

(Free read ebook) Schnelleinstieg Sicher surfen im Web: Zeigen Sie potenziellen Betrügern, wer auf Ihrem Rechner das Sagen hat

## Schnelleinstieg Sicher surfen im Web: Zeigen Sie potenziellen Betrügern, wer auf Ihrem Rechner das Sagen hat

Von Andreas Hein

ebooks | Download PDF | \*ePub | DOC | audiobook

Andreas Hein

Urheberrechtlich geschütztes Material



Produktinformation -Verkaufsrank: #703631 in BcherMarke: FranzisVerffentlicht am: 2015-05-21Abmessungen: 8.27 x .51b x 5.87l, Einband: Taschenbuch160 Seiten | File size: 47.Mb

Von Andreas Hein : Schnelleinstieg Sicher surfen im Web: Zeigen Sie potenziellen Betrügern, wer auf Ihrem Rechner das Sagen hat before purchasing it in order to gage whether or not it would be worth my time, and all praised Schnelleinstieg Sicher surfen im Web: Zeigen Sie potenziellen Betrügern, wer auf Ihrem Rechner das Sagen hat:

KundenrezensionenHilfreichste Kundenrezensionen3 von 4 Kunden fanden die folgende Rezension hilfreich.

Sicherheit beim Bewegen im Internet ist eine Daueraufgabe. Von Benedict Die gute Nachricht ist: Gegen alle möglichen Gefahren im Internet kann man sich wappnen. Dieses Buch hilft dabei. Es sensibilisiert für Betrugsversuche, an die man zuerst gar nicht denkt, und schlägt Sicherheitsvorkehrungen vor.

**ANTIVIREN-PROGRAMME** Ein Windows-System muß bei den von Microsoft eingebauten Schutz notwendig durch ein leistungsfähiges Antivirenprogramm und eine sog. Firewall gegen Eindringlinge abgesichert werden. Der Autor Andreas Hein zahlt die wichtigsten Anbieter auf, aber warum nicht Bitdefender und GDATA? GDATA (Bochum) hat gerade dieser Tage die Cyber-Attacke offenbar eines fremden Geheimdienstes auf das Netz des deutschen Bundestages analysiert, die zu einer schwerwiegenden und vielleicht hoffnungslosen Verseuchung des Systems durch Trojaner geführt hat.

**ONLINE-BANKGESCHÄFTE** sind ein Hauptangriffsziel der Internetkriminalität. Die Absicherung der Transaktionen geschieht mit verschiedenen Verfahren, darunter iTAN, mobileTAN, chipTAN, HBCI und photoTAN, die in Bild und Text gut erklärt werden. Etwas aufwendiger einzurichten sind die sog. Live-Systeme, die kostenlos von Computer-Zeitschriften wie PC-Welt und c't angeboten werden. Sie bieten höchste Sicherheit auch für den Fall, daß sich ein Trojaner bereits im eigenen System eingenistet ist, indem die Verbindung zur Bank über ein separates nicht manipulierbares alternatives Betriebssystem aufgebaut wird. Es wird von einer CD oder einem nicht beschreibbaren Speicherstick gestartet. Diese angepassten Betriebssystemvarianten von Linux (meist Ubuntu) lassen sich von den jeweiligen Webseiten der Zeitschriften herunterladen, die man sich aber selber suchen muß, da sie der Autor nicht angibt (pcwelt.de, heise.de).

**VERSCHLÜSSELUNG** Zur Verschlüsselung von Daten auf der eigenen Festplatte oder zur Speicherung schlägt der Autor folgende vier Anbieter vor: Truecrypt 7-zip.de Boxcryptor.com Safemonk.com Die Seite von letzterem überrascht mit der Meldung: "SafeMonk is saying farewell, but you can keep your sensitive files secure with Sookasa", was die Schnelligkeit der Branche illustriert.

**PAWORT-TRESOR** Für die Verwaltung der eigenen Pässe und ihren Verschluss in einem sog. Passworttresor empfiehlt der Autor den kostenlosen Tresor "keepass.info". Den zwar kostenpflichtigen, aber sehr innovativen Tresor "mobilesitter.de", der von einer Ausgründung der renommierten Fraunhofer-Gesellschaft angeboten wird, hätte er ruhig auch erwähnen können. Selbst der Mini-Sicherheitsratgeber Sicherheit beim Surfen und Kommunizieren im Internet: Was Sie beachten sollten weist darauf hin.

**WLAN** Der Autor geht auf die Gefahren öffentlicher WLAN-Verbindungen ein, läßt aber eine interessante Absicherung, nämlich den Aufbau eines VPN (virtual private network), zu dem es diverse Anbieter gibt, unter den Tisch fallen.

**GEFAHR DURCH SPEICHER-STICKE** Ein Einfallstor für Schadsoftware sind USB-Sticks, also Speicherstifte, die über die USB-Schnittstelle möglicherweise schon bevor das eigene Virenschutzprogramm aktiv geworden ist, auf den Rechner zugreifen. Das ist der Grund, daß viele sicherheitssensibilisierte Firmen den Gebrauch fremder USB-Stifte strikt untersagen. Dieser Weg, auf dem schon erfolgreich Industrieanlagen angegriffen und zerstört wurden, wird vom Autor leider nicht thematisiert.

**FAZIT** Bis auf die erwähnten Lücken ist das ein vollständiger und empfehlenswerter Ratgeber. Wer ihm folgt, ist quasi auf der sicheren Seite. Zwar ließen sich alle Informationen dieses Buches auch im Internet finden, aber nicht in dieser gebündelten Form.

Produktbeschreibung "Checklisten und Sicherheitstipps - entspannt Surfen" Computerviren und Würmer, die weltweit Millionen von PCs befallen und lahmlegen, wie es Melissa und dem I-Love-You-Virus vor 15 Jahren gelang, gibt es heute nicht mehr. Das darf jedoch keineswegs als Entwarnung verstanden werden - ganz im Gegenteil! Es gibt neue Gefahren, die sogar noch gravierendere Folgen haben können.

Erprobte Sicherheitskonzepte für entspanntes Surfen, am Beispiel realer Betgereien vorgestellt (Quelle: Screenshots silktide.com, paypal.de).

Lassen Sie sich den Spaß am Internet nicht verderben... Auch wenn die Aufzählung der potenziellen Gefahren auf den ersten Blick recht abschreckend wirkt, müssen Sie nicht gleich in Panik geraten und auf die Internetnutzung verzichten. Zum Glück gibt es zahlreiche Möglichkeiten, die Risiken so weit zu verringern, daß Sie sich weiterhin weitgehend unbeschwert im Internet bewegen und von den vielfältigen Nutzungsmöglichkeiten profitieren können.

Werden Sie aktiv, handeln Sie und geben Sie Betrügern keine Chance. Dieses Buch ist Ihr Schild gegen Botnetze und Zombie-Rechner, gegen Betgereien beim Onlinebanking, gegen Identitätsdiebstahl, gegen unerwünschte Überwachung und Datenweitergabe - Ihr Schild gegen den alltäglichen Betrug. Sicherheit beim Surfen stellt sich nicht von allein ein. Sie müssen selbst aktiv werden! Dabei ist es nicht mit einer einmaligen Aktion wie der Installation eines Antivirenprogramms getan, sondern Sie sind dauerhaft gefordert, aufmerksam zu bleiben und vorsichtig zu handeln. Dieses Buch hilft Ihnen dabei.

**Inhalt:** Schutz für Computer, Smartphones und Tablets - Web- und E-Mail-Sicherheit - Sicherheit beim Onlinebanking - Sicheres und entspanntes Onlineshopping - Sicherheit bei der mobilen Internetnutzung - Datensicherheit in der Cloud - Datensicherheit in sozialen Netzwerken - Verschlüsselter Nachrichtenaustausch - Wieviel Anonymität darf sein?

Pressestimmen Auszug aus IT-MITTELSTAND 1-2/2016, S. 38: "Das Softcover untersucht, wie man Sicherheit für verschiedene Hardware-Plattformen (PC, Tablet, Smartphone) gewährleisten kann. Die jeweiligen Nutzungsformen erfordern verschiedene Strategien und Vorkehrungen, um Datenmissbrauch und Privatsphäre wirkungsvoll gegen externe Angriffe zu schützen. Betrachtet werden Web-Shopping, E-Mail, Online-Banking, soziale Netzwerke, Cloud-Infrastrukturen und Verschlüsselungsverfahren. Als Leser lernt man unterschiedliche Betrugsversuche zu erkennen und

entsprechend gegenzusteuern." (IT-Mittelstand 1-2/2016, S. 38) Kurzbeschreibung ABZOCKE IM INTERNET? NICHT MIT MIR! Computerviren und Würmer, die weltweit Millionen von PCs befallen und lahmlegen, wie es Melissa und dem I-Love-You-Virus vor 15 Jahren gelang, gibt es heute nicht mehr. Das darf jedoch keineswegs als Entwarnung verstanden werden - ganz im Gegenteil! Es gibt neue Gefahren, die sogar noch gravierendere Folgen haben können. Erprobte Sicherheitskonzepte für entspanntes Surfen, am Beispiel realer Betgereien vorgestellt. Lassen Sie sich den Spaß am Internet nicht verderben ... Auch wenn die Aufzählung der potenziellen Gefahren auf den ersten Blick recht abschreckend wirkt, müssen Sie nicht gleich in Panik geraten und auf die Internetnutzung verzichten. Zum Glück gibt es zahlreiche Möglichkeiten, die Risiken so weit zu verringern, dass Sie sich weiterhin weitgehend unbeschwert im Internet bewegen und von den vielfältigen Nutzungsmöglichkeiten profitieren können. ... werden Sie aktiv, handeln Sie und geben Sie Betrgern keine Chance. Dieses Buch ist Ihr Schild gegen Botnetze und Zombie-Rechner, gegen Betgereien beim Onlinebanking, gegen Identitätsdiebstahl, gegen unerwünschte Überwachung und Datenweitergabe - Ihr Schild gegen den alltäglichen Betrug. Sicherheit beim Surfen stellt sich nicht von allein ein. Sie müssen selbst aktiv werden! Dabei ist es nicht mit einer einmaligen Aktion wie der Installation eines Antivirenprogramms getan, sondern Sie sind dauerhaft gefordert, aufmerksam zu bleiben und vorsichtig zu handeln. Dieses Buch hilft Ihnen dabei. Aus dem Inhalt: Schutz für Computer, Smartphones und Tablets Web- und E-Mail-Sicherheit Sicherheit beim Onlinebanking Sicheres und entspanntes Onlineshopping Sicherheit bei der mobilen Internetnutzung Datensicherheit in der Cloud Datensicherheit in sozialen Netzwerken Verschlüsselte Nachrichtenaustausch Wieviel Anonymität darf sein? über den Autor und weitere Mitwirkende Andreas Hein ist freiberuflicher Autor im Bereich IT und Mitinhaber des Redaktionsbros TexPress. Seit 1995 ist der Diplom-Volkswirt als Fachautor aktiv und befasst sich mit aktuellen IT-Themen. Neben dem Schwerpunktthema Internet befasst er sich besonders intensiv auch mit den Bereichen Sicherheit und Datenschutz.