FBI Library
Subject Bibliography

CYBERCRIME

May 2010

Computer and Information Security Handbook. (2009). Boston, MA : Elsevier.
Call Number: QA76.9.A25
Abstract: Gathers 50 industry experts on computer security issues. Subjects include network forensics, data encryption, homeland security, biometrics, and preventing system intrusion.

Cyber Fraud: Tactics, Techniques, and Procedures. (2009). Boca Raton, FL: CRC Press.
Call Number: HV6773.C93
Abstract: Seventeen authors/editors describe the cyber criminal culture--phishing, pharming, trojans, and pump and dump scams. With examples of fraudulent email scams, organizations can better enhance their computer security.

Cyber-Security and Global Information Assurance: Threat Analysis and Response Solutions. (2009). Hershey, PA: Information Science Reference.
Call Number: QA76.9.A25C918 2009
Abstract: Written by experts from all over the world, the book is divided into four sections which cover black markets, insider threats, security implications, information sharing and honeypots. Concludes with security technologies and emergency response planning.

Cybercrime: Public and Privates Entities Face Challenges in Addressing Cyber Threats. (2007). Washington, DC: GAO.
Abstract: To determine the impact of cybercrime on the economy and security of the US, GAO analyzed multiple reports, studies and surveys and held interviews with public and private officials.

Handbook of Internet Crime. (2010). Cullompton: Willan.
Call Number: HV6733.H36 2010
Abstract: Brings together the leading experts in the field to address the many issues facing criminologists today. Explores the global nature of cybercrime, deviance, policy, and law and regulation in the 21st century.

Information Security: Concerted Response Needed to Resolve Persistent Weaknesses. (2010). Washington, DC: GAO.
Notes: Available full text: http://www.gao.gov/new.items/d10536t.pdf
Abstract: GAO identified five key control categories in 24 major federal agencies--access control, configuration management, segregation of duties, continuity of operations, and security management. Examines the information security weaknesses in these areas and strategies for improvement.

Socioeconomic and Legal Implications of Electronic Intrusion. (2009). Hershey, PA: Information Science Reference.
Call Number: HV6773.S635 2009
Abstract: Analyses four domains--the social and economic dynamic for electronic crime; electronic intrusion; and forensic challenges for intrusion. Provides insights into global theft and spam, identity theft fraud, and electronic crime issues.

Aquilina, J. (2008). Malware Forensics: Investigating and Analyzing Malicious Code. Burlington, MA: Syngress Publishing.
Call Number: QA76.9.A25A68 2008
Abstract: Written by information security experts, provides a how-to guide to responding to a malicious code incident. Features tools, diagrams, examples and checklists along with the legal ramifications and requirements governing malware.

Biegelman, M. (2009). Identity Theft Handbook: Detection, Prevention, and Security. Hoboken, NJ: Wiley.
Call Number: HV6679.B54 2009
Abstract: Beginning with a history of identity theft, the author discusses data breaches, medical identity theft, importance of interactive organized crime, victim rights, rules to stop identity theft, and child identity theft.

Bossler, A. (2010). On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. International Journal of Cyber Criminology, 3(1), 400-420.
Notes: Available from www.cybercrimejournal.com
Abstract: The Internet has provided crime opportunities that could not exist without cyberspace. In an effort to reduce cybercrime victimization, a sample of college students from a single university were studied to see how malware spreads.

Brancik, K. (2008). Insider Computer Fraud: An In-depth Framework for Detecting and Defending Against Insider IT Attacks. Boca Raton, FL: Auerbach Publications.
Call Number: QA76.9A25B725 2008
Abstract: Discusses risk assessment, threat modeling, privacy assessment, cyber security, application security, web services and computer architecture as it relates to insider threat identification and prevention. Contains a cyber-security health check.

Brenner, S. (2010). Cybercrime: Criminal Threats from Cyberspace. Santa Barbara, California: Praeger.
Call Number: HV6773.B75 2010
Abstract: Traces the history of cybercrime and explains the various types--identity theft, stalking, extortion, and viruses. Describes the dilemma facing law enforcement in regard to protecting the privacy of US citizens and the pursuit of cybercriminals.

Carr, J. (2010). Inside Cyber Warfare. Sebastopol, California: O'Reilly Media, Inc.
Call Number: QA76.9.C924C37 2010
Abstract: Details how acts of violence are carried out via the Internet, and the complicated issues involved--such as when should cyber attacks be treated as acts of war. Describes state versus non-state attacks (cyber attacks carried out by an individual). Various legal issues about cyber attacks and legal versus illegal retaliation are covered. Includes how social web sites are being mined for information, and how China is determined to penetrate the networks of the West. Concludes with four scenarios, and options to responding to cyber attacks.

Chiesa, R. (2009). Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking. Boca Raton, FL: Auerbach Publications.
Call Number: HV6773.C477 2009
Abstract: Written by the Italian hacker Raoul Chiesa, who today uses his skills and abilities to find ways to protect networks and computers systems, the work draws from research conducted by the Hackers Profiling Project(HPP), supported by the UN's Interregional Crime and Justice Research Institute(UNICRI). HPP is a multi-year study aimed at applying the behavioral science of criminal profiling to the world of hacking and cybercrime.

Dube, R. (2008). Hardware-based Computer Security Techniques to Defeat Hackers: From Biometrics to Quantum Cryptography. Hoboken, NJ: Wiley.
Call Number: QA76.9A25D8152 2008
Abstract: Provides an overview of security in both hardware and software systems. Issues discussed include password strength and tamper-evident hardware. The last chapter, "Putting It All Together" unites all the topics and shows readers how they can implement the strategies discussed. Also included are two examples of security systems put into practice.

Erickson, J. (2008). Hacking: The Art of Exploitation. San Francisco, CA: No Starch Press.
Call Number: QA76.9A25E75
Abstract: The author introduces Linux C programming from a hacker's perspective. Explains machine architecture, network communications, and existing hacking techniques.

Jacobson, G. (2009). Cybersecurity, Botnets, and Cyberterrorism. New York: Nova Science Publishers.
Call Number: HV6773.J33 2009
Abstract: Discusses how cybercriminals and botnets (large networks of infected PCs) are becoming more sophisticated in their attacks. Describes how terrorist groups could obtain services from cybercriminals to attack the infrastructure of the United States and how to prevent these attacks.

Jaishankar, K. (2008). Identity Related Crime in the Cyberspace: Examining Phishing and Its Impact. International Journal of Cyber Criminology, 2(1), 10-15.
Notes: Available from www.cybercrimejournal.com
Abstract: Describes the growing importance of identity in the age of the Internet, and the rise in identity related cybercrime--especially phishing, done by the use of malware and spam. Many new Internet surfers become victims of phishing--concludes that governments need to create more awareness of this crime as the number of Internet searchers increases.

Knetzger, M. (2008). Investigating High-Tech Crime. Upper Saddle River, NJ: Pearson/Prentice Hall.
Call Number: HV8079.C65K54 2008
Abstract: Provides an overview of the major current computer crimes or cyber crimes and specific investigative techniques needed to combat them. Written for first responders, many practical examples are provided.

Krekel, B. (2009) Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation [Web Page]. URL http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.
Abstract: Discusses the Chinese offensive strategy for information warfare--simultaneous application of electronic warfare and computer network applications against an adversary's command, control, communications, computers, intelligence, surveillance and reconnaissance (C41SR) networks.

Libicki, M. (2009). Cyberdeterrence and Cyberwar. Santa Monica, CA: RAND.
Call Number: U163.L539 2009
Abstract: Discusses operational cyberwar and how cyberdefense remains the Air Force's most important activity within cyberspace. Describes actions governments can take to protect themselves in the face of a cyberattack, including diplomatic, economic, and prosecutional efforts.

Menn, J. (2010). Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet. New York: Public Affairs.
Call Number: HV6773.M46 2010
Abstract: Describes the efforts of Barrett Lyon, an Internet security expert, and Andy Crocker, a British detective, and their work to identify cyber-criminals. Details how Russia and China are protecting Internet criminals because they are helping them build offensive cyber-weapons.

Nhan, J. (2009). Finding a Pot of Gold at the End of an Internet Rainbow: Further Examination of Fraudulent Email Solicitation. International Journal of Cyber Criminology, 3(1), 452-475.
Notes: Available from www.cybercrimejournal.com
Abstract: Discusses unsolicited mass e-mails, spam and the growing problems of fraud and deception. The findings from this study help provide direction for preventing and responding to computer fraud --both legislative and law enforcement efforts.

Pontell, H. (2009). White-Collar Delinquency. Crime, Law and Social Change, 51(1), 147-162.
Notes: http://www.springerlink.com/content/a5q772733j820220/fulltext.pdf
Abstract: Discusses "white-collar delinquency"--computer crimes committed by underage offenders. These acts by computer hackers have evolved into major economic crimes and acts of terrorism--viruses, security breaches, and the buying/selling of copyrighted material. These crimes were once the exclusive realm of the adult. Concludes that more study is needed to understand this juvenile behavior, which is far different from traditional juvenile behavior.

Rennie, L. (2007). An Advanced Model of Hacking. Security Journal, 20(4), 236-251.
Notes: Available full-text from PROQUEST
Abstract: This paper reviews the literature on the motivations that encourage hacking, from the perspective of both informal observation and formal psychological theories. Discusses in depth cyberpolicing, especially in preventing the start of teenagers hacking.

Savirimuthu, J. (2008). Identity Theft and the Gullible Computer User: What Sun Tzu in the Art of War Might Teach. Journal of International Commercial Law & Technology, 3(2), 120-128.
Notes: Available full-text from Academic Search Complete/EBSCO
Abstract: Discusses information security and the role of law, in particular the Fraud Act of 2006 in the UK.

Shostack, A. (2008). The New School of Information Security. Upper Saddle River, NJ: Addison-Wesley.
Call Number: HD30.2.S563 2008
Abstract: The author explains why critical security problems exist and how to solve them. Focuses on breach notification, and how and why that information should be used. Also, a chapter on vendors is provided, along with trusted sites and how certification provides a false sense of security.

United States. Executive Office of the President. (2009) Cyberspace Policy Review Assuring a Trusted and Resilient Information and Communications Infrastructure [Web Page]. URL http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
Call Number: HM851.U55 2009
Abstract: Summarizes the conclusions of a team of cybersecurity experts, and presents a strategy for a reliable and trustworthy digital infrastructure for the future. Concludes that over the past 15 years, the US has failed to keep pace with the threat.

Warren, A. (2007). Stolen Identity: Regulating the Illegal Trade in Personal Data in the 'Data Based Society'. International Review of Law, Computers & Technology, 21(2), 177-190.
Notes: Available full text from Academic Search Complete/EBSCO
Abstract: Examines the current UK government's approach to regulating the illegal flow of personal information. Discusses Privacy Impact Assessments (PIAs) which can reduce the risk of data being traded illegally. PIAs are mandated for new federal public sector projects by the e-Gov Act of 2002--they are not mandated in the UK. With the expansion and merging of government databases, more attention must be given to PIAs.

Wilson, C. (2009). Computer Attack and Cyberterrorism. NY: Nova Science Publishers.
Call Number: HV6773.2W55
Abstract: Describes three types of attacks against computers--cyberattack, physical attack, and electromagnetic attack. Discusses the technical capabilities of terrorists and the effects of a computer network attack against US infrastructure computers. Appendices describe computer viruses, spyware, and bot networks.

Compiled by Cheryl Weidner, 5/10.

This bibliography is a representative selection of materials either owned or available at the FBI Academy Library. Inclusion of an item does not represent an endorsement by the FBI of the material or its author.