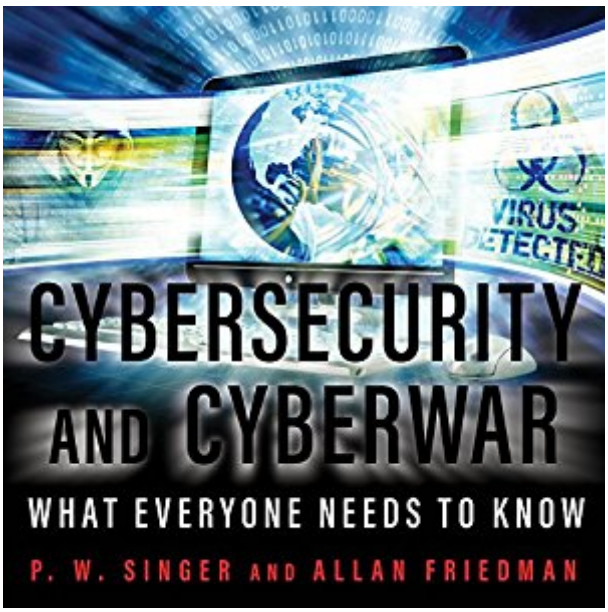
Cybersecurity And Cyberwar: What Everyone Needs To Know



Synopsis

In Cybersecurity and Cyberwar: What Everyone Needs to KnowÃƒâ Ã Â®, New York Times best-selling author P. W. Singer and noted cyberexpert Allan Friedman team up to provide the kind of deeply informative resource book that has been missing on a crucial issue of 21st-century life. Written in a lively, accessible style, filled with engaging stories and illustrative anecdotes, the book is structured around the key question areas of cyberspace and its security: how it all works, why it all matters, and what we can do. Along the way, they take listeners on a tour of the important (and entertaining) issues and characters of cybersecurity, from the Anonymous hacker group and the Stuxnet computer virus to the new cyberunits of the Chinese and US militaries. Cybersecurity and Cyberwar: What Everyone Needs to KnowÃƒâ Ã Â® is the definitive account of the subject for us all, which comes not a moment too soon.

Book Information

Audible Audio Edition
Listening Length: 11 hoursÃ Â andÃ Â 29 minutes
Program Type: Audiobook
Version: Unabridged
Publisher: Tantor Audio
Audible.com Release Date: January 26, 2016
Whispersync for Voice: Ready
Language: English
ASIN: B01AGPGP6Q
Best Sellers Rank: #37 inÃ Â Books > Computers & Technology > Security & Encryption > Privacy & Online Safety #70 inÃ Â Books > Audible Audiobooks > Nonfiction > Computers #77 inÃ Â Books > Audible Audiobooks > Politics & Current Events > Freedom & Security

Customer Reviews

If you’ve worked in IT for a couple of years, and if you have done your part to understand the world in which you are connected, then you might find this book to be written more for the managerial staff who decide on how they are going to invest in IT, and not so much for those who are in the trenches.

Like most people I was looking for answers to my personal LAN security issues and picked this book in the hopes of getting a deeper understanding of how to secure my network. But, I got an

even better deal instead. This book covers the entire state of cyber security issues from car theft by network interference to Cyberwar.The issue of network security has become global in scope and there are no political boundaries in Cyberspace. Nothing separates us personally from being raided by a thief whether he be an individual using an electronic jamer to keep your car unlocked or an employee of the Chinese government using commercial routers to collect personal data against you.The misuse and abuse of Cyberspace is predicated on the natural openness of the design of the Ethernet. Education about the current situation is our primary defense against those who would use this valuable tool against us. And this book does an excellent job of appraising us about the dangers and defenses inherent in this communications medium.This is not a book about how to setup the network security switches on your operating system. This is the book to tell you what has been happening in the entire world of Cyberspace that can affect you directly. Before you can defend yourself you need to know what the threat really is.Most of the book is spent covering the current world level security threat complex. With the exception of Denial of Service and RoboLensing attacks, the book gives the reader very good advice on how to deny the attackers effective access to your computer network. The general answer lies here.As in personal self defense, the answer comes through more effective communication with the security community and application of proper security measures. Reducing your threat cross section by using the approaches detailed in the book will help you to protect your data and your sleep.

In Cybersecurity and Cyberwar, co-authors Peter W. Singer and Allan Friedman provide public policy and national security professionals with a comprehensive overview of cybersecurity matters. In straightforward prose, Singer and Friedman answer key questions in three parts: how it all works, why it matters, and what can be done and address subjects ranging from advanced persistent threats, cyber force structure, options for deterrence, the balance between offense and defense, lessons from public health, to the incentives behind public-private partnerships. To round out the discussion, I would strongly recommend Cybersecurity and Cyberwar in conjunction with with RonaldDeibertÃƒÂ¢Ã â ¬Ã â„¢s Black Code: Inside the Battle for Cyberspace and Thomas RidÃƒÂ¢Ã â ¬Ã â„¢s Cyber War Will Not Take Place.

For those who want to keep up on the latest information of where we are in this cyber world, this book is for you. I just could not put it down. There are so many questions that we don’t find answers to in the local coffee shop. A sip of java and a shrug are not enough. For example, what is Stuxnet? Why is privacy so hard to maintain? Where do viruses and malware come from? Why can’t we catch

cyber villains? What are the larger threats? The smaller threats? What agencies protect us? What is cyber war? How can the ordinary person protect himself on line? So many important questions. Singer and Friedman have shown expertise in answering them, and sometimes with interesting stories from behind the scenes. For me, this is essential reading. And, like all things about computers, time sensitive. Read it now, and hope for a new book next year.

This book is a good high level overview of cybersecurity issues. The book is divided into three main sections: an overview of the internet, its history, and how it works, an examination of the various threats (from criminals to states to patriotic hackers) and both how and why attacks are performed, and then finally a section on what can be done from both a personal and policy level. All the information in the book is from a high level with only a basic amount of technical information. There are several sections that give some detail on particular incidents of hacking (such as stuxnet), but these too only give enough technical detail to help the reader understand what happened.I found the most interesting aspect of the book to be the policy-level discussions of hacking. If a state hacks another state and shuts down a power plant, what constitutes an appropriate response? Does it make sense for the victim state to move the conflict to the ÃƒÂ¢Ã â ¬Ã Å“realÃƒÂ¢Ã â ¬Ã Â• world and bomb an attackerÃƒÂ¢Ã â ¬Ã â„¢s power plant in retaliation? Also, the difficulties of determining just who initiated an attack are explored. All in all, I recommend this book for the reader who want a good overview of an issue that will likely dominate geopolitics in the coming decades.

Infrastructure Protection The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations Cybersecurity for Beginners Cybersecurity Exposed: The Cyber House Rules The Cybersecurity to English Dictionary