Cyber Risks I Mia

A definitive resource for understanding such far-reaching and often interconnected crimes as cyber theft, drug trafficking, human smuggling, identity theft, wildlife poaching, and sex tourism. • Includes primary source documents such as international treaties and conventions related to global crime • Provides quick access to key terms, events, individuals, and organizations playing a key role in combating global crime • Includes suggested sources for additional information in each entry to aid readers who want to examine the topic in more detail • Features scholars and practitioners from more than 10 countries who have specific knowledge of, and experience with, many of the global crimes covered in the work

This three volume book set constitutes the proceedings of the Third International Conference on Machine Learning for Cyber Security, ML4CS 2020, held in Xi'an, China in October 2020. The 118 full papers and 40 short papers presented were carefully reviewed and selected from 360 submissions. The papers offer a wide range of the following subjects: Machine learning, security, privacy-preserving, cyber security, Adversarial machine Learning, Malware detection and analysis, Data mining, and Artificial Intelligence.

'Cyberpsychology' provides a broad-ranging, thought-provoking account of online behaviour and the opportunities, challenges, and risks such behaviour presents. Written by an international team of authors, the book provides diverse perspectives on the impact our interaction with the online landscape has on our identity and behaviour.

With the current security crisis in the Ukraine, border security has become a pressing issue. Both the annexation of Crimea and the temporary occupation of the Donbas region represent serious violations of the country's territorial integrity and of the wider international legal order. This book contains 13 presentations delivered during the two-day NATO Advanced Research Workshop (ARW) 'Addressing Security Risks at the Ukrainian Border through Best Practices on Good Governance – Sources and Counter Measures', which took place in Kyiv, Ukraine, in February 2016. The workshop consisted of 5 expert panels devoted to various aspects of building the integrity of the Ukrainian border management agencies to enhance the border security of the eastern flank of NATO. The topics of these panels were: the integrity of the security sector in Ukraine; corruption as a security risk in border management; institutional tools to combat corruption in border management; increasing preparedness for cross-border crises; and bilateral and multilateral dimensions of international cooperation to enhance the integrity of border management agencies. The workshop contributed to raising awareness of emerging border security challenges, as well as providing a forum for the close cooperation of and the exchange of knowledge between the most relevant local and international agencies. It also made possible the discussion of issues such as the current refugee crisis and the implications - for security - of corruption in border management in a wider context.

Addressing everything from the implications of data mining to the risks raised by the use of social media in the workplace, this guide explains how insurers, agents, brokers, and others can use social media to market their products and services.

This book constitutes the thoroughly refereed post-proceedings of the 5th International Workshop on Critical Information Infrastructure Security, CRITIS 2010, held in Athens, Greece in September 2010. The 12 revised full papers and two poster papers presented went through two rounds of reviewing and improvement and were selected from 30 submissions. The papers included address various techniques to realize the security of systems, communications, and data.

Geek girl Mia Connors has to find her missing friend, solve a murder and clear her name. Read the first book in Julie Anne Lindsey's addictive new mystery series! IT manager Mia Connors is up to her tortoiseshell glasses in technical drama when a glitch in the Horseshoe Falls email system disrupts security and sends errant messages to residents of the gated community. The snafu's timing couldn't be worse—Renaissance Faire season is in full swing and Mia's family's business relies on her presence. Mia doesn't have time to hunt down a computer hacker. Her best friend has disappeared, and she finds another of her friends murdered—in her office. When the hunky new head of Horseshoe Falls security identifies Mia as the prime suspect, her anxiety level registers on the Richter scale. Eager to clear her name, Mia moves into action to locate her missing buddy and find out who killed their friend. But her quick tongue gets her into trouble with more than the new head of security. When Mia begins receiving threats, the killer makes it clear that he's closer than she'd ever imagined. 75,000 words

Risk detection and cyber security play a vital role in the use and success of contemporary computing. By utilizing the latest technological advances, more effective prevention techniques can be developed to protect against cyber threats. Detecting and Mitigating Robotic Cyber Security Risks is an essential reference publication for the latest research on new methodologies and applications in the areas of robotic and digital security. Featuring extensive coverage on a broad range of topics, such as authentication techniques, cloud security, and mobile robotics, this book is ideally designed for students, researchers, scientists, and engineers seeking current research on methods, models, and implementations of optimized security in digital contexts.

This book constitutes the thoroughly refereed post-conference proceedings of the 6th International Conference on Information Security and Cryptology, Inscrypt 2010, held in Shanghai, China, in October 2010. The 35 revised full papers presented were carefully reviewed and selected from 125 submissions. The papers are organized in topical sections on encryption schemes, stream ciphers, sequences and elliptic curves, secure computing, hash functions, key management, digital signatures, privacy and algebraic cryptanalysis, hashing and authentication, and hardware and software issues.

Here's what you get in this book: - 350 practice questions covering the breadth of topics under the Security+ exam, including risk management, application security, and cryptography - Focus on the most frequently asked interview questions. Avoid information overload - Compact format: easy to read, easy to carry, so you can study on-the-go Now, you finally have what you need to crush your cybersecurity certification, and land that dream job. About The Author Mike Spolsky has been building secure software systems since 1999. Early in his career, he developed a lightweight encryption algorithm to secure and sign commerce transactions for mobile phones. His current focus is using machine learning to analyze cyberattacks. He is based in New York City.

Unlock the incredible potential of enterprise risk management There has been much evolution in terms of ERM best practices, experience, and standards and regulation over the past decade. Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives, Second Edition is the revised and updated essential guide to the now immensely popular topic of enterprise risk management (ERM). With contributions from leading academics and practitioners, this book offers insights into what practitioners are doing and what the future holds. You'll discover how you can implement best practices, improve ERM tools and techniques, and even learn to teach ERM. Retaining the holistic approach to ERM that made the first edition such a success, this new edition adds coverage of new topics including cybersecurity risk, ERM in government, foreign exchange risk, risk appetite, innovation risk, outsourcing risk, scenario planning, climate change risk, and much more. In addition, the new edition includes important updates and enhancements to topics covered in the first edition; so much of it has been revised and enhanced that it is essentially an entirely new book. Enterprise Risk Management introduces you to the concepts and techniques that allow you to identify risks and prioritize the appropriate responses. This invaluable guide offers a broad overview, covering key issues while focusing on the principles that drive effective decision making and determine business success. This

comprehensive resource also provides a thorough introduction to ERM as it relates to credit, market, and operational risk, as well as the evolving requirements of the board of directors' role in overseeing ERM. Through the comprehensive chapters and leading research and best practices covered, this book: Provides a holistic overview of key topics in ERM, including the role of the chief risk officer, development and use of key risk indicators and the risk-based allocation of resources Contains second-edition updates covering additional material related to teaching ERM, risk frameworks, risk culture, credit and market risk, risk workshops and risk profiles and much more. Over 90% of the content from the first edition has been revised or enhanced Reveals how you can prudently apply ERM best practices within the context of your underlying business activities Filled with helpful examples, tables, and illustrations, Enterprise Risk Management, Second Edition offers a wealth of knowledge on the drivers, the techniques, the benefits, as well as the pitfalls to avoid, in successfully implementing ERM.

"With astonishing verve, The League of Wives persisted to speak truth to power to bring their POW/MIA husbands home from Vietnam. And with astonishing verve, Heath Hardage Lee has chronicled their little-known story — a profile of courage that spotlights 1960s-era military wives who forge secret codes with bravery, chutzpah and style. Honestly, I couldn't put it down." — Beth Macy, author of Dopesick and Factory Man The true story of the fierce band of women who battled Washington—and Hanoi—to bring their husbands home from the jungles of Vietnam. On February 12, 1973, one hundred and sixteen men who, just six years earlier, had been high flying Navy and Air Force pilots, shuffled, limped, or were carried off a huge military transport plane at Clark Air Base in the Philippines. These American servicemen had endured years of brutal torture, kept shackled and starving in solitary confinement, in rat-infested, mosquito-laden prisons, the worst of which was The Hanoi Hilton. Months later, the first Vietnam POWs to return home would learn that their rescuers were their wives, a group of women that included Jane Denton, Sybil Stockdale, Louise Mulligan, Andrea Rander, Phyllis Galanti, and Helene Knapp. These women, who formed The National League of Families, would never have called themselves "feminists," but they had become the POW and MIAs most fervent advocates, going to extraordinary lengths to facilitate their husbands' freedom—and to account for missing military men—by relentlessly lobbying government leaders, conducting a savvy media campaign, conducting covert meetings with antiwar activists, and most astonishingly, helping to code secret letters to their imprisoned husbands. In a page-turning work of narrative non-fiction, Heath Hardage Lee tells the story of these remarkable women for the first time. The League of Wives is certain to be on everyone's must-read list.

This book argues that we should approach the relationship between climate change and security through the lens of ecosystem resilience.

The Maidan Revolution in Ukraine created an opportunity for change and reforms in a system that had resisted them for 25 years. This report provides an overview of recommendations for the reform of Ukraine s security and defense institutions."

* Book 1 of 2 in the Savage Hope Duet * He thinks I'm a corporate spy. Me--plump, boring Mia James. Yes, I omitted an advanced degree on my resume, but being overqualified to be able to pay rent wasn't how I was going to start my newly single (okay, newly dumped) life. Do I regret doing it? Seeing as how I got a junior secretary position in my field, for the private military company run by billionaire badass CEO Collin Stark no less, I'm going to go with 'no.' No regrets here. Which is what I basically tell Mr. Stark when he starts questioning my motives. Did I mention he's an ex-Army interrogator? Or that he's too intense to put into words? While it's obvious he doesn't trust me, that's probably a good thing. Because something tells me if that hot, hardened man were to ever fully trust a woman, his intensity level over her would be...off the charts. * * * * * She thinks I haven't noticed her all this time. Hell, I'd have to be missing both a brain and functioning balls to overlook the quietly enigmatic woman who's clearly too smart and skilled to be working in any entry-level capacity for me. I don't want to believe Mia's capable of corporate espionage. But given the evidence, it's hard to think otherwise. Not that I seem to be capable of a whole lot of rational thought when I'm around her. She's my own curves-for-days kryptonite--which just makes her that much more dangerous. Is it possible my enemies planted a woman in my company to seduce me (in the most awkwardly tempting way possible)? In the past, I would've said no way in hell. But after getting a taste of just how hot Mia can burn, I'm starting to see it's definitely possible...and damn worth it, either way. * * * * * NOTE: While this is the Collin Stark (CEO of Stark International) mentioned throughout the Savage Trust series, the events of his story actually take place prior to Wrecked, Scarred, and Frayed. Be advised that Collin and Mia's story is a two-part 80K word duet. This is Book 1. Book 2 takes place six months after the end of this book, and as such, the books need to be read in order. The Savage Hope Duet His Trust (Book 1) Her Heart (Book 2) **Also available bundled together as a box set (Savage Hope, The Complete Duet Box Set)** Previously published as Smoke & Curves, Books 1 & 2 (c) 2013, and previously part of the Undeniably His bundled collection (c) 2013, revised throughout with freshly added content, changed/different story scenes, and a new extended ending.

Volume 2: Risk, Threats, and the New Normal explains the new political and technological developments that created new domestic national security threats against the nation and the people of the United States.

This best-selling guide provides a complete, practical, and thoroughly up-to-date introduction to network and computer security. COMPTIA SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS, Seventh Edition, maps to the new CompTIA Security+ SY0-601 Certification Exam, providing comprehensive coverage of all domain objectives to help readers prepare for professional certification and career success. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

THE COMPLETE SAVAGE HOPE DUET. This is Collin & Mia's two-book bundled boxed set from New York Times bestselling author Christa Wick. BOOK ONE: HIS TRUST He thinks I'm a corporate spy. Me--plump, boring Mia James. Yes, I omitted an advanced degree on my resume, but being overqualified to be able to pay rent wasn't how I was going to start my newly single (okay, newly dumped) life. Do I regret doing it? Seeing as how I got a junior secretary position in my field, for the private military company run by billionaire badass CEO Collin Stark no less, I'm going to go with 'no.' No regrets here. Which is what I basically tell Mr. Stark when he starts questioning my motives. Did I mention he's an ex-Army interrogator? Or that he's too intense to put into words? While it's obvious he doesn't trust me, that's probably a good thing. Because something tells me if that hot, hardened man were to ever fully trust a woman, his intensity level

over her would be...off the charts. She thinks I haven't noticed her all this time. Hell, I'd have to be missing both a brain and functioning balls to overlook the quietly enigmatic woman who's clearly too smart and skilled to be working in any entry-level capacity for me. I don't want to believe Mia's capable of corporate espionage. But given the evidence, it's hard to think otherwise. Not that I seem to be capable of a whole lot of rational thought when I'm around her. She's my own curves-for-days kryptonite--which just makes her that much more dangerous. Is it possible my enemies planted a woman in my company to seduce me (in the most awkwardly tempting way possible)? In the past, I would've said no way in hell. But after getting a taste of just how hot Mia can burn, I'm starting to see it's definitely possible...and damn worth it, either way. BOOK TWO: HER HEART I refuse to break. I can't say that I've been through worse, but I still believe I'll survive this. I'm not going to crumble at the seams. If I do, Collin's enemies will have won. And everything we've both lost would have been for nothing. I know it seems crazy to return to my old life and try to get a fresh start in a place with more bad memories than good, courtesy of my crook of a stepfather. But it's all I have. And all I need. At least that's what I keep telling myself. ...Until Collin bursts back into my life. I refuse to let Mia suffer. I may know jack about healing--vengeance seems to be all I'm capable of right now--but that doesn't mean I can't protect her from more pain. God knows my world has caused her enough of that to last a lifetime. I understand her need to start a new life. Hell, I even want that for her...even though I'm sure it'll end up killing me and decimating my hopeless heart for good. But I'll do anything for her. Even this. At least that's what I keep telling myself. ...Until I almost lose her all over again. * * * * * Previously published as Smoke & Curves, Books 1, 2, and 3 (c) 2013, and previously part of the Undeniably His bundled collection (c) 2013, revised throughout with freshly added content, changed/different story scenes, and a new extended ending.

This book constitutes the refereed proceedings of the 21th International Conference on Information and Communications Security, ICICS 2019, held in Beijing, China, in December 2019. The 47 revised full papers were carefully selected from 199 submissions. The papers are organized in topics on malware analysis and detection, IoT and CPS security enterprise network security, software security, system security, authentication, applied cryptograph internet security, machine learning security, machine learning privacy, Web security, steganography and steganalysis.

The increased visibility of transgender people in mainstream media, exemplified by Time magazine's declaration that 2014 marked a "transgender tipping point," was widely believed to signal a civil rights breakthrough for trans communities in the United States. In Terrorizing Gender Mia Fischer challenges this narrative of progress, bringing together transgender, queer, critical race, legal, surveillance, and media studies to analyze the cases of Chelsea Manning, CeCe McDonald, and Monica Jones. Tracing how media and state actors collude in the violent disciplining of these trans women, Fischer exposes the traps of visibility by illustrating that dominant representations of trans people as deceptive, deviant, and threatening are integral to justifying, normalizing, and reinforcing the state-sanctioned violence enacted against them. The heightened visibility of transgender people, Fischer argues, has actually occasioned a conservative backlash characterized by the increased surveillance of trans people by the security state, evident in debates over bathroom access laws, the trans military ban, and the rescission of federal protections for transgender students and workers. Terrorizing Gender concludes that the current moment of trans visibility constitutes a contingent cultural and national belonging, given the gendered and racialized violence that the state continues to enact against trans communities, particularly those of color.

Cyber-risks are moving targets and societal responses to combat cyber-victimization are often met by the distrust of young people. Drawing on original research, this book explores how young people define, perceive, and experience cyber-risks, how they respond to both the messages they are receiving from society regarding their safety online, and the various strategies and practices employed by society in regulating their online access and activities. This book complements existing quantitative examinations of cyberbullying assessing its extent and frequency, but also aims to critique and extend knowledge of how cyber-risks such as cyberbullying are perceived and responded to. Following a discussion of their methodology and their experiences of conducting research with teens, the authors discuss the social network services that teens are using and what they find appealing about them, and address teens' experiences with and views towards parental and school-based surveillance. The authors then turn directly to areas of concern expressed by their participants, such as relational aggression, cyberhacking, privacy, and privacy management, as well as sexting. The authors conclude by making recommendations for policy makers, educators and teens – not only by drawing from their own theoretical and sociological interpretations of their findings, but also from the responses and recommendations given by their participants about going online and tackling cyber-risk. One of the first texts to explore how young people respond to attempts to regulate online activity, this book will be key reading for those involved in research and study surrounding youth crime, cybercrime, youth culture, media and crime, and victimology – and will inform those interested in addressing youth safety online how to best approach what is often perceived as a sensitive and volatile social problem.

Terrorism is not a new phenomenon, but almost all communities, regardless of ethnicity, religion, social status or location, are now increasingly facing the challenge of terrorist threat. What makes a terrorist organization attractive to some citizens? A better understanding of the reasons why individuals choose to join terror groups may well enhance efforts to disrupt the recruitment process of terrorist organizations and thereby support current and future counter-terrorism initiatives. This book presents the proceedings of the NATO Advanced Research Workshop, 'Countering Terrorist Recruitment in the Context of Armed Counter-Terrorism Operations', held in Antalya, Turkey, in May 2015. The goal of the workshop was to share existing ideas and develop new ones to tackle terrorist recruitment. The book contains 18 articles covering topics which include: the role of NATO and other international entities in counter-terrorism; understanding recruitment methods and socialization techniques of terror networks by comparing them to gangs; social media in terrorist recruitment; drug money links with terrorist financing; and counter-terrorism and human rights. The book will be of interest to all those involved in developing, planning and executing prevention programs and policies in relation to both armed and non-armed counter-terrorism operations.

This book introduces game theory as a means to conceptualize, model, and analyze cyber deception. Drawing upon a collection of

deception research from the past 10 years, the authors develop a taxonomy of six species of defensive cyber deception. Three of these six species are highlighted in the context of emerging problems such as privacy against ubiquitous tracking in the Internet of things (IoT), dynamic honeynets for the observation of advanced persistent threats (APTs), and active defense against physical denial-of-service (PDoS) attacks. Because of its uniquely thorough treatment of cyber deception, this book will serve as a timely contribution and valuable resource in this active field. The opening chapters introduce both cybersecurity in a manner suitable for game theorists and game theory as appropriate for cybersecurity professionals. Chapter Four then guides readers through the specific field of defensive cyber deception. A key feature of the remaining chapters is the development of a signaling game model for the species of leaky deception featured in honeypots and honeyfiles. This model is expanded to study interactions between multiple agents with varying abilities to detect deception. Game Theory for Cyber Deception will appeal to advanced undergraduates, graduate students, and researchers interested in applying game theory to cybersecurity. It will also be of value to researchers and professionals working on cybersecurity who seek an introduction to game theory.

This book constitutes the proceedings of the 7th International Workshop on Graphical Models for Security, GramSec 2020, which took place on June 22, 2020. The workshop was planned to take place in Boston, MA, USA but changed to a virtual format due to the COVID-19 pandemic. The 7 full and 3 short papers presented in this volume were carefully reviewed and selected from 14 submissions. The papers were organized in topical sections named: attack trees; attacks and risks modelling and visualization; and models for reasoning about security.

The ASEAN Australia Review is the flagship publication of the ASEAN-Australia Strategic Youth Partnership (AASYP). The 2020 edition features sixteen articles from young authors across Southeast Asia and Australia on diverse range of topics centred around the theme of Australia ASEAN Cooperation.

Miller's Marine War Risks is the only book devoted to drawing together and analysing the insurance of commercial shipping against war risks. It merges analysis of the legal principles, case law, and legislation with the practice of the insurance market in order to provide commentary on difficult questions concerning liabilities, claims, and coverage. With global events becoming more uncertain in the Gulf and elsewhere, the updating of Michael Miller’s classic text will be of great use to legal practitioners, the insurance market, and the shipping industry throughout the world.

Maritime Liabilities in a Global and Regional Context consists of edited versions of the papers delivered at the Institute of International Shipping and Trade Law’s 13th International Colloquium at Swansea Law School in September 2017. Written by a combination of top academics and highly-experienced legal practitioners, these papers have been carefully co-ordinated to give the reader a first-class insight into the issues surrounding maritime liabilities. The book is set out in two parts: - Part I offers a detailed and critical analysis of issues of contemporary importance concerning maritime liabilities - Part 2 discusses contemporary issues concerning the enforcement of maritime liabilities. An invaluable guide to recent legal and practical developments in maritime liabilities, this book is vital reading for both professional and academic readers.

This book identifies and examines the legal challenges facing the shipping industry and ship management today. It first addresses flag state rules and private international law as organisational tools of the shipowner for establishing the applicable legal framework in an age of increasing regulatory activity and extraterritorial effect of legislation. It then focuses on sustainability requirements and the liability of shipping companies managing supply chains and ships as waste. The third section considers challenges stemming from times of financial crisis and deals with the cross-border impact of shipping insolvencies, the UNCITRAL Model Law, and the approaches of different jurisdictions. Finally, the fourth section concerns digitalisation and automation, including delivery on the basis of digital release codes, bills of lading based on blockchain technology, the use of web portals and data sharing, and particular aspects of the law relating to autonomous ships, notably in marine insurance and carriage of goods. The book will be a useful resource for academics and practising lawyers working in shipping and maritime law.

With everything on the line… Flood Zone by Dana Mentink Mia Sandoval’s friend is murdered—and the single mother is a suspect. Her only ally is search-and-rescue worker Dallas Black. Working with the secretive Dallas, Mia discovers he’s as complicated as the murder they’re forced to investigate. Yet as a flood ravages their small Colorado town, a killer is determined that Mia, Dallas and their evidence get swept away to a watery grave. To Save Her Child by Margaret Daley When a young boy goes missing from wilderness day camp, Alaskan search-and-rescue worker Josiah Witherspoon is on the case. The former marine promises to find the child and return him to his mother. But Ella Jackson has a secret that could put them all in danger. Ella and Josiah are ready to risk their lives to save her son, but will they risk their hearts? USA TODAY Bestselling Author Margaret Daley Previously published as Flood Zone and To Save Her Child

Information warfare is upon us. In the last two decades, the U.S. economy's infrastructure has undergone a fundamental set of changes, relying increasingly on its service sector and high technology economy. The U.S. depends on computers, electronic data storage and transfers, and highly integrated communications networks. Its rapidly developing new form of critical infrastructure is exceedingly vulnerable to an emerging host of threats. This detailed volume examines the dangers of, and the evolving U.S. policy response to, cyberterrorism.

The continued growth of e-commerce mandates the emergence of new technical standards and methods that will securely integrate online activities with pre-existing infrastructures, laws and processes. Protocols for Secure Electronic Commerce, Second Edition addresses the security portion of this challenge. It is a full compendium of the protocols for securing online commerce and payments, serving as an invaluable resource for students and professionals in the fields of computer science and engineering, IT security, and financial and banking technology. The initial sections provide a broad overview of electronic commerce, money, payment systems, and business-to-business commerce, followed by an examination of well-known protocols (SSL, TLS, WTLS, and SET). The book also explores encryption algorithms and methods, EDI, micropayment, and multiple aspects of digital money. Like its predecessor, this edition is a general analysis that provides many references to more technical resources. It delivers extensive revisions of previous chapters, along with new chapters on electronic commerce in society, new e-commerce systems, and the security of integrated circuit cards.

This volume addresses American prisoners of war (POW) and missing in action (MIA) cases who were not repatriated following the Korean War, with particular emphasis on whether any American servicemen were transferred to USSR territory during the war. When most of Eastern Europe was struggling with dictatorships of one kind or another, the Democratic Republic of Georgia (1918-1921) established a constitution, a parliamentary system with national elections, an active opposition, and a free press. Like the Democratic Republic of Georgia in 1918, its successors emerged after 1991 from a bankrupt empire, and faced, yet again, the

task of establishing a new economic, political and social system from scratch. In both 1918 and 1991, Georgia was confronted with a hostile Russia and followed a pro-Western and pro-democratic course. The top regional experts in this book explore the domestic and external parallels between the Georgian post-colonial governments of the early twentieth and twenty-first centuries. How did the inexperienced Georgian leaders in both eras deal with the challenge of secessionism, what were their state building strategies, and what did democracy mean to them? What did their electoral systems look like, why were their economic strategies so different, and how did they negotiate with the international community neighbouring threats. These are the central challenges of transitional governments around the world today. Georgia's experience over one hundred years suggests that both history and contemporary political analysis offer the best (and most interesting) explanation of the often ambivalent outcomes.

An easy-to-read guide to protecting your digital life and your family online The rise of new technologies in our lives, which has taken us from powerful mobile phones to fitness trackers and smart appliances in under a decade, has also raised the need for everyone who uses these to protect themselves from cyber scams and hackers. Every new device and online service you use that improves your life also opens new doors for attackers looking to discover your passwords, banking accounts, personal photos, and anything else you want to keep secret. In Cyber Smart, author Bart McDonough uses his extensive cybersecurity experience speaking at conferences for the FBI, major financial institutions, and other clients to answer the most common question he hears: "How can I protect myself at home, on a personal level, away from the office?" McDonough knows cybersecurity and online privacy are daunting to the average person so Cyber Smart simplifies online good hygiene with five simple "Brilliance in the Basics" habits anyone can learn. With those habits and his careful debunking of common cybersecurity myths you'll be able to protect yourself and your family from: Identify theft Compromising your children Lost money Lost access to email and social media accounts Digital security is one of the most important, and least understood, aspects of our daily lives. But it doesn't have to be. Thanks to its clear instruction, friendly tone, and practical strategies, Cyber Smart will help you rest more easily, knowing you and your family are protected from digital attack.

Mia Mia Aboriginal Community DevelopmentHis Trust (Collin & Mia Duet, Book 1 of 2)A hot alpha billionaire romanceChrista Wick