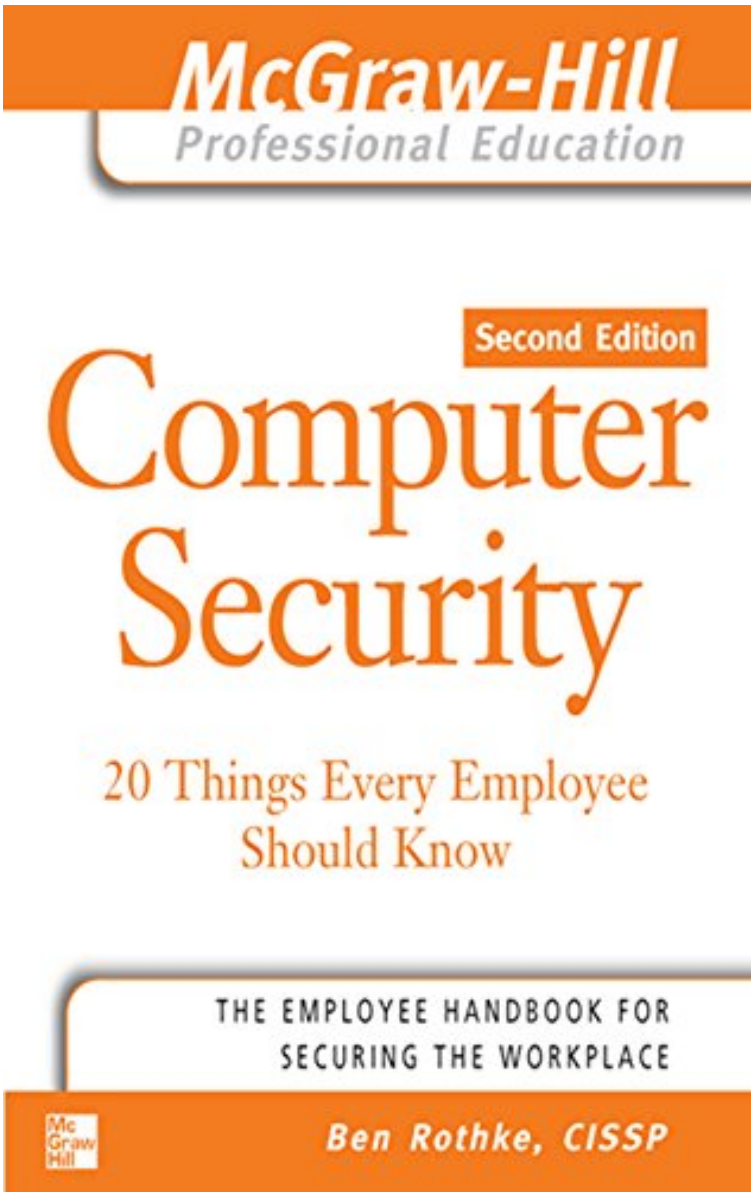
Computer Security: 20 Things Every Employee Should Know (McGraw-Hill Professional Education)

Von Ben Rothke
*DOC | *audiobook | ebooks | Download PDF | ePub*



Produktinformation -Verkaufsrang: #1455098 in eBooksVerffentlicht am: 2006-06-05Erscheinungsdatum: 2006-06-05File Name: B007VC4DAI | File size: 55.Mb

Von Ben Rothke : Computer Security: 20 Things Every Employee Should Know (McGraw-Hill Professional Education) before purchasing it in order to gage whether or not it would be worth my time, and all praised Computer Security: 20 Things Every Employee Should Know (McGraw-Hill Professional Education):

KundenrezensionenHilfreichste Kundenrezensionen1 von 1 Kunden fanden die folgende Rezension hilfreich. Everything Your Employees Need to Know about Computer SecurityVon Donald MitchellHaving served as the person in our firm with the most paranoia about computer security, I have been constantly struck by how careless people can be in this area. It's as though computer security can be assumed to be in place . . . rather than being something that needs to be encouraged, nurtured and observed.While I often read technical manuals on computer security to catch up with the latest, none of those manuals could hope to attract a full reading by anyone who has ever worked for me.I was delighted to find that the Second Edition of Computer Security: 20 Things Every Employee Should Know has everything in it that I hope all my employees will remember to do.The book is brief, it's accurate and it's easy to understand.If you follow Mr. Rothke's advice, most major problems will be avoided.The book opens by explaining about phishing and spyware by explaining what they are and why an employee should want to avoid them. Here's the advice:1. Don't reply or click on links asking for personal or financial information.2. Don't download programs from companies you don't know.3. Keep your computer secure with pop-up blockers, a fire wall, and anti-virus and anti-spyware software.I particularly liked the non-technical advice such as the one on avoiding identity theft.The book also has little case studies of what can go wrong. One of my favorites was an employee who wanted to go home and let a new employee use his security access card so she could keep working.Where there is a technical element, Mr. Rothke keeps that simple. For instance, protection by having a password that contains both numerals and letters is explained in terms of the new programs that can be used to check standard English words and names in a few minutes.There are also useful hints that are unrelated to being an employee such as being aware that your company may be tracking your usage. Do you really want people to know all about your personal habits? If not, don't pursue them at work or on a company device?For more complicated situations, Mr. Rothke explains when to go for help from the company's IT security team. Many people don't realize they can make things worse by trying to fix problems themselves.Nice going, Mr. Rothke!

KurzbeschreibungSecuring corporate resources and data in the workplace is everyones responsibility. Corporate IT security strategies are only as good as the employees awareness of his or her role in maintaining that strategy. This book presents the risks, responsibilities, and liabilities (known and unknown) of which every employee should be aware, as well as simple protective steps to keep corporate data and systems secure. Inside this easy-to-follow guide, youll find 20 lessons you can use to ensure that you are doing your part to protect corporate systems and privileged data. The topics covered include: Phishing and spyware Identity theft Workplace access Passwords Viruses and malware Remote access E-mail Web surfing and Internet use Instant messaging Personal firewalls and patches Hand-held devices Data backup Management of sensitive information Social engineering tactics Use of corporate resources Ben Rothke, CISSP, CISM, is a New York City-based senior security consultant with ThruPoint, Inc. He has more than 15 years of industry experience in the area of information systems security and privacy.KurzbeschreibungSecuring corporate resources and data in the workplace is everyones responsibility. Corporate IT security strategies are only as good as the employees awareness of his or her role in maintaining that strategy. This book presents the risks, responsibilities, and liabilities (known and unknown) of which every employee should be aware, as well as simple protective steps to keep corporate data and systems secure. Inside this easy-to-follow guide, youll find 20 lessons you can use to ensure that you are doing your part to protect corporate systems and privileged data. The topics covered include: Phishing and spyware Identity theft Workplace access Passwords Viruses and malware Remote access E-mail Web surfing and Internet use Instant messaging Personal firewalls and patches Hand-held devices Data backup Management of sensitive information Social engineering tactics Use of corporate resources Ben Rothke, CISSP, CISM, is a New York City-based senior security consultant with ThruPoint, Inc. He has more than 15 years of industry experience in the area of information systems security and privacy.SynopsisThis work uses a friendly approach to cover employee IT security. Each chapter includes a description of a real-world scenario of an employee who deliberately or unknowingly committed an IT security violation.