Discovering Phishing Dropboxes Using Email Metadata

The written word is our primary tool for communication - with colleagues, administrators, stakeholders, and users. Poor use of words can lead to misunderstandings and inefficiencies. Writing effectively will help you be a stronger colleague, manager, and librarian. In this book, you will learn how to: Define your audience and your primary messages Simplify your writing so that it is succinct and understandable Structure your written content so that it is most usable and accessible to your audience Approach different forms of writing in a way that is most effective to getting your message across Establish a voice and tone that reflects the identity of your organization and yourself as a professional The book covers writing for both print and Web-based publications and is aimed at all types of libraries.

Not a week goes by when identity theft isn t mentioned in the media or that a Congressional outcry isn t heard about this unrelenting crime. The first authoritative book on identity theft, Identity Theft Handbook is written by a career professional who has spent over 25 years investigating and preventing identity theft in both the public and private sectors. Its rich real-world content includes interviews with government and private sector thought leaders. As well, the costs of identity theft, future trends, and prevention guidance is discussed. For investigators, auditors, and managers.

CYBER SECURITY AND DIGITAL FORENSICS Cyber security is an incredibly important issue that is constantly changing, with new methods, processes, and technologies coming online all the time. Books like this are invaluable to professionals working in this area, to stay abreast of all of these changes. Current cyber threats are getting more complicated and advanced with the rapid evolution of adversarial techniques. Networked computing and portable electronic devices have broadened the role of digital forensics beyond traditional investigations into computer crime. The overall increase in the use of computers as a way of storing and retrieving high-security information requires appropriate security measures to protect the entire computing and communication scenario worldwide. Further, with the introduction of the internet and its underlying technology, facets of information security are becoming a primary concern to protect networks and cyber infrastructures from various threats. This groundbreaking new volume, written and edited by a wide range of professionals in this area, covers broad technical and socio-economic perspectives for the utilization of information and communication technologies and the development of practical solutions in cyber security and digital forensics. Not just for the professional working in the field, but also for the student or academic on the university level, this is a must-have for any library. Audience: Practitioners, consultants, engineers, academics, and other professionals working in the areas of cyber analysis, cyber security, homeland security, national defense, the protection of national critical infrastructures, cyber-crime, cyber vulnerabilities, cyber-attacks related to network systems, cyber threat reduction planning, and those who provide leadership in cyber security management both in public and private sectors

Cyber Attack Survival Manual: From Identity Theft to The Digital Apocalypse

Proceedings of ICCSDF 2021

Learn the art of human hacking with an internationally renowned expert

Counterterrorism and Cybersecurity

Personal Cybersecurity

The Internet For Dummies

Total Information Awareness

"The Cyber Attack Survival Manual is the rare security awareness book that is both highly informative and interesting. And this is one of the finest security awareness books of the last few years." – Ben Rothke, Tapad Engineering Let two accomplished cyber security experts, Nick Selby and Heather Vescent, guide you through the dangers, traps and pitfalls of online life. Learn how cyber criminals operate and how you can defend yourself and your family from online security threats. From Facebook, to Twitter, to online banking we are all increasingly exposed online with thousands of criminals ready to bounce on the slightest weakness. This indispensable guide will teach you how to protect your identity and your most private financial and personal information.

This comprehensive, technical reference guide provides in-depth information on Apple technical architecture. It will teach the reader how to install and configure machines; architect and maintain networks; enable, customize, tune and troubleshoot a wide range of services; and integrate Mac OS X, Mac OS X Server, and other Apple technologies within a networked environment. The book covers myriad system administration topics from Directory Services integration to Tiger Server deployment, Xsan administration, accountmanagement best practices, security best practices, and more. Following the learning objectives of the Apple Certified System Administrator exam, this book is a perfect supplement to Apple's own training class and a in-depth technical reference for existing system administrators and engineers.

Add cybersecurity to your value proposition and protect your company from cyberattacks Cybersecurity is now a

requirement for every company in the world regardless of size or industry. Start-Up Secure: Baking Cybersecurity into Your Company from Founding to Exit covers everything a founder, entrepreneur and venture capitalist should know when building a secure company in today ’ s world. It takes you step-by-step through the cybersecurity moves you need to make at every stage, from landing your first round of funding through to a successful exit. The book describes how to include security and privacy from the start and build a cyber resilient company. You'll learn the basic cybersecurity concepts every founder needs to know, and you'll see how baking in security drives the value proposition for your startup ’ s target market. This book will also show you how to scale cybersecurity within your organization, even if you aren ’ t an expert! Cybersecurity as a whole can be overwhelming for startup founders. Start-Up Secure breaks down the essentials so you can determine what is right for your start-up and your customers. You ’ ll learn techniques, tools, and strategies that will ensure data security for yourself, your customers, your funders, and your employees. Pick and choose the suggestions that make the most sense for your situation—based on the solid information in this book. Get primed on the basic cybersecurity concepts every founder needs to know Learn how to use cybersecurity know-how to add to your value proposition Ensure that your company stays secure through all its phases, and scale cybersecurity wisely as your business grows Make a clean and successful exit with the peace of mind that comes with knowing your company's data is fully secure Start-Up Secure is the go-to source on cybersecurity for start-up entrepreneurs, leaders, and individual contributors who need to select the right frameworks and standards at every phase of the entrepreneurial journey.

A Guide to Current Legal Issues
Understanding Computers: Today and Tomorrow, Introductory
Prospects for a Better World
Health genetics and new media
Exam CAS-001
SSCP Systems Security Certified Practitioner All-in-One Exam Guide, Third Edition
Cloud Computing for Optimization: Foundations, Applications, and Challenges

Behind the deeply contentious 2020 election stands a real story of a broken election process. Election fraud that alters election outcomes and dilutes legitimate votes occurs all too often, as is the bungling of election bureaucrats. Our election process is full of vulnerabilities that can be — and are — taken advantage of, raising questions about, and damaging public confidence in, the legitimacy of the outcome of elections. This book explores the reality of the fraud and bureaucratic errors and mistakes that should concern all Americans and offers recommendations and solutions to fix those problems.

FROM THE AUTHOR OF THE #1 NATIONAL BESTSELLER JUSTICE ON TRIAL Stunned by the turbulence of the 2020 election, millions of Americans are asking the forbidden question: what really happened? It was a devastating triple punch. Capping their four-year campaign to destroy the Trump presidency, the media portrayed a Democratic victory as necessary and inevitable. Big Tech, wielding unprecedented powers, vaporized dissent and erased damning reports about the Biden family's corruption. And Democratic operatives, exploiting a public health crisis, shamelessly manipulated the voting process itself. Silenced and subjected, the American people lost their faith in the system. RIGGED is the definitive account of the 2020 election. Based on Mollie Hemingway's exclusive interviews with campaign officials, reporters, Supreme Court justices, and President Trump himself, it exposes the fraud and cynicism behind the Democrats' historic power-grab. Rewriting history is a specialty of the radical left, now in control of America's political and cultural heights. But they will have to contend with the determination, insight, and eloquence of Mollie Hemingway. RIGGED is a reminder for weary patriots that truth is still the most powerful weapon. The stakes for our democracy have never been higher.

This book discusses harnessing the real power of cloud computing in optimization problems, presenting state-of-the-art computing paradigms, advances in applications, and challenges concerning both the theories and applications of cloud computing in optimization with a focus on diverse fields like the Internet of Things, fog-assisted cloud computing, and big data. In real life, many problems – ranging from social science to engineering sciences – can be identified as complex optimization problems. Very often these are intractable, and as a result researchers from industry as well as the academic community are concentrating their efforts on developing methods of addressing them. Further, the cloud computing paradigm plays a vital role in many areas of interest, like resource allocation, scheduling, energy management, virtualization, and security, and these areas are intertwined with many optimization problems. Using illustrations and figures, this book offers students and researchers a clear overview of the concepts and practices of cloud computing and its use in numerous complex optimization problems.

PC World
Take Control of Dropbox
Rigged
Identity Theft Handbook
Taxpayer Beware
CASP: CompTIA Advanced Security Practitioner Study Guide Authorized Courseware
Executing Social Engineering Pen Tests, Assessments and Defense

In this lively, entertaining, and informative book, Dean K. Fueroghne guides readers through the complex laws governing the creation of advertising, illuminating a heavily regulated arena at the intersection of free enterprise and consumer protection. Is it acceptable to use images of real people, famous or not? Can Nike talk about Adidas in its promotional campaign? When can money be shown? What constitutes puffery, or deceptive truth, or bait-and-switch advertising? What are the specific rules pertaining to professional businesses, political advertising, or the marketing of alcohol or tobacco? What is the difference between copyright and trademark? Fueroghne answers these questions and more as he covers the complex laws relevant to advertising in all its guises. In addition to discussing specific cases, he explains the reasoning behind the court's decisions and how it affects the business of advertising. Students of strategic communication as well as advertising professionals—from agency account executives and copywriters to art directors and freelance designers—will learn to anticipate when proposed advertising may cause legal problems and how to avoid costly mistakes. Advertising lawyers will also appreciate the book as a handy reference that gathers in one place the many disparate laws affecting marketing and promotion in the United States today.

This fully updated study guide offers complete coverage of every topic on the latest version of the SSCP exam Take the 2018 edition of the challenging Systems Security Certified Practitioner (SSCP) exam with confidence using the detailed information contained in this highly effective self-study guide. The book provides 100% coverage of the revised SSCP Common Body of Knowledge (CBK) as developed by the International Information Systems Security Certification Consortium (ISC)2. Written by bestselling IT security certification author and trainer Darril Gibson, SSCP Systems Security Certified Practitioner All-in-One Exam Guide, Third Edition clearly explains all exam domains. You will get lists of topics covered at the beginning of each chapter, exam tips, practice exam questions, and in-depth answer explanations. Designed to help you pass the exam with ease, SSCP Systems Security Certified Practitioner All-in-One Exam Guide, Third Edition also serves as an essential on-the-job reference. •Features 100% coverage of every objective on the SSCP exam•Electronic content includes 250+ practice questions and a secured book PDF•Written by an industry-recognized expert and experienced trainer

This book features high-quality research papers presented at the International Conference on Applications and Techniques in Cyber Security and Digital Forensics (ICCSDF 2021), held at The NorthCap University, Gurugram, Haryana, India, during April 3–4, 2021. This book discusses the topics ranging from information security to cryptography, mobile application attacks to digital forensics, and from cyber security to blockchain. The goal of the book is to provide 360-degree view of cybersecurity to the readers which include cyber security issues, threats, vulnerabilities, novel idea, latest technique and technology, and mitigation of threats and attacks along with demonstration of practical applications. This book also highlights the latest development, challenges, methodologies as well as other emerging areas in this field. It brings current understanding of common Web vulnerabilities while maintaining awareness and knowledge of contemporary standards, practices, procedures, and methods of Open Web Application Security Project. It also expounds how to recover information after a cybercrime.

Big Data as a Lens on Human Culture
Social Engineering Penetration Testing
Rising Fawn
Uncharted
Our Broken Elections
CASP CompTIA Advanced Security Practitioner Study Guide
Detection, Prevention, and Security

Clare Connor enjoys personal and financial success by teaching people how to be their best selves--she's a professional life coach in a major Southern city. But her life starts to come undone when she experiences first one, then another major financial shock. Her husband has already been acting suspicious. Does he have a woman on the side? The financial fraud unravels the marriage, and he tells her to leave. Clare is thrown on her own devices and gets little help from a divorce lawyer. With the promise of work nearby, she flees to a remote area of the state to get her life together. The earthquakes that forced up the mountains where she now lives reflect the seismic shocks in her own life. Without the financial security she had, Clare struggles with who she is and how she's going to make a comeback. Fate throws her together with some unlikely allies, some of whom are tied to Irish and Italian immigrants in these strange lands. She taps into the power of the area's natural wonders, what is left of her long-forgotten faith, and the tatters of her family's past to face a future that is forever changed.

Reimagine the future of the internet All our devices and gadgets–from our refrigerators to our home security systems, vacuum cleaners, and stereos–are going online, just like our computers did. But once we ' ve successfully connected our devices to the internet, do we have any hope of keeping them, and ourselves, safe from the dangers that lurk beneath the digital waters? In If It ' s Smart, It ' s Vulnerable, veteran cybersecurity professional Mikko Hypponen delivers an eye-opening exploration of the best–and worst–things the internet has given us. From instant connectivity between any two points on the globe to organized ransomware gangs, the net truly has been a mixed blessing. In this book, the author explores the transformative potential of the future of the internet, as well as those things that threaten its continued existence: government surveillance, censorship, organized crime, and more. Readers will also find: Insightful discussions of how law enforcement and intelligence agencies operate on the internet Fulsome treatments of how money became data and the impact of the widespread use of mobile supercomputing technology Explorations of how the internet has changed the world, for better and for worse Engaging stories from Mikko's 30-year career in infosec Perfect for anyone seeking a thought-provoking presentation of some of the most pressing issues in cybersecurity and technology, If It ' s Smart, It ' s Vulnerable will also earn a place in the libraries of anyone interested in the future of the internet.

Learn to think like a hacker to secure your own systems and data Your smartphone, laptop, and desktop computer are more important to your life and business than ever before. On top of making your life easier and more productive, they hold sensitive information that should remain private. Luckily for all of us, anyone can learn powerful data privacy and security techniques to keep the bad guys on the outside where they belong. Hacking For Dummies takes you on an easy-to-follow cybersecurity voyage that will teach you the essentials of vulnerability and penetration testing so that you can find the holes in your network before the bad guys exploit them. You will learn to secure your Wi-Fi networks, lock down your latest Windows 11 installation, understand the security implications of remote work, and much more. You ' ll find out how to: Stay on top of the latest security weaknesses that could affect your business ' s security setup Use freely available testing tools to " penetration test " your network ' s security Use ongoing security checkups to continually ensure that your data is safe from hackers Perfect for small business owners, IT and security professionals, and employees who work remotely, Hacking For Dummies is a must-have resource for anyone who wants to keep their data safe.

Start-Up Secure

If It's Smart, It's Vulnerable

Email and the Everyday

Learn Social Engineering

How to Avoid and Recover from Cybercrime

Medicare

Mac OS X System Administration Reference

Understanding Computers: Today and Tomorrow gives your students a classic introduction to computer concepts with a modern twist! Known for its emphasis on industry insight and societal issues, this text makes concepts relevant to today's career-focused students and has increased emphasis on mobile computing and related issues such as mobile commerce and mobile security. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Get up and running on the Internet—the fast and easyway If you're an Internet newcomer and want to get up to speedwithout all the intimidating technical jargon, The Internet ForDummies has you covered. With over 5,000,000 copies sold,The Internet For Dummies is the #1 choice for Internetnewcomers. Inside, you'll discover how to make the most of the Internet,get accustomed to popular sites, find the information and items youneed fast, and stay away from the bad stuff floating aroundonline. Catches you up on the latest online trends, from socialnetworking sites to blogs and more Includes the latest on Google Chrome, getting good searchresults, and sharing files Covers choosing and connecting to an Internet provider,establishing an e-mail account, getting on the web, and finding thesites that matter most Now in its 14th edition, The Internet ForDummies covers the latest social networking tools, browserfeatures, connection options, safety features, and so much more.Starting out with the basics, it walks you through getting online,picking an Internet provider, getting to know the different webbrowsers, dealing with e-mail and connecting with friends, findingthe hottest sites to share photos and videos—and everythingin between. *Includes all formats and all editions*

Social engineering attacks target the weakest link in an organization's security human beings. Everyone knows these attacks are effective, and everyone knows they are on the rise. Now, Social Engineering Penetration Testing gives you the practical methodology and everything you need to plan and execute a social engineering penetration test and assessment. You will gain fascinating insights into how social engineering techniques including email phishing, telephone pretexting, and physical vectors can be used to elicit information or manipulate individuals into performing actions that may aid in an attack. Using the book's easy-to-understand models and examples, you will have a much better understanding of how best to defend against these attacks. The authors of Social Engineering Penetration Testing show you hands-on techniques they have used at RandomStorm to provide clients with valuable results that make a real difference to the security of their businesses. You will learn about the differences between social engineering pen tests lasting anywhere from a few days to several months. The book shows you how to use widely available open-source tools to conduct your pen tests, then walks you through the practical steps to improve defense measures in response to test results. Understand how to plan and execute an effective social engineering assessment Learn how to configure and use the open-source tools available for the social engineer Identify parts of an assessment that will most benefit time-critical engagements Learn how to design target scenarios, create plausible attack situations, and support various attack vectors with technology Create an assessment report, then improve defense measures in response to test results

Understanding Computers in a Changing Society

The Legal Expert Pages

How the Left Changed the Way You Vote

Writing Effectively in Print and on the Web

How the Media, Big Tech, and the Democrats Seized Our Elections

Financial Mail

“One of the most exciting developments from the world of ideas in decades, presented with panache by two frighteningly brilliant, endearingly unpretentious, and endlessly creative young scientists.” – Steven Pinker, author of The Better Angels of Our Nature Our society has gone from writing snippets of information by hand to generating a vast flood of 1s and 0s that record almost every aspect of our lives: who we know, what we do, where we go, what we buy, and who we love. This year, the world will generate 5 zettabytes of data. (That’s a five with twenty-one zeros after it.) Big data is revolutionizing the sciences, transforming the humanities, and renegotiating the boundary between industry and the ivory tower. What is emerging is a new way of understanding our world, our past, and possibly, our future. In Uncharted, Erez Aiden and Jean-Baptiste Michel tell the story of how they tapped into this sea of information to create a new kind of telescope: a tool that, instead of uncovering the motions of distant stars, charts trends in human history across the centuries. By teaming up with Google, they were able to analyze the text of millions of books. The result was a new field of research and a scientific tool, the Google Ngram Viewer, so groundbreaking that its public release made the front page of The New York Times, The Wall Street Journal, and The Boston Globe, and so addictive that Mother Jones called it “the greatest timewaster in the history of the internet.” Using this scope, Aiden and Michel—and millions of users worldwide—are beginning to see answers to a dizzying array of once intractable questions. How quickly does technology spread? Do we talk less about God today? When did people start “having sex” instead of “making love”? At what age do the most famous people become famous? How fast does grammar change? Which writers had their works most effectively censored by the Nazis? When did the spelling “donut” start replacing the venerable “doughnut”? Can we predict the future of human history? Who is better known—Bill Clinton or the rutabaga? All over the world, new scopes are popping up, using big data to quantify the human experience at the grandest scales possible. Yet dangers lurk in this ocean of 1s and 0s—threats to privacy and the specter of ubiquitous government surveillance. Aiden and Michel take readers on a voyage through these uncharted waters.

From 9/11 to Charlie Hebdo along with Sony-pocalypse and DARPA's $2 million Cyber Grand Challenge, this book examines counterterrorism and cyber security history, strategies and technologies from a thought-provoking approach that encompasses personal experiences, investigative journalism, historical and current events, ideas from thought leaders and the make-believe of Hollywood such as 24, Homeland and The Americans. President Barack Obama also said in his 2015 State of the Union address, "We are making sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism. In this new edition, there are seven completely new chapters, including three new contributed chapters by healthcare chief information security officer Ray Balut and Jean C. Stanford, DEF CON speaker Philip Polstra and security engineer and Black Hat speaker Darren Manners, as well as new commentaries by communications expert Andy Marken and DEF CON speaker Emily Peed. The book offers practical advice for businesses, governments and individuals to better secure the world and protect cyberspace.

Global Problems, Global Solutions: Prospects for a Better World by JoAnn Chirico approaches social problems from a global perspective with an emphasis on using one’s sociological imagination. Perfect for instructors who involve students in research, this text connects problems borne by individuals to regional, global, and historical forces, and stresses the importance of evidence in forming opinions and policies addressing social issues. The book introduces readers to the complexities of the major problems that confront us today such as violent conflict, poverty, climate change, human trafficking and other issues that we encounter in our lives. It book concludes with a chapter on politics and government, underscoring the need for good governance at all levels–and cooperation among many layers of government–to build a better world.

Hacking For Dummies

Apple Training Series

Cyber Security and Digital Forensics

Complete coverage of the new CompTIA Security+ (SY0-601) exam to help you pass on the first attempt, 2nd Edition

Stories of Disclosure, Trust, and Digital Labor

Exam CAS-002

CyberGenetics

An exploration of how email is experienced, understood, and materially structured as a practice spanning our everyday domestic and work lives. Despite its many obituaries, email is not dead. As a global mode of business and personal communication, email outstrips newer technologies of online interaction; it is deeply embedded in our everyday lives. And yet--perhaps because the ubiquity of email has obscured its study--this is the first scholarly book devoted to email as a key historical, social, and commercial site of digital communication in our everyday lives. In Email and the Everyday, Esther Milne examines how email is experienced, understood, and materially structured as a practice spanning the domestic and institutional spaces of daily life.

As internet use and global connectivity have skyrocketed, so too has identity theft. Even though hundreds of millions of people are affected every year by this crime, it remains unclear whose role it is to promote cybersecurity and investigate and prosecute identity theft in the United States. This book explains how identity theft, data breaches, and fraud occur, how to protect oneself against these threats, and what obstacles U.S. law enforcement faces as it seeks to fight back. Full-color photographs, a glossary, and sidebars help readers comprehend this complex issue, which is more pressing than ever for children and young adults.

In FY 2004, the Centers for Medicare & Medicaid Services (CMS) est. that Medicare improperly paid $900 million for durable med. equip., prosthetics, orthotics, & supplies -- in part due to fraud by suppliers. To deter such fraud, CMS contracts with the NCS to verify that suppliers meet 21 standards before they can bill Medicare. NSC verifies adherence to the standards through on-site inspections & document reviews. Recent prosecutions of fraudulent suppliers suggest that there may be weaknesses in NSC's efforts to screen suppliers or in the standards. This report evaluated: NSC's efforts to verify suppliers' compliance with the 21 standards; the adequacy of the standards to screen suppliers; & CMS's oversight of NSC's efforts. Charts & tables.

CompTIA Security+: SY0-601 Certification Guide

Voting Assistance Guide

A Practical Guide for Librarians

Law & Advertising

Challenges and Future Trends

More Effective Screening and Stronger Enrollment Standards Needed for Medical Equipment

BNA's Electronic Information Policy & Law Report

Law & AdvertisingA Guide to Current Legal IssuesRowman & Littlefield

Discover the most prevalent cyber threats against individual users of all kinds of computing devices. This book teaches you the defensive best practices and state-of-the-art tools available to you to repel each kind of threat. Personal Cybersecurity addresses the needs of individual users at work and at home. This book covers personal cybersecurity for all modes of personal computing whether on consumer-acquired or company-issued devices: desktop PCs, laptops, mobile devices, smart TVs, WiFi and Bluetooth peripherals, and IoT objects embedded with network-connected sensors. In all these modes, the frequency, intensity, and sophistication of cyberattacks that put individual users at risk are increasing in step with accelerating mutation rates of malware and cybercriminal delivery systems. Traditional anti-virus software and personal firewalls no longer suffice to guarantee personal security. Users who neglect to learn and adopt the new ways of protecting themselves in their work and private

environments put themselves, their associates, and their companies at risk of inconvenience, violation, reputational damage, data corruption, data theft, system degradation, system destruction, financial harm, and criminal disaster. This book shows what actions to take to limit the harm and recover from the damage. Instead of laying down a code of "thou shalt not" rules that admit of too many exceptions and contingencies to be of much practical use, cloud expert Marvin Waschke equips you with the battlefield intelligence, strategic understanding, survival training, and proven tools you need to intelligently assess the security threats in your environment and most effectively secure yourself from attacks. Through instructive examples and scenarios, the author shows you how to adapt and apply best practices to your own particular circumstances, how to automate and routinize your personal cybersecurity, how to recognize security breaches and act swiftly to seal them, and how to recover losses and restore functionality when attacks succeed. What You'll Learn Discover how computer security works and what it can protect us from See how a typical hacker attack works Evaluate computer security threats to the individual user and corporate systems Identify the critical vulnerabilities of a computer connected to the Internet Manage your computer to reduce vulnerabilities to yourself and your employer Discover how the adoption of newer forms of biometric authentication affects you Stop your router and other online devices from being co-opted into disruptive denial of service attacks Who This Book Is For Proficient and technically knowledgeable computer users who are anxious about cybercrime and want to understand the technology behind both attack and defense but do not want to go so far as to become security experts. Some of this audience will be purely home users, but many will be executives, technical managers, developers, and members of IT departments who need to adopt personal practices for their own safety and the protection of corporate systems. Many will want to impart good cybersecurity practices to their colleagues. IT departments tasked with indoctrinating their users with good safety practices may use the book as training material.

The CompTIA Security+: SY0-601 Certification Guide makes the most complex Security+ concepts easy to understand even for those who have no prior knowledge. Complete with exam tips, practical exercises, mock exams, and exam objective mappings, this is the perfect study guide to help you obtain Security+ certification.

Identity Theft: Private Battle or Public Crisis?

and Everything in Between | 2020 Paperback | Identify Theft | Bitcoin | Deep Web | Hackers | Online Security | Fake News

How Easy is it and what Can We Do to Stop it : Hearing Before the Subcommittee on Government Management, Information, and Technology of the Committee on Government Reform, House of Representatives, One Hundred Sixth Congress, Second Session, July 25, 2000

Global Problems, Global Solutions

Defrauding Medicare

Schemes, Scams, and Cons : Hearing Before the Committee on Finance, United States Senate, One Hundred Seventh Congress, First Session on IRS Oversight, April 5, 2001

Medicare more effective screening and stronger enrollment standards needed for medical equipment suppliers : report to the Chairman, Committee on Finance, U.S. Senate.

Understanding Computers in a Changing Society gives your students a classic introduction to computer concepts and societal issues, delivering content that is relevant to today's career-focused student. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Online genetic testing services are increasingly being offered to consumers who are becoming exposed to, and knowledgeable about, new kinds of genetic technologies, as the launch of a 23andme genetic testing product in the UK testifies. Genetic research breakthroughs, cheek swabbing forensic pathologists and celebrities discovering their ancestral roots are littered throughout the North American, European and Australasian media landscapes. Genetic testing is now capturing the attention, and imagination, of hundreds of thousands of people who can not only buy genetic tests online, but can also go online to find relatives, share their results with strangers, sign up for personal DNA-based musical scores, and take part in research. This book critically examines this market of direct-to-consumer (DTC) genetic testing from a social science perspective, asking, what happens when genetics goes online? With a focus on genetic testing for disease, the book is about the new social arrangements which emerge when a traditionally clinical practice (genetic testing) is taken into new spaces (the internet). It examines the intersections of new genetics and new media by drawing from three different fields: internet studies; the sociology of health; and science and technology studies. While there has been a surge of research activity concerning DTC genetic testing, particularly in sociology, ethics and law, this is the first scholarly monograph on the topic, and the first book which brings together the social study of genetics and the social study of digital technologies. This book thus not only offers a new overview of this field, but also offers a unique contribution by attending to the digital, and by drawing upon empirical examples from our own research of DTC genetic testing websites (using online methods) and in-depth interviews in the United Kingdom with people using healthcare services.

Improve information security by learning Social Engineering. Key Features Learn to implement information security using social engineering Get hands-on experience of using different tools such as Kali Linux, the Social Engineering toolkit and so on Practical approach towards learning social engineering, for IT security Book Description This book will provide you with a holistic understanding of social engineering. It will help you to avoid and combat social engineering attacks by giving you a detailed insight into how a social engineer operates. Learn Social Engineering starts by giving you a grounding in the different types of social engineering attacks,and the damages they cause. It then sets up the lab environment to use different toolS and then perform social engineering steps such as information gathering. The book covers topics from baiting, phishing, and spear phishing, to pretexting and scareware. By the end of the book, you will be in a position to protect yourself and your systems from social engineering threats and attacks. All in all, the book covers social engineering from A to Z , along with excerpts from many world wide known security experts. What you will learn Learn to implement information security using social engineering Learn social engineering for IT security Understand the role of social media in social engineering Get acquainted with Practical Human hacking skills Learn to think like a social engineer Learn to beat a social engineer Who this book is for This book targets security professionals,

security analysts, penetration testers, or any stakeholder working with information security who wants to learn how to use social engineering techniques. Prior knowledge of Kali Linux is an added advantage
Baking Cybersecurity into Your Company from Founding to Exit