1. Record Nr. UNINA9910583387903321

Autore	Kurtz Jennifer Ann
Titolo	Hacking wireless access points : cracking, tracking, and signal jacking / / Jennifer Ann Kurtz, Information Assurance Affiliate Faculty at Regis University ; Richard Kaczmarek, technical editor
Pubbl/distr/stampa	Cambridge, MA : , : Syngress, , [2017] 2017
Edizione	[1st edition]
Descrizione fisica	1 online resource (xv, 155 pages) : illustrations (some color)
Collana	Gale eBooks
Disciplina	004.1675068
Soggetti	Wireless LANs - Security measures Hacking Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	chapter 1. Wireless technology overview -- chapter 2. Wireless adoption -- chapter 3. Blurred edges : fixed and mobile wireless access points -- chapter 4. Hacks against individuals -- chapter 5. WAPs in commercial and industrial contexts -- chapter 6. WAPs in medical environments -- chapter 7. Hacking wireless access points : governmental context -- chapter 8. Noncivilian government context -- chapter 9. Summary and call to action.
Sommario/riassunto	Hacking Wireless Access Points: Cracking, Tracking, and Signal Jacking provides readers with a deeper understanding of the hacking threats that exist with mobile phones, laptops, routers, and navigation systems. In addition, applications for Bluetooth and near field communication (NFC) technology continue to multiply, with athletic shoes, heart rate monitors, fitness sensors, cameras, printers, headsets, fitness trackers, household appliances, and the number and types of wireless devices all continuing to increase dramatically. The book demonstrates a variety of ways that these vulnerabilities can be—and have been—exploited, and how the unfortunate consequences of such exploitations can be mitigated through the responsible use of technology. Explains how the wireless access points in common,

everyday devices can expose us to hacks and threats Teaches how wireless access points can be hacked, also providing the techniques necessary to protect and defend data Presents concrete examples and real-world guidance on how to protect against wireless access point attacks