We Re All Porn Stars Cybersecurity And The Human

Recognizing the habit ways to get this book **We Re All Porn Stars Cybersecurity And The Human** is additionally useful. You have remained in right site to start getting this info. get the We Re All Porn Stars Cybersecurity And The Human member that we meet the expense of here and check out the link.

You could buy guide We Re All Porn Stars Cybersecurity And The Human or get it as soon as feasible. You could speedily download this We Re All Porn Stars Cybersecurity And The Human after getting deal. So, once you require the books swiftly, you can straight acquire it. Its thus unquestionably simple and as a result fats, isnt it? You have to favor to in this proclaim

Trust in Cyberspace - National Research Council 1999-02-08

Whether or not you use a computer, you probably use a telephone, electric power, and a bank. Although you may not be aware of their presence, networked computer systems are increasingly becoming an integral part of your daily life. Yet, if such systems perform poorly or don't work at all, then they can put life, liberty, and property at tremendous risk. Is the trust that weâ€"as individuals and as a societyâ€"are placing in networked computer systems justified? And if it isn't, what can we do to make such systems more trustworthy? This book provides an assessment of the current state of the art procedures for building trustworthy networked information systems. It proposes directions for research in computer and network security, software technology, and system architecture. In addition, the book assesses current technical and market trends in order to better inform public policy as to where progress is likely and where incentives could help. Trust in Cyberspace offers insights into: The strengths and vulnerabilities of the telephone network and Internet, the two likely building blocks of any networked information system. The interplay between various dimensions of trustworthiness: environmental disruption, operator error, "buggy" software, and hostile attack. The implications for trustworthiness of anticipated developments in hardware and software technology, including the consequences of mobile code. The shifts in security technology and research resulting from replacing centralized mainframes with networks of computers. The heightened concern for integrity and availability where once only secrecy mattered. The way in which federal research funding levels and practices have affected the evolution and current state of the science and technology base in this area. You will want to read this book if your life is touched in any way by computers or telecommunications. But then, whose life isn't?

Drug Trafficking and International Security

- Paul Rexton Kan 2016-07-18

Each chapter examines how drug trafficking affects a certain security issue, such as rogue nations, weak and failing states, protracted intrastate conflicts, terrorism, transnational crime, public health, and cyber security. This book provides an understanding of how an array of threats to international security are exacerbated by drug trafficking.

Security and Loss Prevention - Philip Purpura 2007-10-24

Since the first edition of Security and Loss Prevention was published in 1983, much has changed in security and loss prevention considerations. In the past five years alone, security awareness and the need for added business continuity and preparedness considerations has been uniquely highlighted given events such as Katrina, 9/11, the formation of the Department of Homeland Security, and the increase in world terrorist events. This edition of Security and Loss Prevention is fully updated and encompasses the breadth and depth of considerations involved in implementing general loss prevention concepts and security programs within an organization. The book provides proven strategies to prevent and reduce incidents of loss due to legal issues, theft and other crimes, fire, accidental or intentional harm from employees, as well as the many ramifications of corporate mismanagement. The new edition contains a brand new terrorism chapter, along with coverage on background investigations, protection of sensitive information, internal threats, and considerations at select facilities (nuclear, DoD, government and federal). Author Philip Purpura once again demonstrates why students and professionals alike rely on this best-selling text as a timely, reliable resource. - Covers the latest professional security issues surrounding Homeland Security and risks presented by threats of terrorism - Recommended reading for ASIS International's prestigious CPP Certification - Cases provide real-world applications

The Smart Girl's Guide to Privacy - Violet Blue 2015-08-01

The whirlwind of social media, online dating, and mobile apps can make life a dream—or a nightmare. For every trustworthy website, there are countless jerks, bullies, and scam artists who want to harvest your personal information for their own purposes. But you can fight back, right now. In The Smart Girl’s Guide to Privacy, award-winning author and investigative journalist Violet Blue shows you how women are targeted online and how to keep yourself safe. Blue’s practical, user-friendly advice will teach you how to: –Delete personal content from websites –Use website and browser privacy controls effectively –Recover from and prevent identity theft –Figure out where the law protects you—and where it doesn’t –Set up safe online profiles –Remove yourself from people-finder websites Even if your privacy has already been compromised, don’t panic. It’s not too late to take control. Let The Smart Girl’s Guide to Privacy help you cut through the confusion and start protecting your online life.

Artificial Intelligence in Cyber Security: Impact and Implications - Reza Montasari 2021-11-26 The book provides a valuable reference for cyber security experts, digital forensic practitioners and network security professionals. In recent years, AI has gained substantial attention from researchers in both academia and industry, and as a result AI’s capabilities are constantly increasing at an extraordinary pace. AI is considered to be the Fourth Industrial Revolution or at least the next significant technological change after the evolution in mobile and cloud computing technologies. AI is a vehicle for improving the quality of our lives across every spectrum with a broad range of beneficial applications in various sectors. Notwithstanding its numerous beneficial use, AI simultaneously poses numerous legal, ethical, security and privacy challenges that are compounded by its malicious use by criminals. These challenges pose many risks to both our privacy and security at national, organisational and individual levels. In view of this, this book aims to help address some of these challenges focusing on the implication, impact and mitigations of the stated issues. The book provides a comprehensive coverage of not only the technical and ethical issues presented by the use of AI but also the adversarial application of AI and its associated implications. The authors recommend a number of novel approaches to assist in better detecting, thwarting and addressing AI challenges. The book also looks ahead and forecasts what attacks can be carried out in the future through the malicious use of the AI if sufficient defences are not implemented. The research contained in the book fits well into the larger body of work on various aspects of AI and cyber security. It is also aimed at researchers seeking to obtain a more profound knowledge of machine learning and deep learning in the context of cyber security, digital forensics and cybercrime. Furthermore, the book is an exceptional advanced text for Ph.D. and master's degree programmes in cyber security, digital forensics, network security, cyber terrorism and computer science. Each chapter contributed to the book is written by an internationally renowned expert who has extensive experience in law enforcement, industry or academia. Furthermore, this book blends advanced research findings with practice-based methods to provide the reader with advanced understanding and relevant skills.

We're All Porn Stars - Rob May 2017-12-18 According to social media we're all porn stars, find out why this isn't as funny as it often first appears and also pick up lots of other must know tips to stay cyber safe.This little book is designed to be an easy to access primer on the vast subject of cybersecurity, it's aimed at anyone who uses a phone, tablet or a computer who connects to Wi-Fi or has a social media account. It's based on the successful TEDx Talk on the subject which is a 16-minute key point rundown of hugely important a topic. The book is not intended to be exhaustive, but it is an easily accessible for everyone and it's a great eyeopener which incites important conversation both in the home and workplace.

Avatars, Activism and Postdigital Performance - Liam Jarvis 2021-11-18

In the context of the postdigital age, where technology is increasingly part of our social and political world, Avatars, Activism and Postdigital Performance traces how identity can be created, developed, hijacked, manipulated, sabotaged and explored through performance in postdigital cultures. Considering how technology is reshaping performance, this timely collection reveals how we engage in performance practices through expanded notions of intermediality, knotted networks and layering. This book examines the artist as activist and producer of avatars, and how digital doubles, artificial intelligence and semi-automated politics are problematizing and expanding our discussions of identity. Using a range of examples in theatre, film and internet-based performance practices, chapters examine the uncertain boundaries of networked 'informational selves' in mediatized cultures, the impacts of machine algorithms, apps and the consequences of digital legacies. Case studies include James Cameron's Avatar, Blast Theory's Karen, Ontroerend Goed's A Game of You, Randy Rainbow's online videos, Sisters Grimm's Calpurnia Descending, Dead Centre's Lippy and Chekhov's First Play and Jo Scott's practice-as-research in 'place-mixing'. This is an incisive study for scholars, students and practitioners interested in the wider conversations around identity-formation in postdigital cultures.

The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age - Danielle Keats Citron 2022-09-13

The essential road map for understanding—and defending—your right to privacy in the twenty-first century. Privacy is disappearing. From our sex lives to our workout routines, the details of our lives once relegated to pen and paper have joined the slipstream of new technology. As a MacArthur fellow and distinguished professor of law at the University of Virginia, acclaimed civil rights advocate Danielle Citron has spent decades working with lawmakers and stakeholders across the globe to protect what she calls intimate privacy—encompassing our bodies, health, gender, and relationships. When intimate privacy becomes data, corporations know exactly when to flash that ad for a new drug or pregnancy test. Social and political forces know how to manipulate what you think and who you trust, leveraging sensitive secrets and deepfake videos to ruin or silence opponents. And as new technologies invite new violations, people have power over one another like never before, from revenge porn to blackmail, attaching life-altering risks to growing up, dating online, or falling in love. A masterful new look at privacy in the twenty-first century, The Fight for Privacy takes the focus off Silicon Valley moguls to investigate the price we pay as technology migrates deeper into every aspect of our lives: entering our bedrooms and our bathrooms and our midnight texts; our relationships with friends, family, lovers, and kids; and even our relationship with ourselves. Drawing on in-depth interviews with victims, activists, and advocates, Citron brings this headline issue home for readers by weaving together visceral stories about the countless ways that corporate and individual violators exploit privacy loopholes. Exploring why the law has struggled to keep up, she reveals how our current system leaves victims—particularly women, LGBTQ+ people, and marginalized groups—shamed and powerless while perpetrators profit, warping cultural norms around the world. Yet there is a solution to our toxic relationship with technology and privacy: fighting for intimate privacy as a civil right. Collectively, Citron argues, citizens, lawmakers, and corporations have the power to create a new reality where privacy is valued and people are protected as they embrace what technology offers. Introducing readers to the trailblazing work of advocates today, Citron urges readers to join the fight. Your intimate life shouldn't be traded for profit or wielded against you for power: it belongs to you. With Citron as our guide, we can take back control of our data and build a better future for the next, ever more digital, generation.

The Cyber Effect - Mary Aiken 2016

"From one of the world's leading experts in cyberpsychology--a discipline that combines psychology, forensics, and technology--comes a groundbreaking exploration of the impact of technology on human behavior. In the first book of its kind, Mary Aiken applies her expertise in cyber-behavioral analysis to a range of subjects, including criminal activity on the Deep Web and Darknet; deviant behavior; Internet addictions; the impact of technology on the developing child; teenagers and the Web; cyber-romance and cyber-friendships; cyberchondria; the future of artificial intelligence; and the positive effects on our digital selves, such as online altruism"--

The Cybersecurity Self-Help Guide - Arun Soni 2021-10-19

Cybercrime is increasing at an exponential rate. Every day, new hacking techniques and tools are being developed by threat actors to bypass security systems and access private data. Most people do not know how to secure themselves, their devices, and their media shared online. Especially now, cybercriminals appear to be ahead of cybersecurity experts across cyberspace. During the coronavirus pandemic, we witnessed the peak of cybercrime, which is likely to be sustained even after the pandemic. This book is an up-to-date self-help guide for everyone who connects to the Internet and uses technology. It is designed to spread awareness about cybersecurity by explaining techniques and methods that should be implemented practically by readers. Arun Soni is an international award-winning author who has written 159 books on information technology. He is also a Certified Ethical Hacker (CEH v8) from the EC-Council US. His achievements have been covered by major newspapers and portals, such as Business Standard, The Economic Times, Indian Express, The Tribune, Times of India, Yahoo News, and Rediff.com. He is the recipient of multiple international records for this incomparable feat. His vast international exposure in cybersecurity and writing make this book special. This book will be a tremendous help to everybody and will be considered a bible on cybersecurity.

Campaigns on the Cutting Edge - Richard J. Semiatin 2020-04-10

Campaigns on the Cutting Edge evaluates the current trends of today's campaigns and assesses the innovative changes these well-tuned organizations are making on the presidential, congressional, and gubernatorial levels. As technology now allows candidates to announce their candidacies online, raise money through web fundraising, and mobilize supporters via smartphones, these increasingly mobile and integrated campaigns face the growing influence of outside interests. The thoroughly updated Fourth Edition looks at the 2018 midterm election and focuses on the rise of fake news, women′s activism in the #MeToo movement, voter ballot access measures, and the ways in which technology increases the volume of information that campaigns use.

Introduction to Homeland Security - Jane Bullock 2012-01-03

Bullock, Haddow, and Coppola have set the standard for homeland security textbooks, and they follow up best-selling third edition with this substantially improved version. As with its predecessor, the book clearly delineates the bedrock principles of preparing for, mitigating, managing, and recovering from emergencies and disasters. However, this new edition emphasizes their value with improved clarity and focus. What's more, it has been thoroughly revised to include changes that are based on transformations relevant to the political, budgetary, and legal aspects of homeland security that have changed since the 2008 Presidential election (and subsequent change in the administration). These include: new chapters on intelligence and counterterrorism, border security, transportation security, and cybersecurity; an expansion of material on the organization of the Department of Homeland Security; strategic and philosophical changes that are recommended and/or that have occurred as a result of the Quadrennial Homeland Security Review completed in 2010; updated budgetary information on both homeland security programs, and on the homeland security grants that have supported safety and security actions at the state and local levels, as well as in the private sector; and changes in the way the public perceives and receives information about security risk, including the possible elimination of the Homeland Security Advisory System. * New chapter that focuses specifically on the border and transportation security missions * An increased focus on cyber security and infrastructure security, both of which are rapidly growing in importance in the homeland security field among officials at all levels * A companion website that includes a full online Instructor's Guide and PowerPoint Lecture Slides.

Obama's Unending Wars - Jeremy Kuzmarov 2019-07-20

Many academics consider Obama to have been a master foreign policy strategist and shrewd practitioner of the art of realpolitik. This book demonstrates, however, that Obama in reality helped to institutionalize a permanent warfare state that resulted in gross human rights violations and contributed to America's strategic decline. His perpetuation of the War on Terror created more enemies and prompted the United States to lose influence in the Middle East. His Pivot to Asia policy intensified prospects for regional war while his unnecessary and willful military intervention destroyed Libya and drew the Russians in to protect Bashir al-Assad who won Syria's civil war. The Obama administration's heavy-handed interference in Ukraine led to effective Russian counter-moves, promoting a strategic alliance with China and regional integration that is moving the world towards multi-polarity. Obama's Unending Wars provides the first critical, comprehensive and highly documented history of the foreign policy of America's forty-fourth president - the drone king who ordered the bombing of seven Muslim countries, backtracked on a pledge to reduce America's nuclear arsenal, and helped fuel a new Cold War with Russia. During his years in office Obama provided billions of dollars in arms sales to Saudi Arabia as it assisted in the crushing of pro-democracy demonstrators in Bahrain and invaded Yemen. He sanctioned a coup in Honduras which plunged that country into chaos, perpetuated a failed drug war policy and contributed to the recolonization of Africa. While any Democratic Party president would have faced peril in confronting the Pentagon which had carried out a slow coup d'etat over the decades, Obama was rather, in many ways, the most perfect spokesman for the military-industrial complex. Who else but this articulate constitutional law professor could pull off a pro-war speech after winning the Nobel Peace Prize while ramping up drone assassinations and America's network of military bases in Africa and still retain the support of liberal-progressives? As many in the time of Trump now glance nostalgically back to the Obama presidency, this book will help them to see the continuity -- and continuous failure -- of American foreign policy irrespective of the party or figurehead representing it.

Communication Law - Dom Caristi 2018-05-04 Now in its second edition, Communication Law: Practical Applications in the Digital Age is an engaging and accessible text that brings a fresh approach to the fundamentals of mass media law. Designed for students of communication that are new to law, this volume presents its readers with key principles and emphasizes the impact of timely, landmark cases on today's media world, providing an applied learning experience. This new edition offers a brand new chapter on digital media law, a wealth of new case studies, and expanded discussions of current political, social, and cultural issues.

Deep Learning Applications for Cyber Security - Mamoun Alazab 2019-08-14

Cybercrime remains a growing challenge in terms of security and privacy practices. Working together, deep learning and cyber security experts have recently made significant advances in the fields of intrusion detection, malicious code analysis and forensic identification. This book addresses questions of how deep learning methods can be used to advance cyber security objectives, including detection, modeling, monitoring and analysis of as well as defense against various threats to sensitive data and security systems. Filling an important gap between deep learning and cyber security communities, it discusses topics covering a wide range of modern and practical deep learning techniques, frameworks and development tools to enable readers to engage with the cutting-edge research across various aspects of cyber security. The book focuses on mature and proven techniques, and provides ample examples to help readers grasp the key points.

How to Hack Like a God: Master the Secrets of Hacking Through Real Life Scenarios - Sparc Flow 2017-04-17

Follow me on a step-by-step hacking journey where we pwn a high-profile fashion company. From zero initial access to remotely recording board meetings, we will detail every custom script and technique used in this attack, drawn from real-life findings, to paint the most realistic picture possible. Whether you are a wannabe pentester dreaming about real-life hacking experiences or an experienced ethical hacker tired of countless Metasploit tutorials, you will find unique gems in this book for you to try: -Playing with Kerberos -Bypassing Citrix & Applocker -Mainframe hacking -Fileless WMI persistence -NoSQL injections -Wiegand protocol -Exfiltration techniques -Antivirus evasion tricks -And much more advanced hacking techniques I have documented almost every tool and custom script used in this book. I strongly encourage you to test them out yourself and master their capabilities (and limitations) in an environment you own and control. Hack (safely) the Planet! (Previously published as How to Hack a Fashion Brand)

The American Crisis - Writers of The Atlantic 2020-09-15

Some of America’s best reporters and thinkers offer an urgent look at a country in chaos in this collection of timely, often prophetic articles from The Atlantic. The past four years in the United States have been among the most turbulent in our history—and would have been so even without a global pandemic and waves of protest nationwide against police violence. Drawn from the recent work of The Atlantic staff writers and contributors, The American Crisis explores the factors that led us to the present moment: racial division, economic inequality, political dysfunction, the hollowing out of government, the devaluation of truth, and the unique threat posed by Donald Trump. Today’s emergencies expose pathologies years in the making. Featuring leading voices from The Atlantic, one of the country’s most widely read and influential magazines, The American Crisis is a broad and essential look at the condition of America today—and at the qualities of national character that may yet offer hope. With contributions by: Danielle Allen, Anne Applebaum, Yoni Appelbaum, Molly Ball, David W. Blight, Mark Bowden, Ta-Nehisi Coates, Lizabeth Cohen, McKay Coppins, James Fallows, Drew Gilpin Faust, Caitlin Flanagan, Franklin Foer, David Frum, Megan Garber, Michael Gerson, Elizabeth Goitein, David A. Graham, Emma Green, Yuval

Noah Harari, Ibram X. Kendi, Olga Khazan, Adrienne LaFrance, Annie Lowrey, James Mattis, Lin-Manuel Miranda, Angela Nagle, Vann R. Newkirk II, George Packer, Elaina Plott, Jeremy Raff, Jonathan Rauch, Adam Serwer, Clint Smith, Matthew Stewart, Alex Wagner, Tara Westover, and Ed Yong.

Cyber Security and Privacy - Frances Cleary 2015-10-07

This book constitutes the thoroughly refereed selected papers on the 4th Cyber Security and Privacy Innovation Forum, CSP Forum 2015, held in Brussels, Belgium, in April 2015. The 12 revised full papers presented were carefully reviewed and selected from various submissions. The papers are organized in topical sections such as security and privacy in the cloud; security and privacy technologies; risk and trust; research and innovation in cyber security and privacy.

The Quest to Cyber Superiority - Nir Kshetri 2016-07-29

This book explains how major world economies are recognizing the need for a major push in cyber policy environments. It helps readers understand why these nations are committing substantial resources to cybersecurity, and to the development of standards, rules and guidelines in order to address cyber-threats and catch up with global trends and technological developments. A key focus is on specific countries’ engagement in cyberattacks and the development of cyber-warfare capabilities. Further, the book demonstrates how a nation’s technological advancement may not necessarily lead to cyber-superiority. It covers cybersecurity issues with regard to conflicts that shape relationships between major economies, and explains how attempts to secure the cyber domain have been hampered by the lack of an international consensus on key issues and concepts. The book also reveals how some economies are now facing a tricky trade-off between economically productive uses of emerging technologies and an enhanced cybersecurity profile. In the context of current paradigms related to the linkages between security and trade/investment, it also delves into new perspectives that are being brought to light by emerging cybersecurity issues.

Artificial Intelligence - Charles Jennings 2019-05-08

Self-learning machines called AIs are popping up all around us. They will alter our lives as workers, consumers, investors, citizens, patients and students. We all need to get smart about AIs, now! That’s Charles Jennings’ message in his provocative new book, Artificial Intelligence: The Rise of the Lightspeed Learners.

How to Hack Like a Ghost - Sparc Flow 2021-05-11

How to Hack Like a Ghost takes you deep inside the mind of a hacker as you carry out a fictionalized attack against a tech company, teaching cutting-edge hacking techniques along the way. Go deep into the mind of a master hacker as he breaks into a hostile, cloud-based security environment. Sparc Flow invites you to shadow him every step of the way, from recon to infiltration, as you hack a shady, data-driven political consulting firm. While the target is fictional, the corporation’s vulnerabilities are based on real-life weaknesses in today’s advanced cybersecurity defense systems. You’ll experience all the thrills, frustrations, dead-ends, and eureka moments of his mission first-hand, while picking up practical, cutting-edge techniques for penetrating cloud technologies. There are no do-overs for hackers, so your training starts with basic OpSec procedures, using an ephemeral OS, Tor, bouncing servers, and detailed code to build an anonymous, replaceable hacking infrastructure guaranteed to avoid detection. From there, you’ll examine some effective recon techniques, develop tools from scratch, and deconstruct low-level features in common systems to gain access to the target. Spark Flow’s clever insights, witty reasoning, and stealth maneuvers teach you how to think on your toes and adapt his skills to your own hacking tasks. You'll learn: • How to set up and use an array of disposable machines that can renew in a matter of seconds to change your internet footprint • How to do effective recon, like harvesting hidden domains and taking advantage of DevOps automation systems to trawl for credentials • How to look inside and gain access to AWS’s storage systems • How cloud security systems like Kubernetes work, and how to hack them • Dynamic techniques for escalating privileges Packed with interesting tricks, ingenious tips, and links to external resources, this fast-paced, hands-on guide to penetrating modern cloud systems will help hackers of all stripes succeed on their next adventure.

Cybersecurity - Peter W. Singer 2014

An authoritative, single-volume introduction to cybersecurity addresses topics ranging from phishing and electrical-grid takedowns to cybercrime and online freedom, sharing illustrative anecdotes to explain how cyberspace security works and what everyday people can do to protect themselves. Simultaneous.

Strategic Cyber Security - Kenneth Geers 2011

Cybercrime Through an Interdisciplinary Lens - Thomas J. Holt 2016-12-08

Research on cybercrime has been largely bifurcated, with social science and computer science researchers working with different research agendas. These fields have produced parallel scholarship to understand cybercrime offending and victimization, as well as techniques to harden systems from compromise and understand the tools used by cybercriminals. The literature developed from these two fields is diverse and informative, but until now there has been minimal interdisciplinary scholarship combining their insights in order to create a more informed and robust body of knowledge. This book offers an interdisciplinary approach to research on cybercrime and lays out frameworks for collaboration between the fields. Bringing together international experts, this book explores a range of issues from malicious software and hacking to victimization and fraud. This work also provides direction for policy changes to both cybersecurity and criminal justice practice based on the enhanced understanding of cybercrime that can be derived from integrated research from both the technical and social sciences. The authors demonstrate the breadth of contemporary scholarship as well as identifying key questions that could be addressed in the future or unique methods that could benefit the wider research community. This edited collection will be key reading for academics, researchers, and practitioners in both computer security and law enforcement. This book is also a comprehensive resource for postgraduate and advanced undergraduate students undertaking courses in social and technical studies.

Gender and Security in Digital Space - Gulizar Haciyakupoglu 2022-11-10

Digital space offers new avenues, opportunities, and platforms in the fight for gender equality, and for the social, economic, and political participation of women and marginalised communities. However, the very same space plays host to gender inequalities and security threats with gendered implications. This edited volume ventures into complexities at the intersection of gender, security, and digital space, with a particular focus on the persistent problems of access, harassment, and disinformation. Scholars and practitioners in this volume tackle various facets of the issue, presenting an array of research, experiences, and case studies that span the globe. This knowledge lends itself to potential policy considerations in tackling inequalities and threats with gendered implications in cyber space towards digital spaces that are safe and equal. This book is a must-read for students, scholars, and practitioners seeking to expand their knowledge on the gendered threats in digital space and potential remedies against them.

The Midnight Star - Marie Lu 2017-10-03

The thrilling finale to the New York Times bestselling Young Elites series from “hit factory” Marie Lu #1 New York Times bestselling author Marie Lu concludes Adelina's story with this haunting and hypnotizing final installment to the Young Elites series. Adelina Amouteru is done suffering. She’s turned her back on those who have betrayed her and achieved the ultimate revenge: victory. Her reign as the White Wolf has been a triumphant one, but with each conquest her cruelty only grows. The darkness within her has begun to spiral out of control, threatening to destroy all she's gained. When a new danger appears, Adelina’s forced to revisit old wounds, putting not only herself at risk, but every Elite. In order to preserve her empire, Adelina and her Roses must join the Daggers on a perilous quest—though this uneasy alliance may prove to be the real danger.

Deep Fakes - Michael Filimowicz 2022-02-28

Deep Fakes: Algorithms and Society focuses on the use of artificial intelligence technologies to produce fictitious photorealistic audiovisual clips that are indistinguishable from traditional video media. For over a century, the indexical relationship of the photographic image, and its related media of film and video, to the scene of capture has served as a basis for truth claims. Historically, the iconicity of these images has featured a causal traceback to actual light rays in a particular time and space, which were fixed by chemical reactions or digital sensors to the resultant image. Today, photorealistic audiovisual media can be generated from deep learning networks which sever any connection to an actual event. Should society instantiate new regimes to manage this new challenge to our sense of reality and the traditional evidential capacities of the ‘mechanical image?’ How do these images generate information disorder while also providing the basis for legitimate tools used in entertainment and creative industries? Scholars and students from many backgrounds, as well as policy makers, journalists and the general reading public will find a multidisciplinary approach to questions posed by deep fake research from Communication, International Studies, Writing and Rhetoric.

Future Crimes - Marc Goodman 2015-02-24 NEW YORK TIMES and WALL STREET JOURNAL BESTSELLER ONE OF THE WASHINGTON POST'S 10 BEST BOOKS OF 2015 One of the world’s leading authorities on global security, Marc Goodman takes readers deep into the digital underground to expose the alarming ways criminals, corporations, and even countries are using new and emerging technologies against you—and how this makes everyone more vulnerable than ever imagined. Technological advances have benefited our world in immeasurable ways, but there is an ominous flip side: our technology can be turned against us. Hackers can activate baby monitors to spy on families, thieves are analyzing social media posts to plot home invasions, and stalkers are exploiting the GPS on smart phones to track their victims’ every move. We all know today’s criminals can steal identities, drain online bank accounts, and wipe out computer servers, but that’s just the beginning. To date, no computer has been created that could not be hacked—a sobering fact given our radical dependence on these machines for everything from our nation’s power grid to air traffic control to financial services. Yet, as ubiquitous as technology seems today, just over the horizon is a tidal wave of scientific progress that will leave our heads spinning. If today’s Internet is the size of a golf ball, tomorrow’s will be the size of the sun. Welcome to the Internet of Things, a living, breathing, global information grid where every physical object will be online. But with greater connections come greater risks. Implantable medical devices such as pacemakers can be hacked to deliver a lethal jolt of electricity and a car's brakes can be disabled at high speed from miles away. Meanwhile, 3-D printers can produce AK-47s, bioterrorists can download the recipe for Spanish flu, and cartels are using fleets of drones to ferry drugs across borders. With explosive insights based upon a career in law enforcement and counterterrorism, Marc Goodman takes readers on a vivid journey through the darkest recesses of the Internet. Reading like science fiction, but based in science fact, Future Crimes explores how bad actors are primed to hijack the technologies of tomorrow, including robotics, synthetic biology, nanotechnology, virtual reality, and artificial intelligence. These fields hold the power to create a world of unprecedented abundance and prosperity. But the technological bedrock upon which we are building our common future is deeply unstable and, like a house of cards, can come crashing down at any moment. Future Crimes provides a mind-blowing glimpse into the dark side of technological innovation and the unintended consequences of our connected world. Goodman offers a way out with clear steps we must take to survive the progress unfolding before us. Provocative, thrilling, and ultimately empowering, Future Crimes will serve as an urgent call to action that shows how we can take back control over our own devices and harness technology's tremendous power for the betterment of humanity—before it's too late.

Fictional Immorality and Immoral Fiction - Garry Young 2021-01-15

It is commonplace for fictional content to depict immoral activities: the kidnapping of a politician, for example, or the elaborate theft of a national treasure, or perhaps the gruesome proclivities of a sadistic murderer. These and similar depictions can be found across a range of media, and in varying degrees of detail and realism.

Fictional Immorality and Immoral Fiction examines potential conditions for transforming fictional immorality into immoral fiction, in order to establish what makes a depiction of fictional immorality and/or one’s engagement with it immoral. To achieve this aim, Garry Young analyzes fictional content, its meaning, one’s motivation for engaging with it, and the medium in which the fiction is presented (such as film, literature, theatre, video games) using philosophical inquiry. The end result is a systematic examination of fictional immorality, which contributes toward debates on the morality of depicting and engaging with fictional immorality, as well as the reach of censorship and other forms of prohibition, especially when the act depicted is of the kind that would be most egregious if carried out in reality.

I, Warbot - Kenneth Payne 2021-12-01
Artificial Intelligence is going to war. Intelligent weapon systems are here today, and many more are on the way tomorrow. Already, they're reshaping conflict--from the chaos of battle, with pilotless drones, robot tanks and unmanned submersibles, to the headquarters far from the action, where generals and politicians use technology to weigh up what to do. AI changes how we fight, and even how likely it is that we will. In battle, warbots will be faster, more agile and more deadly than today's crewed weapons. New tactics and concepts will emerge, with spoofing and swarming to fool and overwhelm enemies. Strategies are changing too. When will an intelligent machine escalate, and how can it be deterred? Can robots predict the future? And what happens to the 'art of war' as machines themselves become creative? Autonomous warfare makes many people uneasy. An international campaign against 'killer robots' hopes to ban AI from conflict. But the genie is out--AI weapons are too useful for states to outlaw. Still, crafting sensible rules for warbots is possible. This fascinating book shows how it might be done.

Ten Strategies of a World-Class Cybersecurity Operations Center - Carson Zimmerman 2014-07-01

Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.

Cybersecurity for Industrial Control Systems - Tyson Macaulay 2012-02-02

As industrial control systems (ICS), including SCADA, DCS, and other process control networks, become Internet-facing, they expose crucial services to attack. Threats like Duqu, a sophisticated worm found in the wild that appeared to share portions of its code with the Stuxnet worm, emerge with increasing frequency. Explaining how to develop and implement an effective cybersecurity program for ICS, Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS provides you with the tools to ensure network security without sacrificing the efficiency and functionality of ICS. Highlighting the key issues that need to be addressed, the book begins with a thorough introduction to ICS. It discusses business, cost, competitive, and regulatory drivers and the conflicting priorities of convergence. Next, it explains why security requirements differ from IT to ICS. It differentiates when standard IT security solutions can be used and where SCADA-specific practices are required. The book examines the plethora of potential threats to ICS, including hijacking malware, botnets, spam engines, and porn dialers. It outlines the range of vulnerabilities inherent in the ICS quest for efficiency and functionality that necessitates risk behavior such as remote access and control of critical equipment. Reviewing risk assessment techniques and the evolving risk assessment process, the text concludes by examining what is on the horizon for ICS security, including IPv6, ICSv6 test lab designs, and IPv6 and ICS sensors.

Fatal System Error - Joseph Menn 2010-10-26 In 2004, a California computer whiz named Barrett Lyon uncovered the identity of a hacker running major assaults on business websites. Without fully grasping the repercussions, he set on an investigation that led him into the heart of the Russian mob. Cybercrime was evolving. No longer the domain of small-time thieves, it had been discovered by sophisticated gangs. They began by attacking corporate websites but increasingly stole financial data from consumers and defense secrets from governments. While Barrett investigated the cutting edge of technology crime, the U.S. government struggled to catch up. Britain, however, was a different story. In the late 1990s, the Queen herself had declared safe e-commerce a national security priority. Agents from the London-based National Hi-Tech Crime Unit sought out Barrett and enlisted his help. They also sent detective Andrew Crocker, a Welsh former boxer, to Russia to track down and prosecute the hackers—and to find out who they worked for. Fatal System Error penetrates both the Russian cyber-mob and the American mafia as the two fight over the Internet’s massive spoils. It takes readers into the murky hacker underground, traveling the globe from San Francisco to Costa Rica, London, and Russia. Using unprecedented access to mob businesses and Russian officials, it shows how top criminals earned protection from the Russian government—and how Barrett Lyon and Andrew Crocker got closer to the titans of the underground economy than any previous outsider. Together, their stories explain why cybercrime is much worse than you thought—and why the Internet might not survive.

Digital Gender-Sexual Violations - Matthew Hall 2022-10-26

This groundbreaking book argues that the fundamental issues around how victim-survivors of digital gender-sexual violations (DGSVs) are abused can be understood in terms of gender and sexual dynamics, constructions, positioning and logics. The book builds upon Hall and Hearn's previous work, Revenge Pornography, but has been substantially reworked to examine other forms of DGSV such as upskirting and sexual deepfakes, as well as the latest research and debates in the field. Facilitated by developments in internet and mobile technologies, the non-consensual posting of real or fake sexually explicit images of others for revenge, entertainment, homosocial status or political leverage has become a global phenomenon. Using discourse and thematic analytical approaches, this text examines digital, survey and interview data on gendered sexual violences, abuses, and violations. The words of both the perpetrators and victim-survivors are presented, showing the impact on victim-survivors and the complex ways in which phallocentric power relations and existing hegemonic masculinities are reinforced and invoked by perpetrators to position girls and women as gendered and sexualised commodities to be traded, admired, violated or abused for the needs of individual men or groups of men. Hall, Hearn and Lewis explore their research in a broader social and political context, evaluating and suggesting changes to existing legislative frameworks, education, victim support, and practical and policy interventions against DGSV, along with wider political considerations. This is a unique resource for students, academics and researchers as well as professionals dealing with issues around digital gender-sexual violations.

Feminist Legal Theory (Second Edition) - Nancy Levit 2016-01-15

Feminist legal theory is one of the most dynamic fields in the law, and it affects issues ranging from child custody to sexual harassment. Since its initial publication in 2006, Feminist Legal Theory: A Primer has received rave reviews. Now, in the completely updated second edition of this outstanding primer, Nancy Levit and Robert R.M. Verchick introduce the diverse strands of feminist legal theory and discuss an array of substantive legal topics, pulling in recent court decisions, new laws, and important shifts in culture and technology. The book centers on feminist legal theories, including equal treatment theory, cultural feminism, dominance theory, critical race feminism, lesbian feminism, postmodern feminism, and ecofeminism. Readers will find new material on women in politics, gender and globalization, and the promise and danger of expanding social media. Updated statistics and empirical analysis appear throughout. The authors, prominent experts in the field, also address feminist legal methods, such as consciousness-raising and storytelling. The primer offers an accessible and pragmatic approach to feminist legal theory. It demonstrates the ways feminist legal theory operates in real-life contexts, including domestic violence, reproductive rights, workplace discrimination, education, sports, pornography, and global issues of gender. The authors highlight a sweeping range of cutting-edge topics at the intersection of law and gender, such as single-sex schools, abortion, same-sex marriage, rape on college campuses, and international trafficking in women and girls. At its core, Feminist Legal Theory shows the importance of the roles of law and feminist legal theory in shaping contemporary gender issues.

Cybersecurity And Legal-regulatory Aspects - Gabi Siboni 2021-01-04
Cyberspace has become a critical part of our lives and as a result is an important academic research topic. It is a multifaceted and dynamic domain that is largely driven by the business-civilian sector, with influential impacts on national security. This book presents current and diverse matters related to regulation and jurisdictive activity within the cybersecurity context. Each section includes a collection of scholarly articles providing an analysis of questions, research directions, and methods within the field.The interdisciplinary book is an authoritative and comprehensive reference to the overall discipline of cybersecurity. The coverage of the book will reflect the most advanced discourse on related issues.

Worm - Mark Bowden 2011-09-27
From the bestselling author of Black Hawk Down, the gripping story of the Conficker worm—the cyberattack that nearly toppled the world. The Conficker worm infected its first computer in November 2008, and within a month had infiltrated 1.5 million computers in 195 countries. Banks, telecommunications companies, and critical government networks—including British Parliament and the French and German military—became infected almost instantaneously. No one had ever seen anything like it. By January 2009, the worm lay hidden in at least eight million computers, and the botnet of linked computers it had created was big enough that an attack might crash the world. In this “masterpiece” (The Philadelphia Inquirer), Mark Bowden expertly lays out a spellbinding tale of how hackers, researchers, millionaire Internet entrepreneurs, and computer security experts found themselves drawn into a battle between those determined to exploit the Internet and those committed to protecting it.

The Sea We Swim In: How Stories Work in a Data-Driven World - Frank Rose 2021-06-29

A practical guide to "narrative thinking," and why it matters in a world defined by data. In The Sea We Swim In, Frank Rose leads us to a new understanding of stories and their role in our lives. For decades, experts from many fields—psychologists, economists, advertising and marketing executives—failed to register the power of narrative. Scientists thought stories were frivolous. Economists were knee-deep in theory. Marketers just wanted to cut to the sales pitch. Yet stories, not reasoning, are the key to persuasion. Whether we're aware of it or not, stories determine how we view the world and our place in it. That means the tools of professional storytellers—character, world, detail, voice—can unlock a way of thinking that's ideal for an age in which we don't passively consume media but actively participate in it. Building on insights from cognitive psychology and neuroscience, Rose shows us how to see the world in narrative terms, not as a thesis to be argued or a pitch to be made but as a story to be told. Leading brands and top entertainment professionals already understand the vast potential of storytelling. From Warby Parker to Mailchimp to The Walking Dead, Rose explains how they use stories to establish their identity and turn ordinary people into fans—and how you can do the same.

Successful Cybersecurity Professionals - Steven Brown 2020-09-18

This book provides a unique perspective into the mindset of psychology and cybersecurity. It presents a view of incorporating the latest research in cybersecurity and behavior. The newest cybersecurity challenge is not just understanding cybercriminals' behavior, but our behavior as well, and to realize that some of behaviors could lead us in making bad cybersecurity decisions. By using models and literature rooted in psychology and comparing those to cybersecurity attacks, this book will help those who make crucial cybersecurity decisions to protect their organization, even better decisions. Dr. Brown also presents even a possible theory of cybersecurity. Key areas include: behaviorism; learning models; cybersecurity vulnerabilities; stereotypes; cybersecurity traits; conditioned response; social engineering; deep fakes.

TIME Cybersecurity - The Editors of TIME 2018-01-19

Mysterious and dark, the many dangers of the internet lurk just below the sunny surface of social media, online shopping and cat videos. Now, in a new Special Edition from the Editors of TIME, comes Cybersecurity: Hacking, the Dark Web and You to help you understand the dangers posed by hackers, cyber criminals and other bad actors on the internet. Those potentially at risk include: individuals (your personal photography and communications, your finances and more); businesses and international relations; and our government (think interference in the November 2016 United States elections). Clear and concise, this Special Edition features up-to-the-minute information, graphics, and statistics as well as a hacking glossary to help you better understand the threats that lie in wait behind each keystroke. Cybersecurity is filled with compelling stories about hacks and hackers, the battle against revenge porn, Google’s elite guard against rising digital threats, and it also includes a step-by-step guide to help you defend against scammers and viruses. For anyone who uses the internet—and that’s pretty much all of us—Cybersecurity is a thorough examination of the security challenges of technology today, and how to overcome them to stay safe online.