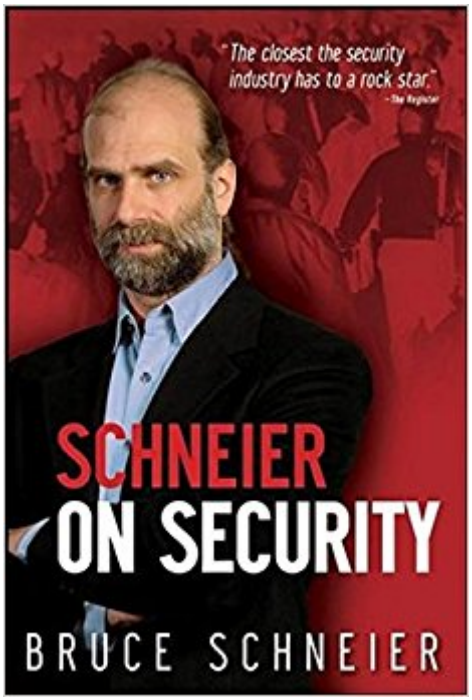
Schneier On Security



Synopsis

Presenting invaluable advice from the world?s most famous computer security expert, this intensely readable collection features some of the most insightful and informative coverage of the strengths and weaknesses of computer security and the price people pay -- figuratively and literally -- when security fails. Discussing the issues surrounding things such as airplanes, passports, voting machines, ID cards, cameras, passwords, Internet banking, sporting events, computers, and castles, this book is a must-read for anyone who values security at any level -- business, technical, or personal.

Book Information

Hardcover: 336 pages

Publisher: Wiley; 1 edition (September 29, 2008)

Language: English

ISBN-10: 0470395354

ISBN-13: 978-0470395356

Product Dimensions: 6.4 x 1.1 x 9.3 inches

Shipping Weight: 1.3 pounds (View shipping rates and policies)

Average Customer Review: 4.3 out of 5 starsÂ Â See all reviewsÂ (17 customer reviews)

Best Sellers Rank: #972,143 in Books (See Top 100 in Books) #234 inÂ Books > Computers & Technology > Certification > CompTIA #568 inÂ Books > Computers & Technology > Security & Encryption > Privacy & Online Safety #1836 inÂ Books > Computers & Technology > Networking & Cloud Computing > Networks, Protocols & APIs

Customer Reviews

There is a perception in both the private and government sector, that security, both physical and digital, is something you can buy. Witness the mammoth growth of airport security products following 9/11, and the sheer number of vendors at security conferences. With that, government officials and corporate executives often think you can simply buy products and magically get instant security by flipping on the switch. The reality is that security is not something you can buy; it is something you must ’get’.Perhaps no one in the world gets security like author Bruce Schneier does. Schneier is a person who I am proud to have as a colleague [Schneier and I are both employed by the same parent company, but work in different divisions, in different parts of the country]. Schneier on Security is a collection of the best articles that Bruce has written from June 2002 to June 2008, mainly from his Crypto-Gram Newsletter, his blog, and other newspapers and

magazine. The book is divided into 12 sections, covering nearly the entire range of security issues from terrorism, aviation, elections, economics, psychology, the business of security and much more.Two of the terms Schneier uses extensively throughout the book are intelligence and economics. From an intelligence perspective, he feels that Washington has spent far too much on hardware and other trendy security devices that create a sense of security theater. The security theater gives an aura and show of security, but in reality, has little real effect.The lack of intelligence is most manifest with airports, which are a perfect example of misguided security. Schneier notes that current trends in US airport security requires that people remove their shoes, due to a one-time incident with shoe-based explosive.

Schneier’s security mantras are:Security is a trade off.Security is about people, not technology.Security is about failure, not success.Security is obtained by skilled intelligence gathering.Because Schneier presents a collection of previously published articles and blog posts he repeats himself a lot, but that’s OK as it reinforces the mantras all the more strongly.When he writes of airport security, for instance. If our name is on a no-fly list, the clerk at the check in desk will not be permit us to board our flight. Why should he? If he does and we are terrorists, he’s fired and maybe prosecuted. If he doesn’t allow us aboard despite the fact we are upstanding citizens, he is praised for doing his job. Are we more secure? No. A genuine terrorist will probably avoid using a name on a no-fly list. And who manages this list? Can we check if our name is on it? No, we can’t. If we do find out we are on the list, e.g. by being refused boarding for no adequate reason, can we get our name off it? No, there’s no appeal process. The no-fly list is a bad system, it effectively sentences people without due process.Compare this with the 1999 attempt to sneak explosives into the US from Canada. The culprit wasn’t arrested because his name or license plate number were on a watch list but because a trained border crossing agent, Diana Dean, recognized suspicious behaviour and decided to investigate further. What led to her decision cannot be quantified or turned into a procedure, her instincts were honed by years of experience.The applicable mantra in both cases is "Security is obtained by skilled intelligence gathering". Read the book for illustrations of the other mantras.

Everything You need to know about Hacking, Computer Hacking, and Security ... Bugs, Security Breach, how to hack) CompTIA Security+ Guide to Network Security Fundamentals (with CertBlaster Printed Access Card) Securing Web Services with WS-Security: Demystifying WS-Security, WS-Policy, SAML, XML Signature, and XML Encryption Programmer's Ultimate Security DeskRef: Your programming security encyclopedia Security Risk Management: Building an Information Security Risk Management Program from the Ground Up Security Analysis: Sixth Edition, Foreword by Warren Buffett (Security Analysis Prior Editions) 6 Months to 6 Figure Passive Income: Anyone Can Do It - Guide to Guaranteed Financial Security .. Make Money While You Sleep (Personal Financial Security) Security Risk Assessment: Managing Physical and Operational Security The Myths of Security: What the Computer Security Industry Doesn't Want You to Know Dynamic Networks and Cyber-Security: 1 (Security Science and Technology) Human Security For All: A Tribute to Sergio Vieira de Mello (International Humanitarian Affairs) Eternal Security: Can You Be Sure? Hacking: How to Hack Computers, Basic Security and Penetration Testing Security, Audit and Control Features SAP R/3: A Technical and Risk Management Reference Guide, 2nd Edition Firewalls Don't Stop Dragons: A Step-By-Step Guide to Computer Security for Non-Techies Active Defense: A Comprehensive Guide to Network Security Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning