Wie sicher sind Ihre Daten?

Mit Freunden chatten, Infos oder Fotos austauschen – für viele Menschen sind die sozialen Netzwerke eine tolle Möglichkeit, Kontakte zu pflegen. Doch wie sicher sind Sie im Internet unterwegs? Machen Sie den Test auf den nächsten Seiten und finden Sie heraus, wie gut Sie sich und Ihre Daten bereits jetzt schützen.

1. Wenn im Internet nach persönlichen Daten gefragt wird, füllen Sie dann alle Felder aus?
   Ja ○ Nein ○

2. Über Facebook oder Google+ bekommen Sie eine Freundschaftsanfrage von einem Unbekannten. Lehnen Sie die Freundschaft ab?
   Ja ○ Nein ○

3. Im Mailpostfach findet sich Post von einem unbekannten Absender mit dem Betreff „Guck dir das mal an“ und einem Dateianhang. Öffnen Sie die Datei?
   Ja ○ Nein ○

4. Auf einer Feier schießen Sie von einigen Gästen Fotos. Posten Sie die schönsten Bilder sofort?
   Ja ○ Nein ○

5. Im Urlaub nutzen Sie einen öffentlichen Rechner, um schnell Ihre E-Mails zu checken. Loggen Sie sich danach sicher aus und löschen Sie die Browser-Daten?
   Ja ○ Nein ○

6. Via Facebook oder Google+ kommt die Meldung, den eigenen Status zu aktualisieren. Ignorieren Sie die Nachricht?
   Ja ○ Nein ○

7. Sind Sie überzeugt davon, dass Ihre Passwörter sicher sind?
   Ja ○ Nein ○

8. Haben Sie Ihrem privaten Ärger schon mal über Facebook, Twitter, Google+ oder ein anderes soziales Netzwerk Luft gemacht?
   Ja ○ Nein ○

9. Sie haben eine interessante Info im Netz gefunden. Klicken Sie den „Like“- oder „Gefällt mir“-Button an?
   Ja ○ Nein ○

10. Prüfen Sie die Sicherheitseinstellungen auf Ihrem Smartphone regelmäßig?
    Ja ○ Nein ○

Bitte umblättern! Die Auflösung finden Sie auf der folgenden Seite.

Auflösung

1. **Ideal ist: Nein**
   Geben Sie nur Infos weiter, die unbedingt nötig sind. In sozialen Netzwerken sollte man seine Adresse nicht nennen, der Onlineversandhändler braucht sie aber, um die Ware ausliefern zu können. Lesen Sie die AGBs und Datenschutzerklärungen der Anbieter genau. Mehr dazu unter *www.verbraucher-sicher-online.de*

2. **Ideal ist: Ja**
   Ist ein Fremder als „Freund" im sozialen Netzwerk zugelassen, kann er sich gezielt über Sie informieren – und die Daten missbrauchen, um z. B. in Ihrem Namen im Internet einzukaufen. Gegen einen solchen Identitätsdiebstahl kann man sich nur mit einer Anzeige bei der Polizei wehren. Daher gilt: Unbekannten keinen Zugang zu privaten Daten ermöglichen.

3. **Ideal ist: Nein**
   Kriminelle nutzen Mails, um schädliche Programme („Trojaner") auf fremden Rechnern zu installieren. Damit können Passwörter ausgespäht werden. Daher sollten Sie Dateien und Links von unbekannten Absendern besser nicht öffnen, sondern gleich löschen. Auch E-Mails von einem vertrauten Absender können einen Trojaner enthalten. Schutz bieten Spamfilter, die regelmäßig aktualisiert werden sollten. Mehr dazu unter *www.bsi-fuer-buerger.de*

4. **Ideal ist: Nein**
   Ohne Einwilligung dürfen Fotos von Dritten nicht im Internet veröffentlicht werden. Das gilt auch für Websites, die sich über Passwörter schützen lassen. Wenn doch ein Foto auftaucht, muss der Betreiber des Accounts aufgefordert werden, die Fotos wieder zu löschen. Mehr Infos unter *www.surfer-haben-rechte.de*

5. **Ideal ist: Ja**
   Über öffentliche Computer können fremde Daten leicht ausgespäht werden. Nach dem Besuch einer privaten Website reicht es deshalb nicht, das Browser-Fenster zu schließen, sondern man muss sich aus der Anwendung „ausloggen". Experten empfehlen, auf fremden Computern zudem „Cookies" und den Browserdatenverlauf zu löschen. Je nach Browser findet man das unter „Einstellungen" oder „Sicherheit".

6. **Ideal ist: Nein**
   Betreiber von sozialen Netzwerken nutzen persönliche Daten der Mitglieder, um damit Geld zu verdienen. Auch deshalb werden die Möglichkeiten zur Einstellung der „Privatsphäre" häufig verändert. Das Verbraucherministerium rät, nur solche Infos preiszugeben, die man auch auf einer Plakatwand veröffentlichen würde. Mehr auf *www.mecodia.de → Tipps*

7. Ideal ist: Ja

Sichere Passwörter enthalten mind. acht Buchstaben in Groß- und Kleinschreibung, Zahlen und Sonderzeichen. Für verschiedene Dienste sollten unterschiedliche Passwörter benutzt werden, die idealerweise regelmäßig verändert werden. Um sich komplizierte Passwörter zu merken, kann man Eselsbrücken nutzen: Aus dem Weihnachtslied „Ihr Kinderlein kommet, oh kommet doch all" wird so im ersten Schritt „IKkokda". Jetzt einige Buchstaben durch Zahlen ersetzen und Sonderzeichen ergänzen, fertig ist das sichere Passwort: „1K!k0k%d4".

8. Ideal ist: Nein

Private Unmutsäußerungen sollten privat bleiben, besonders solche rund um den Job. Über den Chef oder Kollegen in sozialen Netzwerken zu lästern, ist absolut tabu. Wer Infos über die Firma weitergibt, riskiert eine fristlose Kündigung. Vorsicht auch mit „witzigen" Bemerkungen oder Bildern. Bei Bewerbungsverfahren schauen Personalentscheider oft nach, wie sich ein Kandidat auf Google+, Facebook oder Tumblr präsentiert.

9. Ideal ist: Nein

Über „Gefällt mir"-Buttons können Betreiber von sozialen Netzwerken ein Bewegungsprofil der Nutzer erstellen. Wer das vermeiden will, sollte Seiten mit zweistufigen Buttons bevorzugen: Mit dem ersten Klick aktiviert man den Button. Erst mit dem zweiten Klick wird das „Gefällt mir" gesendet. Damit werden dann auch Daten an Facebook, Google oder Twitter übermittelt.

10. Ideal ist: Ja

Wer nicht möchte, dass die eigenen Daten unkontrolliert weitergegeben werden, sollte auf seinem Smartphone die Sicherheitseinstellungen regelmäßig überprüfen. Vorsicht ist besonders beim Herunterladen von neuen Apps geboten. Häufig erlaubt man schon mit einem Klick, dass über die App Daten vom Handy weitergeleitet werden. Mehr über Sicherheitsrisiken von Apps: *www.apptesting.de*