Acces PDF Procedures And Techniques Tactics Fraud Cyber

As recognized, adventure as competently as experience not quite lesson, amusement, as capably as settlement can be gotten by just checking out a ebook **Procedures And Techniques Tactics Fraud Cyber** then it is not directly done, you could endure even more with reference to this life, in relation to the world.

We meet the expense of you this proper as competently as easy pretentiousness to acquire those all. We allow Procedures And Techniques Tactics Fraud Cyber and numerous book collections from fictions to scientific research in any way. among them is this Procedures And Techniques Tactics Fraud Cyber that can be your partner.

KEY=CYBER - GRANT ZACHARY

CYBER FRAUD

TACTICS, TECHNIQUES AND PROCEDURES

CRC Press With millions lost each year, cyber crime has evolved from a minor nuisance to a major concern involving well-organized actors and highly sophisticated organizations. Combining the best of investigative journalism and technical analysis, Cyber Fraud: Tactics, Techniques, and Procedures documents changes in the culture of cyber criminals and explores the innovations that are the result of those changes. The book uses the term Botnet as a metaphor for the evolving changes represented by this underground economy. Copiously illustrated, this engaging and engrossing book explores the state of threats present in the cyber fraud underground. It discusses phishing and pharming, trojans and toolkits, direct threats, pump-and-dump scams, and other fraud-related activities of the booming cyber-underground economy. By examining the geopolitical and socio-economic foundations of a cyber threat landscape, the book specifically examines telecommunications infrastructure development, patterns and trends of internet adoption and use, profiles of specific malicious actors, threat types, and trends in these areas. This eye-opening work includes a variety of case studies — including the cyber threat landscape in Russia and Brazil. An in-depth discussion is provided on the Russian Business Network's (RBN) role in global cyber crime as well as new evidence on how these criminals steal, package, buy, sell, and profit from the personal financial information of consumers. Armed with this invaluable information, organizations and individuals will be better able to secure their systems and develop countermeasures to disrupt underground fraud.

CYBER FRAUD

TACTICS, TECHNIQUES, AND PROCEDURES

With millions lost each year, cyber crime has evolved from a minor nuisance to a major concern involving well-organized actors and highly sophisticated organizations. Combining the best of investigative journalism and technical analysis, Cyber Fraud : Tactics, Techniques, and Procedures documents changes in the culture of cyber criminals and explores the innovations that are the result of those changes. The book uses the term Botnet as a metaphor for the evolving changes represented by this underground economy. Copiously illustrated, this engaging and engrossing book explores the state of threat.

DIGITAL MULTIMEDIA: CONCEPTS, METHODOLOGIES, TOOLS, AND APPLICATIONS

CONCEPTS, METHODOLOGIES, TOOLS, AND APPLICATIONS

IGI Global Contemporary society resides in an age of ubiquitous technology. With the consistent creation and wide availability of multimedia content, it has become imperative to remain updated on the latest trends and applications in this field. Digital Multimedia: Concepts, Methodologies, Tools, and Applications is an innovative source of scholarly content on the latest trends, perspectives, techniques, and implementations of multimedia technologies. Including a comprehensive range of topics such as interactive media, mobile technology, and data management, this multi-volume book is an ideal reference source for engineers, professionals, students, academics, and researchers seeking emerging information on digital multimedia.

CYBER CRIME STRATEGY

The Stationery Office The Government published the UK Cyber Security Strategy in June 2009 (Cm. 7642, ISBN 97801017674223), and established the Office of Cyber Security to provide strategic leadership across Government. This document sets out the Home Office's approach to tackling cyber crime, showing how to tackle such crimes directly through the provision of a law enforcement response, and indirectly through cross-Government working and through the development of relationships with industry, charities and other groups, as well as internationally. The publication is divided into five chapters and looks at the following areas, including: the broader cyber security context; cyber crime: the current position; the Government response and how the Home Office will tackle cyber crime.

ECCWS 2019 18TH EUROPEAN CONFERENCE ON CYBER WARFARE AND SECURITY

Academic Conferences and publishing limited

CYBER SECURITY AUDITING, ASSURANCE, AND AWARENESS THROUGH CSAM AND CATRAM

IGI Global With the continued progression of technologies such as mobile computing *and the internet of things (IoT), cybersecurity has swiftly risen to a prominent field of global interest. This has led to cyberattacks and cybercrime becoming much more sophisticated to a point where cybersecurity can no longer be the exclusive responsibility of an organization's information technology (IT) unit. Cyber warfare is becoming a national issue and causing various governments to reevaluate the current defense strategies they have in place. Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM provides emerging research exploring the practical aspects of reassessing current cybersecurity measures within organizations and international governments and improving upon them using audit and awareness training models, specifically the Cybersecurity Audit Model (CSAM) and the Cybersecurity Awareness Training Model (CATRAM). The book presents multi-case studies on the development and validation of these models and frameworks and analyzes their implementation and ability to sustain and audit national cybersecurity strategies. Featuring coverage on a broad range of topics such as forensic analysis, digital evidence, and incident management, this book is ideally designed for researchers, developers, policymakers, government officials, strategists, security professionals, educators, security analysts, auditors, and students seeking current research on developing training models within cybersecurity management and awareness.*

ENCYCLOPEDIA OF INFORMATION SCIENCE AND TECHNOLOGY, THIRD EDITION

IGI Global "This 10-volume compilation of authoritative, research-based articles contributed by thousands of researchers and experts from all over the world emphasized modern issues and the presentation of potential opportunities, prospective solutions, and future directions in the field of information science and technology"--Provided by publisher.

ETHICAL HACKING TECHNIQUES AND COUNTERMEASURES FOR CYBERCRIME PREVENTION

IGI Global As personal data continues to be shared and used in all aspects of society, the protection of this information has become paramount. While cybersecurity should protect individuals from cyber-threats, it also should be eliminating any and all vulnerabilities. The use of hacking to prevent cybercrime and contribute new countermeasures towards protecting computers, servers, networks, web applications, mobile devices, and stored data from black hat attackers who have malicious intent, as well as to stop against unauthorized access instead of using hacking in the traditional sense to launch attacks on these devices, can contribute emerging and advanced solutions against cybercrime. Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention is a comprehensive text that discusses and defines ethical hacking, including the skills and concept of ethical hacking, and studies the countermeasures to prevent and stop cybercrimes, cyberterrorism, cybertheft, identity theft, and computer-related crimes. It broadens the understanding of cybersecurity by providing the necessary tools and skills to combat cybercrime. Some specific topics include top cyber investigation trends, data *security of consumer devices, phases of hacking attacks, and stenography for secure image transmission. This book is relevant for ethical hackers, cybersecurity analysts, computer forensic experts, government officials, practitioners, researchers, academicians, and students interested in the latest techniques for preventing and combatting cybercrime.*

CYBERCRIME THROUGH AN INTERDISCIPLINARY LENS

Taylor & Francis 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.

JOURNAL OF LAW & CYBER WARFARE: THE NEW FRONTIER OF WARFARE

Lulu.com FOREWORD Cyber Warfare, What are the Rules? By Daniel B. Garrie ARTICLES Cyber Attacks and the Laws of War By Michael Gervais If You Wish Cyber Peace, Prepare for Cyber War: The Need for the Federal Government to Protect Critical Infrastructure From Cyber Warfare. By Michael Preciado They Did it For the Lulz: Future Policy Considerations in the Wake of Lulz Security and Other Hacker Groups' Attacks on Stored Private Customer Data By Jesse Noa A New Perspective on the Achievement of Psychological Effects from Cyber Warfare Payloads: The Analogy of Parasitic Manipulation of Host Behavior By Dr. Mils Hills

INDUSTRY OF ANONYMITY

INSIDE THE BUSINESS OF CYBERCRIME

Harvard University Press Jonathan Lusthaus lifts the veil on cybercriminals in the most extensive account yet of the lives they lead and the vast international industry *they have created. Having traveled to hotspots around the world to meet with hundreds of law enforcement agents, security gurus, hackers, and criminals, he charts how this industry based on anonymity works.*

INSTRUMENTS OF PUBLIC LAW

DIGITAL TRANSFORMATION DURING THE PANDEMIC

Taylor & Francis The Covid 19 pandemic has revealed the need to verify the existing principles of functioning of public authorities, in relation to various decision-making processes, both at the conceptual level and at law implementation. The action of the legislator and public administration towards the society and the economy is conducted using peculiar instruments to control the public administration system. These instruments are likely to be of a public or private law nature. This book takes a comparative approach to examine the issues related to digital transformation in the times of a pandemic regarding the use of public-law instruments in Poland and the wider European context. In particular, the research aims to identify what stage the development of digital solutions in the state's organization and its authorities has reached, including the organization of public administration; what the has pandemic changed. Exploring the concepts of digital transformation, pandemic and public-law instruments, it provides an analysis of European and national public-law instruments using digital solutions, security and cybersecurity during a pandemic, and concrete issues such as public administration, health protection and social security, economic activity and the system of public finances, and education during the pandemic is performed. Establishing whether particular solutions are durable and to what extent they create a certain standard of response to a threat, it makes recommendations for determining which of the existing solutions is useful for the functioning of the state and its organs and facilitates the performance of their tasks.

ANTI-FRAUD RISK AND CONTROL WORKBOOK

John Wiley & Sons – How to measure your organization's fraud risks – Detecting fraud before it's too late – Little-known frauds that cause major losses – Simple but powerful anti-fraud controls Proven guidance for fraud detection and prevention in a practical workbook format An excellent primer for developing and implementing an anti-fraud program, Anti-Fraud Risk and Control Workbook engages readers in an absorbing self- paced learning experience to develop familiarity with the practical aspects of fraud detection and prevention. Whether you are an internal or external auditor, accountant, senior financial executive, accounts payable professional, credit manager, or financial services manager, this invaluable resource provides you with timely discussion on: Why no organization is immune to fraud The human element of fraud Internal fraud at employee and management levels Conducting a successful fraud risk assessment Basic fraud detection tools and techniques Advanced fraud detection tools and techniques Written by a recognized expert in the field of fraud detection and prevention, this effective workbook is filled with interactive exercises, case studies, and chapter quizzes and shares industry-tested methods for detecting, preventing, and reporting fraud. Discover how to become more effective in *protecting your organization against financial fraud with the essential techniques and tools in Anti-Fraud Risk and Control Workbook.*

PRACTICAL FRAUD PREVENTION

"O'Reilly Media, Inc." Over the past two decades, the booming ecommerce and fintech industries have become a breeding ground for fraud. Organizations that conduct business online are constantly engaged in a cat-and-mouse game with these invaders. In this practical book, Gilit Saporta and Shoshana Maraney draw on their fraud-fighting experience to provide best practices, methodologies, and tools to help you detect and prevent fraud and other malicious activities. Data scientists, data analysts, and fraud analysts will learn how to identify and quickly respond to attacks. You'll get a comprehensive view of typical incursions as well as recommended detection methods. Online fraud is constantly evolving. This book helps experienced researchers safely guide and protect their organizations in this ever-changing fraud landscape. With this book, you will: Examine current fraud attacks and learn how to mitigate them Find the right balance between preventing fraud and providing a smooth customer experience Share insights across multiple business areas, including ecommerce, banking, cryptocurrency, anti-money laundering, and ad tech Evaluate potential risks for a new vertical, market, or product Train and mentor teams by boosting collaboration and kickstarting brainstorming sessions Get a framework of fraud methods, fraud-fighting analytics, and data science methodologies

ECCWS2014-PROCEEDINGS OF THE 13TH EUROPEAN CONFERENCE ON CYBER WAREFARE AND SECURITY

ECCWS 2014

Academic Conferences Limited

CYBER WARFARE

BUILDING THE SCIENTIFIC FOUNDATION

Springer This book features a wide spectrum of the latest computer science research relating to cyber warfare, including military and policy dimensions. It is the first book to explore the scientific foundation of cyber warfare and features research from the areas of artificial intelligence, game theory, programming languages, graph theory and more. The high-level approach and emphasis on scientific rigor provides insights on ways to improve cyber warfare defense worldwide. Cyber Warfare: Building the Scientific Foundation targets researchers and practitioners working in cyber security, especially government employees or contractors. Advanced-level students in computer science and electrical engineering with an interest in security will also find this content valuable as a secondary textbook or reference.

GUIDE TO CYBER THREAT INFORMATION SHARING

CreateSpace As the magnitude and complexity of cyberspace increases, so too does *the threat1 landscape. Cyber attacks have increased in both frequency and sophistication resulting in significant challenges to organizations that must defend their infrastructure from attacks by capable adversaries. These adversaries range from individual attackers to well-resourced groups operating as part of a criminal enterprise or on behalf of a nation-state. These adversaries are persistent, motivated, and agile; and employ a variety of tactics, techniques, and procedures (TTPs) to compromise systems, disrupt services, commit financial fraud, expose sensitive information, and steal intellectual property. To enhance incident response actions and bolster cyber defenses, organizations must harness the collective wisdom of peer organizations through information sharing and coordinated incident response. This publication expands upon the guidance introduced in Section 4, Coordination and Information Sharing of NIST Special Publication (SP) 800-61, Computer Security Incident Handling Guide and explores information sharing, coordination, and collaboration as part of the incident response life cycle. This publication assists organizations in establishing, participating in, and maintaining information sharing relationships throughout the incident response life cycle. The publication explores the benefits and challenges of coordination and sharing, presents the strengths and weaknesses of various information sharing architectures, clarifies the importance of trust, and introduces specific data handling considerations. The goal of the publication is to provide guidance that improves the efficiency and effectiveness of defensive cyber operations and incident response activities, by introducing safe and effective information sharing practices, examining the value of standard data formats and transport protocols to foster greater interoperability, and providing guidance on the planning, implementation, and maintenance of information sharing programs.*

E-INFRASTRUCTURE AND E-SERVICES FOR DEVELOPING COUNTRIES

13TH EAI INTERNATIONAL CONFERENCE, AFRICOMM 2021, ZANZIBAR, TANZANIA, DECEMBER 1-3, 2021, PROCEEDINGS

Springer Nature This book constitutes the thoroughly refereed proceedings of the 13th International Conference on e-Infrastructure and e-Services for Developing Countries, AFRICOMM 2021, held in Zanzibar, Tanzania, in December 2021. The 31 full papers presented were carefully selected from 78 submissions. The papers discuss issues and trends, resent research, innovation and experiences related to e-Infrastructure and e-Services along with their associated policy and regulations with a deep focus on developing countries. In recognition of the challenges imposed by the COVID-19 pandemic, the conference organized a workshop to share experience on digital leaning and teaching at the time of pandemic, which garnered 3 papers.

RESEARCH ANTHOLOGY ON HUMAN RESOURCE PRACTICES FOR THE MODERN WORKFORCE

IGI Global Human resource departments have been a crucial part of business practices for decades and particularly in modern times as professionals deal with multigenerational workers, diversity initiatives, and global health and economic *crises. There is a necessity for human resource departments to change as well to adapt to new societal perspectives, technology, and business practices. It is important for human resource managers to keep up to date with all emerging human resource practices in order to support successful and productive organizations. The Research Anthology on Human Resource Practices for the Modern Workforce presents a dynamic and diverse collection of global practices for human resource departments. This anthology discusses the emerging practices as well as modern technologies and initiatives that affect the way human resources must be conducted. Covering topics such as machine learning, organizational culture, and social entrepreneurship, this book is an excellent resource for human resource employees, managers, CEOs, employees, business students and professors, researchers, and academicians.*

DISRUPTIVE TECHNOLOGY: CONCEPTS, METHODOLOGIES, TOOLS, AND APPLICATIONS

CONCEPTS, METHODOLOGIES, TOOLS, AND APPLICATIONS

IGI Global The proliferation of entrepreneurship, technological and business innovations, emerging social trends and lifestyles, employment patterns, and other developments in the global context involve creative destruction that transcends geographic and political boundaries and economic sectors and industries. This creates a need for an interdisciplinary exploration of disruptive technologies, their impacts, and their implications for various stakeholders widely ranging from government agencies to major corporations to consumer groups and individuals. Disruptive Technology: Concepts, Methodologies, Tools, and Applications is a vital reference source that examines innovation, imitation, and creative destruction as critical factors and agents of socio-economic growth and progress in the context of emerging challenges and opportunities for business development and strategic advantage. Highlighting a range of topics such as IT innovation, business strategy, and sustainability, this multi-volume book is ideally designed for entrepreneurs, business executives, business professionals, academicians, and researchers interested in strategic decision making using innovations and competitiveness.

THE UK CYBER SECURITY STRATEGY

LANDSCAPE REVIEW, CROSS GOVERNMENT

The Stationery Office The cost of cyber crime to the UK is currently estimated to be between £18 billion and £27 billion. Business, government and the public must therefore be constantly alert to the level of risk if they are to succeed in detecting and resisting the threat of cyber attack. The UK Cyber Security Strategy, published in November 2011, set out how the Government planned to deliver the National Cyber Security Programme through to 2015, committing £650 million of additional funding. Among progress reported so far, the Serious Organised Crime Agency repatriated more than 2.3 million items of compromised card payment details to the financial sector in the UK and internationally since 2011, preventing a potential economic loss of more than £500 million. In the past year, moreover, the public reported to Action

Fraud over 46,000 reports of cyber crime, amounting to £292 million worth of attempted fraud. NAO identifies six key challenges faced by the Government in implanting its cyber security strategy in a rapidly changing environment. These are the need to influence industry to protect and promote itself and UK plc; to address the UK's current and future ICT and cyber security skills gap; to increase awareness so that people are not the weakest link; to tackle cyber crime and enforce the law; to get government to be more agile and joined-up; and to demonstrate value for money. The NAO recognizes, however, that there are some particular challenges in establishing the value for money

CYBER FRAUDS, SCAMS AND THEIR VICTIMS

Taylor & Francis Crime is undergoing a metamorphosis. The online technological revolution has created new opportunities for a wide variety of crimes which can be perpetrated on an industrial scale, and crimes traditionally committed in an offline environment are increasingly being transitioned to an online environment. This book takes a case study-based approach to exploring the types, perpetrators and victims of cyber frauds. Topics covered include: An in-depth breakdown of the most common types of cyber fraud and scams. The victim selection techniques and perpetration strategies of fraudsters. An exploration of the impact of fraud upon victims and best practice examples of support systems for victims. Current approaches for policing, punishing and preventing cyber frauds and scams. This book argues for a greater need to understand and respond to cyber fraud and scams in a more effective and victim-centred manner. It explores the victim-blaming discourse, before moving on to examine the structures of support in place to assist victims, noting some of the interesting initiatives from around the world and the emerging strategies to counter this problem. This book is essential reading for students and researchers engaged in cyber crime, victimology and international fraud.

CYBERCRIME INVESTIGATORS HANDBOOK

John Wiley & Sons The investigator’s practical guide for cybercrime evidence identification and collection Cyber attacks perpetrated against businesses, governments, organizations, and individuals have been occurring for decades. Many attacks are discovered only after the data has been exploited or sold on the criminal markets. Cyber attacks damage both the finances and reputations of businesses and cause damage to the ultimate victims of the crime. From the perspective of the criminal, the current state of inconsistent security policies and lax investigative procedures is a profitable and low-risk opportunity for cyber attacks. They can cause immense harm to individuals or businesses online and make large sums of money—safe in the knowledge that the victim will rarely report the matter to the police. For those tasked with probing such crimes in the field, information on investigative methodology is scarce. The Cybercrime Investigators Handbook is an innovative guide that approaches cybercrime investigation from the field-practitioner’s perspective. While there are high-quality manuals for conducting digital examinations on a device or network that has been hacked, the Cybercrime Investigators Handbook is the first guide on how to commence an investigation from *the location the offence occurred—the scene of the cybercrime—and collect the evidence necessary to locate and prosecute the offender. This valuable contribution to the field teaches readers to locate, lawfully seize, preserve, examine, interpret, and manage the technical evidence that is vital for effective cybercrime investigation. Fills the need for a field manual for front-line cybercrime investigators Provides practical guidance with clear, easy-to-understand language Approaches cybercrime form the perspective of the field practitioner Helps companies comply with new GDPR guidelines Offers expert advice from a law enforcement professional who specializes in cybercrime investigation and IT security Cybercrime Investigators Handbook is much-needed resource for law enforcement and cybercrime investigators, CFOs, IT auditors, fraud investigators, and other practitioners in related areas.*

RISK CENTRIC THREAT MODELING

PROCESS FOR ATTACK SIMULATION AND THREAT ANALYSIS

John Wiley & Sons This book introduces the Process for Attack Simulation & Threat Analysis (PASTA) threat modeling methodology. It provides an introduction to various types of application threat modeling and introduces a risk-centric methodology aimed at applying security countermeasures that are commensurate to the possible impact that could be sustained from defined threat models, vulnerabilities, weaknesses, and attack patterns. This book describes how to apply application threat modeling as an advanced preventive form of security. The authors discuss the methodologies, tools, and case studies of successful application threat modeling techniques. Chapter 1 provides an overview of threat modeling, while Chapter 2 describes the objectives and benefits of threat modeling. Chapter 3 focuses on existing threat modeling approaches, and Chapter 4 discusses integrating threat modeling within the different types of Software Development Lifecycles (SDLCs). Threat modeling and risk management is the focus of Chapter 5. Chapter 6 and Chapter 7 examine Process for Attack Simulation and Threat Analysis (PASTA). Finally, Chapter 8 shows how to use the PASTA risk-centric threat modeling process to analyze the risks of specific threat agents targeting web applications. This chapter focuses specifically on the web application assets that include customer's confidential data and business critical functionality that the web application provides. • Provides a detailed walkthrough of the PASTA methodology alongside software development activities, normally conducted via a standard SDLC process • Offers precise steps to take when combating threats to businesses • Examines real-life data breach incidents and lessons for risk management Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis is a resource for software developers, architects, technical risk managers, and seasoned security professionals.

EXPOSING FRAUD

SKILLS, PROCESS AND PRACTICALITIES

John Wiley & Sons Foreword by James D. Ratley, CFE, President and CEO, Association *of Certified Fraud Examiners Beyond the basics—tools for applied fraud management In Exposing Fraud: Skills, Process, and Practicalities, anti-fraud expert Ian Ross provides both ideas and practical guidelines for applying sound techniques for fraud investigation and detection and related project management. The investigative principles in this book are truly universal and can be applied anywhere in the world to deal with any of the range of fraud types prevalent in today's business environments. Topics covered include cyber fraud, the psychology of fraud, data analysis techniques, and the role of corporate and international culture in criminal behavior, among many others. Ensure an optimal outcome to fraud investigations by mastering real-world skills, from interviewing and handling evidence to conducting criminal proceedings. As technologies and fraud techniques become more complex, fraud investigation must increase in complexity as well. However, this does not mean that time-tested strategies for detecting criminals have become obsolete. Instead, it means that a hands-on approach to fraud detection and management is needed more than ever. The book does just that: Takes a unique practical approach to the business of detecting, understanding, and dealing with fraud of all types Aids in the development of key skills, including conducting investigations and managing fraud risk Covers issues related to ethically and efficiently handling impulsive and systemic fraud, plus investigating criminals who may be running multiple scams Addresses fraud from a global perspective, considering cultural and psychological factors that influence fraudsters Unlike other fraud investigation books on the market, Exposing Fraud develops the ethical and legal foundation required to apply theory and advice in real-world settings. From the simple to the complex, this book demonstrates the most effective application of anti-fraud techniques.*

ENCYCLOPEDIA OF CRIMINAL ACTIVITIES AND THE DEEP WEB

IGI Global As society continues to rely heavily on technological tools for facilitating business, e-commerce, banking, and communication, among other applications, there has been a significant rise in criminals seeking to exploit these tools for their nefarious gain. Countries all over the world are seeing substantial increases in identity theft and cyberattacks, as well as illicit transactions, including drug trafficking and human trafficking, being made through the dark web internet. Sex offenders and murderers explore unconventional methods of finding and contacting their victims through Facebook, Instagram, popular dating sites, etc., while pedophiles rely on these channels to obtain information and photographs of children, which are shared on hidden community sites. As criminals continue to harness technological advancements that are outpacing legal and ethical standards, law enforcement and government officials are faced with the challenge of devising new and alternative strategies to identify and apprehend criminals to preserve the safety of society. The Encyclopedia of Criminal Activities and the Deep Web is a three-volume set that includes comprehensive articles covering multidisciplinary research and expert insights provided by hundreds of leading researchers from 30 countries including the United States, the United Kingdom, Australia, New Zealand, Germany, Finland, South Korea, Malaysia, and more. This comprehensive encyclopedia provides the most diverse findings and new methodologies for monitoring and *regulating the use of online tools as well as hidden areas of the internet, including the deep and dark web. Highlighting a wide range of topics such as cyberbullying, online hate speech, and hacktivism, this book will offer strategies for the prediction and prevention of online criminal activity and examine methods for safeguarding internet users and their data from being tracked or stalked. Due to the techniques and extensive knowledge discussed in this publication it is an invaluable addition for academic and corporate libraries as well as a critical resource for policy makers, law enforcement officials, forensic scientists, criminologists, sociologists, victim advocates, cybersecurity analysts, lawmakers, government officials, industry professionals, academicians, researchers, and students within this field of study.*

COMBATTING CYBERCRIME AND CYBERTERRORISM

CHALLENGES, TRENDS AND PRIORITIES

Springer This book comprises an authoritative and accessible edited collection of chapters of substantial practical and operational value. For the very first time, it provides security practitioners with a trusted reference and resource designed to guide them through the complexities and operational challenges associated with the management of contemporary and emerging cybercrime and cyberterrorism (CC/CT) issues. Benefiting from the input of three major European Commission funded projects the book's content is enriched with case studies, explanations of strategic responses and contextual information providing the theoretical underpinning required for the clear interpretation and application of cyber law, policy and practice, this unique volume helps to consolidate the increasing role and responsibility of society as a whole, including law enforcement agencies (LEAs), the private sector and academia, to tackle CC/CT. This new contribution to CC/CT knowledge follows a multi-disciplinary philosophy supported by leading experts across academia, private industry and government agencies. This volume goes well beyond the guidance of LEAs, academia and private sector policy documents and doctrine manuals by considering CC/CT challenges in a wider practical and operational context. It juxtaposes practical experience and, where appropriate, policy guidance, with academic commentaries to reflect upon and illustrate the complexity of cyber ecosystem ensuring that all security practitioners are better informed and prepared to carry out their CC/CT responsibilities to protect the citizens they serve.

CYBERSECURITY

CURRENT WRITINGS ON THREATS AND PROTECTION

McFarland & Company Billions of people are connected through billions of devices across the globe. In the age of this massive internet, professional and personal information is being transmitted and received constantly, and while this access is convenient, it comes at a risk. This handbook of cybersecurity best practices is for public officials and citizens, employers and employees, corporations and consumers. Essays also address the development of state-of-the-art software systems and hardware for public and private organizations.

SCENE OF THE CYBERCRIME

*Elsevier When it comes to computer crimes, the criminals got a big head start. But the law enforcement and IT security communities are now working diligently to develop the knowledge, skills, and tools to successfully investigate and prosecute Cybercrime cases. When the first edition of "Scene of the Cybercrime" published in 2002, it was one of the first books that educated IT security professionals and law enforcement how to fight Cybercrime. Over the past 5 years a great deal has changed in how computer crimes are perpetrated and subsequently investigated. Also, the IT security and law enforcement communities have dramatically improved their ability to deal with Cybercrime, largely as a result of increased spending and training. According to the 2006 Computer Security Institute's and FBI's joint Cybercrime report: 52% of companies reported unauthorized use of computer systems in the prior 12 months. Each of these incidents is a Cybecrime requiring a certain level of investigation and remediation. And in many cases, an investigation is mandates by federal compliance regulations such as Sarbanes-Oxley, HIPAA, or the Payment Card Industry (PCI) Data Security Standard. Scene of the Cybercrime, Second Edition is a completely revised and updated book which covers all of the technological, legal, and regulatory changes, which have occurred since the first edition. The book is written for dual audience; IT security professionals and members of law enforcement. It gives the technical experts a little peek into the law enforcement world, a highly structured environment where the "letter of the law" is paramount and procedures must be followed closely lest an investigation be contaminated and all the evidence collected rendered useless. It also provides law enforcement officers with an idea of some of the technical aspects of how cyber crimes are committed, and how technology can be used to track down and build a case against the criminals who commit them. Scene of the Cybercrime, Second Editions provides a roadmap that those on both sides of the table can use to navigate the legal and technical landscape to understand, prevent, detect, and successfully prosecute the criminal behavior that is as much a threat to the online community as "traditional" crime is to the neighborhoods in which we live. Also included is an all new chapter on Worldwide Forensics Acts and Laws. * Companion Web site provides custom tools and scripts, which readers can download for conducting digital, forensic investigations. * Special chapters outline how Cybercrime investigations must be reported and investigated by corporate IT staff to meet federal mandates from Sarbanes Oxley, and the Payment Card Industry (PCI) Data Security Standard * Details forensic investigative techniques for the most common operating systems (Windows, Linux and UNIX) as well as cutting edge devices including iPods, Blackberries, and cell phones.*

CYBER PERSISTENCE THEORY

REDEFINING NATIONAL SECURITY IN CYBERSPACE

Oxford University Press A bold re-conceptualization of the fundamentals driving behavior and dynamics in cyberspace. Most cyber operations and campaigns fall short of activities that states would regard as armed conflict. In Cyber Persistence

Theory, Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett argue that a failure to understand this strategic competitive space has led many states to misapply the logic and strategies of coercion and conflict to this environment and, thus, suffer strategic loss as a result. The authors show how the paradigm of deterrence theory can neither explain nor manage the preponderance of state cyber activity. They present a new theory that illuminates the exploitive, rather than coercive, dynamics of cyber competition and an analytical framework that can serve as the basis for new strategies of persistence. Drawing on their policy experience, they offer a new set of prescriptions to guide policymakers toward a more stable, secure cyberspace.

SOFT COMPUTING FOR SECURITY APPLICATIONS

PROCEEDINGS OF ICSCS 2021

Springer Nature

ESSENTIALS OF ONLINE PAYMENT SECURITY AND FRAUD PREVENTION

John Wiley & Sons Essential guidance for preventing fraud in the card-not-present (CNP) space This book focuses on the prevention of fraud for the card-not-present transaction. The payment process, fraud schemes, and fraud techniques will all focus on these types of transactions ahead. Reveals the top 45 fraud prevention techniques Uniquely focuses on eCommerce fraud essentials Provides the basic concepts around CNP payments and the ways fraud is perpetrated If you do business online, you know fraud is a part of doing business. Essentials of On-line Payment Security and Fraud Prevention equips you to prevent fraud in the CNP space.

CYBERCRIME AND CLOUD FORENSICS: APPLICATIONS FOR INVESTIGATION PROCESSES

APPLICATIONS FOR INVESTIGATION PROCESSES

IGI Global While cloud computing continues to transform developments in information technology services, these advancements have contributed to a rise in cyber attacks; producing an urgent need to extend the applications of investigation processes. Cybercrime and Cloud Forensics: Applications for Investigation Processes presents a collection of research and case studies of applications for investigation processes in cloud computing environments. This reference source brings together the perspectives of cloud customers, security architects, and law enforcement agencies in the developing area of cloud forensics.

EXPLORING CAREERS IN CYBERSECURITY AND DIGITAL FORENSICS

Rowman & Littlefield Exploring Careers in Cybersecurity and Digital Forensics serves as a career guide, providing information about education, certifications, and tools to help those making career decisions within the cybersecurity field.

INTERIOR, ENVIRONMENT, AND RELATED AGENCIES APPROPRIATIONS FOR 2012

HEARINGS BEFORE A SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS, HOUSE OF REPRESENTATIVES, ONE HUNDRED TWELFTH CONGRESS, FIRST SESSION

REPORT ON SELECTED SOLUTIONS OF LAW, BUSINESS AND TECHNOLOGIES PREVENTING CRIMES

Wydawnictwo Instytutu Wymiaru Sprawiedliwości Raport jest pierwszym tego typu opracowaniem w polskim piśmiennictwie, szczególnie w tak oryginalnym i profesjonalnym ujęciu. [...] Integralną i niezwykle ważną dla percepcji raportu część stanowią załączniki, które poszerzają zakres wiedzy zawartej w opracowaniu, ułatwiając jej zrozumienie. [...] Raport zawiera autorskie ujęcie zjawiska relatywnie nowego w praktyce życia gospodarczego i proponuje zasady oraz metody zarządzania nim. Charakteryzuje się właściwym, interdyscyplinarnym podejściem. Napisano go na podstawie aktualnej – głównie angielskiej – literatury oraz z wykorzystaniem badań własnych autorów. Odpowiada na pilne i rosnące zapotrzebowanie praktyki gospodarczej. Jest innowacyjną pozycją na polskim rynku wydawniczym. Prof. dr hab. Bohdan Jeliński Uniwersytet Gdański Praca jest oryginalnym osiągnięciem naukowym, wypełniającym lukę w słabo zbadanym jak dotąd obszarze zapobiegania przestępczości w sektorach: finansowym, ubezpieczeniowym i energetycznym oraz w obszarze zarządzania zasobami ludzkimi. Proponowane rozwiązania przyczynią się do poprawy skuteczności działania w analizowanych sektorach. Płk dr hab. Tomasz Kośmider, prof. ASW Akademia Sztuki Wojennej w Warszawie Raport prezentuje innowacyjne rozwiązania w kwestii zarówno produktów zapobiegających przestępczości, jak i procesów zarządczych przedstawionych w szczególności w rozdziale dotyczącym zarządzania ludźmi. Opracowanie ukazuje również, z jakimi wyzwaniami natury prawnej może mierzyć się w przyszłości ustawodawca na szczeblu krajowym i ponadnarodowym, w tym unijnym. [...] Raport może przyczynić się także do podjęcia dalszych badań nad cyberprzestępczością w Polsce. Dr hab. Krystyna Nizioł, prof. US Uniwersytet Szczeciński

INTELLIGENCE ANALYSIS IN SOCIAL MEDIA

Emil Girdan The global security environment, dominated and dependent on information and communication technology, generates an accumulation of disruptive factors for society. This volume, in direct accordance with technological developments that have facilitated information avalanche and (anonymous) communication, has required interdisciplinary research in areas such as: psychology, sociology, computer science, social media communication and legislation. The research aims to establish whether social media platforms, through the actions they facilitate, can pose risks and threats to national security and to identify premises in order to stimulate strategies that should be followed to avoid transforming various forms of online communication into a potentiating and generating factor of crime, *radical or extremist opinions, mass manipulation, etc. At the same time, the research offers an alternative vision on approaching the concept of intelligence in the context of the development of social media networks (SocMInt) and promotes ways to improve and streamline how to achieve objectives that can be successfully applied, including in business intelligence. In this regard, a case study is conducted on the effects of CoVid-19 pandemic (SARS-CoV-2 coronavirus) from the perspective of law enforcement agencies. Although the individually exploitation of SocMInt does not provide a comprehensive answer, it must be used in the initial stages of decision-making and effort-making, due to the low costs compared to other Int disciplines. The volume does not present a solution to current problems, but through its didactic, documentary and informative nature it offers professional support at high standards to analysts and managers in decision making.*

CYBERCRIME IN PROGRESS

THEORY AND PREVENTION OF TECHNOLOGY-ENABLED OFFENSES

Routledge The emergence of the World Wide Web, smartphones, and computers has transformed the world and enabled individuals to engage in crimes in a multitude of new ways. Criminological scholarship on these issues has increased dramatically over the last decade, as have studies on ways to prevent and police these offenses. This book is one of the first texts to provide a comprehensive review of research regarding cybercrime, policing and enforcing these offenses, and the prevention of various offenses as global change and technology adoption increases the risk of victimization around the world. Drawing on a wide range of literature, Holt and Bossler offer an extensive synthesis of numerous contemporary topics such as theories used to account for cybercrime, policing in domestic and transnational contexts, cybercrime victimization and issues in cybercrime prevention. The findings provide a roadmap for future research in cybercrime, policing, and technology, and discuss key controversies in the existing research literature in a way that is otherwise absent from textbooks and general cybercrime readers. This book is an invaluable resource for academics, practitioners, and students interested in understanding the state of the art in social science research. It will be of particular interest to scholars and students interested in cybercrime, cyber-deviance, victimization, policing, criminological theory, and technology in general.

CYBERSECURITY AND SECURE INFORMATION SYSTEMS

CHALLENGES AND SOLUTIONS IN SMART ENVIRONMENTS

Springer This book provides a concise overview of the current state of the art in cybersecurity and shares novel and exciting ideas and techniques, along with specific cases demonstrating their practical application. It gathers contributions by both academic and industrial researchers, covering all aspects of cybersecurity and addressing issues in secure information systems as well as other emerging areas. The content comprises high-quality research articles and reviews that promote a multidisciplinary approach and reflect the latest advances, challenges, requirements and methodologies. Thus, the book investigates e.g. security vulnerabilities, *cybercrime, and privacy issues related to big data analysis, as well as advances in digital forensics, secure smart city services, and risk mitigation strategies for devices employing cyber-physical systems. Given its scope, the book offers a valuable resource for students, researchers, IT professionals and providers, citizens, consumers and policymakers involved or interested in the modern security procedures needed to protect our information and communication resources. Its goal is to foster a community committed to further research and education, and one that can also translate its findings into concrete practices.*

CYBER GUERILLA

Syngress Much as Che Guevara's book Guerilla Warfare helped define and delineate a new type of warfare in the wake of the Cuban revolution in 1961, Cyber Guerilla will help define the new types of threats and fighters now appearing in the digital landscape. Cyber Guerilla provides valuable insight for infosec professionals and consultants, as well as government, military, and corporate IT strategists who must defend against myriad threats from non-state actors. The authors take readers inside the operations and tactics of cyber guerillas, who are changing the dynamics of cyber warfare and information security through their unconventional strategies and threats. This book draws lessons from the authors' own experiences but also from illustrative hacker groups such as Anonymous, LulzSec and Rebellious Rose. Discusses the conceptual and ideological foundation of hackers and hacker groups Provides concrete footholds regarding hacker group strategy Discusses how cyber guerillas are changing the face of cyber warfare and cyber security through asymmetrical, flexible and stealthy means and methods Explains the tactics, techniques, and procedures these hacker groups use in their operations Describes how cyber guerrillas and hackers use the media and influence the public Serves as a must-have guide for anyone who wants to understand—or is responsible for defending against—cyber warfare attacks