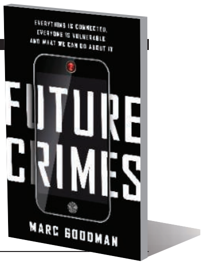
IMAGE: MAGNILION/ISTOCKPHOTO

TECHNOLOGY

Cyber crime 2.0

In a world where everything is connected, how will we balance security and privacy?

By **Dov Greenbaum**


EVERYTHING IS CONNECTED, EVERYONE IS VULNERABLE AND WHAT WE CAN DO ABOUT IT
FUTURE CRIMES
MARC GOODMAN

Future Crimes
Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It
Marc Goodman
Doubleday, 2015. 462 pp.

In *Future Crimes*, author Marc Goodman takes the reader on a well-researched whirlwind tour of Internet-based crime. According to Goodman, the shadowy "Crime Inc." (his catch-all term for all that is malicious on the Internet) is a virtually unstoppable force that, combined with the trend toward a global Internet of Things, leaves us more susceptible to criminal activity than ever.

Although we may legitimately fear Big Brother, and particularly the National Security Agency, which seems to be able to surveil us as it pleases, Goodman reminds us that we must also remain vigilant against criminal enterprises that trade in our identities, credit card numbers, and other personal and private information. According to Goodman, we are very much complicit in the vulnerable position in which we find ourselves. Goaded on by free software services, we wantonly share our most intimate and private information online for others to gather and sell, ignoring the maxim "If you're not paying for it, you're not the customer, you're the product."

Alarmingly, it turns out that all this time online hasn't made us any less gullible. According to Goodman, even sophisticated users can be duped into believing falsified information presented on our trusted devices. In one example, Goodman recounts how, in August 2000, a 23-year-old community college student successfully manipulated the stock market by posting a fake press release about an investigation into a Nasdaq-traded company to an Internet newswire. Investors lost over a hundred million dollars within minutes when the press release went viral.

The title of the book is somewhat of a misnomer. In addition to discussing the future of Internet crime, Goodman provides many engaging examples of past and current online criminal activities. In many of these examples, Goodman describes how bad actors have exploited a number of everyday devices. For example, in one relatively benign case, hackers commandeered webcams, alarms, computer peripherals, and even refrigerators to send out hundreds of thousands of malicious e-mail messages. Goodman instills a fear of imminent disaster by encouraging us to consider what could have happened had the devices been part of more critical infrastructure, such as Internet-enabled artificial limbs, automobiles, avionics, or advanced traffic control systems.

There are numerous hardware and/or software implementations that could be employed by the typical layperson to avoid becoming a victim of the criminal capers described in the book, including, at minimum, encrypting our e-mail, keeping current with security patches and antivirus software, and employing robust aliases. However, Goodman glosses over many of these tools. Perhaps this is because the benefits associated with these technologies come at a relatively high price, requiring users to sacrifice conveniences such as easy-to-remember passwords and user-friendly, but less rigorous, security protocols.

For all the good that security-promoting technologies have to offer, they can't seem to shake negative connotations. The very use of encryption technologies, for example, has been viewed by some as incriminating (*1*). Recently, the United Kingdom's Prime Minister David Cameron threatened to shut down popular messaging applications that employ encryption, including Facebook's WhatsApp and Apple's iMessage, arguing that these sites represent safe havens for terrorist communications (*2*). Such a knee-jerk reaction to established and wildly popular technologies would harm freedom of expression and would likely prove ineffective. Not only could terrorists and criminals turn to a myriad of alternative solutions to encrypt their communications, there is also no indication that being able to intercept encrypted messages is of any value in thwarting terrorism (*3*). Such governmental efforts tend to create additional privacy concerns for the general public, can disincentivize innovation in these and related areas of technology, and can result in additional costs—for example, those associated with developing compliance technologies, which are then passed on to the consumer.

There is no easy solution for finding the balance between security and privacy. The best we can hope for is to encourage discussions early on in the development of new technologies such that reasonable concerns are adequately addressed without impeding innovation. Books like *Future Crimes* will be helpful in starting these conversations.

The reviewer is at the Zvi Meitar Institute for Legal Implications of Emerging Technologies, Radzyner Law School, Interdisciplinary Center, Herzliya, Israel; and Yale University, Department of Molecular Biophysics and Biochemistry, New Haven, CT, USA. E-mail: dov.greenbaum@yale.edu

REFERENCES

1. N. Kayyali, K. Rodriguez, Security is not a crime—Unless you're an anarchist, Electronic Frontier Foundation, 16 January 2015; https://www.eff.org/deeplinks/2015/01/security-not-crime-unless-youre-anarchist.
2. C. Bennet, Britain could ban Snapchat, WhatsApp, *The Hill*, 13 January 2015; http://thehill.com/policy/cybersecurity/229307-britain-could-ban-snapchat-whatsapp.
3. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 2 July 2014; www.pclob.gov/library/702-Report.pdf.

10.1126/science.aaa7298

Cyber crime 2.0
Dov Greenbaum (April 9, 2015)
Science **348** (6231), 193. [doi: 10.1126/science.aaa7298]

Science (print ISSN 0036-8075; online ISSN 1095-9203) is published weekly, except the last week in December, by the American Association for the Advancement of Science, 1200 New York Avenue NW, Washington, DC 20005.