Sicher in sozialen Netzwerken: Vom Cybermobbing bis zur staatlichen berwachung Tipps Anleitungen zum Schutz persnlicher Daten

Von Manuel Ziegler
*audiobook | *ebooks | Download PDF | ePub | DOC*

Produktinformation -Verkaufsrang: #680419 in BcherVerffentlicht am: 2015-11-09Erscheinungsdatum: 2015-11-09Abmessungen: 9.02 x .79b x 6.38l, Einband: Gebundene Ausgabe324 Seiten | File size: 70.Mb

Von Manuel Ziegler : Sicher in sozialen Netzwerken: Vom Cybermobbing bis zur staatlichen berwachung Tipps Anleitungen zum Schutz persnlicher Daten before purchasing it in order to gage whether or not it would be worth my time, and all praised Sicher in sozialen Netzwerken: Vom Cybermobbing bis zur staatlichen berwachung Tipps Anleitungen zum Schutz persnlicher Daten:

KundenrezensionenHilfreichste Kundenrezensionen2 von 2 Kunden fanden die folgende Rezension hilfreich. Ein Buch das das Thema TECHNISCH, POLITISCH, SOZIOLOGISCH und aus NUTZERSICHT exzellent beschreibtVon Rudolf SiebenhoferDen Band von Manuel Ziegler finde ich deshalb so herausragend, weil er dieses hochbrisante Thema - eigentlich knnte der Titel auch heien: "(UN)Sicher in (UN)sozialen Netzwerken" - sehr umfassend aufbereitet. Und der Autor bringt es im Kapitel 9 des Buches: "Am Totenbett der Privatsphre"auch auf den Punkt: Wenn soziale Netzwerke wie Facebook, Twitter, YouTube, Google+, XING, LinkedIN, Instagram und Whatsapp genutzt werden, muss eben auf Privatsphre verichtet werden (S. 274).Warum das alles so ist, bereitet der Autor den Lesern sehr gut technisch auf und bietet Lsungen und Alternativen an, wie die Risiken wenigstens minimiert werden knnen, zeigt aber auch klar auf wo die einzige Alternative darin besteht einige soziale Netzwerke berhaupt nicht zu nutzen wenn einem der Schutz der Privatsphre wichtig ist.Er zeigt das an einer Reihe von kommerziellen und privaten "sozialen" Netzwerken auf einem Detaillierungsgrad, der auch fr nicht IT-Spezialisten verstndlich sein sollte.Das Buch geht aber in vielen der 10 Kapitel technisch sehr viel tiefer ins Detail und bietet auch viele hilfreiche Links fr entsprechende Sicherheitsmanahmen.Am allerspannendsten fand ich aber die ausfhrliche Beschreibung aller bisher bekannten Dinge, die Edward Snowdon aufgedeckt hat. Und dabei geht es weniger um die skandalsen Inhalte, sondern um die nicht minder skandalsen, rechtsbrechenden technischen Praktiken, die zeigen wie und warum das Internet heute statt wie intendiert dezentral mittlerweile so zentral angreifbar und "auslesbar" fr "Datensammler" mit kommerziellen Absichten, autoritr-berwachenden Absichten, oder kriminellen Absichten ist.Ein Buch, das Schockwirkung fr viele Benutzer von Apps und sozialen Netzwerken haben msste und bei allen Sicherheitsschulungen von Anwendern - ob privat oder in Unternehmen - als "Pflichtlektre" empfohlen werden sollte. Mir ist der Band bei meinen Workshops fr IT-Sicherheit jedenfalls eine gute Hilfe.Und dem Autor sei gedankt fr seinen mutigen Kampf um die Privatsphre im Internet, der aber nur erfolgreich sein kann, wenn die Nutzer mitmachen..... "DENN SIE WISSEN NICHT WAS SIE TUN" sollte eigentlich nach der Lektre dieses Buches keine Ausrede mehr sein.0 von 0 Kunden fanden die folgende Rezension hilfreich. Hinterlsst einen sehr gemischten EindruckVon WeltenWandererDas Buch stellt viele Dienste und Apps vor, aber manche eher detailliert, andere total oberflchlich. An wenigen Stellen merkt man, dass der Autor noch Student ist und sein Studienfach die Informatik ist. Meistens gelingt es ihm jedoch, alle Punkte verstndlich aus Anwendersicht zu beschreiben.Leider stehen einem guten Lesefluss aber viele unntig verschachtelte und unverstndliche Stze im Weg. Hier nur drei von Dutzenden von Beispielen:(Kapitel 1.2) "Durch die Omniprsenz von Nachrichtenagenturen, Bloggern, Politikern, Unternehmen und anderen Nutzern, die Informationen zum aktuellen Tagesgeschehen ber soziale Medien verbreiten, in der Hosentasche der Nutzer haben sich die sozialen Medien auch zu einer wichtigen Nachrichtenplattform fr viele Menschen entwickelt."(Kapitel 4) "Seit damals klar htte sein mssen, welche Aufwnde Nachrichtendienste, insbesondere die NSA, die die in Bad Aibling liegende Station unterhalten hatte, betreiben, um an die Kommunikationsdaten einfacher Brger zu gelangen."(Kapitel 5.5) "Die Tatsache, dass Unternehmen, brigens keineswegs demokratische Einrichtungen, sondern vielmehr streng hierarchisch aufgebaute, autoritre Organisationen, nicht nur einen sehr groen Einfluss auf die Meinungsbildung vieler Menschen haben, sondern letztendlich auch die Geschichte vieler Menschen kontrollieren, bedroht nicht nur die Privatsphre der Menschen - die ist ohnehin bereits verloren -, sondern auch die Demokratie." (Spoiler: Dieser Satz knnte als gute Zusammenfassung des gesamten Buches herhalten.)Ebenfalls strend empfand ich Inkonsistenzen in unterschiedlichen Bereichen:Inkonsistente Schreibweisen, z. B. in Kapitel 2.5: Parship, Parship, PARSHIP oder ElitePartner, ElitePartner, Elite-Partner.Inkonsistenter Umgang mit Nachweisen/Belegen, z. B.. Kapitel 2.3.4 Skype: Obwohl Skype nach Aussagen des Autors mehr Mitglieder hat als Twitter, Xing und LinkedIn, handelt er diesen Dienst im Gegensatz zu den anderen mit zwei krglichen Abstzen ab. Der zweite Absatz besteht aus folgender Aussage, zu der leider jegliche Quellen oder Abhilfemglichkeiten fehlen: "Besonders dann, wenn Sie in Erwgung ziehen, Skype fr den Austausch besonders sensibler Informationen zu nutzen, beispielsweise fr geschftliche (...), sollten Sie Vorsicht walten lassen, denn obwohl Skype ursprnglich ein sehr sicheres Kommunikationsprotokoll nutzte, hat die Sicherheit der Kommunikation bis heute drastisch abgenommen, sodass Angreifer, allen voran die NSA, aber im Grunde auch jeder beliebige andere Angreifer, dazu in der Lage sind, die Kommunikation zwischen zwei Kommunikationspartnern zu verfolgen."Inkonsistente Darstellungen: Nutzungsbedingungen werden dargestellt fr Facebook, Google+, YouTube, Xing, Flirt- und Erotikplattformen aber nicht fr LinkedIn, Skype oder Partnerbrsen; Einstellungsmglichkeiten werden dargestellt fr Facebook, Google+, Xing, LinkedIn, aber nicht fr YouTube oder Skype. Wie man die Standardsuchmaschine ndert, wird beschrieben fr Firefox, Chrome und Safari, aber nicht fr den Internet Explorer.Inkonsistente Gliederungen mal mit Nummerierung, mal ohne, z. B. besteht Abschnitt 10.2.2.2 aus einem nummerierten Unterpunkt ("10.2.2.2.1 DuckDuckGo") und vier nicht nummerierten ("Orweb"," ChatSecure", "Proxy-Konfiguration am Beispiel der Twitter-App").Viele der genannten Punkte stren, wie gesagt, nur den Lesefluss. Andere jedoch, wie fehlende Punkte in der Darstellung, hinterlassen Zweifel an der Sorgfalt des Autors beim Recherchieren und Strukturieren.Ich habe das Buch als Kindle-Ebook gekauft. Dabei fielen mir zustzliche Punkte auf, die das Lesen unntig beschwerlich machten, aber vielleicht nicht die gedruckte Ausgabe betreffen: Das Buch enthlt viele Tabellen. Manche davon sind so gro/breit (z. B. Tabelle 5.1), dass sie selbst auf dem PC-Bildschirm mit der Kindle-App in Vollbilddarstellung kaum vollstndig lesbar sind. Auerdem werden anscheinend viele Abschnitte wie

Praxistipps, Listings, Weblinks, ja selbst nummerierte berschriften als Tabellen dargestellt, was zu unschner Anzeige fhrt. (Durch den konsequenteren Einsatz von CSS htte der Verlag das sicher vermeiden knnen). Manche Abbildungen (Screenshots vom Smartphone) erscheinen mit riesiger Schrift, andere dagegen (z. B. Ausschnitte aus Chats) mit kaum leserlichem Inhalt, dafr wird aber gerade in diesen Abbildungen viel Platz vergeudet fr verpixelte Teilnehmerbilder.Zusammenfassend finde ich das Buch inhaltlich einigermaen OK, aber in Darstellung und z.T. der Recherche nicht besonders gut gelungen.0 von 0 Kunden fanden die folgende Rezension hilfreich. Gutes BuchVon Philipp KnigDas Buch finde ich gut zur Aufklrung der Sicherheit im Internet. Seit den Enthllungen von Edward Snowden wei man, dass unter anderem Deutschland von den USA ausspioniert wird. Seit diesem Zeitpunkt ist auch der Datenschutz vielen Personen wichtiger geworden.In dem Band werden viele Soziale Netzwerke vorgestellt, Kritik dazu geuert und Lsungen und Alternativen angeboten.Man lernt wie groe Konzerne wie Facebook eigentlich mit den eigenen Daten umgehen und wie man sich davor schtzen kann.Manche soziale Netzwerke werden nur oberflchlich vorgestellt, was schade ist.Ab Kapitel 10 wird mehr auf das technische eingegangen und es werden auch Programme und Links zu Schutzmanahmen angeboten."Sicher in sozialen Netzwerken" ist ein Buch, das den Leser wachrtteln soll.Wer sich also fr Online-Sicherheit interessiert, dem knnte dieses Buch gefallen.

Pressestimmen"Wirklich praktisch sind die Hinweise fr sicheres Browsing (Nutzung von Addons, TOR, Orbot, Orweb), Chat-Apps (TextSecure), E-Mail-Verkehr und Passwortverwaltung. Warnungen von Phishing, Identitts- und Datendiebstahl sind immer wieder angebracht, solange viele Netznutzer allzu blauugig unterwegs sind. Fr eine dezidierte Auseinandersetzung mit Internet- und Kommunikationssicherheit ist Zieglers Buch ein guter Startschuss (...)." Reinhard Schmitz, c't, 28.05.2016Alle, die das Social Web bewusst und vorsichtig nutzen wollen, drften mit dieser Lektre also ein Rundum-Komplettpaket bekommen. t3n, 42/2015"Abgerundet wird das sehr informative Buch durch so wichtige Aspekte wie Identitts- und Datendiebstahl, Rufmord und Cybermobbing und Gruppenzwang und Gruppendynamik. Dabei gibt Manuel Ziegler immer praktische Tipps zu einem sicheren Umgang mit den sozialen Netzwerken." Computer und Arbeit, Februar 2016Kurzbeschreibung- Fr Internet- und insbesondere Social Media-Nutzer- Vorstellung aller bedeutenden Netzwerke: Facebook, Google+, Twitter, YouTube, Instagram, XING, LinkedIn, WhatsApp, Snapchat, TextSecure, Wickr, C-Date, Friendscout24, eDarling - Aktuelle Infos und Zusatzmaterialien auf der AutorenwebsiteSoziale Interaktion findet heute verstrkt ber das Internet und insbesondere soziale Netzwerke statt. Das ist einfach und kostenlos. Privatsphre gibt es dabei jedoch kaum. Die Betreiber sozialer Netzwerke betreiben ebenso wie staatliche Behrden auf der gesamten Welt einen unvorstellbaren Aufwand, um Sie als Nutzer, Ihre Interessen, Ihre Sehnschte, ja sogar Ihre Gedanken besser kennenzulernen.Egal, ob mithilfe von Social Media-Buttons Ihre Browser History oder von Nachrichtendiensten wie der NSA all Ihre Kommunikationsdaten im Web aufgezeichnet werden, die Konsequenzen einer totalen berwachung sind vielfltig, auf keinen Fall jedoch sind sie positiv fr Sie selbst.In diesem Buch lernen Sie, wie Sie sich bestmglich vor den Trackingtechnologien der Internet-Spione schtzen, welche Gefahren auerdem in sozialen Netzwerken lauern und nicht zuletzt auch, welche sozialen Netzwerke welche Aufgaben und Erwartungen erfllen.Sicher in sozialen Netzwerken ist ein Buch fr den Kampf um Privatsphre im Internet.AUS DEM INHALT //Nutzungsbedingungen sozialer Netzwerke // Online-Dating-Plattformen // Gruppendynamiken // Identittsdiebstahl // Cybermobbing // Tracking Geolocation // Staatliche berwachung und Zensur // Phishing- und Man-in-the-Middle-Angriffe // Manahmen zum Schutz der Privatsphre, wie z.B.: Browser-Einstellungen, E-Mail-Verschlsselung und Anonymisierung mit Torber den Autor und weitere MitwirkendeManuel Ziegler studiert Informatik an der TU Mnchen, hlt Vortrge zur Sicherheit in sozialen Netzwerken und ist Autor mehrerer Bcher.