How To Hack An Atm Machine Guide

PDF--to most of the world it stands for that rather tiresome format used for documents downloaded from the web. Slow to load and slower to print, hopelessly unsearchable, and all but impossible to cut and paste from, the Portable Document Format doesn't inspire much affection in the average user. But PDFs done right is another story. Those who know the ins and outs of this format know that it can be much more than electronic paper. Flexible, compact, interactive, and even searchable, PDF is the ideal way to present content across multiple platforms. PDF Hacks unveils the true promise of Portable Document Format, going way beyond the usual PDF as paged output mechanism. PDF expert Sid Steward draws from his years of analyzing, extending, authoring, and embellishing PDF documents to present 100 clever hacks--tools, tips, quick-and-dirty or not-so-obvious solutions to common problems. PDF Hacks will show you how to create PDF documents that are far more powerful than simple representations of paper pages. The hacks in the book cover the full range of PDF functionality, from the simple to the more complex, including generating, manipulating, annotating, and consuming PDF information. You'll learn how to manage content in PDF, navigate it, and reuse it as necessary. Far more than another guide to Adobe Acrobat, the book covers a variety of readily available tools for generating, deploying, and editing PDF. The little-known tips and tricks in this book are ideal for anyone who works with PDF on a regular basis, including web developers, pre-press users, forms creators, and those who generate PDF for distribution. Whether you want to fine-tune and debug your existing PDF documents or explore the full potential the format offers, PDF Hacks will turn you into a PDF power user.

As one of the applications in Microsoft Office, Word is the dominant word-processing program for both Windows and Mac users. Millions of people around the globe use it. But many, if not most, of them barely skim the surface of what is possible with Microsoft Word. Seduced by the application's supposed simplicity, they settle for just what's obvious--even if it doesn't satisfy their wants and needs. They may curse the wretched Bullets and Numbering buttons multiple times a day or take hours to change the font size of every heading in a lengthy report, yet they're reluctant to dig deeper to take advantage of Word's immense capabilities and limitless customization tools.Let Word Hacks be your shovel. Let it carve your way into Word and make this most popular and powerful application do precisely what you want it to do. Filled with insider tips, tools, tricks, and hacks, this book will turn you into the power user you always wanted to be. Far beyond a tutorial, Word Hacks assumes you have a solid working knowledge of the application and focuses on showing you exactly how to accomplish your pressing tasks, address your frequent annoyances, and solve even your most complex problems.Author Andrew Savikas examines Word's advanced (and often hidden) features and delivers clever, time-saving hacks on taming document bloat, customization, complex search and replace, Tables of Contents and indexes, importing and exporting files, tables and comments, and even using Google as a dictionary! With him as your guide, you'll soon be understanding--and hacking--Word in ways you never thought possible.Covering Word 2000, 2002 and Word 2003, Word Hacks exposes the inner workings of Word and releases your inner hacker; with it, you will be equipped to take advantage of the application s staggering array of advanced features that were once found only in page layout programs and graphics software and turning Word into your personal productivity powerhouse.

Originally published in hardcover in 2019 by Doubleday.

For more than 20 years, Network World has been the premier provider of information, intelligence and insight for network and IT executives responsible for the digital nervous systems of large organizations. Readers are responsible for designing, implementing and managing the voice, data and video systems their companies use to support everything from business critical applications to employee collaboration and electronic commerce.

Hacked Again details the ins and outs of cybersecurity expert and CEO of a top wireless security tech firm Scott Schober, as he struggles to understand: the motives and mayhem behind his being hacked. As a small business owner, family man and tech pundit, Scott finds himself leading a compromised life. By day, he runs a successful security company and reports on the latest cyber breaches in the hopes of offering solace and security tips to millions of viewers. But by night, Scott begins to realize his worst fears are only a hack away as he falls prey to an invisible enemy. When a mysterious hacker begins to steal thousands from his bank account, go through his trash and rake over his social media identity; Scott stands to lose everything he worked so hard for. But his precarious situation only fortifies Scott's position as a cybersecurity expert and also as a harbinger for the fragile security we all cherish in this digital life. Amidst the backdrop of major breaches such as Target and Sony, Scott shares tips and best practices for all consumers concerning email scams, password protection and social media overload: Most importantly, Scott shares his own story of being hacked repeatedly and bow he has come to realize that the only thing as important as his own cybersecurity is that of his readers and viewers. Part cautionary tale and part cyber self-help guide, Hacked Again probes deep into the dark web for truths and surfaces to offer best practices and share stories from an expert who has lived as both an enforcer and a victim in the world of cybersecurity. Book jacket.

This book is dedicated to advances in the field of user authentication. The book covers detailed description of the authentication process as well as types of authentication modalities along with their several features (authentication factors). It discusses the use of these modalities in a time-varying operating environment, including factors such as devices, media and surrounding conditions, like light, noise, etc. The book is divided into several parts that cover descriptions of several biometric and non-biometric authentication modalities, single factor and multi-factor authentication systems (mainly, adaptive), negative authentication system, etc. Adaptive strategy ensures the incorporation of the existing environmental conditions on the selection of authentication factors and provides significant diversity in the selection process. The contents of this book will prove useful to practitioners, researchers and students. The book is suited to be used a text in advanced/graduate courses on User Authentication Modalities. It can also be used as a textbook for professional development and certification coursework for practicing engineers and computer scientists.

Vegans. Skateboarders. Trekkies. The Cult of the Individual is alive and well and expressing itself all over America--and this book proves it. With this enlightening (and sometimes frightening) field guide, you'll delve into the customs, mores, and motivations behind every type of fan, geek, and superfreak, including: Swingers Hackers Dungeon Masters Happening Artists Cryptozoologists Utopians Bohemians Shriners Oenophiles Deadheads From music to food, sports to fashion, there are people who take their "hobbies" to an extreme the rest of us can only imagine. With this book, you'll get a bird's-eye view of these hobbies gone wild--from sea to shining sea!

Practical guide that can be used by executives to make well-informed decisions on cybersecurity issues to better protect their business Emphasizes, in a direct and uncomplicated way, how executives can identify, understand, assess, and mitigate risks associated with cybersecurity issues Covers 'What to Do When You Get Hacked?' including Business Continuity and Disaster Recovery planning, Public Relations, Legal and Regulatory issues, and Notifications and Disclosures Provides steps for integrating cybersecurity into Strategy; Policy and Guidelines; Change Management and Personnel Management Identifies cybersecurity best practices that executives can and should use both in the office and at home to protect their vital information

From a desolate cell located at a remote, state-of-the-art prison facility in Northern Ontario, inmate Brian Beasley plans his escape. Convicted of embezzlement when he masterfully infiltrated a banks computer system, Beasley and a would-be journalist assigned to write about his story secretly plan to break him free and make their way to Brazil a place with lax extradition laws where he can stay below the radar and just enjoy life. But once Brian and his accomplice Gracie Brown get to Brazil, all plans are off as a notorious gang lord compels them into his service to steal millions of dollars during the Games in Rio. In Heist during the Rio Games, follow the twists and turns as Brian Beasley and Gracie Brown try to navigate the drama, danger, and suspense of orchestrating one of the biggest heists in history, all set against the colorful, vibrant backdrop of Rio de Janeiro and the Summer Games. But as Beasleys skills are put to the test in the service of Brazils most infamous gangster, everything may not be as it seems especially when Brazils leading police investigator starts looking into his longtime archenemys plans. Whether friends or foes, accomplices or authorities, a mystery unfolds between a group of high-risk players that could reveal an exciting, lucrative next chapter in their lives or else land them behind bars.

Johnny Long's last book sold 12,000 units worldwide. Kevin Mitnick's last book sold 40,000 units in North America. As the cliché goes, information is power. In this age of technology, an increasing majority of the world's information is stored electronically. It makes sense then that we rely on high-tech electronic protection systems to guard that information. As professional hackers, Johnny Long and Kevin Mitnick get paid to uncover weaknesses in those systems and exploit them. Whether breaking into buildings or slipping past industrial-grade firewalls, their goal has always been the same: extract the information using any means necessary. After hundreds of jobs, they have discovered the secrets to bypassing every conceivable high-tech security system. This book reveals those secrets; as the title suggests, it has nothing to do with high technology. • Dumpster Diving Be a good sport and don’t read the two “D” words written in big bold letters above, and act surprised when I tell you hackers can accomplish this without relying on a single bit of technology (punny). • Tailgating Hackers and ninja both like wearing black, and they do share the ability to slip inside a building and blend with the shadows. • Shoulder Surfing If you like having a screen on your laptop so you can see what you’re working on, don’t read this chapter. • Physical Security Locks are serious business and lock technicians are true engineers, most backed with years of hands-on experience. But what happens when you take the age-old respected profession of the locksmith and sprinkle it with hacker ingenuity? • Social Engineering with Jack Wiles Jack has trained hundreds of federal agents, corporate attorneys, CEOs and internal auditors on computer crime and security-related topics. His unforgettable presentations are filled with three decades of personal "war stories" from the trenches of Information Security and Physical Security. • Google Hacking A hacker doesn’t even need his own computer to do the necessary research. If he can make it to a public library, Kinko's or Internet cafe, he can use Google to process all that data into something useful. • P2P Hacking Let’s assume a guy has no budget, no commercial hacking software, no support from organized crime and no fancy gear. With all those restrictions, is this guy still a threat to you? Have a look at this chapter and judge for yourself. • People Watching Skilled people watchers can learn a whole lot in just a few quick glances. In this chapter we’ll take a look at a few examples of the types of things that draws a no-tech hacker’s eye. • Kiosks What happens when a kiosk is more than a kiosk? What happens when the kiosk holds airline passenger information? What if the kiosk holds confidential patient information? What if the kiosk holds cash? • Vehicle Surveillance Most people don’t realize that some of the most thrilling vehicular espionage happens when the cars aren't moving at all!

Digital RobberyATM Hacking and ImplicationsSpringer Nature

WINNER OF THE FT & McKINSEY BUSINESS BOOK OF THE YEAR AWARD 2021 The instant New York Times bestseller 'A terrifying exposé' The Times 'Part John le Carré . . . Spellbinding' New Yorker 'Engaging and troubling . . . This secretive market is difficult to penetrate, but Perlroth has dug deeper than most' Economist Zero day: a software bug that allows a hacker to break in and scamper through the world's computer networks invisibly until discovered. One of the most coveted tools in a spy's arsenal, a zero day has the power to tap into any iPhone, dismantle safety controls at a chemical plant and shut down the power in an entire nation – just ask the Ukraine. Zero days are the blood diamonds of the security trade, pursued by nation states, defense contractors, cybercriminals, and security defenders alike. In this market, governments aren't regulators; they are clients – paying huge sums to hackers willing to turn over gaps in the Internet, and stay silent about them. This Is How They Tell Me the World Ends is cybersecurity reporter Nicole Perlroth's discovery, unpacked. A intrepid journalist unravels an opaque, code-driven market from the outside in – encountering spies, hackers, arms dealers, mercenaries and a few unsung heroes along the way. As the stakes get higher and higher in the rush to push the world's critical infrastructure online, This Is How They Tell Me the World Ends is the urgent and alarming discovery of one of the world's most extreme threats.

A complete library of the hottest, never-before-published underground hack variations In his highly provocative books, Hack Attacks Revealed (0-471-41624-X) and Hack Attacks Denied (0-471-41625-8), corporate hack master John Chirillo described the tools, techniques, and primary code that hackers use to exploit network security loopholes and then shows specific methods for blocking these attacks. However, now that so many of their standard techniques have been revealed, underground hackers and cyberpunks are again skirting the system, going beyond primary code, and resorting to using complex code variations of old techniques. That's where this book breaks new ground--by providing, for the first time, the most comprehensive compendium of all the complex variations of these techniques, both historical and current, that the hacking underground doesn't want you to see. It offers astounding details on just about every tool used by those who break into corporate networks--information that will go a long way toward helping you close any remaining security gaps. An ideal companion volume to the other Hack Attacks books, Hack Attacks Complete: o Covers hacks from the 1970s all the way to new millennium hacks o Details every permutation, variation, and category of hacking tools o Categorizes hacks for easy reference, with such categories as hacking, cracking, phreaking, spying, anarchy and underground spite, and hack/phreak technical library

It's no mystery why Larry Siegel remains THE best-selling author in Criminal Justice. Professor Siegel is known for presenting real-life stories of crime, criminals and the hottest debates in the field, and CRIMINOLOGY: THE CORE, 7th Edition, doesn't disappoint. This four-color paperback is concise and affordable. Real-world material clarifies concepts and theories, equipping students with a solid foundation in modern criminology. Grounded in Siegel's signature style--cutting-edge theory plus meticulous research--the book covers all sides of an issue without taking a political or theoretical position and provides a broad view of the field's interdisciplinary nature. This edition includes the latest insights into political crime; terrorism (e.g., ISIS); white-collar, blue-collar and green-collar crime; cybercrime; transnational crime (e.g. human trafficking) and many other topics. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

In the race to compete in today’s fast-moving markets, large enterprises are busy adopting new technologies for creating new products, processes, and business models. But one obstacle on the road to digital transformation is placing too much emphasis on technology, and not enough on the types of processes technology enables. What if different lines of business could build their own services and applications—and decision-making was distributed rather than centralized? This report explores the concept of a digital business platform as a way of empowering individual business sectors to act on data in real time. Much innovation in a digital enterprise will increasingly happen at the edge, whether it involves business users (from marketers to data scientists) or IoT devices. To facilitate the process, your core IT team can provide these sectors with the digital tools they need to innovate quickly. This report explores: Key cultural and organizational changes for developing business capabilities through cross-functional product teams A platform for integrating applications, data sources, business partners, clients, mobile apps, social networks, and IoT devices Creating internal API programs for building innovative edge services in low-code or no-code environments Tools including Integration Platform as a Service, Application Platform as a Service, and Integration Software as a Service The challenge of integrating microservices and serverless architectures Event-driven architectures for processing and reacting to events in real time You’ll also learn about a complete pervasive integration solution as a core component of a digital business platform to serve every audience in your organization.

Every day, businesses, investors, and consumers are grappling with the seismic changes technology has brought to the banking and finance industry. The Money Hackers is the dramatic story of fintech’s major players and explores how these disruptions are transforming even money itself. Whether you’ve heard of fintech or not, it’s already changing your life. Have you ever “Venmoed” someone? Do you think of investing in Bitcoin--even though you can’t quite explain what it is? If you’ve deposited a check using your iPhone, that’s fintech. And if you’ve gone to a bank branch and discovered it has been closed and shuttered for good, odds are that’s because of fintech too. The Money Hackers focuses on some of fintech’s most powerful disruptors--a ragtag collection of financial outsiders and savants--and uses their incredible stories to explain not just how the technology works, but how the Silicon Valley thinking behind the technology, ideas like friction, hedonic adaptation, democratization, and disintermediation, is having a drastic effect on the entire banking and finance industry. Turn to this remarkable new guide to: Feel empowered with the knowledge needed to spot the opportunities the next wave of fintech disruptions will bring. Understand the critical pain points that fintech is resolving, through a profile of the major finsurgents behind the disruption. Topic areas include Friction (featuring founders of Venmo), Aggregate and Automate (featuring Adam Dell, founder of Open Table and brother of Michael Dell), and Rise of the Machines (featuring Jon Stein, founder of robo-advisor Betterment). Learn about some of the larger-than-life characters behind the fintech movement. The Money Hackers tells the fascinating story of fintech--how it began, and where it is likely taking us.

Now that there’s software in everything, how can you make anything secure? Understand how to engineer dependable systems with this newly updated classic In Security Engineering: A Guide to Building Dependable Distributed Systems, Third Edition Cambridge University professor Ross Anderson updates his classic textbook and teaches readers how to design, implement, and test systems to withstand both error and attack. This book became a best-seller in 2001 and helped establish the discipline of security engineering. By the second edition in 2008, underground dark markets had let the bad guys specialize and scale up; attacks were increasingly on users rather than on technology. The book repeated its success by showing how security engineers can focus on usability. Now the third edition brings it up to date for 2020. As people now go online from phones more than laptops, most servers are in the cloud, online advertising drives the Internet and social networks have taken over much human interaction, many patterns of crime and abuse are the same, but the methods have evolved. Ross Anderson explores what security engineering means in 2020, including: How the basic elements of cryptography, protocols, and access control translate to the new world of phones, cloud services, social media and the Internet of Things Who the attackers are – from nation states and business competitors through criminal gangs to stalkers and playground bullies What they do – from phishing and carding through SIM swapping and software exploits to DDoS and fake news Security psychology, from privacy through ease-of-use to deception The economics of security and dependability – why companies build vulnerable systems and governments look the other way How dozens of industries went online – well or badly

THE CROWS ARE GATHERING. WAR IS COMING. For years, every intelligence agency in the world has been chasing the elusive terrorist known only as The Moroccan. But when James Hicks and his clandestine group known as the University thwart a bio-terror attack against New York City and capture The Moroccan, they find themselves in the crosshairs of their own intelligence community. The CIA, NSA, DIA and the Mossad are still hunting for for The Moroccan and will stop at nothing to get him. Hicks must find a way to keep the other agencies at bay while he tries to break The terrorist and uncover what else he is planning. When he ultimately surrenders information that leads to the most wanted terrorist in the world, Hicks and his team find themselves in a strange new world where allies become enemies, enemies become allies and the fate of the University - perhaps even the Western world - may hang in the balance. Can Hicks and the University survive an onslaught from A MURDER OF CROWS?

In 2016, economic globalization suffered a severe crisis after over half a century of smooth development, and deglobalization was running mountains high. Not only did it trigger domestic political discord in major countries like the United States, Britain, France and Germany, but also led to international economic and political disputes among Western countries, intensifying strategic competition between major powers. With the arrival of 2017, through the perilous waves of deglobalization and the consequent international political upheavals, we find that the post Cold War era that we were familiarized with, is coming to a rapid end, ushering in a new international political era, full of uncertainties. This annual book presents Chinese scholars' views, opinions and predictions on global political and security issues, as well as China's strategic choice. It covers a wide range of important issues concerning international security, ranging from the assessment of Sino-US relations, Russian-American relations, the counter terrorism situation in the Middle East, the political situation in Taiwan and cross-Strait relations, Brexit and the refugee problem, and the strategic situation in the South China Sea, to the judgment of the strategic posture in countries and regions like Japan, the Korean Peninsula, Southeast Asia, Latin America and Africa. Also covered are the analysis of the strategic posture in cyber space, outer space (as well as their governance), and discussion on China's international strategic choice in the wave of deglobalization. Contents: World Disputes and China's Strategic Options in the Context of the Globalization Crisis — A General Review of the International Strategic Situation and China's National Security in 2016 (Qi Dapeng)Sino-US Relations during the US Presidential Election Year (CAO Xianyu and XU Qiyu)An Assessment of the Strategic Trends of Russian–American Relations (YANG Lei)The Middle East Counter-Terrorism Situation and Its Impacts (LI Xiaolu)An Assessment of Japan's Strategic Trends (WU Huaizhong)A Review of the Strategic Situation on the Korean Peninsula (LU Yin)An Analysis of the Political Situation in Taiwan and the Posture in Cross-Strait Relations (WANG Shushen)An Evaluation of the Strategic Situation in Southeast Asia (ZHAO Yi)The Impact of Brexit and the Refugee Problem on the European Union (WANG Shuo)An Evaluation of the Strategic Situation in Latin America (WU Hongying, SUN Yanfeng, YANG Shouguo, CAO Ting and LI Meng)The Characteristics of Security Situation in Africa (XU Weizhong, YU Wensheng, WANG Lei and SUN Hong)An Assessment of the Strategic Situation in the South China Sea (DUAN Kejing)A Strategic Posture Review of International Cyberspace (WEN Baihua)Space Situational Assessment and Space Governance (CHEN Guoying)China's International Strategic Choice in the Wave of Deglobalization (Zheng Yongnian and Zhang Chi) Readership: Students and researchers interested in international relations of major powers, China's security and foreign policy. Keywords: International Relations;National Security;Policy Studies;ChinaReview:0

This is a book that will create enormous debate within the technical and the counter-terrorism communities. While there will be the inevitable criticism that the material contained in the book could be used maliciously, the fact is that this knowledge is already in the hands of our enemies. This book is truly designed to inform while entertaining (and scaring) the reader, and it will instantly be in demand by readers of "Stealing the Network: How to Own the Box" * A meticulously detailed and technically accurate work of fiction that exposes the very real possibilities of such an event occurring * An informative and scary insight into the boundries of hacking and cyber-terrorism * Written by a team of the most accomplished cyber-security specialists in the world

If you've bought or sold items through eBay, or through hundreds of other online sites, then you're familiar with PayPal, the online payment service. With PayPal, a valid email address, and a credit card or bank account, you can easily send and receive payments online. Not a bank or financial institution itself, PayPal describes its service as one that builds on the financial infrastructure of bank accounts and credit cards, and using advanced propriety fraud prevention systems, creates a safe, global, real-time payment solution. Put simply, PayPal provides the means for people to conduct financial transactions online, instantly and securely. But there's more to PayPal than meets the eye. PayPal Hacks shows you how to make the most of PayPal to get the most out of your online business or transactions. Authors Shannon Sofield of Payloadz.com and PayPal evangelist David Nielsen guide you through the rigors of using and developing with PayPal. Whether you're building an ecommerce site using PayPal as a transaction provider, or simply trying to pay for an eBay auction without getting burned, PayPal Hacks will give you the skinny on this leading global online payment service. The collection of tips and tricks in PayPal Hacks shows you how to find or even build the right tools for using PayPal to buy and sell on eBay or as a transaction provider for ecommerce on your own site. Written for all PayPal users, from those just starting out to those developing sophisticated ecommerce sites, this book begins with the basics such as setting up your account, then moves quickly into specific tips and tools for buyers, sellers, and developers. With PayPal Hacks, you can: Learn extra steps to help protect yourself while buying or selling on eBay Save time and money with advanced tips and undocumented features Learn dozens of easy-to-follow procedures to help you request and receive payments and fill orders Use PayPal to handle subscriptions, affiliate systems, and donations Create and customize your customers' checkout process Effortlessly integrate PayPal's shopping cart system into your own website Implement digital fulfillment with Instant Payment Notification (IPN) and Payment Data Transfer (PDT) Develop and distribute ecommerce applications with the PayPal API Each hack consists of a task to be accomplished or a creative solution to a problem, presented in a clear, logical, and task-oriented format. PayPal Hacks provides the tools and details necessary to make PayPal more profitable, more flexible, and more convenient.

Banking Made Easy E-book (PDF Format) is helpful to all those who want to learn everything relating to banking. Banking is the backbone of the finance industry. This book is for you if You are preparing for banking exams like SBI PO, IBPS PO, IBPS Officer. you want to win a banking competition. You are serious about your career in banking industry. You want to increase your basic knowledge of banking industry. If you are new in banking industry or want to update your knowledge. If you want to grow your banking skills and improve in this industry.

For more than 40 years, Computerworld has been the leading source of technology news and information for IT influencers worldwide. Computerworld's award-winning Web site (Computerworld.com), twice-monthly publication, focused conference series and custom research form the hub of the world's largest global IT media network.

A complete library of the hottest, never-before-published underground hack variations In his highly provocative books, Hack Attacks Revealed (0-471-41624-X) and Hack Attacks Denied (0-471-41625-8), corporate hack master John Chirillo described the tools, techniques, and primary code that hackers use to exploit network security loopholes and then shows specific methods for blocking these attacks. However, now that so many of their standard techniques have been revealed, underground hackers and cyberpunks are again skirting the system, going beyond primary code, and resorting to using complex code variations of old techniques. That's where this book breaks new ground--by providing, for the first time, the most comprehensive compendium of all the complex variations of these techniques, both historical and current, that the hacking underground doesn't want you to see. It offers astounding details on just about every tool used by those who break into corporate networks--information that will go a long way toward helping you close any remaining security gaps. An ideal companion volume to the other "Hack Attacks" books, Hack Attacks Complete: o Covers hacks from the 1970s all the way to new millennium hacks o Details every permutation, variation, and category of hacking tools o Categorizes hacks for easy reference, with such categories as hacking, cracking, phreaking, spying, anarchy and underground spite, and hack/phreak technical library

This book begins with a broader discussion of cybercrime and attacks targeting ATMs and then focuses on a specific type of cybercrime named "ATM Hacking." It discusses ATM Hacking from a more full scope of aspects, including technology, modus operandi, law enforcement, socio-economic and geopolitical context, and theory development. After unpacking a classic case of ATM Hacking and its modus operandi, implications for cybersecurity and prevention, intra- and inter-agency collaboration, and theory development are presented. This book also demonstrates the analysis of extensive qualitative data collected from a high-profile case in which European criminal group hacked into a London voice mail server belonging to a Taiwanese financial institution -- First Commercial Bank,. Then it programmed dozens of ATMs to "spit out" millions of dollars of cash. The successful crackdown on this type of crime is rare, if not unique, while the number of similar crimes has increased enormously in recent years and the trend seem to continue unabatingly. Further, the implications go beyond a country or a continent. Intra- and inter-agency collaboration among players of law enforcement is essential to the case especially in the police context of "turf jealousies." The authors seek to document the ways in which agencies collaborate, as well as the perceived benefits and challenges of cooperation. Whether the broader political and contextual climates in which these agencies operate, limit the extent to which they can cooperate. This book is useful as a reference for researchers and professionals working in the area of cybercrime and cybersecurity. University professors can also use this book as a case study for senior seminars or graduate courses.

This comprehensive and engaging textbook provides a fresh and sociologically-grounded examination of how deviance is constructed and defined and what it means to be classed a deviant. Covers an array of deviances, including sexual, physical, mental, and criminal, as well as deviances often overlooked in the literature, such as elite deviance, cyber-deviance, and deviant occupations Examines the popular notions and pseudoscientific explanations upon which the most pervasive myths surrounding deviance and deviants are founded Features an analytical through-line assessing the complex and multifaceted relationship between deviance and the media Enhanced with extensive pedagogical features, including a glossary of key terms, lists of specific learning outcomes in each chapter, and critical thinking questions designed to assess those outcomes Comprehensive instructor ancillaries include PowerPoint slides, a test bank for each chapter, instructor outlines, and sample activities and projects; a student study guide also is available

It's here! The 23rd annual edition in the popular Uncle John's Bathroom Reader series. The big brains at the Bathroom Readers' Institute have come up with 544 all-new pages full of incredible facts, hilarious articles, and a whole bunch of other ways to, er, pass the time. With topics ranging from history and science to pop culture, wordplay, and modern mythology, Heavy Duty is sure to amaze and entertain the loyal legions of throne sitters. Read about… * Sideshow secrets * The worst movie ever made * The hidden dangers of watching the Super Bowl * The father of the shopping mall * The physics of breakfast cereal * How to speak dog, and how to crack a safe * The unluckiest train ride of all time * The origins of casino games * Powering your car with pee * Keith Moon, bathroom bomber And much, much more!

HTML5 -- HTML injection & cross-site scripting (XSS) -- Cross-site request forgery (CSRF) -- SQL injection & data store manipulation -- Breaking authentication schemes -- Abusing design deficiencies -- Leveraging platform weaknesses -- Browser & privacy attacks.

It's scientifically proven: this book is full of seriously strange stuff! This amazing volume from the Bathroom Readers' Institute contains the strangest short science articles from dozens of Bathroom Readers—along with 50 all-new pages. From the oddest theories to the most astounding discoveries to the biggest blunders, Strange Science has all the facts your professors didn't teach you, but should have. It's packed with earth-shattering eurekas, outlandish inventions, silly "scientific" studies, and the stories behind the weirdos who made it all happen. Put on your lab coat and get ready to discover... The freakiest franken-foods scientists have created Bad movie science: when Hollywood gets it wrong One dentist's quest to clone John Lennon Unbelievable inventions, such as the Bird Trap and Cat Feeder...for people who really hate birds How scientists have solved some of history's most stupefying mysteries Schrodinger simplified: What's up with the cat in the box? Real-life time travelers (or so they claim) Everyday products made with radium...until people started dying How to hypnotize a chicken The seven-year-long study that found earthquakes are not caused by catfish waving their tails...and other breakthrough findings And much, much more!

If you've bought or sold items through eBay, or through hundreds of other online sites, then you're familiar with PayPal, the online payment service. With PayPal, a valid email address, and a credit card or bank account, you can easily send and receive payments online. Not a bank or financial institution itself, PayPal describes its service as one that builds on the financial infrastructure of bank accounts and credit cards, and using advanced propriety fraud prevention systems, creates a safe, global, real-time payment solution. Put simply, PayPal provides the means for people to conduct financial transactions online, instantly and securely.But there's more to PayPal than meets the eye. PayPal Hacks shows you how to make the most of PayPal to get the most out of your online business or transactions. Authors Shannon Sofield of Payloadz.com and PayPal evangelist David Nielsen guide you through the rigors of using and developing with PayPal. Whether you're building an ecommerce site using PayPal as a transaction provider, or simply trying to pay for an eBay auction without getting burned, PayPal Hacks will give you the skinny on this leading global online payment service.The collection of tips and tricks in PayPal Hacks shows you how to find or even build the right tools for using PayPal to buy and sell on eBay or as a transaction provider for ecommerce on your own site. Written for all PayPal users, from those just starting out to those developing sophisticated ecommerce sites, this book begins with the basics such as setting up your account, then moves quickly into specific tips and tools for buyers, sellers, and developers.With PayPal Hacks, you can: Learn extra steps to help protect yourself while buying or selling on eBay Save time and money with advanced tips and undocumented features Learn dozens of easy-to-follow procedures to help you request and receive payments and fill orders Use PayPal to handle subscriptions, affiliate systems, and donations Create and customize your customers' checkout process Effortlessly integrate PayPal's shopping cart system into your own website Implement digital fulfillment with Instant Payment Notification (IPN) and Payment Data Transfer (PDT) Develop and distribute ecommerce applications with the PayPal API Each hack consists of a task to be accomplished or a creative solution to a problem, presented in a clear, logical, and task-oriented format. PayPal Hacks provides the tools and details necessary to make PayPal more profitable, more flexible, and more convenient.

Protect your organization from scandalously easy-to-hack MFA security “solutions” Multi-Factor Authentication (MFA) is spreading like wildfire across digital environments. However, hundreds of millions of dollars have been stolen from MFA-protected online accounts. How? Most people who use multifactor authentication (MFA) have been told that it is far less hackable than other types of authentication, or even that it is unhackable. You might be shocked to learn that all MFA solutions are actually easy to hack. That’s right: there is no perfectly safe MFA solution. In fact, most can be hacked at least five different ways. Hacking Multifactor Authentication will show you how MFA works behind the scenes and how poorly linked multi-step authentication steps allows MFA to be hacked and compromised. This book covers over two dozen ways that various MFA solutions can be hacked, including the methods (and defenses) common to all MFA solutions. You’ll learn about the various types of MFA solutions, their strengthens and weaknesses, and how to pick the best, most defensible MFA solution for your (or your customers') needs. Finally, this book reveals a simple method for quickly evaluating your existing MFA solutions. If using or developing a secure MFA solution is important to you, you need this book. Learn how different types of multifactor authentication work behind the scenes See how easy it is to hack MFA security solutions—no matter how secure they seem Identify the strengths and weaknesses in your (or your customers’) existing MFA security and how to mitigate Author Roger Grimes is an internationally known security expert whose work on hacking MFA has generated significant buzz in the security world. Read this book to learn what decisions and preparations your organization needs to take to prevent losses from MFA hacking.

This edited volume presents the diversity of comparative criminology research in Asia, and the complex theoretical and methodological issues involved in conducting comparative research. With contributors both from the West and the East exploring these questions, the Editors have created a balanced resource, as well as set an agenda for future research. The increasing pace of globalization means that researchers should be armed with an understanding of how criminal justice systems work across the world. In the past, comparative research largely compared Western countries to each other, or involve d researchers from a Western perspective examining an Asian country, with models and theories developed in the West considered to have universal applications. This work aims to correct that gap, by providing a critical examination of comparative research, presenting quantitative and qualitative research data, and asking new questions that challenge prevailing research norms and provide an agenda for future research. This work will be of interest for researchers across the field of Criminology, particularly those with an interest in International and Comparative Research, research on or about Asia, and related disciplines such as Sociology, Demography, and Social Policy. “This fine collection that goes to the rich distinctiveness of Asian criminology. The editors have brought together a wonderful collection of authors mainly from the region. The distinctiveness of values and relational practices in Asia are recurrent themes that are well developed in this book and help us to make sense of patterns of crime and criminal justice in Asia.” John Braithwaite, Australian National University “What theoretical, methodological, and practical issues must we confront in conducting cross-cultural studies encompassing Western and Asian countries? Comparative Criminology in Asia discusses these issues and presents exemplary comparative research. The introductory chapter and the introduction to each part by the co-editors are lucid and highly educational. This collection must be required reading for every serious scholar and aspiring graduate student in Asian countries so that criminological and criminal justice studies will be brought to a much higher level o f sophistication.” Setsuo Miyazawa, UC Hastings “Can there be – and should there be -- a distinctive Asian criminology? What would this involve? The answer depends on what one thinks of the universalistic explanatory claims of Western criminology. Will these claims become self- fulfilling as these societies add to colonial influences a more deliberate borrowing of criminal justice models and established ways of pursuing discipline of criminology? Or will a more critical spirit prevail? This welcome edited collection by Liu, Travers and Chang provides an excellent starting point for reflecting on these and other questions. Rather than attempting to provide descriptions of the variety of similarities and differences in this region (though there are some fascinating case studies of these) the focus is even more on exploring the theoretical approa ches and methodologies used in comparing institutional and cultural differences by Asian criminologists and others.” David Nelken, King’s College, London “Criminologists can no longer ignore the impact of globalization on the pattern and amount of crime as we experienced recently, nor can we ignore the global change of criminal justice policies to deal with crime. There is, therefore, a desperate need to collect data on how crime and criminal justice are influenced by globalization across Asian countries. On the other hand, there are debates on the issue of culture-specific vs. pan-culture theories of crime. This collection addresses both issues in an interesting way. Its publication is timely and welcome.” Chuen-Jim Sheu, National Taipei University

Dissecting the Hack: The F0rb1dd3n Network, Revised Edition, deals with hackers and hacking. The book is divided into two parts. The first part, entitled “The F0rb1dd3n Network, tells the fictional story of Bob and Leon, two kids caught up in an adventure where they learn the real-world consequence of digital actions. The second part, “Security Threats Are Real (STAR), focuses on these real-world lessons. The F0rb1dd3n Network can be read as a stand-alone story or as an illustration of the issues described in STAR. Throughout The F0rb1dd3n Network are “Easter eggs —references, hints, phrases, and more that will lead readers to insights into hacker culture. Drawing on The F0rb1dd3n Network, STAR explains the various aspects of reconnaissance; the scanning phase of an attack; the attacker’s search for network weaknesses and vulnerabilities to exploit; the various angles of attack used by the characters in the story; basic methods of erasing information and obscuring an attacker’s presence on a computer system; and the underlying hacking culture. Revised edition includes a completely NEW STAR Section (Part 2) Utilizes actual hacking and security tools in its story- helps to familiarize a newbie with the many devices and their code Introduces basic hacking techniques in real life context for ease of learning

Cash and Dash: How ATMs and Computers Changed Banking uses the invention and development of the automated teller machine (ATM) to explain the birth and evolution of digital banking, from the 1960s to present day. It tackles head on the drivers of long-term innovation in retail banking with emphasis on the payment system. Using a novel approach to better understanding the industrial organization of financial markets, Cash and Dash contributes to a broader discussion around innovation and labour-saving devices. It explores attitudes to the patent system, formation of standards, organizational politics, the interaction between regulation and strategy, trust and domestication, maintenance versus disruption, and the huge undertakings needed to develop online real-time banking to customers.

Unlock The Keys To Manage, Budget And Save Money Money makes the world go ‘round. Or so they say. Money can be a gateway to a great and comfortable life: nice house, luxury cars, expensive education, etc. Money spent wisely can allow you to purchase these things while still living a contented life. However, in the same way that it can bring great joy and prosperity, it can also bring a great deal of stress. Without proper management, money becomes a curse instead of a boon, leading to stress, depression, and anxiety. In fact, the leading cause of fights in relationships is money and how it is managed. When not armed with the proper money management techniques, you can easily fall into money troubles. Unexpected expenses such as medical emergencies, veterinarian visits, and unforeseen mechanical or house repairs as well as overspending on frivolous items such as café coffee and fast food can quickly make your paycheck disappear. It can make looking at your bank account a painful and surprising experience. If this sounds familiar and you want to learn how to save up for big purchases, get yourself out of debt, and learn budgeting tools, then it's time to start handling money like the experts to having more of it. In “Money Management and Budgeting Hacks,” discover how to: - Track and categorize the different expenses - Create a budget of allowable areas for spending - Adjust spending habits to have more money left over - Set and prioritize financial goals to creating wealth - Create plans of action to keep yourself in good hands - Methods to control your budget and prevent overspending - Use credit wisely from ruining your financial future - See the difference between good debt and bad debt - Delay gratification for successful personal budgeting and investment - Track where your money goes and commit to following the money trail …and more for you to unlock! By taking the time to learn money saving tips and tricks, you can take control of your spending, create strong budgets, and get back on financial track for a less stressful and more enjoyable life.

Professional travel writer Brooke Wilkinson covers the when, where, and how to, discussing packing, safety, and travel etiquette, along with fundamental tips on hotels, car rentals, airlines, and more in Pocket Posh Tips for Travelers.

Achieve all of your financial goals with these 300 easy solutions to all your personal finance questions—from paying off your student loans to managing investments. Are you looking for ways to decrease your spending…and start increasing your savings? Need some simple advice for maximizing your investments? Want to start planning for your retirement but don’t know where to start? It’s now easier than ever to achieve all your financial goals! Many people are afraid to talk about money, which means that you might be missing some of the best money-saving skills out there! In Money Hacks you will learn the basics of your finances so you can start making every penny count. Whether you’re trying to pay down debt, start an emergency fund, or make the smartest choice on a major purchase, this book is chock-full of all the useful hacks to make your money work for you in every situation!

"This book presents in-depth insight through a case study approach into the current state of research in ICT as well as identified successful approaches, tools and methodologies in ICT research"--Provided by publisher.

This compact, highly engaging book examines the international legal regulation of both the conduct of States among themselves and conduct towards individuals, in relation to the use of cyberspace. Chapters introduce the perspectives of various stakeholders and the challenges for international law. The author discusses State responsibility and key cyberspace rights issues, and takes a detailed look at cyber warfare, espionage, crime and terrorism. The work also covers the situation of non-State actors and quasi-State actors (such as IS, or ISIS, or ISIL) and concludes with a consideration of future prospects for the international law of cyberspace. Readers may explore international rules in the areas of jurisdiction of States in cyberspace, responsibility of States for cyber activities, human rights in the cyber world, permissible responses to cyber attacks, and more. Other topics addressed include the rules of engagement in cyber warfare, suppression of cyber crimes, permissible limits of cyber espionage, and suppression of cyber-related terrorism. Chapters feature explanations of case law from various jurisdictions, against the background of real-life cyber-related incidents across the globe. Written by an internationally recognized practitioner in the field, the book objectively guides readers through on-going debates on cyber-related issues against the background of international law. This book is very accessibly written and is an enlightening read. It will appeal to a wide audience, from international lawyers to students of international law, military strategists, law enforcement officers, policy makers and the lay person.