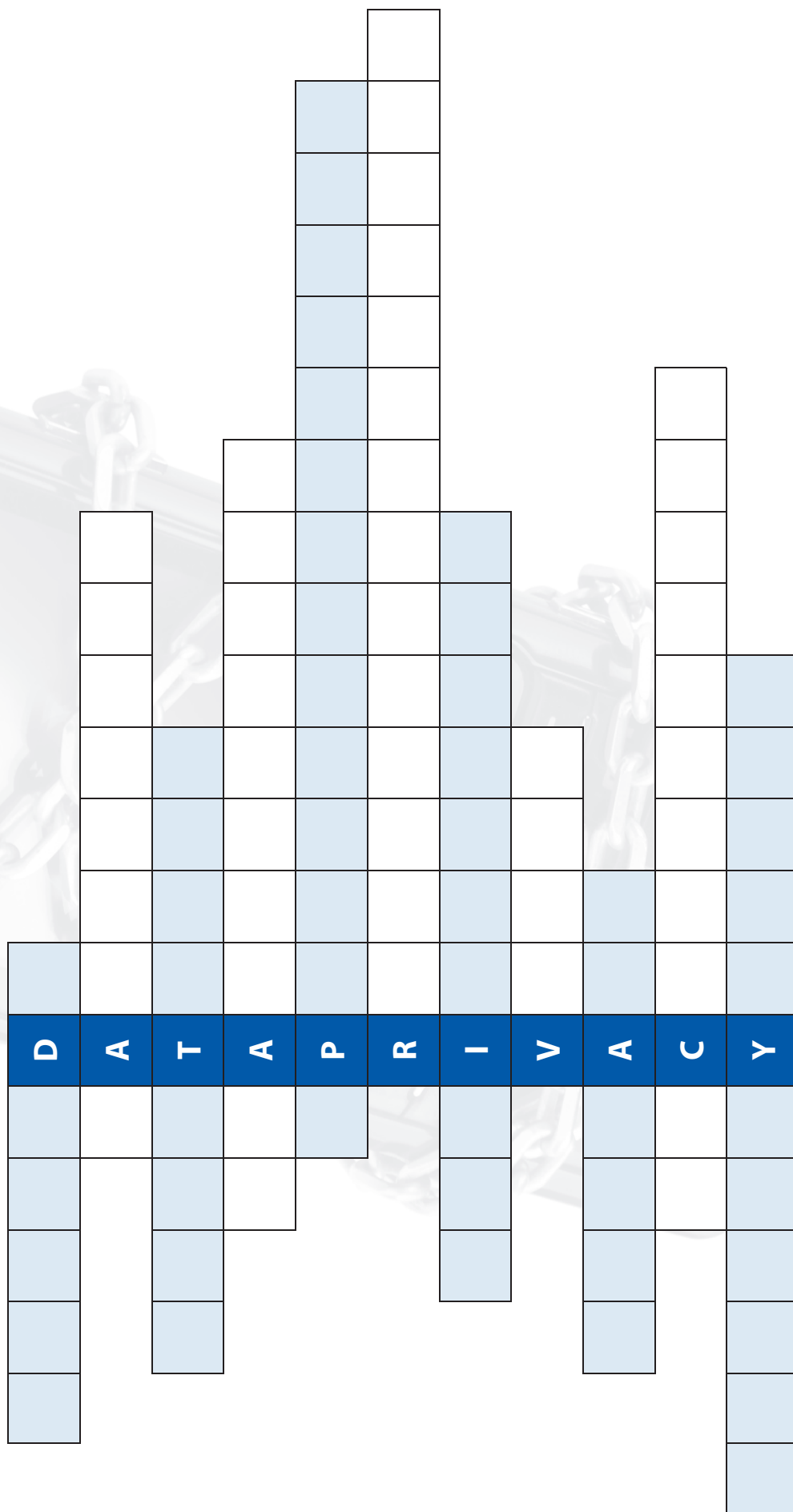
Words to help you:

to block – sperren | to require – anfordern, verlangen | balance – Gutschrift | to remain – (ver-)bleiben, bestehen bleiben |
to allocate – zuweisen, vergeben | to retrieve – abrufen | to issue – ausstellen



Smart & safe?

Try to match the right terms with the riddle!



- It provides the mobile phone not only with reception, but also helps to locate it.
- An April fool's joke? Not at all! This is no hoax, this is to fight crime. Therefore it has become law in Austria since 1 April 2012.
- Its name reflects its aim! It provides information about where a mobile phone is located.
- The name alone shows that this interface for data transmission via radio is by no means toothless: as regards data security it likes to show its teeth and makes naïve interface users sometimes look quite pale.
- The individual Member States are free to decide how to implement it in detail. However, if it is not implemented by a national law within the prescribed period, as it was the case in Austria with retention of data, the Member State in default is adjudicated.
- Sounds like an up-to-date service on traffic jams! Actually it provides information about when you were connected with whom via the mobile phone and for how long.
- If necessary, withdrawing this little chip from circulation protects you from further damage.
- In the past this was an issue especially with computers. Today it makes every smartphone a small PC. And as the smartest mobile phone does not work if it is defective, a special focus is laid thereon already when buying a mobile phone.
- It is no good, neither for you nor for your mobile phone! You both fall ill if you catch one.
- When typing it in you get certain information from your mobile phone. For example, if you type in *#06#, the IMEI number of your mobile phone is displayed which is unique and unmistakable.
- A brand-new mobile phone has them. And only them. If they are restored, everything else is deleted.



[illegible]

Smart & Safe

Be smart!



The following cases were part of the introduction into the topic of „data protection“. Now that you are a professional in mobile data protection, it is up to you: Create tips what to do to avoid the described risk!



An app with hidden possibilities

Paul S. was excited: thanks to a new app he was able to integrate his private photos into the film sets of recent blockbusters by pressing just one button! He had never ever sent as many multimedia messages like after he had installed this app. All his friends could admire themselves side by side with their movie heroes.

However, an unpleasant surprise was soon to come. What Paul S. did not know was that the app was far more powerful. And he himself had allowed the app and its operators to be so powerful. In order to be able to install the

app Paul S. had to give the app operators some authorisations, among other things access to his personal contacts and his call list. Data protectors now assume that such data was not only collected, but had also been passed on. And Paul S. now is afraid that he and his friends will in future receive loads of spam text messages and that his private photos may appear on any given websites.



Missed calls can be expensive ...

Sandra S. hardly could believe her eyes when she looked at her last mobile phone bill: she had been charged EUR 30 for calls to value-added service numbers which she just could not explain to herself! She calmed down and called the billing hotline of her mobile radio provider. Only when they asked for calls from unknown numbers she remembered the missed calls she had found on her mobile phone some time ago. She had always tried to call back but had only reached weird answering machine loops. Obviously she had called value-added services without noticing it! Her

contact at the hotline offered her to block her mobile phone for value-added service numbers.



Free app may be expensive ...

Last week Isabelle F., a student from Upper Austria, fell victim to a malicious attack of mobile phone hackers. Together with a free app she also received a free but unwanted Trojan which sent text messages to all her contacts without her noticing it. Only when her classmates asked her why she sent empty text messages she became suspicious. However, she found no empty text message in her outbox. Only when she called her mobile radio provider she learned that she had already exceeded the number of included free text messages and that approx. 300 text messages had

been sent from her mobile phone per day.



Hello, here I am!

Luke, Matthew and Jacob, three students from Deutschlandsberg, had planned everything very well. They started off on time in the morning and instead of going to school then went to the train station. They took the 8.05 train and went to Graz: they had planned to go shopping instead of attending school. They had even thought of changing their Facebook status several times during their little trip, always using similar phrases like: „I feel sooo sick“. Thanks to their new smartphones this was no problem at all. However, they had overlooked the fact that on their Facebook sites

they had activated the function to automatically detect their location and state it on their profile together with every new status message. So their status messages read „I feel sooo sick“; however, Graz and not their home town was stated as their location on all three profiles. So the three truants got caught very quickly thanks to their digital lead.



Alter ego

Florian E. was very happy with his new smartphone. He was so happy that he did not even think about his old mobile phone any more, which he had sold with profit. Until last Friday, when his colleague left the office and said: „Don't go too far, Loverboy85!“ Mr. E first looked puzzled; then, after he had asked several times, his colleague felt pity for him and explained what this „Loverboy“ thing was all about. He showed Mr. E the profile of a single man with the username „Loverboy85“ on a well-known online dating portal. And this profile was actually loaded with private

photos of Mr. E. Mr. E. made some research and found out that the buyer of his old smartphone had found the photos and had created a profile on the online portal „just for fun“!




Zeynep K. & the subscription

Zeynep K. always wanted a new ringtone. So she was thrilled when she found her favorite song for download as a ringtone in a new app. Was also quite easy: She only had to confirm „Buy“ and could download her new ringtone. The rude awakening came quickly, however. Because suddenly, the entire balance was used up on her prepaid card. With her click on „Buy“ she not only ordered one ringtone, but a full subscription.

Vocabulary

			
abbreviation	Abkürzung	misuse	Missbrauch
access	Zugriff	mobile phone	Handy
accounting purpose	Rechnungszweck	mobile radio provider	Mobilfunkbetreiber
additional service	Zusatzservice	mobile radio station	Mobilfunkstation
approval of a court	richterliche Genehmigung	operating system	Betriebssystem
area	Bereich	personal data	persönliche Daten
as a rule	aus Prinzip	phone memory	Telefonspeicher
backup	Sicherung	point-to-point radio	Richtfunk
balance	Gutschrift	public prosecutor	Staatsanwalt
bargain	Schnäppchen	radio cell	Funkzelle
battery	Akku	radio switching station	Funkvermittlungsstation
call	Anruf	radio wave	Funkwelle
call forwarding	Rufweiterleitung	reception	Empfang
call redirection	Rufumleitung	requirement	Anliegen
caller	Anrufer	retention of data	Vorratsdatenspeicherung
commencement	Beginn	satellite system	Satellitensystem
connection	Verbindung	secrecy	Geheimhaltung
consent	Zustimmung	security lapse	Sicherheitslücke
content data	Inhaltsdaten	security risk	Sicherheitsrisiko
contract	Vertrag	sensitive data	sensible Daten
corresponding receiver	Empfangsstation	signal transit time	Signallaufzeit
data deserving special protection	besonders schutzwürdige Daten	significance	Stellenwert, Bedeutung
data protection authority	Datenschutzbehörde	sky-rocketing	rasant ansteigend
data trace	Datenspur	space	Weltall
data traffic	Datenverkehr	storage place	Speicherplatz
data volume	Datenvolumen	store card	Kundenkarte
duration	Dauer	subscriber	Teilnehmer
emergency service	Notfalldienst	surveillance system	Aufsichtsstelle
EU Directive	EU Richtlinie	sweepstake	Gewinnspiel
exchange of data	Datenaustausch	technological impact assessment	Technikfolgenabschätzung
factory reset	Werkseinstellung	theft	Diebstahl
free home	frei Haus	to allocate	zuweisen, vergeben
frequency	Häufigkeit	to apply	zutreffen
intersection	Schnittpunkt	to ascertain	ermitteln
legal protection	Rechtsschutz	to avoid	vermeiden
master data	Stammdaten	to be aware of	sich einer Sache bewusst sein
message	Nachricht	to bear	in sich bergen

	
to block	sperren
to charge	verrechnen
to contribute to something	zu etwas beitragen
to create	produzieren
to delete	löschen
to determine	feststellen, bestimmen
to enter	eingeben, eintreten
to estimate	abschätzen, ermessen
to forward	weiterleiten, versenden
to fulfil	erfüllen
to grant	gewähren
to identify	identifizieren
to install	installieren
to issue	ausstellen
to locate	lokalisieren
to maintain	erhalten, wahren
to monitor	abhören, überwachen
to orbit	umkreisen
to prosecute	gerichtlich verfolgen
to provide	versorgen
to record	aufnehmen
to remain	(ver-)bleiben, bestehen bleiben
to remove	entfernen
to request	fordern
to require	anfordern, verlangen
to restore	wiederherstellen
to retrieve	abrufen
to state	angeben, erklären, behaupten
to stipulate	festlegen
to store	speichern
to take into account	berücksichtigen
to transmit	übertragen, senden
to turn on	einschalten
to weigh something	etwas abwägen
traffic data	Verkehrsdaten
Trojan	Trojaner
user manual	Gebrauchsanweisung
weather forecast	Wettervorhersage