Review

Phishing and communication channels: a guide to identifying and mitigating phishing attacks
Sonowal G., Apress, New York, NY, 2021. 240 pp. Type: Book (978-1-484277-43-0)

Date Reviewed: Jan 12 2023

Full Text

It is not far-fetched to say that most (if not all) *CR* readers have been subjected to some sort of phishing attack--and even more likely if we consider the wide taxonomy of activities that Sonowal's book covers. Can we as individuals identify them before falling prey? Can we as systems administrators detect them before our users are delivered potentially harmful content? Can we as application programmers write secure code that thwarts the most common attacks? Are there nontechnical resources that can be applied to combat phishing?

And, above all, what is phishing? It is a generic term that can be applied to many different kinds of Internet scams where victims are lured to divulge their credentials (login information, bank card numbers, or whatever personal information of value is sought) to attackers. This book presents many different specific terms for each of the many attack types.

The book aims at teaching readers the necessary skills for answering the above questions. The list of topics covered by each of the chapters is very comprehensive and wide-ranging: from the socio-historical development of Internet phishing, presenting attacks that have become important milestones since the first documented Internet personal information gathering attack, in 1987, to legal and artificial intelligence (AI)-driven ways to detect and fend off phishing attempts.

While not a very large book, it covers a very wide range of topics. This necessarily means that many of them are covered in a very brief way. Each chapter tackles a very different angle on phishing, which means the topics are covered in a succinct, telegraphic way: many concepts are presented as one or two paragraphs, very often fitting several of them on the same page.

Indeed, the topic list is too broad, and probably the book would have benefited from having a more narrow focus. As an example, while attacks to the Dynamic Host Configuration Protocol (DHCP) protocol (responsible for delivering IP addresses to computers on a local network) can lead to a local attacker delivering deceitful content to users, the impact is on the local network only--and, in my opinion, it can barely be considered relevant to this book. And while only one page is spent on this attack, there are many similar topics throughout.

There is little connection throughout the sections of each chapter. Focus jumps from one attack type to another, or from one training method to another, or from one legal solution to another, somewhat abruptly and without building on previous concepts. The way it is structured might make it better suited as a reference work, but it is harder to use as reading material. Some typographical changes would probably make the book easier to read. I found the decision to have each little topic presented as a separate subsection disrupted my reading flow.

Having a separate bibliography section for each chapter was a good idea. Given that the content is so different between each chapter, the bibliography sections are kept topically relevant, increasing the feeling of the work as a reference rather than as a book for learning about a topic.

The book has four appendixes that don't focus on phishing but on artificial intelligence (AI) methods. Not only are they thematically different, but the pace and language also shifts, tending more to mathematical definitions. This would make sense if AI-based methods were more thoroughly covered, but they were only presented in the second half of the last chapter. It is hard for me to justify the author's inclusion of them.

The book as a whole is indisputably interesting and covers a rich breadth of topics, but it is not an easy cover-to-cover read. Better thematic threading in a future edition would be most welcome. The intended audience is intermediate; experts in different areas of computing will benefit from reading about their respective interests, but the book assumes an introductory to intermediate level throughout.

Reviewer: Gunnar Wolf Review #: CR147536

SHARE

Would you recommend this review? yes no Enter

Other reviews under "**Security and Protection**":

	Date
CIRCAL and the representation of communication, concurrency, and time Milne G. ACM Transactions on Programming Languages and Systems 7(2): 270-298, 1985. Type: Article	Oct 1 1985
Computer security risk management Palmer I., Potter G., Van Nostrand Reinhold Co., New York, NY, 1989. Type: Book (9780442302900)	Apr 1 1991
Computers at risk , National Academy Press, Washington, DC, 1991. Type: Book (9780309043885)	Oct 1 1991

more...

E-Mail This Printer-Friendly