Datenschutz geht alle an!

Erweiterung zum Kapitel „Konsumieren mit Köpfchen“, Schulbuch Seite. 60–61
und „Was haben Haushalte mit der Gesellschaft zu tun?“, Schulbuch Seite 80–81

KURZ ERKLÄRT
Daten – das neue Öl?
Warum?

Mit persönlichen Daten kann man zB:

- Wahrscheinlichkeiten für Erkrankungen errechnen;
- Rasterfahndungen erleichtern;
- Risiken bei Versicherungen abwägen;
- Kaufvorschläge machen („Du hast vorgestern jenes Kosmetikprodukt gekauft, aus diesem Grund wird dir ein ähnliches Produkt vorgeschlagen.“).

Der Schutz der Daten ist ein Menschenrecht!

Werden Daten zu Unrecht genutzt, hat jeder das Recht auf das Löschen der Daten.

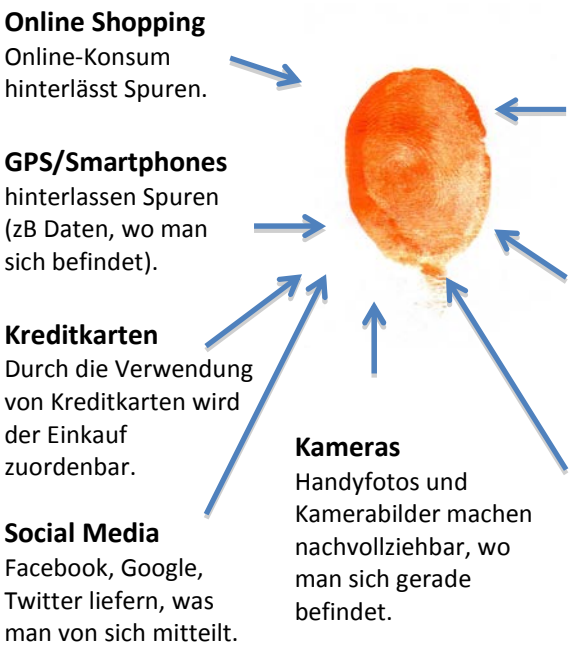
Sind Daten falsch, hat man das Recht auf eine Berichtigung.

Handy, Google, Gromsocial[1], Twitter, Facebook, Blogging – Plattformen, Tumblr ... Wer in sein will, ist dabei!

„Big Data“: das neue Schlagwort

Daten bezeichnet man heute als das „neue Öl“. Wer sie hat, wird reich, kann die Zukunft vorhersagen, vielleicht sogar verändern. Weil Daten so wertvoll geworden sind, ist die Gefahr des Datenmissbrauchs groß. Es braucht das Bewusstsein, sie zu schützen.

Unser digitaler Fingerabdruck



Online Shopping
Online-Konsum hinterlässt Spuren.

GPS/Smartphones
hinterlassen Spuren (zB Daten, wo man sich befindet).

Kreditkarten
Durch die Verwendung von Kreditkarten wird der Einkauf zuordenbar.

Social Media
Facebook, Google, Twitter liefern, was man von sich mitteilt.

Kameras
Handyfotos und Kamerabilder machen nachvollziehbar, wo man sich gerade befindet.

Kundenkarten
Bei jedem Einkauf im Supermarkt hinterlassen wir Spuren dank Bonus- und Kundenkarten.

Internet
Seitenaufrufe und Suchanfragen beim Surfen werden registriert.

Persönliche Daten
Gesundheitsakte, Versicherungspolizzen, Grundbucheinträge: Vieles bleibt nicht persönlich.

Welche Daten sind schützenswert?

Datenschutz müssen alle jene beachten, die Daten benutzen oder verarbeiten (Behörden, Betriebe, Schulen, Private).

Der Datenschutz bezieht sich auf

- die **Ermittlung** von Daten,
- die **Speicherung** von Daten,
- die **Auswertung** von Daten und
- die **Weitergabe** von Daten.

[1] *Groms* (sprich Grums) ist ein Sammelbegriff für Internetsurfer unter 15 Jahren.

Glaube nicht alles, das im Internet behauptet wird …

Wie erkennst du sichere Webseiten?

- Die Webadresse beginnt so: **https**
- Das Symbol **„Schloss“** ist das Zeichen für Sicherheit.

Kommt dir im Internet etwas komisch vor?

Hier kannst du dir Rat holen: **Rat auf Draht** unter der Telefonnummer **147** oder bei www.saferinternet.at.

Welche Daten müssen geschützt werden?

1. Personenbezogene Daten: Name, Adresse, Alter, E-Mail-Adresse, Passwörter, Kontodaten, Kontoauszüge.
2. Sensible Daten: Informationen aus Gesundheitsakten (Befunde), ethnische Herkunft, Versicherungspolizzen, körperliche Merkmale wie zB die Augenfarbe, Interessen, Gewohnheiten wie zB Einkaufsgewohnheiten.
Im Falle der Nutzung einer Kundenkarte oder der Bestellung im Internet mit den Angaben der persönlichen Daten stimmt man meist auch der Verarbeitung von persönlichen Daten zu („Ich stimme den Geschäftsbedingungen zu.“).

Warum sind sensible und personenbezogene Daten zu schützen?
Immer wieder hört man die Aussage: „Es ist mir egal, was man mit den Daten macht, ich habe ja nichts zu verbergen.“ Diese Aussage ist aber nur die halbe Wahrheit. Man muss sich nämlich vor allem fragen: **Was machen Andere mit meinen/unseren Daten?**

Sicher in sozialen Netzwerken

1. Achte auf deine Privatsphäre!
Bei den meisten sozialen Netzwerken kannst du dein Profil so einstellen, dass es wirklich nur deine Freunde sehen können und kein Fremder. Lass deine Dokumente nicht unbeaufsichtigt liegen oder kopieren.
2. Auch im Internet hat niemand etwas zu verschenken!
Lass Gratisangebote, die Name und Adresse abfragen, unbeachtet. Falle auch nicht auf eine Information hinein, dass du bei einem Gewinnspiel gewonnen hast, ohne dass du je mitgemacht hast. Nichts ist umsonst.
3. Sei vorsichtig so genannten Freunden gegenüber!
Nicht jeder, der mit dir befreundet sein will, hat gute Absichten. Immer wieder kommt es vor, dass sich Erwachsene hinter dem Profil von „Freunden“ verstecken, um an Kinder und Jugendliche heranzukommen.
4. Schütze dich vor allem selbst!
Achte darauf, welche Informationen du über dich und andere preisgibst. Poste auch keine Fotos, Videos oder Texte von dir und anderen, die dir später peinlich sein könnten. Bei der **Veröffentlichung von Fotos, Dokumenten und Daten** von anderen ohne deren Einverständnis begehst du eine **Datenschutzverletzung** und machst dich **strafbar**.

ZUSAMMENFASSUNG

Persönliche und sensible Daten müssen bewusst geschützt werden, weil ihr Missbrauch verlockend ist. Je weniger wir uns um Datenschutz bemühen, umso mehr werden wir zum Spielball krimineller Machenschaften mit Daten. Facebook & Co sind häufig Ursache für Verletzungen der Privatsphäre. Wichtig ist, genau zu überlegen, was man in sozialen Medien von sich preisgibt.

Arbeitsaufgaben zu: Datenschutz geht alle an!

1 Ordne richtig zu.

(1) sensible Daten (2) personenbezogene/persönliche Daten

E-Mail-Adresse ____
Röntgenbefund ____
Haarfarbe: rot ____
Geburtsdatum ____
Geht Montag und Mittwoch einkaufen. ____
Name ____
Postleitzahl des Wohnortes ____

2 Begründe, warum Datenschutz ein Anliegen für uns alle sein muss.
Die folgenden Begriffe sollen dich dabei unterstützen:

VIEL GELD VERDIENEN – MISSBRAUCH – KRIMINELLE VERWENDUNG

_____

_____

_____

_____

3 Finde heraus, ob die angeführten Bereiche der Datenverwendung tatsächlich unter den Datenschutz fallen.

	Datenschutz	
Du gibst deine Sozialversicherungsnummer in der Apotheke an (= Datenermittlung).	ja	nein
Du postest alle Bilder von deinem Geburtstagsfest auf Facebook (= Weitergabe von Daten).	ja	nein
Du übergibst dem praktischen Arzt die CD mit deinem Röntgenbefund. Die Sprechstundenhilfe speichert den Befund im Ordinationscomputer (= Datenspeicherung).	ja	nein
Die Mitarbeiterin einer Bank verarbeitet die Abbuchungen mit der Bankomatkarte auf dem Kontodatenblatt (= Weiterverarbeitung von Daten).	ja	nein

4 Du findest hier drei alltägliche Datenschutzfallen.
Diskutiert in Dreier-Gruppen die dahinter stehenden Datenschutzprobleme und mögliche Folgen.

1. Lisa lässt sich auf Facebook über ihre Chefin aus.
2. Chris lädt via Facebook seine Freunde zu einer Party. Statt acht Freunden kommen 70.
3. Rolando erhält ein Mail mit der Nachricht, dass ein Freund gerade in London ist und bestohlen wurde. Der Freund bittet um eine schnelle Geldüberweisung.

Lösungen zu: Datenschutz geht alle an!

1 Ordne richtig zu.

(1) sensible Daten (2) personenbezogene/persönliche Daten

E-Mail-Adresse	2
Röntgenbefund	1
Haarfarbe: rot	1
Geburtsdatum	2
Geht Montag und Mittwoch einkaufen.	1
Name	2
Postleitzahl des Wohnortes	2

2 Begründe, warum Datenschutz ein Anliegen für uns alle sein muss.

Die folgenden Begriffe sollen dich dabei unterstützen:

Mit Daten kann man heute viel Geld verdienen. Computer ermöglichen es, aus Daten Wahrscheinlichkeiten zu berechnen, die Daten in persönliche Marketingmaßnahmen umzusetzen oder Daten kriminell zu verwenden (zB Kreditkartenmissbrauch). Wir werden manipulierbar, wenn wir nicht auf unsere Privatsphäre achten.

3 Finde heraus, ob die angeführten Bereiche der Datenverwendung tatsächlich unter den Datenschutz fallen.

	Datenschutz	
Du gibst deine Sozialversicherungsnummer in der Apotheke an (= Datenermittlung).	ja	nein
Du postest alle Bilder von deinem Geburtstagsfest auf Facebook (= Weitergabe von Daten).	ja	nein
Du übergibst dem praktischen Arzt die CD mit deinem Röntgenbefund. Die Sprechstundenhilfe speichert den Befund im Ordinationscomputer (= Datenspeicherung).	ja	nein
Die Mitarbeiterin einer Bank verarbeitet die Abbuchungen mit der Bankomatkarte auf dem Kontodatenblatt (= Weiterverarbeitung von Daten).	ja	nein

4 Du findest hier drei alltägliche Datenschutzfallen.

Diskutiert in Dreier-Gruppen die dahinter stehenden Datenschutzprobleme und mögliche Folgen.

1. Lisa lässt sich auf Facebook über ihre Chefin aus.

2. Chris lädt via Facebook seine Freunde zu einer Party. Statt acht Freunden kommen 70.

3. Rolando erhält ein Mail mit der Nachricht, dass ein Freund gerade in London ist und bestohlen wurde. Der Freund bittet um eine schnelle Geldüberweisung.

Erläuterung siehe nächste Seite.

Problemstellung:

1. Daten auf Facebook lassen sich kaum löschen, sodass auch nach Jahren derartige Verhaltensweisen negativ verwendet werden können. Viele Personalbüros schauen auf Facebook und checken so die Firmenloyalität bzw. andere Verhaltensweisen der Bewerber. Daher sehr genau überlegen, auf welche Weise man sich äußert und wen man an seinen Informationen teilhaben lässt. Auch keine Fotos posten, die beruflich betrachtet problematisch sein könnten. In sozialen Netzwerken niemals über andere zu schimpfen, ist eine wesentliche Regel. Mobbing kann über Jahre zurückverfolgt werden, sodass Jugendsünden oft ein späteres Drama verursachen.

Nicht über **finanzielle Nöte** in sozialen Netzwerken diskutieren.
Die Kreditschutzorganisationen (zB KSV = Kreditschutzverband 1860) benutzen die Sozialen Medien, um Auskünfte über potenzielle Kreditnehmerinnen und Kreditnehmer zu erhalten. Der Kredit wird möglicherweise abgelehnt, weil die Postings über die finanziellen Probleme die Bonität (= Kreditwürdigkeit) verringert haben, auch wenn dieser Fall schon lange zurückliegt.

2. Dieses Problem stellt sich immer wieder, weil Jugendliche es versäumen, ihren echten Freundeskreis in den Social Media zu definieren. Für andere wiederum ist es eine gesuchte Herausforderung, solche Feste zu stören. Vielfach sind große Schäden dadurch entstanden, auch weil sich die Jugendlichen nicht trauen, bei Erwachsenen oder bei der Polizei Hilfe zu holen.

Daher auch keine Massen-SMS versenden – das könnte eine ebensolche Reaktionskette zur Folge haben.

Eine weitere häufige Problemstellung, die unbedingt zu besprechen ist: Jeder möchte gerne sexy und anziehend sein. Daher gehört das Machen von sexy Fotos unter Freundinnen und Freunden zum Alltag von Jugendlichen. Oft werden diese Fotos dann auf Facebook oder anderen Plattformen gepostet oder per MMS verschickt. Geht die Freundschaft dann auseinander, können diese Fotos sehr rasch sehr peinlich werden, weil daraus leicht Mobbing-Material wird. Man hat dann keine Kontrolle mehr darüber, wohin die Fotos gelangen und wie sie verwendet werden. Daher ist „Sexting“ (= Wortkombination aus Sex und Texting) – das Posten von Nacktaufnahmen – zu einem häufigen Problem geworden. Es gibt leider kein wirksames Mittel dagegen, nur eine Regel: **Sexy Fotos einfach nicht weiterschicken oder posten.**

3. Bei diesem Problem ist der Computer gehackt/gecrackt worden. Alle E-Mail-Kontakte werden mit dem gleichen Trick angeschrieben, es wird der Notfall vorgetäuscht und um eine Überweisung gebeten. Und wer hilft nicht gerne? Daher tappen immer wieder Leute in diese Falle. Meist ist ein bestimmter Ablauf gegeben.

1. Kontaktnahme per E-Mail: Je nach Reaktion Rückfrage – Wo bist du genau? Was ist passiert? Dann kommt die nächste Nachricht mit der Information, wie das Geld überwiesen werden soll (fast immer mit Western Union). Spätestens jetzt muss telefonisch mit dem scheinbar Betroffenen Kontakt aufgenommen werden – der Fall sollte sich klären. Wird tatsächlich Geld überwiesen, kann das Geld nicht mehr zurückgeholt werden – es ist verloren (entgegen einer Banküberweisung). Daher wählen Kriminelle häufig die

Überweisung mit Western Union oder mittels Ukash-Code.[2] Hier steht das Geld der Gegenseite sofort bar zur Verfügung. Auch ein zwischengeschalteter Treuhänder ist keine Garantie, dass alles rechtens ist. Der Treuhänder existiert entweder gar nicht oder ist Partner der Gegenseite.

Eine weitere Methode ist, dass Betroffene Mahnungen bekommen, weil sie angeblich etwas widerrechtlich heruntergeladen oder ein anderes Problem verursacht haben (zB auch Kinderpornografie). Oft haben diese Mahnungen auch eine ZIP-Datei im Anhang. Wird diese ZIP-Datei geöffnet, nistet sich ein Virus (meist ein Trojaner) auf dem PC ein, der ev. einen Zugriff auf den PC ermöglicht.

Besondere Vorsicht ist auch geboten bei Internetangeboten von Luxusgütern zu besonders günstigen Preisen (Uhren, iPhone etc.). Häufig trifft nach der Bestellung nicht einmal die Fälschung ein. Falls die Fälschung dann noch in die Hände des Zolls gelangt, drohen sowohl eine Strafe und eine Vernichtung des Produktes bzw. ist sogar eine gerichtliche Verfolgung durch den Markeninhaber möglich.

Mehr und mehr sind auch **Scams** (das sind Spams mit betrügerischer Absicht) im Umlauf. Hiervor kann man sich am besten schützen, indem man besonders vorsichtig ist bei der Auswahl seiner Freunde in sozialen Netzwerken.

Weiterführende Links

Saferinternet.at: Unterrichtsmaterial Schutz der Privatsphäre im Internet

Saferinternet.at-Leitfäden zum Schutz der Privatsphäre in Sozialen Netzwerken

Saferinternet.at: Flyer Alles Facebook

Microsoft Safety & Security Center: Tipps & Tools für optimale Sicherheitseinstellungen am Computer, für den digitalen Datenschutz und die Online-Sicherheit

Internet Ombudsmann: Kostenlose Online-Beratung und Streitschlichtung bei Problemen mit Online-Shopping, Datenschutz & Urheberrecht: http://www.ombudsmann.at

Arbeiterkammer: Kostenlose Konsumentenberatung in jedem Bundesland: http://www.arbeiterkammer.at

Bundeskriminalamt – Meldestelle Against Cybercrime: Bei Verdacht auf Internetbetrug: mailto:against-cybercrime@bmi.gv.at

Saferinternet.at: Tipps und Infos zur sicheren Internet- und Handynutzung: http://www.saferinternet.at/staysafe, www.facebook.com/saferinternetat

Rat auf Draht: Notruf für Kinder und Jugendliche – rund um die Uhr, anonym, kostenlos. Einfach 147 wählen: http://www.rataufdraht.at

BMWFJ: In der Medien-Jugend-Info gibt's Infos, Beratung und Seminare für Jugendliche zur kompetenten Mediennutzung: http://www.bmwfj.gv.at/mji

[2] Ukash ist eine bargeldlose Zahlungsform. Man kauft eine Karte für einen bestimmten Betrag und erhält einen PIN-Code, den man bei der Bezahlung weitergibt, sodass der Zahlungsnehmer den Betrag ausbezahlt erhält.