

Link: <https://www.computerwoche.de/a/15-tipps-fuer-einen-sicheren-mobilen-zugang,2350309>

Soziale Netzwerke

15 Tipps für einen sicheren mobilen Zugang

Datum: 05.08.2010
Autor(en): Andrea König

Social Networking macht erst mit dem Handy richtig Spaß. Mobile User sollten jedoch einige Sicherheitsregeln beachten, um Datendiebstahl und das Ausspionieren der Privatsphäre zu verhindern. Die EU-Sicherheitsbehörde ENISA gibt Ratschläge.

Soziale Netzwerke wachsen außergewöhnlich schnell. Bei den Hamburger IT-Strategietagen bat **Microsofts**¹ Deutschland-Chef Marcel Schneider um Handzeichen der **Facebook**²-Nutzer und kaum eine Hand blieb unten.

Konsequenzen zeichnen sich bereits ab. Umso beliebter Plattformen wie Facebook werden, umso größer wird die Nachfrage nach sofortigem und kontinuierlichem Zugang über das Mobiltelefon - dem mobilen sozialen Netzwerk (MSN). Zu Facebook haben beispielsweise mehr als 65 Millionen Nutzer über ihr **Mobilgerät**³ Zugang. 2012 sollen es 134 Millionen Menschen sein.

Viele MSN-Nutzer nutzen ihr Telefon auch als Backup-Gerät für geschäftliche Mails, persönliche Daten, Kontaktangaben, Bilder und Passwörter. Geht so ein Gerät verloren, kann enormer Schaden entstehen. Etwa dann, wenn es illegalerweise benutzt wird, um auf MSNs zuzugreifen.

Wer mit seinem **Mobiltelefon**⁴ soziale Netzwerke nutzt, sollte Möglichkeiten kennen, wie man die Netzwerke sicherer nutzen kann. Schädigende Folgen wie Datenverlust oder Rufschädigung lassen sich vermeiden. So kündigte beispielsweise Virgin Atlantic Airlines 13 Mitarbeitern, die Kommentare auf Facebook veröffentlicht hatten, mit denen sie etwa die Sauberkeit der Firmenflotte und die Passagiere kritisiert hatten.

Veröffentlichen mit Hirn

Die 15 goldenen Regeln der EU-Sicherheitsbehörde ENISA beim Umgang mit mobiler sozialen Netzwerken lauten:

1. Überlegen Sie gut, welche Bilder, Videos und Informationen Sie in einem sozialen Netzwerk preisgeben.
2. **Veröffentlichen**⁵ Sie nie sensible Daten wie Ihre Adresse, Ihr Geburtsdatum oder Ihre Bankverbindung.
3. Denken Sie über ein Pseudonym nach. Ein Nickname kann helfen, Ihre Identität und Privatsphäre zu wahren.
4. Nehmen Sie keine Freundschaftsanfragen von Personen an, die Sie nicht kennen. Sie müssen sich nicht verpflichtet fühlen, jemanden als Freund zu bestätigen.

5. Verifizieren Sie Ihre Kontakte. Stellen Sie sicher, dass es sich tatsächlich um besagte Personen handelt.

6. Wenn Sie einem **sozialen Netzwerk**⁶ beitreten, registrieren Sie sich mit Ihrer privaten Mail-Adresse. Veröffentlichen Sie nicht zu viele Informationen über Ihren Arbeitsplatz, vor allem keine vertraulichen.

7. Bevor Sie etwas über Ihren Arbeitgeber veröffentlichen, machen Sie sich genaue Gedanken über die Wirkung der Worte oder Bilder.

8. Vermischen Sie nicht Privates mit **Beruflichem**⁷. Sie können schließlich nicht kontrollieren, welche Informationen Freunde über Sie veröffentlichen, die dann auch Ihrem Arbeitgeber zugänglich werden.

Lesen Sie die AGBs von sozialen Netzwerken

9. Ihr Profil geht ohne Ihre Zustimmung niemanden etwas an. Bevor Sie sich mit Ihrem **Mobiltelefon**⁸ einloggen, sollten Sie sich vergewissern, dass niemand in Ihrem Umfeld versucht mitzulesen.

10. Lassen Sie Ihr **Mobiltelefon**⁹ nicht aus den Augen. Im schlimmsten Fall könnte sich jemand unter Ihrem Namen in ein soziales Netzwerk einloggen und falsche Informationen veröffentlichen.

11. Stellen Sie Ihr **Handy**¹⁰ nie so ein, dass es sich an Passwörter erinnert und speichern Sie Passwörter auch nicht an anderen Stellen in Ihrem Handy ab. Versuchen Sie unbedingt, sich Passwörter zu merken.

12. Nutzen Sie die Sicherheitsvorkehrungen, die Ihr Handy bietet. Sperren Sie die Tastatur, wenn das Handy nicht genutzt wird und schützen Sie das Gerät mit einer PIN. Machen Sie eine Sicherheitskopie auf Ihrem Rechner, falls das Handy gestohlen werden sollte.

13. Achten Sie darauf, was Sie über andere schreiben.

14. Lesen Sie sich die AGBs der sozialen Netzwerke auch wirklich durch.

15. Überprüfen Sie Ihre Profileinstellungen in sozialen Netzwerken. Sie sollten festlegen, dass nur bestätigte Kontakte lesen und sehen können, was Sie über sich veröffentlichen.

Die goldenen Regeln stammen aus dem Bericht "Online as soon as it happens". Veröffentlicht wurde dieser von der **Europäischen Agentur für Netz- und Informationssicherheit ENISA**¹¹. ENISA ist die Anlauf- und Beratungsstelle in Fragen der Netz- und Informationssicherheit für die EU-Mitgliedstaaten und die EU-Organe. Der Sitz der Agentur ist in **Heraklion**¹² auf der griechischen Insel Kreta. Direktor ist der ehemalige BSI-Chef Udo Helmbrecht.

Links im Artikel:

¹ <http://www.microsoft.com/de/de/default.aspx>

² <http://www.facebook.com/>

³ <https://www.computerwoche.de/netzwerke/mobile-wireless/2350214/>

⁴ <https://www.computerwoche.de/netzwerke/mobile-wireless/2350104/>

⁵ <https://www.cio.de/strategien/2215392/>

⁶ <https://www.cio.de/strategien/2222238/>

⁷ <http://geschaeftskunden-center.telekom.de/>

⁸ <https://www.computerwoche.de/netzwerke/mobile-wireless/2349223/>

⁹ <https://www.computerwoche.de/netzwerke/mobile-wireless/2349223/>

¹⁰ <https://www.computerwoche.de/fileserver/idgwpcw/files/1802.pdf>

¹¹ <http://www.enisa.europa.eu/>

¹² <http://www.heraklion.gr/en>

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.