
ISBN: 978-0-3215-8668-0

Price: $49.99

With half a billion unique visitors and a smorgasbord of productivity-enhancing applications, Google.com is arguably the hottest Website on the Internet. And there is no doubt that users in enterprise and home environments have come to strongly rely on it for a variety of day-to-day applications. Beyond Web search, which is its staple, Google offers other Web application services such as an online calendar, book search, document and spreadsheet editing, social networking, language translation, patent search, and voice over Internet communications.

These applications are typically delivered via “the cloud”—where Google both stores critical data and performs critical computation. The Web browser is basically a conduit through which users can both get a glimpse of and access Google’s massive back end intelligence and computing capabilities. Whether users realize it or not, in this type of model, they are entrusting Google with large amounts of information. There is tremendous potential for a rogue insider or wily attacker to gain access to a treasure trove of end-user information. For example, with Google’s patent search, the content of search queries can be especially revealing about the types of intellectual property the end user wants to protect. In addition, if a Google application contains a vulnerability, an attacker can potentially exploit it to access sensitive data on your computer, a vulnerability that at one time existed with Google’s Desktop search.

These examples and others form the basis for Greg Conti’s *Googling Security: How Much Does Google Know About You?* He provides a thorough and well-researched treatment of the security and privacy ramifications of using Internet services like Google. He describes in careful detail what information trail users leave behind when using Google applications. This trail includes information that can both be used to identify users, as well as what topics they are interested in.

For enterprises, a tradeoff is necessitated if their end users are to use free services and applications such as Google. On the one hand, enterprises want to enable employees to be efficient via best-of-breed technologies such as Google. On the other hand, they need to be wary of what kinds of information Google and other related companies collect on their employees—including the associated security risks. While Conti focuses on Google, the concepts he describes are not specific to Google by any means. And as more cloud-based solutions become available, enterprises need to understand the security risks associated with each one in order to make decisions that protect the privacy of their employees and businesses.

Zulfikar Ramzan (Ph.D.) is technical director and architect with Symantec’s Security Technology and Response group and co-author of *Crimeware: Understanding New Attacks and Defenses.*


ISBN: 978-0-470-38688-0

Price: $24.99

What is the most recent For Dummies book you have read? I have been a fan of this particular book series for some time. *Green IT For Dummies* is a new addition to it—and a welcome one. By taking a conversational approach to the topic, the authors present the subject matter in an easy-to-read format, complete with anecdotal comments and case studies. And in keeping with other For Dummies books, the cartoons are amusing.

One of the most attractive aspects of this book is the comprehensive manner in which Green IT is covered. Many other books about environmentally sustainable IT tend to focus on one aspect, such as the data center—or even just one particular area of the data center. However, this book takes a refreshing approach by covering not only the data center and endpoints, but other relevant topics such as the office environment, waste, organizations, conferencing, Web-based tools, ways to extend the life of older assets, government legislation, and the home office. In fact, the appendix even features worksheets to assist the reader in establishing a baseline.

One of the limitations of a book on such a broad subject matter is that there isn’t space to delve into any of the topics in detail. The authors would serve their readers better and offset the lack of detail on each topic by organizing the scattered Web addresses cited throughout the book so that they can be easily accessed. This is a highly recommended enhancement for the edition.

Regardless, *Green IT For Dummies* is a good introduction to the topic, as it is written for both the non-technical and tech-savvy reader.

Jose Iglesias is vice president of Global Solutions in Symantec’s Office of the CTO and leads Symantec’s Green IT effort. He is a co-author of various books, including Symantec Yellow Books.