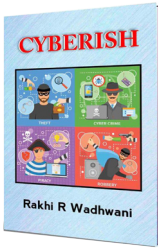
Cyber Books (An Initiative by) Scholastic Seed Inc.

A book is a number of pieces of paper, usually with words printed on them, which are fastened together and fixed inside a cover of stronger paper or cardboard. Cyber books can be a new initiative by Scholastic Seed Inc. The purpose behind this is to make students, learners and researchers familiar with the latest books available on cyber and upcoming technology which either relates to cyber or revolves around that.



Book Name: **Cyberish**
Author Name: **Rakhi R Wadhwani**
Reviewer Name: **Dr. Shilpa Agrawal**, Psychologist and Educationist

The book “Cyberish” provides an honest overview of the history and key issues in cyber-security for those wondering just how real the threats are.

Cyberish aims to cover the history as well as the size of cyber-crime, cyber espionage, cyber-warfare and a few of related online threats.

It all started with war 2 code breakers and MIT students exploring the communication system. Although Steven Levy's Hackers continues to be the classic read on the initial meaning of 'hackers', it's nice to figure out mention here. Author Rakhi R Wadhwani indicates that it wasn't until phone hacker John Draper was sent to prison that criminals must see phone phreaking in action. However, it wasn't until the 90s that there are juicy enough targets to induce them really fascinated by computer hacking.

This section can be a potted history of how hacks progressed from breaking into Prince Philip's mailbox on the Prestel service, to Russian criminals recruiting local hackers who knew how to enter the banks, to political and activist hacking in eastern Europe geared toward giving people free access to information, to the rise of viruses and malware as mass vandalism within the 90s, and so the beginnings of large-scale criminal attacks.

Even if you've followed security issues for ages, there are interesting nuggets: the concept of a self-replicating program goes all the way back to computer pioneer John Neumann, as an example, while the first virus 'in the wild' was for the Apple II.

The history of cyber-espionage is additionally a good overview, majoring on reports from intelligence services covering the large-scale, organized attacks that are speculated to be seizing from small, targeted break-ins at specific companies. Are Russia and China hovering up IP from Western countries in an exceedingly very concerted attempt to exploit our R&D work? One MI5 report mentions two unnamed companies that have lost money or business opportunities through holding theft.

The author makes several useful points about how everyone must remember of hacking. Security hardware company RSA got hacked because the attackers targeted their recruitment team with social engineering techniques, as an example. Sharing your personal data online puts you at risk of fraud (52 percent folks share details that show up as security questions, a recent Intel survey points out). And if you wonder why such an enormous amount of malicious Android apps in Google Play only encourage hovering up the contents of your address book, it'd be to check email addresses scraped from websites to figure out if it's worth sending them spam.

These are the familiar old crimes, attacks, protests and acts of vandalism — but committed using modern tools, that produces them easier to commit, harder to induce caught at and absolute to own more widespread or more serious effects.

After this much sense, the chapter on botnets is strangely melodramatic. Of all the online threats, why do these reek of science fiction? With few known samples of cyber-criminals and cyber-spies, we get an odd section contrasting scientist with free software champion Richard Stallman, and a list of universities where you will be ready to study cyber-spying to induce employment in counter-intelligence. The brief mention of 'cyber mules' who collect the proceeds of the various online crimes disguises the actual fact that the go-betweens receiving the products ordered together with your stolen MasterCard can be the 000 reason it's so hard to forestall these reasonably thefts.

The section on child safety sits barely oddly with the rest of the book — but Author Rakhi incorporates a background in covering smut, and it does mean the book covers almost the entire range of security issues. The good judgment point that you just must both teach children to look at out and practice good computer security yourself is additionally welcome.

These are the familiar old crimes, attacks, protests and acts of vandalism — but committed using modern tools. That produces them easier to commit, harder to induce caught at and guaranteed to possess more widespread or more serious effects. However, "the essence of the crimes remains the same: bad people wanting your money, individuals desirous to victimize others or societies and corporations need to steal their competitors' secrets".

Once you've finished reading the “Cyberish”, it should be clear that online threats are serious because we're now smitten by the technology. But you still must structure your own mind on quite how dangerous those threats are. If you too recall the name of your loved one who doesn't take computer security seriously enough, or who is worrying unduly about the cyber security, this might be an honest present to educate them with.

A must read for all netizens, students and teachers too. My best wishes.