

1. Record Nr.	UNINA9910220060403321
Autore	Dimmock Mark
Titolo	Ethics for A-Level : For AQA Philosophy and OCR Religious Studies // Mark Dimmock, Andrew Fisher
Pubbl/distr/stampa	Cambridge, : Open Book Publishers, 2018
ISBN	979-1-03-650078-7
Descrizione fisica	1 online resource (262)
Altri autori (Persone)	FisherAndrew
Soggetti	Ethics & moral philosophy
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	<p>"What does pleasure have to do with morality? What role, if any, should intuition have in the formation of moral theory? If something is a simulatedâ, can it be immoral? This accessible and wide-ranging textbook explores these questions and many more. Key ideas in the fields of normative ethics, metaethics and applied ethics are explained rigorously and systematically, with a vivid writing style that enlivens the topics with energy and wit. Individual theories are discussed in detail in the first part of the book, before these positions are applied to a wide range of contemporary situations including business ethics, sexual ethics, and the acceptability of eating animals. A wealth of real-life examples, set out with depth and care, illuminate the complexities of different ethical approaches while conveying their modern-day relevance.</p> <p>This concise and highly engaging resource is tailored to the Ethics components of AQA Philosophy and OCR Religious Studies, with a clear and practical layout that includes end-of-chapter summaries, key terms, and common mistakes to avoid. It should also be of practical use for those teaching Philosophy as part of the International Baccalaureate.</p> <p>Ethics for A-Level is of particular value to students and teachers, but Fisher and Dimmock's precise and scholarly approach will appeal to anyone seeking a rigorous and lively introduction to the challenging subject of ethics."</p>

2. Record Nr.	UNINA9911009185503321
Autore	Katz Sarah
Titolo	Digital Earth : Cyber Threats, Privacy and Ethics in an Age of Paranoia
Pubbl/distr/stampa	Ely : , : IT Governance Ltd, , 2022 ©2022
ISBN	9781787783607 178778360X
Edizione	[1st ed.]
Descrizione fisica	1 online resource (108 pages)
Disciplina	005.8
Soggetti	LAW / Computer & Internet COMPUTERS / Security / General LAW / Communications LAW / Criminal Law / General
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Title -- Copyright -- About the author -- Acknowledgements -- Contents -- Introduction -- Chapter one: The spike in phishing amid the COVID-19 pandemic -- Key terms for this chapter -- Chaos theory in cyber threat mitigation -- The application of chaos theory to the assessment of phishing attacks -- Chapter two: A glance at the history of phishing mitigation practices -- The risk of phishing to federal health care agencies -- Applications of chaos theory in cyber threat mitigation, including phishing attacks -- Machine learning tools for phishing prevention -- Persuasive factors used in phishing attacks -- User awareness of email legitimacy verification techniques -- Chapter three: The hard truth - How little many users understand about identifying malicious emails -- Tackling email headers -- Next steps: Computer- assisted threat detection -- Chapter four: Disinformation versus misinformation in a post-COVID world -- Global information sharing -- Content moderators -- How to spot misinformation -- Managing content moderation: In theory and practice -- Next steps: Head above water in cyberspace -- Chapter five: Cyber terrorism and the firepower of social media -- Why convey a message to the masses? -- Making it look alluring -- Using social media to attract and recruit

-- Next steps: Keep an eye on that friend request -- Chapter six: Drones - A search and rescue solution or the all-seeing eye in the sky? -- The technicalities of civilian privacy in UAV criminal investigation -- San Jose as a case study -- Those opposed -- Those in favor -- Calming the public outcry -- Balancing technological surveillance measures with public interest -- Next steps: Securing the wireless target -- Recent developments -- Chapter seven: Tying it all together -- Appendix A: Bibliography -- Further reading.

Sommario/riassunto

An accessible introduction to the most prevalent cyber threats in our current climate, this book discusses cyber terrorism, phishing, and ransomware attacks, and provides advice on how to mitigate such threats in our personal and professional lives.
