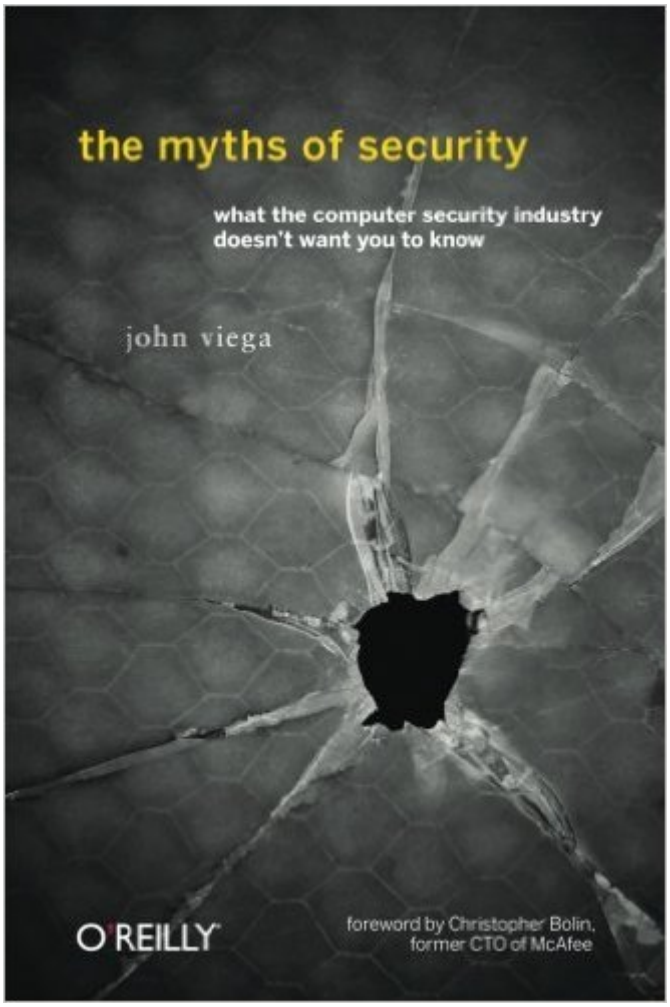
The Myths Of Security: What The Computer Security Industry Doesn't Want You To Know



Synopsis

If you think computer security has improved in recent years, The Myths of Security will shake you out of your complacency. Longtime security professional John Viega, formerly Chief Security Architect at McAfee, reports on the sorry state of the industry, and offers concrete suggestions for professionals and individuals confronting the issue. Why is security so bad? With many more people online than just a few years ago, there are more attackers -- and they’re truly motivated. Attacks are sophisticated, subtle, and harder to detect than ever. But, as Viega notes, few people take the time to understand the situation and protect themselves accordingly. This book tells you:Why it’s easier for bad guys to "own" your computer than you thinkWhy anti-virus software doesn’t work well -- and one simple way to fix itWhether Apple OS X is more secure than WindowsWhat Windows needs to do betterHow to make strong authentication pervasiveWhy patch management is so badWhether there’s anything you can do about identity theftFive easy steps for fixing application security, and moreProvocative, insightful, and always controversial, The Myths of Security not only addresses IT professionals who deal with security issues, but also speaks to Mac and PC users who spend time online.

Book Information

Paperback: 264 pages
Publisher: O’Reilly Media; 1 edition (June 29, 2009)
Language: English
ISBN-10: 0596523025
ISBN-13: 978-0596523022
Product Dimensions: 5.5 x 0.7 x 8.5 inches
Shipping Weight: 9.6 ounces (View shipping rates and policies)
Average Customer Review: 3.7 out of 5 starsÂ Â See all reviewsÂ (35 customer reviews)
Best Sellers Rank: #1,273,199 in Books (See Top 100 in Books) #87 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Administration > Disaster & Recovery #96 inÂ Books > Computers & Technology > Computer Science > AI & Machine Learning > Expert Systems #190 inÂ Books > Computers & Technology > Security & Encryption > Viruses

Customer Reviews

Let me start by saying I usually like John Viega’s books. I rated Building Secure Software 5 stars back in 2005 and 19 Deadly Sins of Software Security 4 stars in 2006. However, I must not be the target audience for this book, and I can’t imagine who really would be. The book mainly addresses

consumer concerns and largely avoids the enterprise. However, if most consumers think "antivirus" when they think "security," why would they bother reading The Myths of Security (TMOS)?TMOS is strongest when Viega talks about the antivirus (or antimalware, or endpoint protection, or whatever host-centric security mechanism you choose) industry. I didn't find anything to be particularly "myth-shattering," however. I have to agree with two of the previous reviewers. Many of the "chapters" in this book could be blog posts. The longer chapters could be longer blog posts. The lack of a unifying theme really puts TMOS at a disadvantage compared to well-crafted books. I was not a huge fan of The New School of Information Security or Geekonomics (both 4 stars), but those two titles are better than TMOS.If you want to read books that will really help you think properly about digital security, the two must-reads are still Secrets and Lies by Bruce Schneier and Security Engineering, 2nd Ed by Ross Anderson. I would avoid Bruce's sequel, Beyond Fear -- it's ok, but he muddles a few concepts. (Heresy, I know!) I haven't read Schneier on Security, but I imagine it is good given the overall quality of his blog postings.If you want to shatter some serious myths, spend time writing a book on the "80% myth," which is stated in a variety of ways by anyone who is trying to demonstrate that insider threats are the worst problem facing digital security.

The Myths of Security: What the Computer Security Industry Doesn't Want You to Know is an interesting and thought-provoking book. Ultimately, the state of information security can be summed up in the book's final three sentences, in which John Viega writes that 'real, timely improvement is possible, but it requires people to care a lot more [about security] than they do. I'm not sure that's going to happen anytime soon. But I hope it does.'The reality is that while security evangelists such as Viega write valuable books such as this, it is for the most part falling on deaf ears. Most people don't understand computer security and its risks, and therefore places themselves and the systems they are working in danger. Malware finds computers to load on, often in part to users who are oblivious to the many threats.Much of the book is made up of Viega's often contrarian views of the security industry. With so much hype abound, many of the often skeptical views he writes about, show what many may perceive are information security truths, are indeed security myths.From the title of the book, one might think that there is indeed a conspiracy in the computer security industry to keep users dumb and insecure. But as the author notes in chapter 45 -- An Open Security Industry, the various players in the computer security industry all work in their own fiefdoms. This is especially true when it comes to anti-virus, with each vendor to a degree reinventing the anti-virus wheel. The chapter shows how sharing amongst these companies is heavily needed. With that, the book's title of What the Computer Security Industry Doesn't Want You to Know is clearly meant to

be provocative, but not true-life.The book is made up of 48 chapters, on various so called myths.

I expected much more from John Viega, but this book has so much unsubstantiated opinion and reads like an arrogant and ill thought out blog, that I want to return the book for a refund.Chapter 5, "Test of a Good Security Product: Would I Use It?", he then lists some he uses and those he doesn't:Under the "he does use it" category: "I've been forced to run god-awful VPN (virtual private net-work) software at work (usually the crappy Cisco client). This allows me to access my company's resources even when I'm not actually in the office."So I take it the god-awful software is a pass of this test? And the use of VPN software to access internal office network resources is a revelation?Under the "he does NOT use it" category: he lists firewalls and his reasoning? Because he does not need to use one at home, on account that his cable MODEM and wireless router are NAT capable and therefore hosts behind them are not externally addressable. So firewalls fail the "good security product" test because John Viega does not need them at home? Seriously?He then ends the "does NOT use" category with "Any other consumer security product"!In Chapter 16, "The Cult of Schneier", he has a few stabs at Bruce Schneier, but does not give any specifics with the technical depth that Bruce Schneier deserves. He complains that Applied Cryptography is overly referred to by Schneier cultists, given that it has been 13 years since it was updated and the field has advanced since then. He uses MD5 as an example of something that was considered very strong then but not now. From my recollection of that brilliant cryptography foundation, Bruce mentioned that MD5 was suspected to have a weakness.

Dream Body: Breaking the Lies and Myths of the Fitness Industry so You Can Build Lean, Hard Muscle and Shred Fat Using Simple and Proven Techniques That Get Results Understanding Greek Myths (Myths Understood (Crabtree)) Living Well with Endometriosis: What Your Doctor Doesn't Tell That You Need to Know (Living Well (Collins)) by Morris. Kerry-Ann (2006) Paperback Muscle Myths: 50 Health & Fitness Mistakes You Don't Know You're Making: Build Healthy Muscle Why Doesn't My Floppy Disk Flop?: And Other Kids' Computer Questions Answered by the CompuDudes So, You Want to Be a Coder?: The Ultimate Guide to a Career in Programming, Video Game Creation, Robotics, and More! (Be What You Want) You Wouldn't Want to Be a Shakespearean Actor!: Some Roles You Might Not Want to Play You Wouldnt Want to Be a Shakespearean Actor!: Some Roles You Might Not Want to Play So, You Want to Work with the Ancient and Recent Dead?: Unearthing Careers from Paleontology to Forensic Science (Be What You Want) The MBA Reality Check: Make the School You Want, Want You Business Negotiation: 20 Steps To Negotiate With Results, Making Deals, Negotiation Strategies, Get What You Want, When You Want It, Achieve Brilliant Results, Negotiation Genius, Leadership