Cybercrime

Cybercrime is a growing problem in the modern world. Despite the many advantages of computers, they have spawned a number of crimes, such as hacking and virus writing, and made other crimes more prevalent and easier to commit, including music piracy, identity theft and child sex offences. Understanding the psychology behind these crimes helps to determine what motivates and characterises offenders and how such crimes can be prevented. This textbook on the psychology of the cybercriminal is the first written for undergraduate and postgraduate students of psychology, criminology, law, forensic science and computer science. It requires no specific background knowledge and covers legal issues, offenders, effects on victims, punishment and preventative measures for a wide range of cybercrimes. Introductory chapters on forensic psychology and the legal issues of cybercrime ease students into the subject, and many pedagogical features in the book and online provide support for the student.

Cybercrime

The Psychology of Online Offenders

GRÁINNE KIRWAN AND ANDREW POWER

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

Published in the United States of America by Cambridge University Press, New York

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107004443

First published 2011, 2013
Second Edition 2012
Reprinted 2013

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication data

Kirwan, Grainne, 1978–
Cybercrime : the psychology of online offenders / Gráinne Kirwan and Andrew Power.
pages cm
Includes bibliographical references.
ISBN 978-1-107-00444-3 (Hardback) – ISBN 978-0-521-18021-4 (Paperback)
1. Computer crimes–Psychological aspects. 2. Criminal psychology. I. Power, Andrew, 1965–. II. Title.
HV6773.K567 2013
364.16′8–dc23

2012049448

ISBN 978-1-107-00444-3 Hardback
ISBN 978-0-521-1802-1 Paperback

Additional resources for this publication at www.cambridge.org/kirwan-power

CONTENTS

DETAILED CONTENTS

ILLUSTRATIONS

TABLES

PREFACE

This textbook examines the psychology of cybercrime. It aims to be useful to both undergraduate and postgraduate students from a wide variety of disciplines, including criminology, psychology and information technology. Because of the diversity of backgrounds of potential readers, this book presumes no prior knowledge of either the psychological or technological aspects of cybercrime – key concepts in both areas are defined as they arise in the chapters that follow. The chapters consider research that has been conducted in each area, but also apply psychological theories and models to each type of cybercrime. The chapters also consider many aspects of each cybercrime – they do not simply consider the offender, but also effects on the victims, suitable punishments, potential preventative measures and comparisons to similar offline offences. Most chapters stand alone, so it is possible for the reader to dip in to any point in the book. However, most readers may wish to start with Chapters 1 and 2, which provide an overview of forensic psychological theory and of cybercrime. We hope that you enjoy reading this book as much as we enjoy researching this evolving and cutting-edge topic.

Overview of the book

This book is divided into four sections. The first two chapters introduce the reader to the key concepts involved – specifically forensic psychology and cybercrimes. Following this, the book considers offences that could not exist without the use of computers; hacking and malware. The third section (Chapters 5 to 9) considers crimes that can occur without computers but that have become more prevalent or easier because of technology – such as copyright infringement, fraud, identity theft, terrorism, bullying, stalking, child pornography and sexual predation of children. The final chapter considers crime in virtual worlds. A little more detail on the contents of each chapter is included below.

- Chapter 1 provides a brief overview of cybercrime, before describing the discipline of forensic psychology and exploring various theories of crime that were originally proposed to explain offline criminal events.
- Chapter 2 examines how cybercrimes can be considered from a legal perspective. In particular, it investigates how governance and soft law might be useful when contemplating suitable approaches to cybercrime.
- Chapter 3 considers the psychology of hackers, describing their methods and motives, and exploring the profile and personality characteristics of hackers.

There has been a considerable amount of research completed on hacking, compared to many other cybercrimes, and this research is evaluated.

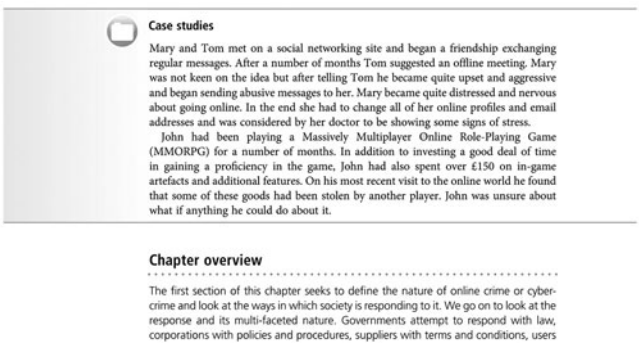
- Chapter 4 explores malware – computer viruses, worms, spyware and other malicious software. A history of malware is provided, along with a description of the motives, profile and personality of offenders.
- Chapter 5 investigates identity theft and online fraud. Comparisons are made to similar offline offences, and the chapter explores why potential victims may be particularly vulnerable to these offences.
- Chapter 6 considers child-related online offences. The diagnosis and characteristics of paedophiles are described, before examining how this research informs our understanding of online child predators and users of online child pornography.
- Chapter 7 investigates both cyberbullying and cyberstalking. For each, it examines how the behaviour is similar to, or different from, its offline equivalent. The methods by which each is carried out, as well as the traits of perpetrators and victims, are identified.
- Chapter 8 considers digital piracy and copyright infringement. The psychology of offenders is examined, with particular focus on how psychological phenomena (such as neutralisations and social learning) and psychological theories (such as the theory of planned behaviour) can contribute to our understanding of these offences.
- Chapter 9 examines cyberterrorism. It identifies how terrorists use the internet, while exploring the literature examining the psychology of terrorists. Conflicting definitions of cyberterrorism are assessed.
- Chapter 10 explores the rather unusual case of disruptive behaviour in virtual worlds. While the term 'crime' is used to describe these in this book, they are not necessarily recognised by offline authorities as criminal events. Nevertheless, if the same event took place offline, it would most certainly be considered a crime, and so they are considered in depth here.

Pedagogical features

Each chapter in the book includes a number of pedagogical features that are designed to aid student learning as well as providing lecturers with ideas and resources for classroom activities. Some additional resources are also available on the companion website for the book.

Chapter resources

Some case studies are provided in each chapter, giving examples of how the cybercrimes considered in the chapter might affect internet users. In most cases these are fictional, but Chapters 3 and 4 (on hackers and malware respectively) include examples of real life cases.



Case studies

Mary and Tom met on a social networking site and began a friendship exchanging regular messages. After a number of months Tom suggested an offline meeting. Mary was not keen on the idea but after telling Tom he became quite upset and aggressive and began sending abusive messages to her. Mary became quite distressed and nervous about going online. In the end she had to change all of her online profiles and email addresses and was considered by her doctor to be showing some signs of stress.

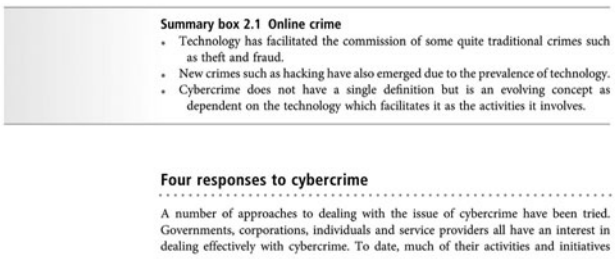
John had been playing a Massively Multiplayer Online Role-Playing Game (MMORPG) for a number of months. In addition to investing a good deal of time in gaining a proficiency in the game, John had also spent over £150 on in-game artefacts and additional features. On his most recent visit to the online world he found that some of these goods had been stolen by another player. John was unsure about what if anything he could do about it.

Chapter overview

The first section of this chapter seeks to define the nature of online crime or cybercrime and look at the ways in which society is responding to it. We go on to look at the response and its multi-faceted nature. Governments attempt to respond with law, corporations with policies and procedures, suppliers with terms and conditions, users

The case studies are directly followed by sections providing an overview of the chapter and definitions of key concepts.

Throughout the chapters, summary boxes are provided. These summary boxes reiterate the key points in the preceding section(s), and are useful in reinforcing student learning. Students can also use these sections to check that they thoroughly understand key concepts in the area before moving on to the next section.



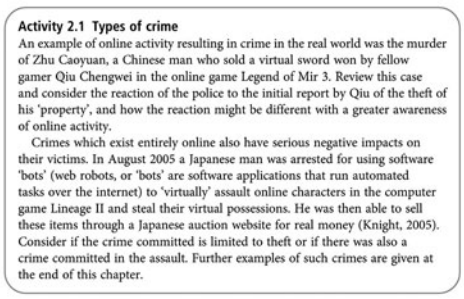
Summary box 2.1 Online crime

- Technology has facilitated the commission of some quite traditional crimes such as theft and fraud.
- New crimes such as hacking have also emerged due to the prevalence of technology.
- Cybercrime does not have a single definition but is an evolving concept as dependent on the technology which facilitates it as the activities it involves.

Four responses to cybercrime

A number of approaches to dealing with the issue of cybercrime have been tried. Governments, corporations, individuals and service providers all have an interest in dealing effectively with cybercrime. To date, much of their activities and initiatives

Each chapter includes a number of potential activities that students can complete either alone or in class. These are distributed at key points throughout the chapters, and often require little additional resources except an internet-enabled computer.

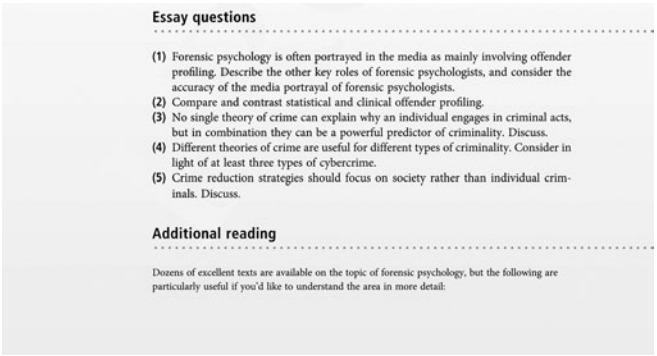


Activity 2.1 Types of crime

An example of online activity resulting in crime in the real world was the murder of Zhu Caoyuan, a Chinese man who sold a virtual sword won by fellow gamer Qiu Chengwei in the online game Legend of Mir 3. Review this case and consider the reaction of the police to the initial report by Qiu of the theft of his 'property', and how the reaction might be different with a greater awareness of online activity.

Crimes which exist entirely online also have serious negative impacts on their victims. In August 2005 a Japanese man was arrested for using software 'bots' (web robots, or 'bots' are software applications that run automated tasks over the internet) to 'virtually' assault online characters in the computer game Lineage II and steal their virtual possessions. He was then able to sell these items through a Japanese auction website for real money (Knight, 2005). Consider if the crime committed is limited to theft or if there was also a crime committed in the assault. Further examples of such crimes are given at the end of this chapter.

Towards the end of each chapter, some sample essay questions are included. Lecturers may wish to set assignments using these questions, or students may wish to test their knowledge of the topic by preparing answers.



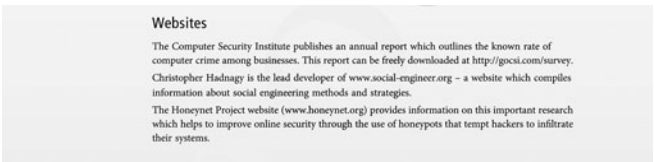
Essay questions

(1) Forensic psychology is often portrayed in the media as mainly involving offender profiling. Describe the other key roles of forensic psychologists, and consider the accuracy of the media portrayal of forensic psychologists.
(2) Compare and contrast statistical and clinical offender profiling.
(3) No single theory of crime can explain why an individual engages in criminal acts, but in combination they can be a powerful predictor of criminality. Discuss.
(4) Different theories of crime are useful for different types of criminality. Consider in light of at least three types of cybercrime.
(5) Crime reduction strategies should focus on society rather than individual criminals. Discuss.

Additional reading

Dozens of excellent texts are available on the topic of forensic psychology, but the following are particularly useful if you'd like to understand the area in more detail:

At the end of each chapter, a list of suggested additional reading is included. These vary from chapter to chapter, but generally include both websites and books/journal articles. These readings allow students who have interest in specific topics to read about them in more depth.



Websites

The Computer Security Institute publishes an annual report which outlines the known rate of computer crime among businesses. This report can be freely downloaded at http://gocsi.com/survey.

Christopher Hadnagy is the lead developer of www.social-engineer.org – a website which compiles information about social engineering methods and strategies.

The Honeynet Project website (www.honeynet.org) provides information on this important research which helps to improve online security through the use of honeypots that tempt hackers to infiltrate their systems.

Online resources

The companion website for this textbook includes additional resources for students and lecturers. Specific resources are provided for each chapter.

Summaries of the key points in each chapter are included. Also available are a collection of links – some to useful external websites with relevant content, and some to journals that specialise in publishing papers on the specific topic. Students can follow these links to search for relevant literature in the area.

One or more online activities are provided for each chapter. In some cases these involve testing student learning, especially of typologies or multi-faceted concepts, although there are other types of activities included.

A short multiple-choice quiz is provided for each chapter, to allow students to test their own learning.

Finally, discussion boards are provided so that students can collaboratively examine key debates relating to the subject area.

About the authors

Gráinne Kirwan and Andrew Power work in the Institute of Art, Design and Technology (IADT) in Dun Laoghaire, Dublin (www.iadt.ie).

Gráinne Kirwan is a lecturer in psychology, teaching on both a BSc (Hons) in Applied Psychology and an MSc in Cyberpsychology. She lectures in topics including forensic psychology, cyberpsychology, computer-mediated communication and the psychology of virtual reality and artificial intelligence. Her doctorate research examined the ethics, motives and interpersonal relationships of hackers. She also holds an MSc in Applied Forensic Psychology, a Postgraduate Certificate in Third Level Learning and Teaching and an MLitt in Psychology by Research.

Andrew Power is Head of the Faculty of Film, Art and Creative Technologies at the Institute of Art, Design and Technology; prior to this Andrew spent 18 years in the ICT industry. Originally trained as an engineer, Andrew holds an MA from the University of Dublin, an MBA from the University of Strathclyde and his doctoral research in Queens University Belfast examined the links between social networking and active citizenship. Andrew has taught and supervised student research at both undergraduate and postgraduate level.

Acknowledgements

We would like to thank all those in Cambridge University Press who worked with us during the development of this book. Particular thanks go to Hetty Marx, who reviewed the original proposal and who has been the source of great advice and support. We would also like to thank Ed Robinson, Josephine Lane and Carrie Parkinson who clarified several of our queries during the writing process.

We are fortunate to work in an environment where our students and colleagues perpetually encourage us to examine cutting-edge topics in fascinating disciplines. We would like to thank all the staff and students in IADT who have provided their support during lectures, in meetings and in the canteen over more cups of coffee than we can count.

The photographs in Illustrations 2.1, 4.1 and 9.1 were designed and taken by Claire Burke, whose creativity and flair have helped to illustrate key topics. All other illustrations in the book (with the exception of Illustration 4.2) were prepared and photographed by Liam Kirwan, who sadly passed away during the writing of this book. We're thankful for his talent, enthusiasm and support when preparing these images for us.

While a very enjoyable process, writing a book is also very time-consuming. We're especially grateful to our long-suffering families and friends who have excused our absences while we tap away at keyboards. Particular thanks to Glen and Eleanor, and to Shannon and Rachel, for their good-humoured encouragement and patience during the writing of this book.