

# Crime On-Line

---

*Correlates, Causes, and Context*

SECOND EDITION

Edited by

**Thomas J. Holt**

MICHIGAN STATE UNIVERSITY

CAROLINA ACADEMIC PRESS

Durham, North Carolina

Copyright © 2013  
Thomas J. Holt  
All Rights Reserved

Library of Congress Cataloging-in-Publication Data

Crime on-line : correlates, causes, and context / [edited by] Thomas J. Holt. -  
- 2nd ed.

p. cm.

Includes bibliographical references and index.

ISBN 978-1-61163-105-0 (alk. paper)

1. Computer crimes. I. Holt, Thomas J., 1978-

HV6773.C763 2012

364.16'8--dc23

2012042057

CAROLINA ACADEMIC PRESS  
700 Kent Street  
Durham, North Carolina 27701  
Telephone (919) 489-7486  
Fax (919) 493-5668  
www.cap-press.com

Printed in the United States of America

*This work is dedicated to the contributors to this text, as well as to those young scholars whose research will steer the field of inquiry into cybercrimes and Internet-based deviance over the next decade.*



# Contents

Tables and Figures	xi
Acknowledgments	xv
<b>1 Crime On-Line: Correlates, Causes, and Context</b>	
<i>Thomas J. Holt</i>	3
Defining and Measuring Cybercrime	6
Cybercrime Framework	10
Cyber-trespass	10
Cyber-deception/Theft	11
Cyber-porn and Obscenity	13
Cyber-violence	15
The Structure of This Book and Its Contributions	16
References	18
<b>2 Hacker Woodstock: Observations on an Off-line Cyber Culture at the Chaos Communication Camp 2011</b>	
<i>Patrick T. Kinkade, Michael Bachmann, and Brittany Smith-Bachmann</i>	27
Hacker Culture	29
Perspectives, Procedures, and Settings	34
Identity Assignments within a Grounded Online Culture	37
The Emergent Grounded Hacker Culture	44
The Vocabulary of Motives	48
Conclusion	51
References	53
<b>3 The Evolution of Online Piracy: Challenge and Response</b>	
<i>Johnny Nhan</i>	61
Review of the Literature	62
Individual Motivations and Factors Influencing Participation in Piracy	
Activities	62
The Impact and Harm of Piracy	65

Enforcement of Piracy Laws	65
Timeline	67
The Digital Transition: From Hard Goods to Soft Goods	67
Website Hosting Music	68
Peer-to-Peer: The Napster Era	69
Peer-to-Peer: BitTorrent Era	70
Litigation	72
Internet Culture	74
Conclusion and Limitations	75
References	76
<b>4 Understanding Online Work-at-Home Scams through an Analysis of Electronic Mail and Websites</b>	
<i>Sarah Turner, Heith Copes, Kent R. Kerley, and Gary Warner</i>	81
Work-at-Home Scams	82
Online Fraud in Context	83
Data and Methodology	85
Analysis of Emails	88
Analysis of Websites	94
Discussion and Conclusions	104
References	107
<b>5 Internet Child Pornography: Legal Issues and Investigative Tactics</b>	
<i>Marcus K. Rogers and Kathryn C. Seigfried-Spellar</i>	109
Scope and Context	110
The COPINE Project	113
The Courts and COPINE	115
A Hypothetical Case Study	117
Criticisms of Court Image Classifications	119
Classification System for the United States	121
Technical Investigations	122
Lanning Model	123
Krone Model	124
Rogers and Seigfried-Spellar Hybrid Model	126
Case Study	130
Conclusions	136
References	137
<b>6 Examining Cyberstalking and Bullying: Causes, Context, and Control</b>	
<i>Catherine Marcum</i>	141
Cyberbullying	142

Prevention of Cyberbullying	145
Cyberstalking	146
Prevention of Cyberstalking	149
Emergence of Legislation	149
Addressing Free Speech Issues	151
Conclusion	152
References	153
<b>7 The Internet as a Tool for Terrorists: Implications for Physical and Virtual Worlds</b>	
<i>Marjie T. Britz</i>	159
Defining Terrorism	161
Traditional Definitions of Cyberterrorism	164
Operationalizing Cyberterrorism as a Multipurpose Tool	165
Propaganda, Information Dissemination, and Recruitment	166
The Internet as a Medium of Communication	173
Training, Research, and Facilitation	176
As an Attack Vector	179
Conclusions	183
References	184
<b>8 Industrial Control Systems and Cybercrime</b>	
<i>Aunshul Rege</i>	191
Industrial Control Systems	192
Industrial Control System Vulnerabilities	194
Industrial Control System Threats	196
Critical Infrastructure Cybercrime Cases	197
Oil and Gas Infrastructure	199
Transportation Infrastructure	199
Sewage Infrastructure	200
Finance and Communication Infrastructure	200
Power Infrastructure	201
The Brief Criminological Industrial Control System Cybercrime Research	201
Expanding the Criminological Lines of Inquiry	205
Primary Data Collection	206
Offender Decision-Making, Crime Scripts, and Situational Crime Prevention	206
Simulation Studies and Agent Based Modeling	208
Trend Analysis	208
Physical Components of Industrial Control System Cyberattacks	209

Glossary	210
References	211
<b>9 Examining State and Local Law Enforcement Perceptions of Computer Crime</b>	
<i>Thomas J. Holt, Adam M. Bossler, and Sarah Fitzgerald</i>	219
Policing Computer Crime	221
Data	224
Findings	225
Demographic Composition	225
Investigations	227
Attitudes toward Computer Crime	229
Perceptions of Computer Crime Offending	231
Awareness of Technology	236
Discussion and Conclusions	238
References	240
<b>Contributors</b>	245
<b>Index</b>	249



# Tables and Figures

## Tables

<b>4</b>	<b>Understanding Online Work-at-Home Scams through an Analysis of Electronic Mail and Websites</b>	<b>81</b>
Table 1	Message Content of Work-at-Home Email	89
Table 2	Personalization and Targeting of Work-at-Home Email Content	90
Table 3	Message Legitimacy Claims in Work-at-Home Email	91
Table 4	Financial Aspects of Work-at-Home Email	92
Table 5	Branding and Legitimacy Work-at-Home Email	93
Table 6	Layout of Work-at-Home Websites	94
Table 7	Advertised Work Opportunities in Work-at-Home Websites	99
Table 8	Testimonials and Gender in Work-at-Home Websites	100
Table 9	Financial Matters in Work-at-Home Websites	101
Table 10	Legitimacy of Work-at-Home Websites	103
Table 11	Information About Work-at-Home Websites	103
Table 12	Compete Rankings of Work-at-Home Websites	104
<b>5</b>	<b>Internet Child Pornography: Legal Issues and Investigative Tactics</b>	
Table 1.	The Suggested Canadian System for Classifying Images Seized in Child Pornography Related Cases	117
Table 2	Classification System of Images Seized from Child Pornography Cases Suggested for the United States of America by Rogers and Seigfried-Spellar	124
Table 3A	Lanning Computer Offender Typology	128
Table 3B	Rogers Seigfried-Spellar Hybrid Model	128
<b>8</b>	<b>Industrial Control Systems and Cybercrime</b>	
Table 1	Summary of Industrial Control Systems, Vulnerabilities and Threats	198

Table 2	Summary of Industrial Control System Cybercrime Incidents	202
---------	---	-----

## 9 Examining State and Local Law Enforcement Perceptions of Computer Crime

Table 1	Size and Geographic Location of Law Enforcement Agencies	225
Table 2	The Percentage of Officers Trained for Digital Evidence and Computer Crime	227
Table 3	Types of Computer Crimes Investigated by State and Local Agencies	228
Table 4	Number of Active Cases Involving Digital Evidence or Computer Crime	229
Table 5	Officers' Reported Attitudes Toward Computer Crimes	230
Table 6	Perceived Severity of Computer Crimes	232
Table 7	Perceived Frequency of Computer Crimes	234
Table 8	Perceived Threat of Cyberterror Attacks from Multiple Nations	235
Table 9	Knowledge of Terms Related to Computer Technology and Computer Crime	236
Table 10	Knowledge of Terms Related to Computer Technology and Computer Crime	237

## Figures

4	Understanding Online Work-at-Home Scams through an Analysis of Electronic Mail and Websites	81
Figure 1	Example of Piggybacking Website	95
Figure 2	Example of News Report Website	95
Figure 3	Reader Comments from News Report Website	96
Figure 4	Work-at-Home Website Asking for Personal Information	97
Figure 5	Work-at-Home Website Asking for Registration	97
Figure 6	Example of Work-at-Home "Regular" Website	97
Figure 7	Example of Website Asking to Make a Purchase	98
Figure 8	Example of "Other" Type of Work-at-Home Website	99
Figure 9	Image of Check Found on Work-at-Home Website	102

**5 Internet Child Pornography: Legal Issues and Investigative Tactics**

Figure 1	A Hypothetical Collection of Images	118
Figure 2	Directory Listing	131
Figure 3	Recycle Bin	131
Figure 4	User Accounts	132
Figure 5	Cookies Folder	132
Figure 6	Cookie Content Information	133
Figure 7	Browser History	134
Figure 8	Browser History	135

# Acknowledgments

As the field of criminological research on cybercrime continues to evolve, I am grateful to the many individuals whose assistance and contributions to this edited work facilitated its creation, value, and applicability. I am very grateful to those authors whose revised chapters help document the shifts in policy and practice in the field. Also, my thanks go to those authors whose chapters are appearing in this second edition for the first time. Their research is helping to shape the field and includes several scholars whose work provides excellent insights into underexamined issues in the field. These contributions compose the intellectual core of this work, and should help define and identify new areas of research in criminology and criminal justice. As the empirical investigation of cybercrime gains greater prominence in the social sciences, my hope is that this work will provide guidance to the discipline. I must also thank the various reviewers whose feedback helped improve the quality and theoretical impact of the chapters who appear in this work. Great thanks are also due to the publishing team at Carolina Academic Press, especially Beth Hall for her assistance throughout the creation and submission of this second edition. I appreciate all of their efforts to market the book and ensure its success. Finally, I would like to thank my family and friends for all of their support throughout this process, most especially my wife Karen for all of her love and assistance.