FOREWORD REVIEWS THE INDIE WE LOVE.

Clarion Review ★★★★½ TECHNOLOGY

Digital Danger: AI, Cybersecurity, and the Fight for Our Future

Eric Cole
Amplify Publishing
(208pp)
979-889138952-6

A practical guide to navigating contemporary technological challenges, Digital Danger *pairs overviews of how hackers operate with clear enumerations of the steps that individuals can take to safeguard themselves against developing threats.*

Former white-hat CIA hacker Eric Cole's revealing technology guide *Digital Danger* concerns the threats posed by cybercriminals.

Arguing that cybersecurity is more important in an era of artificial intelligence, the book outlines the extent of the threat, policy failings, and methods for keeping devices safe and secure. It asserts that all people are potential targets and critiques how the legal system lags behind technological advancements. Distinctions are drawn between cybersecurity approaches at home, at work, and in public, and the book does an able job of encouraging people to cultivate safe habits, including being aware, making use of verification options, and adopting two-factor authentication.

After outlining the risks and costs of cyberattacks and how artificial intelligence has been used to automate attacks—indeed, the book's enumeration of various types of cyberattacks, including SIM swapping, number hijacking, smishing, vishing, and QR-ishing is thorough—the book addresses the practical protective measures one can take online. Each chapter examines different security measures relating to computers, smartphones, and streaming, drawing on personal stories and insights from Cole's decades within the cybersecurity field.

Edifying insights about the ways in which hackers exploit human psychology and about how AI iterates attacks toward success are proffered. The book's anonymous anecdotes are less persuasive, though, because of their limited details, and some commentary, as about people's average screen-time usage, appear sans supporting sources. Further, the excessive use of subheadings and bullet-point lists makes its progression choppy at times.

Nonetheless, the book is sobering when it comes to detailing the international scope of cybercrime, the lack of jurisdiction that law enforcement agencies often run into, and the patchwork of policies that fail to provide cohesive protection against cyberattacks. It is clinical in its diagnoses, too, asserting that the average age of congresspeople means that too many are unfamiliar with the technology they could be regulating to keep their constituents safe. Its proposals are persuasive as well, thanks to its direct, concrete language, as when outlining all of the ways in which cyberattacks erode trust in institutions like hospitals, schools, and elections.

An eye-opening technology guide, *Digital Danger* empowers people by informing them about how artificial intelligence scales up the speed and severity of cyberattacks.

JOSEPH S. PETE (April 17, 2026)