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.
## CONTENTS

Detailed table of contents  

List of illustrations  

List of tables  

Preface  

1  Psychology of cybercrime  

2  Cybercrimes and cyberlaw  

3  Hackers  

4  Malware  

5  Identity theft and fraud  

6  Child predation and child pornography online  

7  Cyberbullying and cyberstalking  

8  Digital piracy and copyright infringement  

9  Cyberterrorism  

10  Crime in virtual worlds  

References  

Index
DETAILED CONTENTS

Preface xvii
Overview of the book xvii
Pedagogical features xviii
  Chapter resources xviii
  Online resources xx
About the authors xx
Acknowledgements xxi

1 Psychology of cybercrime 1

Case studies 1
Chapter overview 1
Forensic psychology 2
Cybercrime: a brief introduction 3
Components of forensic psychology 4
  Offender profiling 4
  Psychological disorders and offender assessment 6
  Punishment, rehabilitation and risk assessment 8
  Police psychology 11
  Cybercrime juries 12
  Victims 13
  Crime prevention 15
  Forensic psychology – conclusion 16
Theories of crime 16
  Levels of explanation of crime 16
Societal, community, socialisation influence and individual theories 17
  Applying theories of crime to cybercrime 18
## Detailed contents

- Social construction of crime 18
- Biological theories of crime 18
- Learning theories and crime 20
- Eysenck’s theory of crime 21
- Other trait theories of crime 21
- Psychoanalytic theories of crime 22
- Addiction and arousal theory 22
- Neutralisation theory 23
- Labelling theory 24
- Geographical theories 24
- Routine activity theory 25

**Conclusion** 26

**Essay questions** 26

**Additional reading** 26

## 2 Cybercrimes and cyberlaw

- **Case studies** 28
- **Chapter overview** 28
- **Online crime** 28

**Four responses to cybercrime**

- Government response, the law of the land 32
- Private or corporate response, the rules of the game 33
- Technical response, the law as code 34
- User response, negotiated law 35

**A soft law approach** 36

**Governance** 40

**Social networking** 45

**Conclusion** 49

**Essay questions** 49

**Additional reading** 50
3 Hackers

Case studies

Chapter overview

Definitions and prevalence rates
- Hacking definitions
- Types of hacking attack
- Known prevalence rates

Methods of hackers

Motives of hackers
- Theories regarding hacker motives
- Empirical work examining hacker motives

Profile and personality characteristics of offenders
- Demographic characteristics
- Ethical positions

The hacker ethic

Subscription to the hacker ethic and justifications for breaches
- Interpersonal relationships
- Other personality characteristics

Hacker groups versus lone hackers

Punishment

Prevention methods

Conclusion

Essay questions

Additional reading

4 Malware

Case studies

Chapter overview

Definitions and prevalence rates
- Prevalence
## Detailed contents

**Types of malware** 81

**A brief history of malware** 84

**Methods of malware production and distribution** 86

**Motives of malware producers and disseminators** 88
  - Financial motives 89
  - Intellectual challenges and avoiding boredom 89
  - Social factors 90
  - Vengeance 90
  - Vandalism 90

**Profile and personality characteristics of offenders** 92

**Prevention methods** 96

**Conclusion** 100

**Essay questions** 101

**Additional reading** 101

### 5 Identity theft and fraud

**Case studies** 103

**Chapter overview** 103

**Definitions and prevalence rates** 104

**Similar offline offences** 107

**Methods of attack** 108
  - Social networking site fraud 109
  - Online dating fraud 111
  - Conference fraud 112
  - Phishing 113
  - Advance fee fraud 116

**Human susceptibility to online fraud and identity theft** 118

**Effects on victims** 121

**Prevention methods** 122

**Conclusion** 124
## Detailed contents

- Definitions and prevalence 148
- Methods of cyberbullying and comparison to ‘traditional’ bullying 150
- Traits of cyberbullies 154
- Victims of cyberbullying 155
- Possible solutions to cyberbullying 156

**Cyberstalking** 157
- Definitions and prevalence 158
- Methods of cyberstalking 159
- Traits of cyberstalkers 162
- Victims of cyberstalking 164
- Possible solutions to cyberstalking 165

**Conclusion** 167

**Essay questions** 167

**Additional reading** 168

### 8 Digital piracy and copyright infringement 169

- **Case studies** 169
- **Chapter overview** 169
- **Definitions** 170
- **Methods of copyright infringement** 173
- **Psychology of offenders** 176
  - Demographic characteristics 176
  - Motivations 176
  - Self-control and social learning theory 178
  - Neutralisations and ethical positions 179
  - The theory of reasoned action, the theory of planned behaviour and optimism bias 181
- **Punishment and solutions** 182
  - Deterrence 183
  - Preventative controls 185
  - Other solutions 186
## Detailed contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conclusion</td>
<td>187</td>
</tr>
<tr>
<td>Essay questions</td>
<td>187</td>
</tr>
<tr>
<td>Additional reading</td>
<td>188</td>
</tr>
<tr>
<td><strong>9 Cyberterrorism</strong></td>
<td>189</td>
</tr>
<tr>
<td>Case studies</td>
<td>189</td>
</tr>
<tr>
<td>Chapter overview</td>
<td>189</td>
</tr>
<tr>
<td>Definitions</td>
<td>190</td>
</tr>
<tr>
<td><strong>Online activities of terrorists</strong></td>
<td>192</td>
</tr>
<tr>
<td>– Cyberterror attacks</td>
<td>193</td>
</tr>
<tr>
<td>– Hacktivism versus cyberterrorism</td>
<td>195</td>
</tr>
<tr>
<td>– Recruitment of new members</td>
<td>195</td>
</tr>
<tr>
<td>– Networking</td>
<td>196</td>
</tr>
<tr>
<td>– Fundraising</td>
<td>197</td>
</tr>
<tr>
<td>– Gathering and dissemination of information</td>
<td>197</td>
</tr>
<tr>
<td><strong>Radicalisation</strong></td>
<td>198</td>
</tr>
<tr>
<td><strong>Motives of terrorism and cyberterrorism</strong></td>
<td>200</td>
</tr>
<tr>
<td><strong>Psychology of cyberterrorists</strong></td>
<td>201</td>
</tr>
<tr>
<td>– Personality and profile</td>
<td>201</td>
</tr>
<tr>
<td>– Psychological abnormalities</td>
<td>203</td>
</tr>
<tr>
<td>– Comparison to offline terrorists</td>
<td>204</td>
</tr>
<tr>
<td><strong>Effects on victims</strong></td>
<td>205</td>
</tr>
<tr>
<td>Conclusion</td>
<td>205</td>
</tr>
<tr>
<td>Essay questions</td>
<td>206</td>
</tr>
<tr>
<td>Additional reading</td>
<td>206</td>
</tr>
<tr>
<td><strong>10 Crime in virtual worlds</strong></td>
<td>207</td>
</tr>
<tr>
<td>Case studies</td>
<td>207</td>
</tr>
<tr>
<td>Chapter overview</td>
<td>207</td>
</tr>
<tr>
<td>Understanding virtual worlds</td>
<td>207</td>
</tr>
<tr>
<td>Detailed contents</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td><strong>Types of crime</strong></td>
<td>209</td>
</tr>
<tr>
<td>– Property crimes</td>
<td>210</td>
</tr>
<tr>
<td>– Crimes against the person</td>
<td>210</td>
</tr>
<tr>
<td><strong>Incidence and motivation</strong></td>
<td>212</td>
</tr>
<tr>
<td><strong>Effects on victims</strong></td>
<td>213</td>
</tr>
<tr>
<td><strong>Victim aid</strong></td>
<td>217</td>
</tr>
<tr>
<td><strong>Policing, prevention and punishment</strong></td>
<td>219</td>
</tr>
<tr>
<td><strong>Future trends and research</strong></td>
<td>221</td>
</tr>
<tr>
<td><strong>Conclusion</strong></td>
<td>222</td>
</tr>
<tr>
<td><strong>Essay questions</strong></td>
<td>222</td>
</tr>
<tr>
<td><strong>Additional reading</strong></td>
<td>222</td>
</tr>
<tr>
<td><strong>References</strong></td>
<td>224</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>251</td>
</tr>
<tr>
<td>Illustration</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1.1</td>
<td>Offender profiling and suspect characteristics (photograph by Liam Kirwan)</td>
</tr>
<tr>
<td>1.2</td>
<td>Self-blaming and victim-blaming (photograph by Liam Kirwan)</td>
</tr>
<tr>
<td>1.3</td>
<td>Fowler’s Phrenology Head (photograph by Liam Kirwan)</td>
</tr>
<tr>
<td>2.1</td>
<td>Online crime (photograph by Claire Burke)</td>
</tr>
<tr>
<td>3.1</td>
<td>White, black and grey hat hackers (photograph by Liam Kirwan)</td>
</tr>
<tr>
<td>3.2</td>
<td>Shredding documents can help to prevent infiltration by dumpster diving (photograph by Liam Kirwan)</td>
</tr>
<tr>
<td>4.1</td>
<td>Types of malware (photograph by Claire Burke)</td>
</tr>
<tr>
<td>4.2</td>
<td>Timeline of malware</td>
</tr>
<tr>
<td>5.1</td>
<td>Identity theft (photograph by Liam Kirwan)</td>
</tr>
<tr>
<td>5.2</td>
<td>Choosing strong passwords (photograph by Liam Kirwan)</td>
</tr>
<tr>
<td>8.1</td>
<td>Cost of piracy (photograph by Liam Kirwan)</td>
</tr>
<tr>
<td>8.2</td>
<td>Analogue media (photograph by Liam Kirwan)</td>
</tr>
<tr>
<td>9.1</td>
<td>Cyberterrorism (photograph by Claire Burke)</td>
</tr>
<tr>
<td>3.1 Categories of hackers</td>
<td>page 56</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>3.2 Theorised motives of hackers</td>
<td>63</td>
</tr>
<tr>
<td>4.1 Types of malware</td>
<td>82</td>
</tr>
<tr>
<td>4.2 Protection motivation theory and malware infection prevention</td>
<td>97</td>
</tr>
<tr>
<td>5.1 Overview of methods of online fraud and identity theft</td>
<td>110</td>
</tr>
<tr>
<td>6.1 The ten levels of child pornography content outlined by COPINE</td>
<td>139</td>
</tr>
<tr>
<td>6.2 UK ‘SAP’ scale (Sentencing Guidelines Council, 2007, p. 109)</td>
<td>140</td>
</tr>
<tr>
<td>6.3 Krone’s (2004) typology of internet child pornography offenders</td>
<td>141</td>
</tr>
<tr>
<td>7.1 Common cyberbullying methods</td>
<td>152</td>
</tr>
<tr>
<td>7.2 Common cyberstalking behaviours</td>
<td>160</td>
</tr>
<tr>
<td>9.1 Definitions of cyberterrorism</td>
<td>191</td>
</tr>
</tbody>
</table>
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.
Preface

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.
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.

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.

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.
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.

**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. In what combinations they can be a powerful predictor of criminality. Discuss.
4. Different theories of crime are useful for different types of criminal. Consider the relationship between them.
5. Crime prevention strategies should focus on society rather than individual criminal. Discuss.

**Additional reading**

Diverse resources are available on the topic of forensic psychology but the following are particularly useful if you wish to understand the area in more detail:

**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).
Preface

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.