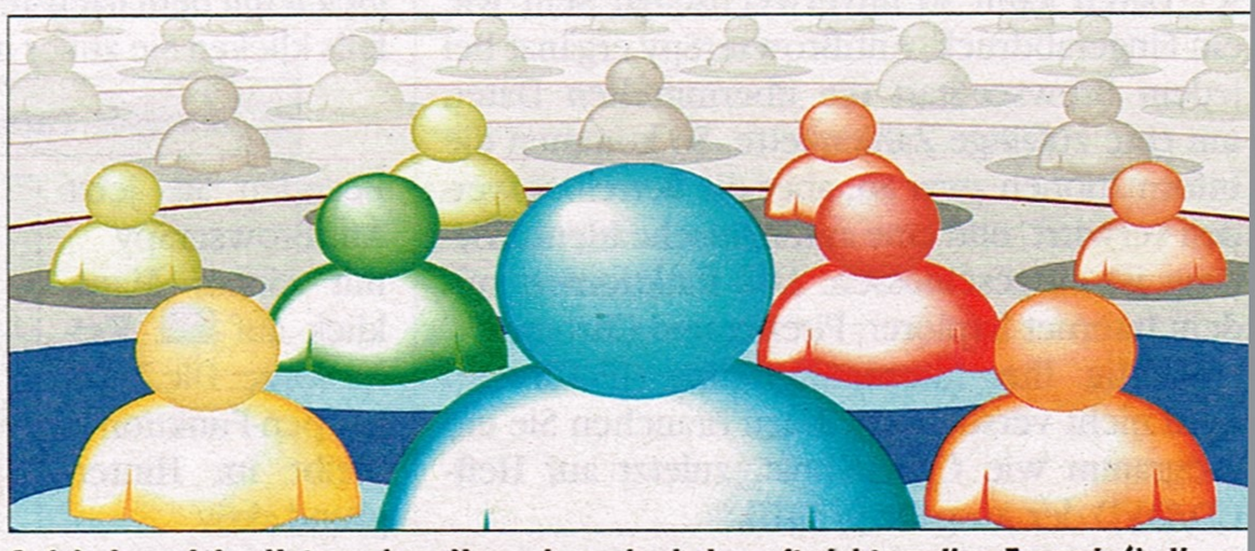
3 PRIVATSPHÄRE IM INTERNET BEWAHREN

Soziale Netzwerke sind prima geeignet, andere Leute kennenzulernen. Das Prinzip: Sie veröffentlichen Ihren Steckbrief („persönliches Profil") beim jeweiligen Internetdienst, etwa Facebook. Per Mausklick nehmen Sie andere Mitglieder in Ihr persönliches Netzwerk auf, machen sie also zu „Freunden". Auf Ihrer Profilseite lassen sich auch Fotos und Kommentare einstellen. Aber Achtung: Manche Netzwerke sind so voreingestellt, dass die Fotos, Profile und Kommentare für alle sichtbar sind – auch für wildfremde Personen. Das zu ändern, ist oft recht aufwendig.

COMPUTERBILD hat die Standard-Einstellungen von sechs beliebten sozialen Netzwerken überprüft. Das Ergebnis: Je nach Anbieter können erhebliche Anpassungen nötig sein (Facebook) oder fast gar keine (SchülerVZ).

Wie Sie zukünftig alle Plattformen nutzen können, ohne dabei Ihre Privatsphäre aufzugeben, steht auf den folgenden Seiten.



Gefahr in sozialen Netzwerken: Normalerweise haben oft nicht nur Ihre Freunde (hell- und dunkelblauer Bereich) Zugriff auf Ihre Fotos und Beiträge, sondern auch deren Freunde (dunkelgrauer Bereich) – und sogar völlig fremde Mitglieder (hellgrauer Bereich).

DIE 10 GOLDENEN REGELN

1 MACHEN SIE SICH VERTRAUT

Soziale Netzwerke lassen sich viel sicherer nutzen, wenn klar ist, wie sie funktionieren. Machen Sie sich zu Beginn mit allen Funktionen vertraut. Folgen Sie nicht der Aufforderung, sofort alle möglichen Infos von sich preiszugeben: Ihre Profil-Infos können Sie nach und nach ergänzen.

2 SCHÜTZEN SIE IHRE IDENTITÄT

Vor der Anmeldung bei einem sozialen Netzwerk sollten Sie sich eine anonyme E-Mail-Adresse bei einem Gratis-Anbieter zulegen – etwa GMX oder Web.de. Verwenden Sie auf keinen Fall ihre normale oder gar geschäftliche Mail-Adresse. Nennen Sie nie Postadressen und Telefonnummern.

3 VORSICHT VOR UNBEKANNTEN KONTAKTEN

Seien Sie vorsichtig bei der Eintragung anderer Netzwerk-Mitglieder als „Freunde". Sie würden einem fremden Menschen schließlich auch nicht „im echten Leben" sofort die gesamte Lebensgeschichte erzählen oder private Fotos zeigen. Im sozialen Netzwerk sollten Sie es ebenso handhaben.

4 SEIEN SIE SPARSAM MIT INFORMATIONEN

Sie können zwar bei allen Netzwerken einstellen, wer welche Informationen über Sie lesen darf. Noch einfacher ist es aber, besonders sensible Bereiche wie „Beziehungsstatus" oder „politische Interessen" einfach nicht auszufüllen. So ist ein Missbrauch mit Sicherheit ausgeschlossen.

5 SCHUTZ-EINSTELLUNGEN ANPASSEN

Nehmen Sie sich ausreichend Zeit: Prüfen Sie jede einzelne Privatsphäre-Einstellung ganz genau. Entscheiden Sie für sich selbst, wer welche Informationen über Sie bekommen soll. Wie das bei den sechs beliebtesten Netzwerken funktioniert, lesen Sie auf den folgenden Seiten.

6 DRITTANWENDUNGEN VERMEIDEN

Vorsicht vor Kontrollverlust: Viele soziale Netzwerke bieten Zusatzprogramme wie Spiele oder Kalender an – und die sammeln wiederum Daten. Selbst „Freunde", die solche Anwendungen nutzen, können so Informationen über Sie weitergeben, wenn Sie es nicht verhindern.

7 KEINEN FREUNDE-FINDER NUTZEN

Viele soziale Netzwerke können Ihre persönlichen E-Mail-Adressbücher (etwa von GMX) durchsuchen, um so bereits registrierte Freunde zu finden. Dabei speichern sie auch Mail-Adressen von Nicht-Mitgliedern und nutzen sie später für Mitglieder-Werbung. Nutzen Sie das Angebot besser nicht.

8 FREUNDESLISTE SAUBER HALTEN

Netzwerk-Mitglieder, die Sie zu „Freunden" erklärt haben, können sich hinterher als nervig oder hinterhältig erweisen. Zögern Sie in einem solchen Fall nicht, diese falschen Freunde wieder von Ihrer Liste zu entfernen. Die „Kündigung" wird dem Mitglied nicht mitgeteilt.

9 LASSEN SIE IHRE DATEN IM NETZWERK

Informationen aus sozialen Netzwerken haben woanders nichts zu suchen: Meiden Sie daher Zusatzprogramme (siehe Regel 6) und Eintragungen in Suchmaschinen wie Google. Klicken Sie auf anderen Internetseiten nicht auf Vernetzungs-Links* wie Facebooks „Gefällt mir!".

10 SCHÜTZEN SIE IHREN PC

Soziale Netzwerke sind ein beliebtes Ziel für Viren-Programmierer. Darum gilt auch hier: Klicken Sie nicht unbedacht auf jeden Link, und schützen Sie Ihren PC mit einem aktuellen Virenschützer und einer Firewall (etwa Kaspersky Internet Security CBE 10, auf Heft-CD/DVD).