

## Sicherheit Lektion 6 Online-Community

- ✗ Vertrauliche Infos
- ✗ Einstellungen und Privatsphäre
- ✗ Chancen und Gefahren
  
- ✓ Soziale Netzwerke bieten Menschen eine Plattform zum Austauschen gemeinsamer Interessen, interaktiven Spielen, Plaudern, Kontakt halten, uvm. Beachten Sie einfach einige Grundregeln in Bezug auf vertrauliche Daten, Privatsphäre-Einstellungen und Kontakten zu Fremden.

### Aufgabe

Recherchen:  [www.klicksafe.de](http://www.klicksafe.de),  
[www.saferinternet.at](http://www.saferinternet.at)

#### 1. Vertrauliche Infos

Immer wieder höre ich vor allem von jüngeren Teilnehmenden, dass es doch nicht schlimm sei, wenn Fremde die eigene E-Mail-Adresse wüssten. Und die Fotos stellt man doch online, damit sie gesehen würden.

Was aber, wenn man leichtfertig die E-Mail-Adresse gepostet hat und nun der Posteingang mit unerwünschten Nachrichten zugemüllt wird? Gar nicht zu reden von den Schadensprogrammen, die im Anhang mitgesendet werden.

Und was, wenn die Fotos auf Seiten erscheinen, mit deren Inhalt man lieber nichts zu tun haben möchte oder in einem Zusammenhang auftauchen, der einem auch nicht lieb ist?

#### 2. Einstellungen und Privatsphäre

Bevor Sie sich bei einer Online-Community registrieren, legen Sie einen weiteren E-Mail-Account an. Geben Sie dabei fiktive Daten an. Damit vermeiden Sie unerwünschte Werbung und sollte schon mal jemand herausfinden, wie Sie per E-Mail zu erreichen sind, dann kommt die Nachricht wenigstens nicht an Ihre echte Adresse.

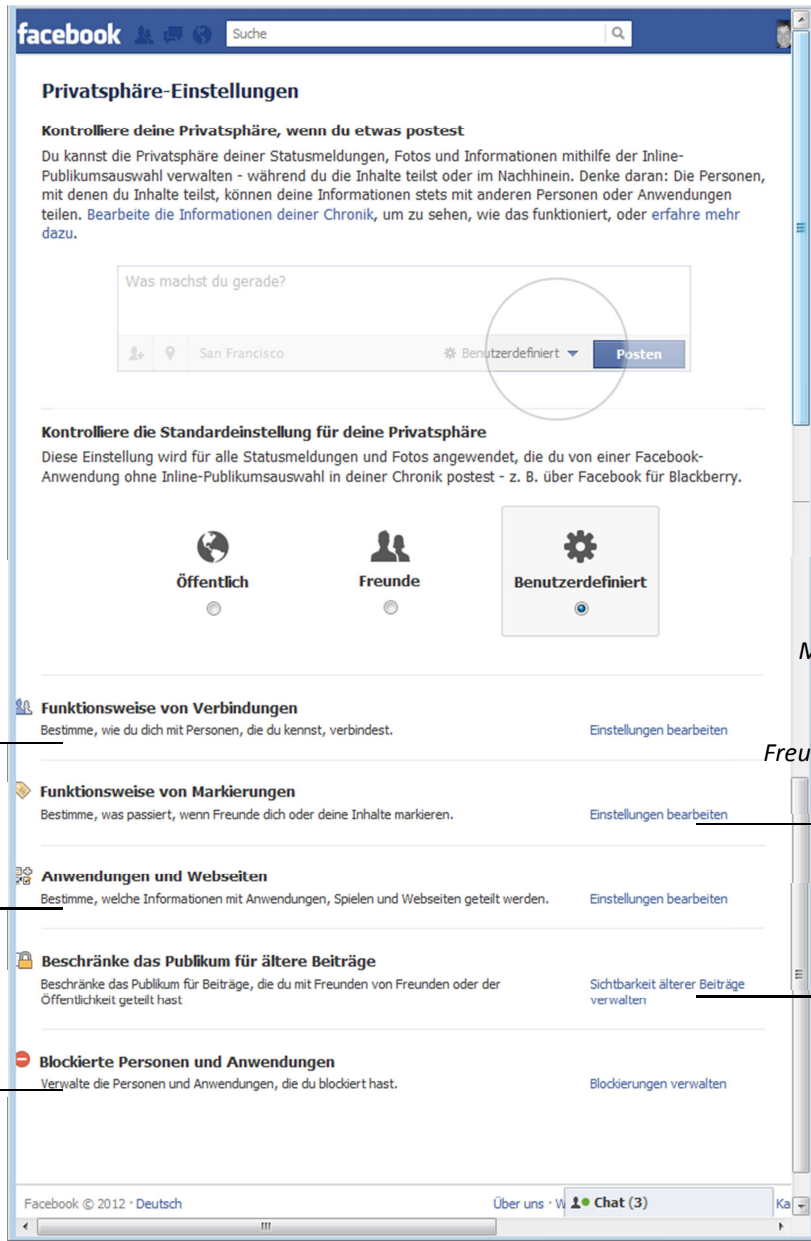
Leider ist der Button *Gefällt mir* auf Facebook aus datenschutzrechtlicher Hinsicht bedenklich. Weil nämlich die IP-Adresse an Facebook übermittelt wird und so Cookies auf Ihrem Rechner hinterlassen werden. Über diese kleinen Informationsdateien können unter Umständen verschiedene Daten über Ihr Nutzungsverhalten erhoben werden.

Wählen Sie das Bild sorgfältig aus. Später können manche Fotos peinlich sein.

Nutzen Sie soziale Netzwerke sicher und richtig: Facebook & Co verfügen über private Einstellungen. Nutzen Sie diese Sicherheitseinstellungen. Überlegen Sie, ob Ihr Geburtsdatum angezeigt werden soll. Ist die Angabe von Familienstand, Ausbildung, Beruf und persönliche Aktivitäten wirklich wichtig? Diese Daten können sehr einfach für Werbezwecke genutzt / missbraucht werden.

Prüfen Sie Freundschaftsanfragen. Wählen Sie Menschen, die Sie kennen.

Abgebildet sehen Sie die Privatsphäre-Einstellungen auf Facebook, Stand Februar 2012.



Wer kann per Name oder Kontaktinformationen nach der Chronik suchen: Alle – Freunde von Freunden – Freunde

Bearbeiten Sie die Einstellungen, was Sie und andere teilen

Blockieren Sie Nutzer, Anwendungsanfragen und Veranstaltungseinladungen

Chronik überprüfen  
Markierung überprüfen  
Maximale Sichtbarkeit der Chronik  
Markierungsvorschläge  
Freunde können angeben, wo Sie sich befinden

Bestimmen Sie die Sichtbarkeit für ältere Beiträge

### 3. Chancen und Gefahren

Online-Communities bieten virtuelle Gemeinschaften online. Egal zu welchem Thema, Gleichgesinnte tauschen sich hier schnell und unkompliziert aus und bleiben miteinander in Kontakt. Doch Vorsicht bei Cyber-Mobbing, Cyber-Grooming, falsche Identitäten, arglistige Links oder Nachrichten und irreführende Infos.

**Cyber-Mobbing** ist wie Mobbing in der Klasse oder Firma, nun aber online mit einem bedeutend größeren Veröffentlichungs-Radius.

**Cyber-Grooming** bedeutet das gezielte Ansprechen von Kindern und Jugendlichen mit dem Ziel sexueller Kontakte.

Wer eine **falsche Identität** für illegale Tätigkeiten annimmt, ist ein Predator (englisch für *Räuber, Raubtier*).

Daneben gibt es **arglistige Links oder Nachrichten**, die zu problematischen Websites führen, um beispielsweise Schadensprogramme zu installieren.

### 4. Internetnutzung kontrollieren

Der *Safer Internet Day* am 7. Februar 2012 ergab, dass Österreichs Eltern Nachholbedarf bei der Interneterziehung haben. Erwerben Sie Medienkompetenz und kümmern Sie sich direkt mit Ihrem Kind / Ihren Kindern um eine gezielte und sichere Internetnutzung:

- ▶ Surfen Sie mit Ihren Kindern
- ▶ Besprechen Sie die Vorzüge und Chancen, aber auch die Gefahren
- ▶ Beschränken Sie die Zeit im Internet
- ▶ Schützen Sie den Rechner mit einem Antiviren-Programm, einer Firewall und regelmäßigen Software-Updates
- ▶ Warnen Sie Ihre Kinder vor der Weitergabe persönlicher Daten
- ▶ Thematisieren Sie, in wie weit die Informationen überprüft sind und der Wahrheit entsprechen

## Sicherheit Schritt sechs Privatsphäre in der Online-Community

## Übung und Selbststudium

1. Damit Facebook bei einem Klick auf den Button *Gefällt mir* keine Cookies auf der eigenen Festplatte installieren kann, gibt es für Browser einen **Facebook Blocker**. Finden Sie heraus, wo Sie den Blocker herunterladen und installieren Sie ihn.
2. Informieren Sie sich über Interneterziehung beispielsweise unter [www.klicksafe.de](http://www.klicksafe.de) oder unter [www.saferinternet.at](http://www.saferinternet.at).
3. Checken Sie die benutzerdefinierten Einstellungen auf Facebook: Wer sieht und darf Dinge kommentieren, die Sie mit anderen teilen, sich an Ihrer Pinnwand befinden oder in denen Sie markiert wurden?
4. Checken Sie Ihre Privatsphäre-Einstellungen auf Facebook: Können Freunde von Personen, die auf Ihren Fotos und Beiträgen markiert wurden, diese sehen? Deaktivieren Sie das Kontrollkästchen.

## Testen Sie Ihr Wissen

1. Wie nennt man das Annehmen einer falschen Identität?
2. Was ist Cyber-Grooming?
3. Warum ist der Button *Gefällt mir* auf Facebook datenschutzrechtlich bedenklich?

## Notizen