Built Environment Cybersecurity

- Data Security in Transit and at Rest
- Application Software Security
- Endpoint Device Security
- Network Architecture Security
- Network Perimeter Security
- Physical Security
- Employee Training, Policies and Procedures

Ernest Schirmer, Senior Associate, Building Technology Systems, WSP USA, One Penn Plaza, New York, NY 10019

The nation's energy grid is constantly under attack by hackers.

In fiscal year 2014, there were 79 hacking incidents at energy companies that were investigated by the Computer Emergency Readiness Team, a division of the Department of Homeland Security. There were 145 incidents the previous year.

The outermost defenses aren't holding up. Between April 2013 and 2014, hackers managed to break into 37% of energy companies, according to a survey by ThreatTrack Security.

Cybersecurity firm FireEye (FEYE) identified nearly 50 types of malware that specifically target energy companies in 2013 alone, according to its annual report. Energy firms get hit with more spy malware than other industries, according to a 2014 study by Verizon (VZ).

In March, TrustedSec discovered spy malware in the software that a major U.S. energy provider uses to operate dozens of turbines, controllers and other industrial machinery. It had been there for a year -- all because one employee clicked on a bad link in an email.

76 Percent of North American Utilities Expect Moderate Cyberattack Risk

Oct 4, 2017

POWER Engineering

Videos Webcasts White Papers Events Magazine Jobs

POWER-GEN

HOME GAS COAL RENEWABLES O&M ONSITE POWER NUCLEAR ENERGY ST

Home » More O&M Industry News » Video: What Do Russia's Hacks Mean for the U.S. Power Grid?

Video: What Do Russia's Hacks Mean for the U.S. Power Grid?

03/15/2018

US Accuses Russia of Ongoing Operation to Hack Energy Grid

03/15/2018

News

New York Technology

Cybersecurity A Pressing Concern As Real Estate Companies Bring Sensitive Data Online

March 15, 2018 | Berdon LLP | Staff Reporter, Bisnow

Facebook Twitter LinkedIn Email Print

Christopher Bowns/Flickr

Although commercial real estate deals primarily with tangible assets, it is becoming an increasingly information-intensive industry, generating a number of highly sensitive and exploitable records and contracts.

TECHNOLOGY

New gaming and hospitality cybersecurity alliance formed by Retail ISAC

Securing Vehicle to Vehicle Communications using Blockchain through Visible Light and Acoustic Side-Channels

Sean Rowan, Michael Clear, Mario Gerla*, Meriel Huggard, Ciarán Mc Goldrick
School of Computer Science and Statistics, Trinity College Dublin, Ireland
Department of Computer Science, UCLA, Los Angeles, USA*
sprowan@tcd.ie, clearm@tcd.ie, gerla@cs.ucla.edu*, Meriel.Huggard@cs.tcd.ie, Ciaran.McGoldrick@sess.tcd.ie

black hat WEBCASTS

REGISTER NOW

PLEASE JOIN US FOR THE NEXT INSTALLMENT IN THE BLACK HAT WEBCAST SERIES

Incorporating Human Vulnerability Assessments into your Threat Assessment Model

Thursday, March 29, 2018

08:00AM - 09:00AM PT

60 MINUTES, INCLUDING Q&A

This presentation will discuss the ways in which simulated phishing tests and training is presently being conducted by small and large for-profit and federal government organizations. Next, using data from actual pen-tests and different forms of training, the presentation will discuss the strengths and limits of each approach. Finally, the presentation will provide alternative ways to go beyond simply assessing clicks to more accurately assessing and tracking employee cyber vulnerability within the organization by focusing on the employee cognitive-behavioral patterns. Read More>>

Sponsored by: COFENSE

MIT Technology Review

Topics+ The Dow

BUSINESS OF BLOCKCHAIN MIT Technology Review

Intelligent Machines

NSA's Own Hardware Backdoors May Still Be a "Problem from Hell"

Revelations that the NSA has compromised hardware for surveillance highlights the vulnerability of computer systems to such attacks.

by Tom Simonite October 8, 2013

FEATURED STORY

Off-The-Shelf Smart Devices Found Easy To Hack

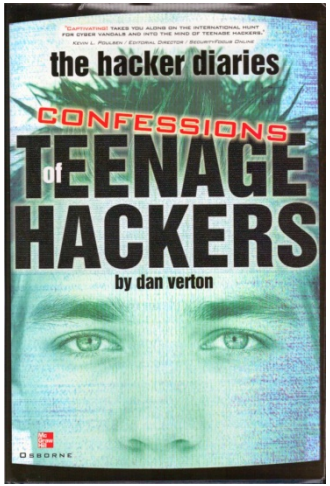
Off-the-shelf devices that include baby monitors, home security cameras, doorbells, and thermostats were easily co-opted by cyber researchers at Ben-Gurion University of the Negev (BGU). As part of their...

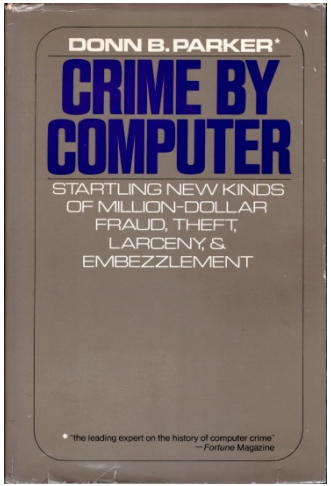
1 in 3 Michigan workers tested opened fake 'phishing' email

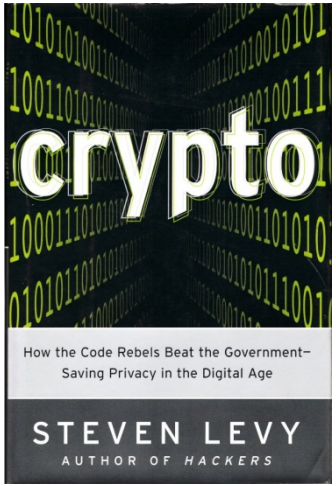
March 16, 2018 by David Eggert

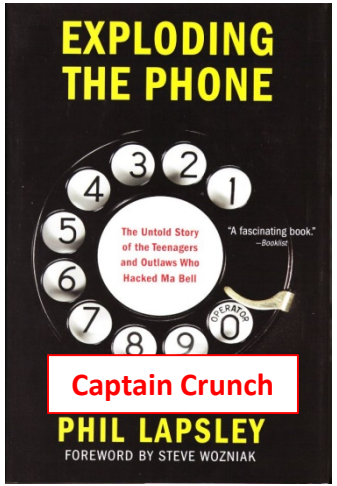
Credit: CC0 Public Domain

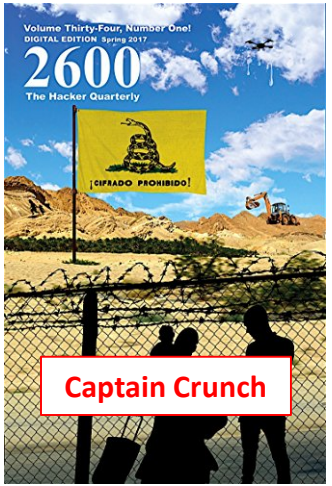
Michigan auditors who conducted a fake "phishing" attack on 5,000 randomly selected state employees said Friday that nearly one-third opened the email, a quarter clicked on the link and almost one-fifth entered their user ID and password.

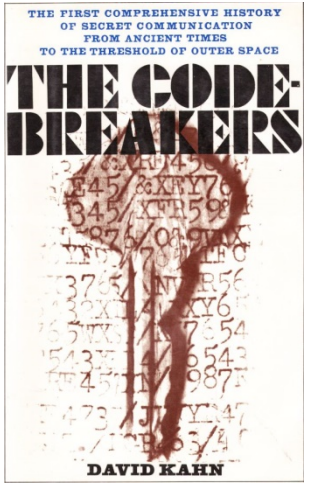

the hacker diaries
CONFESSIONS of TEENAGE HACKERS
by dan verton
OSBORNE

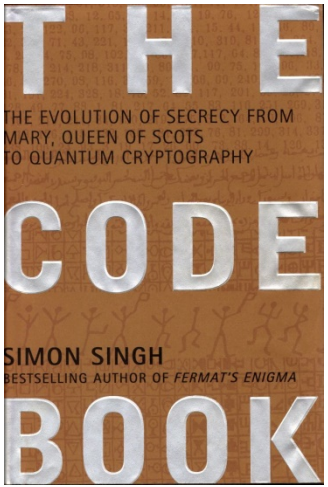

DONN B. PARKER
CRIME BY COMPUTER
STARTLING NEW KINDS OF MILLION-DOLLAR FRAUD, THEFT, LARCENY & EMBEZZLEMENT
"the leading expert on the history of computer crime"
—Fortune Magazine

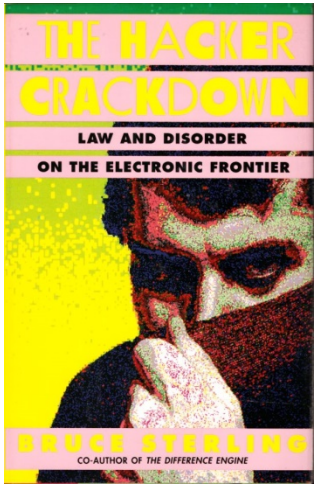

crypto
How the Code Rebels Beat the Government–Saving Privacy in the Digital Age
STEVEN LEVY
AUTHOR OF HACKERS

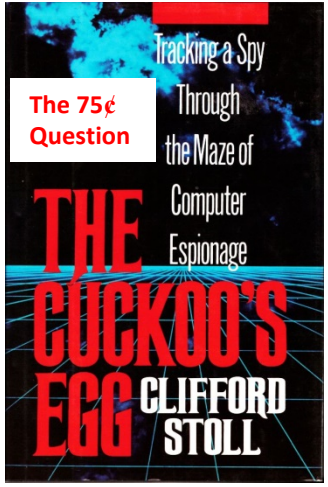

EXPLODING THE PHONE
The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell
"A fascinating book."
—Booklist
Captain Crunch
PHIL LAPSLEY
FOREWORD BY STEVE WOZNIAK

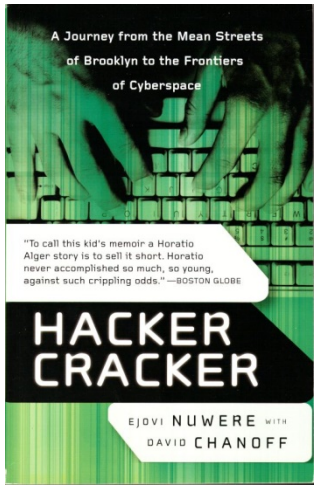

Volume Thirty-Four, Number One!
DIGITAL EDITION Spring 2017
2600
The Hacker Quarterly
¡CIFRADO PROHIBIDO!
Captain Crunch

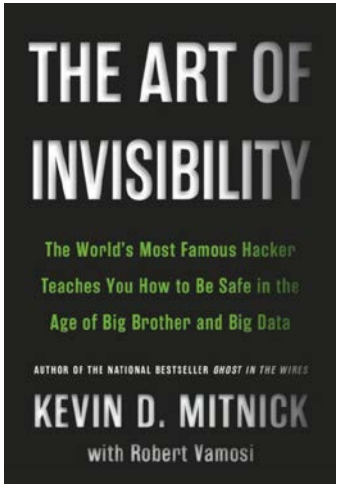

THE FIRST COMPREHENSIVE HISTORY OF SECRET COMMUNICATION FROM ANCIENT TIMES TO THE THRESHOLD OF OUTER SPACE
THE CODE-BREAKERS
DAVID KAHN

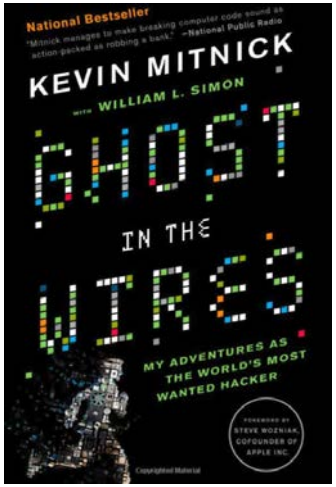

THE
THE EVOLUTION OF SECRECY FROM MARY, QUEEN OF SCOTS TO QUANTUM CRYPTOGRAPHY
CODE
SIMON SINGH
BESTSELLING AUTHOR OF FERMAT'S ENIGMA
BOOK

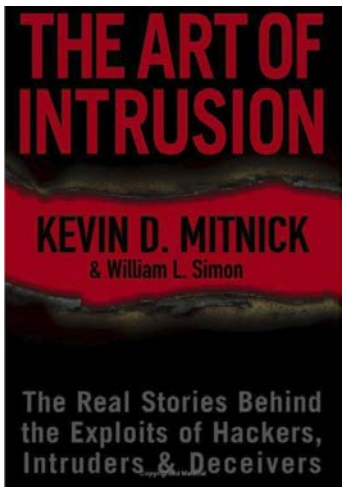

THE HACKER CRACKDOWN
LAW AND DISORDER ON THE ELECTRONIC FRONTIER
BRUCE STERLING
CO-AUTHOR OF THE DIFFERENCE ENGINE

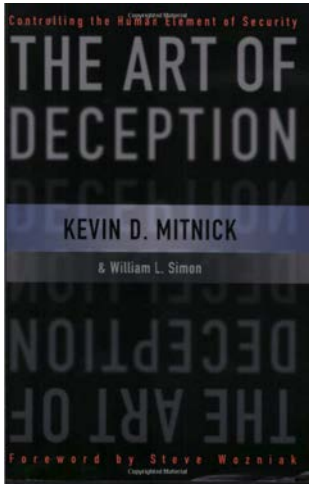

The 75¢ Question
Tracking a Spy Through the Maze of Computer Espionage
THE CUCKOO'S EGG
CLIFFORD STOLL

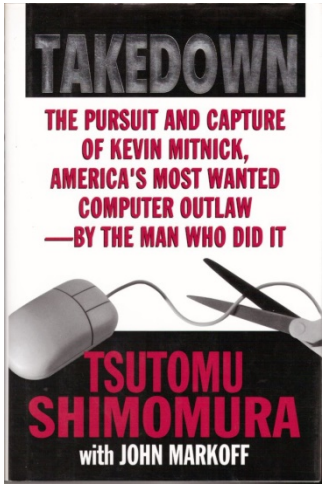

A Journey from the Mean Streets of Brooklyn to the Frontiers of Cyberspace
"To call this kid's memoir a Horatio Alger story is to sell it short. Horatio never accomplished so much, so young, against such crippling odds." —BOSTON GLOBE
HACKER CRACKER
EJOVI NUWERE WITH DAVID CHANOFF

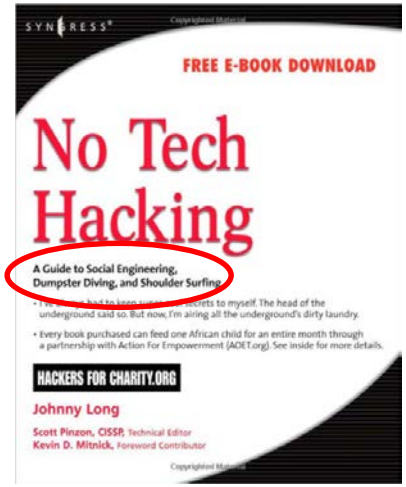












- **The biggest threat to an organization is a disgruntled employee.**
- **Social Engineering is easier, faster and cheaper than hacking.**
- **Training, policies, procedures and physical security are an integral part of Cybersecurity.**

Technology

Cybersecurity: Plan for the worst, and expect to be hacked despite all best efforts A panel presented by NJBIZ

March 19, 2018 at 3:00 AM

Cyberattacks on American businesses large and small regularly bubble up in the mainstream press, but having to deal with such incidents — before, during or all-too-often after the fact — are a daily fact of life for company executives and entrepreneurs.

SEMPER VIGILANS

TRUST AND VERIFY

SEE SOMETHING, SAY SOMETHING