I Love Hacking Il Meglio Della Rivista 2600 La Bibbia Degli Hacker

Debora Tonelli Introduzione Gerand Mannion Church in the World: Theology Goes Public Giovanni Pernigotto Teologia e spazio pubblico in Italia Stefanie Knauss La teologia nello spazio accademico pubblico tra rischi e opportunità Davide Zordan La pratica teologica e l'economia della rivoluzione cristiana Debora Tonelli La Bibbia tra testo e dottrina Sandra Mazzolini Chiesa e culture umane: una riflessione ecclesiologica Stella Morra Voci di corpi silenziosi: rileggere l'atto del credere Paolo Costa In cammino verso dove? Metamorfosi secolare della religiosità contemporanea Debora Spini La “religione” negli spazi pubblici delle democrazie avanzate Valentina Chizzola Mutamenti nei paradigmi antropologici: neuroscienze e responsabilità Note Recensioni

A cybersecurity expert and former Google privacy analyst's urgent call to protect devices and networks against malicious hackers? New technologies have provided both incredible convenience and new threats. The same kinds of digital networks that allow you to hail a ride using your smartphone let power grid operators control a country's electricity--and these personal, corporate, and government systems are all vulnerable. In Ukraine, unknown hackers shut off electricity to nearly 230,000 people for six hours. North Korean hackers destroyed networks at Sony Pictures in retaliation for a film that mocked Kim Jong-un. And Russian cyberattackers leaked Democratic National Committee emails in an attempt to sway a U.S. presidential election. And yet despite such documented risks, government agencies, whose investigations and surveillance are stymied by encryption, push for a weakening of protections. In this accessible and riveting read, Susan Landau makes a compelling case for the need to secure our data, explaining how we must maintain cybersecurity in an insecure age.

Presents step-by-step instructions for repurposing a variety of electronic appliances and equipment, including computers, cell phones, and scanners, into other items.

Gives a critique of Michelangelo's works as well as highlights from his life

“One of the finest books on information security published so far in this century—easily accessible, tightly argued, superbly well-sourced, intimidatingly perceptive.” —Thomas Rid, author of Active Measures “The best examination I have read of how increasingly dramatic developments in cyberspace are defining the ‘new normal’ of geopolitics in the digital age. Buchanan...captures the dynamics of all of this truly brilliantly.” —General David Petraeus, former Director of the CIA and Commander of Coalition Forces in Iraq and Afghanistan Few national-security threats are as potent—or as nebulous—as cyber attacks. Ben Buchanan reveals how hackers are transforming spycraft and statecraft, catching us all in the crossfire, whether we know it or not. Ever since WarGames, we have been bracing for the cyberwar to come, conjuring images of exploding power plants and mass panic. But while cyber attacks are now disturbingly common, they don’t look anything like we thought they would. Packed with insider information based on interviews, declassified files, and forensic analysis of company reports, The Hacker and the State sets aside fantasies of cyber-annihilation to explore the real geopolitical competition of the digital age. Tracing the conflict of wills and interests among modern nations, Ben Buchanan reveals little-known details of how China, Russia, North Korea, Britain, and the United States hack one another in a relentless struggle for dominance. His analysis moves deftly from underseas cable taps to underground nuclear sabotage, from blackouts and data breaches to billion-dollar heists and election interference. Buchanan brings to life this continuous cycle of espionage and deception, attack and counterattack, destabilization and retaliation. He explains why cyber attacks are far less destructive than we anticipated, far more pervasive, and much harder to prevent. With little fanfare and far less scrutiny, they impact our banks, our tech and health systems, our democracy, and every aspect of our lives. Quietly, insidiously, they have reshaped our national-security priorities and transformed spycraft and statecraft. The contest for geopolitical advantage has moved into cyberspace. The United States and its allies can no longer dominate the way they once did. The nation that hacks best will triumph.

Kevin David Mitnick was cyberspace's most wanted hacker. Mitnick could launch missiles or cripple the world's financial markets with a single phone call - or so went the myth. The FBI, phone companies, bounty hunters, even fellow hackers pursued him over the Internet and through cellular airways. But while Mitnick's alleged crimes have been widely publicized, his story has never been told. Now Jonathan Littman takes us into the mind of a serial hacker. Drawing on over fifty hours of telephone conversations with Mitnick on the run, Littman reveals Mitnick's double life; his narrow escapes; his new identities, complete with college degrees of his choosing; his hacking techniques and mastery of "social engineering"; his obsession with revenge.

Chronicles the life of the computer programmer, known for the launch of the operating system GNU Project, from his childhood as a gifted student to his crusade for free software.

Politica, cultura, economia.

It's true that some people spend years studying Italian before they finally get around to speaking the language. But here's a better idea. Skip the years of study and jump right to the speaking part. Sound crazy? No, it's language hacking. Unlike most traditional language courses that try to teach you the rules of Italian, #LanguageHacking shows you how to learn and speak Italian through proven memory techniques, unconventional shortcuts and conversation strategies perfected by one of the world's greatest language learners, Benny Lewis, aka the Irish Polyglot. Using the language hacks -shortcuts that make learning simple - that Benny mastered while learning his 11 languages and his 'speak from the start' method, you will crack the language code and exponentially increase your language abilities so that you can get fluent faster. It's not magic. It's not a language gene. It's not something only "other people" can do. It's about being smart with how you learn, learning what's indispensable, skipping what's not, and using what you've learned to have real conversations in Italian from day one. The Method #LanguageHacking takes a modern approach to language learning, blending the power of online social collaboration with traditional methods. It focuses on the conversations that learners need to master right away, rather than presenting language in order of difficulty like most courses. This means that you can have conversations immediately, not after years of study. Each of the 10 units culminates with a speaking 'mission' that prepares you to use the language you've learned to talk about yourself. Through the language hacker online learner community, you can share your personalized speaking 'missions' with other learners - getting and giving feedback and extending your learning beyond the pages of the book . You don't need to go abroad to learn a language any more.

What if your greatest secrets became public? For the students at Alexandria Prep, a series of hacks leads to a scandalous firestorm—and the students are left wondering whose private photos and messages will be exposed next. It’s Pretty Little Liars meets WikiLeaks. ONE HACK. EVERY SECRET. EXPOSED. Alexandria Prep is in total social chaos. Someone—no one knows who—has hacked into the phones of the school’s social royalty and leaked their personal messages and photos. At first it was funny—everyone loved watching the dirty private lives of those they envied become public. But when things escalate,

the students realize anyone could be a target. When Anna returns to school for senior spring, she's initially grateful that all eyes are on everyone else's problems...and not on her humiliating breakup with her basketball-star boyfriend. But as the hacks begin to shatter lives and threaten futures, Anna races to protect those she loves—as well as her own devastating secrets. If only the students of Alexandria Prep could turn back the clock so they knew then what they know now: sometimes we share too much. ? "This debut novel is timely, cautionary, and compelling." —VOYA, starred review "In an age of adult anxieties over digital privacy, this book is #relevant." —Kirkus Reviews

“Amy Webb found her true love after a search that's both charmingly romantic and relentlessly data-driven. Anyone who uses online dating sites must read her funny, fascinating book.”—Gretchen Rubin, #1 New York Times bestselling author of The Happiness Project After yet another disastrous date, Amy Webb was preparing to cancel her JDate membership when epiphany struck: her standards weren't too high, she just wasn't approaching the process the right way. Using her gift for data strategy, she found which keywords were digital-man magnets, analyzed photos, and then adjusted her (female) profile to make the most of that intel. Then began the deluge—dozens of men who actually met her own stringent requirements wanted to meet her. Among them: her future husband, now the father of her child.

As editor of the Guardian, one of the world's foremost newspapers, Alan Rusbridger abides by the relentless twenty-four-hour news cycle. But increasingly in midlife, he feels the gravitational pull of music—especially the piano. He sets himself a formidable challenge: to fluently learn Chopin's magnificent Ballade No. 1 in G minor, arguably one of the most difficult Romantic compositions in the repertory. With pyrotechnic passages that require feats of memory, dexterity, and power, the piece is one that causes alarm even in battle-hardened concert pianists. He gives himself a year. Under ideal circumstances, this would have been a daunting task. But the particular year Rusbridger chooses turns out to be one of frenetic intensity. As he writes in his introduction, "Perhaps if I'd known then what else would soon be happening in my day job, I might have had second thoughts. For it would transpire that, at the same time, I would be steering the Guardian through one of the most dramatic years in its history." It was a year that began with WikiLeaks' massive dump of state secrets and ended with the Guardian's revelations about widespread phone hacking at News of the World. "In between, there were the Japanese tsunami, the Arab Spring, the English riots . . . and the death of Osama Bin Laden," writes Rusbridger. The test would be to "nibble out" twenty minutes per day to do something totally unrelated to the above. Rusbridger's description of mastering the Ballade is hugely engaging, yet his subject is clearly larger than any one piece of classical music. Play It Again deals with focus, discipline, and desire but is, above all, about the sanctity of one's inner life in a world dominated by deadlines and distractions. What will you do with your twenty minutes?

The definitive guide to hacking the world of the Internet of Things (IoT) -- Internet connected devices such as medical devices, home assistants, smart home appliances and more. Drawing from the real-life exploits of five highly regarded IoT security researchers, Practical IoT Hacking teaches you how to test IoT systems, devices, and protocols to mitigate risk. The book begins by walking you through common threats and a threat modeling framework. You'll develop a security testing methodology, discover the art of passive reconnaissance, and assess security on all layers of an IoT system. Next, you'll perform VLAN hopping, crack MQTT authentication, abuse UPnP, develop an mDNS poisoner, and craft WS-Discovery attacks. You'll tackle both hardware hacking and radio hacking, with in-depth coverage of attacks against embedded IoT devices and RFID systems. You'll also learn how to: • Write a DICOM service scanner as an NSE module • Hack a microcontroller through the UART and SWD interfaces • Reverse engineer firmware and analyze mobile companion apps • Develop an NFC fuzzer using Proxmark3 • Hack a smart home by jamming wireless alarms, playing back IP camera feeds, and controlling a smart treadmill The tools and devices you'll use are affordable and readily available, so you can easily practice what you learn. Whether you're a security researcher, IT team member, or hacking hobbyist, you'll find Practical IoT Hacking indispensable in your efforts to hack all the things REQUIREMENTS: Basic knowledge of Linux command line, TCP/IP, and programming

Benny Lewis, who speaks over ten languages—all self-taught—runs the largest language-learning blog in the world, Fluent In 3 Months. Lewis is a full-time "language hacker," someone who devotes all of his time to finding better, faster, and more efficient ways to learn languages. Fluent in 3 Months: How Anyone at Any Age Can Learn to Speak Any Language from Anywhere in the World is a new blueprint for fast language learning. Lewis argues that you don't need a great memory or "the language gene" to learn a language quickly, and debunks a number of long-held beliefs, such as adults not being as good of language learners as children.

Winner of the Compton Crook Award: This tale of genetically modified killers of the future is “a genuine page-turner . . . Don't miss it” (Locus). Two hundred years after a nuclear apocalypse forced humanity to flee earth, humans still remember the most feared warriors of that planet—the Paratwa, genetically modified killers who occupy two bodies controlled by one vicious mind. The legendary Paratwa named Reemul, known as the Liege-Killer, was the strongest of them all. Now someone has revived Reemul from stasis and sent him to terrorize the peaceful orbital colonies of Earth. Is this an isolated incident, or has the one who unleashed this terrible power announced a gambit for control over the entire human race?

Un modo inedito di fare marketing scientifico, misurabile e scalabile “Growth” significa “crescita”. “Hacking” significa “trovare soluzioni non convenzionali a dei problemi”. Il Growth Hacking è infatti un nuovo modo di fare marketing: un metodo scientifico che si basa interamente sui dati e abbatte le pareti tra il design, la programmazione e la comunicazione. Tutte queste competenze vengono riunite nella figura del growth hacker, che ha come unico obiettivo quello di far crescere i numeri che contano per l'azienda, in ogni modo possibile. Per la prima volta in Italia, questo libro offre una visione d'insieme su tutte le tecniche utilizzate dagli imprenditori della Silicon Valley per lanciare un prodotto innovativo, partendo da zero e arrivando a milioni di utenti. Dal metodo “Lean” alla progettazione di esperimenti di marketing, questo volume traccia un percorso di crescita utile sia a professionisti e studenti, che vogliono abbracciare questa nuova corrente di pensiero, sia ad imprenditori che vogliono investire nelle loro idee, ma non sanno da dove partire o come sbloccare una crescita stagnante. Non si tratta di un trucco, ma di replicare nella tua azienda gli stessi processi che hanno trasformato startup come Airbnb, Dropbox, Facebook e molte altre nei colossi che sono oggi. Questo è il Growth Hacking.

JUMPSTART YOUR NEW AND EXCITING CAREER AS A PENETRATION TESTER The Pentester BluePrint: Your Guide to Being a Pentester offers readers a chance to delve deeply into the world of the ethical, or "white-hat" hacker. Accomplished pentester and author Phillip L. Wylie and cybersecurity researcher Kim Crawley walk you through the basic and advanced topics necessary to understand how to make a career out of finding vulnerabilities in systems, networks, and applications. You'll learn about the role of a penetration tester, what a pentest involves, and the prerequisite knowledge you'll need to start the educational journey of becoming a pentester. Discover how to develop a plan by assessing your current skillset and finding a starting place to begin growing your knowledge and skills. Finally, find out how to become employed as a pentester by using social media, networking strategies, and community involvement. Perfect for IT workers and entry-level information security professionals, The Pentester BluePrint also belongs on the bookshelves of anyone seeking to transition to the exciting and in-demand field of penetration testing. Written in a highly approachable and accessible style, The Pentester BluePrint avoids unnecessarily technical lingo in favor of concrete advice and practical strategies to help you get your start in pentesting. This book will teach you: The foundations of pentesting, including basic IT skills like operating systems, networking, and security systems The development of hacking skills and a hacker mindset Where to find educational options, including college and university classes, security training providers, volunteer work, and self-study

Which certifications and degrees are most useful for gaining employment as a pentester How to get experience in the pentesting field, including labs, CTFs, and bug bounties
While many resources for network and IT security are available, detailed knowledge regarding modern web application security has been lacking—until now. This practical guide provides both offensive and defensive security concepts that software engineers can easily learn and apply. Andrew Hoffman, a senior security engineer at Salesforce, introduces three pillars of web application security: recon, offense, and defense. You'll learn methods for effectively researching and analyzing modern web applications—including those you don't have direct access to. You'll also learn how to break into web applications using the latest hacking techniques. Finally, you'll learn how to develop mitigations for use in your own web applications to protect against hackers. Explore common vulnerabilities plaguing today's web applications Learn essential hacking techniques attackers use to exploit applications Map and document web applications for which you don't have direct access Develop and deploy customized exploits that can bypass common defenses Develop and deploy mitigations to protect your applications against hackers Integrate secure coding best practices into your development lifecycle Get practical tips to help you improve the overall security of your web applications
The Complete Official Guide to Cyberpunk 2077 is a massive book covering everything in the game. With details on every last challenge and feature, the guide offers streamlined progression through the entire adventure, as well as a commanding expertise on all key systems. 100% authoritative: all branching paths, all side quests, all rewards, and all endings fully mapped out; also includes optional challenges, mini-games, unlockables, secrets, and more. Foolproof explanations: every mission, every game mechanic, every meaningful choice covered with accessible solutions. Hi-res maps of Night City: each annotated with locations of collectibles and points of interest. Reference & Analysis Chapter: in-depth coverage of all major game systems, including character progression, abilities, perks, Street Cred, Trophies/Achievements, among others. At-a-glance Walkthroughs: annotated screenshots and sequential steps show optimal ways through every mission. Expert Combat Strategies: practical, reproducible tactics to crush all enemies and bosses. Comprehensive references: all-inclusive appraisals of all items and weapons – including statistics and unlock conditions. Spoiler-sensitive: carefully designed to avoid spoilers, ensuring you can read without ever ruining your appreciation of the story. Instant searches: print navigation systems and an extensive index give you immediate access to the information you need. Concept art: direct from the development team and beautifully laid out
The ultimate compendium of growth hacks for the modern digital marketer, written by marketing veterans Jeff Goldenberg (Head of Growth at Borrowell and TechStars Mentor) and Mark Hayes (CEO of Rocketshp, and founder of one of the world's first growth hacking agencies). Are you ready to skyrocket your companies growth? Learn, the most effective tools, software and technology for digital and startup marketers; 100 must-know growth hacks to take your business to the next level (focusing on 3 key areas: product-market fit, transition to growth and scale); Insider info from leading startups whocasing the best growth hacks and exactly how they did it.
L'ebook che non si limita a mostrare come funzionano le tecniche di exploit, ma spiega come svilupparle, ritorna in due ebook.Jon Erickson guida il lettore in un percorso di iniziazione alle tecniche hacker. Ancora una volta il presupposto è che conoscere i metodi, le logiche, la teoria e i fondamenti scientifici che stanno alla base dell'hacking stesso, rappresenta l'unica via per costruire sistemi sicuri.Se la prima edizione di questo libro, pubblicata sul finire del 2003 e tradotta in undici lingue, aveva ottenuto vasti consensi confermati da ampie vendite, la seconda, ora disponibile in formato EPUB, porta la conoscenza delle tecniche dell'hacking a un nuovo livello.Volume 1: argomenti in breve- Introduzione all'hacking- Programmazione in C e Assembly- Tecniche di exploit- Vulnerabilità buffer overflow- Exploit da stringa di formato- Introduzione alle reti: modello OSI e socket- Sniffing di rete
In an era of accelerating technology and increasing complexity, how should we reimagine the emancipatory potential of feminism? How should gender politics be reconfigured in a world being transformed by automation, globalization and the digital revolution? These questions are addressed in this bold new book by Helen Hester, a founding member of the 'Laboria Cuboniks' collective that developed the acclaimed manifesto 'Xenofeminism: A Politics for Alienation'. Hester develops a three-part definition of xenofeminism grounded in the ideas of technomaterialism, anti-naturalism, and gender abolitionism. She elaborates these ideas in relation to assistive reproductive technologies and interrogates the relationship between reproduction and futurity, while steering clear of a problematic anti-natalism. Finally, she examines what xenofeminist technologies might look like in practice, using the history of one specific device to argue for a future-oriented gender politics that can facilitate alternative models of reproduction. Challenging and iconoclastic, this visionary book is the essential guide to one of the most exciting intellectual trends in contemporary feminism.
SPLITS HACKING IS THE KEY The biggest problem that most athletes and practitioners have isn't the determination and dedication to learn the splits; it's understanding how to do it following the right path. Have you ever wanted to learn the splits, started with your training program but didn't get there? Or maybe you just want to close that little gap between you and the floor in a split that has been giving you troubles for so many years...I know, splits are just awesome. Everyone wants to do them, right? And for a good reason: they're not only impressive to see, but they're also so useful to master the flexibility of your body! Splits Hacking was written to help you discover how to train for the splits with the correct exercises and methodologies. In this book, I'll teach you everything you need to know to finally touch the floor in the splits, even if you start from the absolute ZERO and you've always wanted to learn these amazing stretching positions. It doesn't matter how hard you train. What makes the real difference is how you do your stretches; what kind of stretches you do; and the training program you follow. I'm Elia Bartolini, and I'm a flexibility coach. As a teenager, my dream was to reach the splits; but you know what? I had no idea how to do it. So I started looking for exercises, methodologies, and coaches that could help me get there. It took some time to develop my splits, and thanks to that, I figured out a clear path to follow to master these stretching positions. At that point, I thought... "Ok, this could have worked for me, but would it also work for others?". So I decided to test it out. In the following years, I've worked with many different practitioners worldwide, and I taught many people how to reach the splits. The path I figured out has also been working with them. So, why not put it into a book? This book will help you find your path so that you can enjoy your training and the fantastic journey towards the splits...
Presents ten PC-based hacking projects, including a home television server, an in-counter kitchen PC, and a wireless RS-232 link.
If you wish to enter the world of ethical hacking, this book is for you. Ethical Hacking: A Comprehensive Beginner's Guide to Learn and Master Ethical Hacking will walk you through the processes, skills, and tools you need to succeed. If you want to master ethical hacking, then this is the book you have been looking for. Inside you will learn the important lessons you need to master the basics of ethical hacking.

No matter if you are a beginner or a knowledgeable IT professional, this book will enhance your skills and make you the best ethical hacker you can be. When it comes to honing your talents and seeking certification, this book provides you with the information you need to take the next step. This book covers everything you need to get started and move forward with ethical hacking.This book will prepare you to reach your goals in ethical hacking and will teach you the complex information behind packets, protocols, malware, and network infrastructure. Don't let this opportunity to enhance your skills pass. Stop wishing to know about ethical hacking, take the plunge, and purchase Ethical Hacking: A Comprehensive Guide to Learn and Master Hacking today!Inside you will find The knowledge of how to attack computer systems to find weaknesses Master what it means to be an ethical hacker Learn about the tools and terminology you need to get started Contemplate the difference between ethical hackers and system attackers Determine vulnerabilities, exploits, and weaknesses in computer systems Gain in-depth knowledge about the processes of enumeration, sniffing, port scanning, and network mapping Learn about malware and how to infect networks, servers, and computers with ease Everything you need to know to master evading intrusion detection systems Have fun with the techniques behind system hacking, social engineering, hacking the web, and the cloud Have fun with the techniques behind system hacking, social engineering, hacking the web, and the cloud And more . . .

Meditation can be a fog of uncertainty, with the practitioner never quite knowing if they're getting it right, never knowing if they're, “good enough.” What if we could wipe away the mystery? What if we could clear the chaos of the mind? This is meditation broken down into it's essential principles; giving you a strategy for the entire process of self-inquiry. With the proper program interiorization is easy. Buckle up; the engine of self-realization is about to be unmasked.

Violent Python shows you how to move from a theoretical understanding of offensive computing concepts to a practical implementation. Instead of relying on another attacker’s tools, this book will teach you to forge your own weapons using the Python programming language. This book demonstrates how to write Python scripts to automate large-scale network attacks, extract metadata, and investigate forensic artifacts. It also shows how to write code to intercept and analyze network traffic using Python, craft and spoof wireless frames to attack wireless and Bluetooth devices, and how to data-mine popular social media websites and evade modern anti-virus. Demonstrates how to write Python scripts to automate large-scale network attacks, extract metadata, and investigate forensic artifacts Write code to intercept and analyze network traffic using Python. Craft and spoof wireless frames to attack wireless and Bluetooth devices Data-mine popular social media websites and evade modern anti-virus

Harden the human firewall against the most current threats Social Engineering: The Science of Human Hacking reveals the craftier side of the hacker’s repertoire—why hack into something when you could just ask for access? Undetectable by firewalls and antivirus software, social engineering relies on human fault to gain access to sensitive spaces; in this book, renowned expert Christopher Hadnagy explains the most commonly-used techniques that fool even the most robust security personnel, and shows you how these techniques have been used in the past. The way that we make decisions as humans affects everything from our emotions to our security. Hackers, since the beginning of time, have figured out ways to exploit that decision making process and get you to take an action not in your best interest. This new Second Edition has been updated with the most current methods used by sharing stories, examples, and scientific study behind how those decisions are exploited. Networks and systems can be hacked, but they can also be protected; when the “system” in question is a human being, there is no software to fall back on, no hardware upgrade, no code that can lock information down indefinitely. Human nature and emotion is the secret weapon of the malicious social engineering, and this book shows you how to recognize, predict, and prevent this type of manipulation by taking you inside the social engineer’s bag of tricks. Examine the most common social engineering tricks used to gain access Discover which popular techniques generally don’t work in the real world Examine how our understanding of the science behind emotions and decisions can be used by social engineers Learn how social engineering factors into some of the biggest recent headlines Learn how to use these skills as a professional social engineer and secure your company Adopt effective counter-measures to keep hackers at bay By working from the social engineer’s playbook, you gain the advantage of foresight that can help you protect yourself and others from even their best efforts. Social Engineering gives you the inside information you need to mount an unshakeable defense.

Chicago has many treasures. The Magnificent Mile and Wrigley Field, wonderful public art and parks, beautiful bridges and skylines. But the true heart and the real treasure of the city are its children. This book is devoted to Chicago's children. Come along as they travel to worlds within worlds, becoming storybook characters who follow the Yellow Brick Road, sip tea in Wonderland, tame a tiger, live in a shoe, climb a magic beanstalk to bring home a golden-egg-laying hen, turn a frog into a prince, meet fairies and dragons. Continue as they step into painted canvases to inhabit scenes from other times and places. After climbing down from those framed worlds, they explore the city, high-fiving the victorious Chicago Bears, joining penguins at the theater, and leaping across State Street Bridge aboard African impalas. The kids are the story. The book is their adventure. Its door swings open. . . For kids of all ages. 168 pages and 150 illustrations. Unlimited dreams.

"Minimalismo" è l'arte di saper riconoscere lo stretto necessario. Il "minimalismo digitale" è l'applicazione di questa idea alle tecnologie. Pensare la vita senza smartphone, internet e social network oggi ci sembra quasi impossibile, eppure fino a qualche anno fa la maggior parte di questi strumenti non esisteva. Le società della Silicon Valley hanno sfruttato le più avanzate scoperte della psicologia e delle neuroscienze per tenerci incollati ai loro dispositivi, dando vita alla cosiddetta "economia dell'attenzione": noi siamo il prodotto e gli inserzionisti pubblicitari sono gli acquirenti. Cal Newport, professore di computer science e saggista, ritiene che il modo migliore per riprendere il controllo sia il minimalismo digitale: una filosofia che prevede di fare un passo indietro e ripensare il nostro rapporto con la tecnologia in maniera attiva. Minimalismo digitale spiega (supportato da solide basi scientifiche) perché dovremmo sposare questa visione, quali vantaggi ci porterà e condivide il percorso studiato e testato dall'autore per emanciparci dai nostri dispositivi digitali, per tornare ad avere il pieno controllo del nostro tempo e per decidere senza condizionamenti quali sono le attività che realmente hanno valore per noi e ci rendono felici.

THE BESTSELLING CLASSIC ON 'FLOW' – THE KEY TO UNLOCKING MEANING, CREATIVITY, PEAK PERFORMANCE, AND TRUE HAPPINESS Legendary psychologist Mihaly Csikszentmihalyi's famous investigations of "optimal experience" have revealed that what makes an experience genuinely satisfying is a state of consciousness called flow. During flow, people typically experience deep enjoyment, creativity, and a total involvement with life. In this new edition of his groundbreaking classic work, Csikszentmihalyi ("the leading researcher into ‘flow states’" —Newsweek) demonstrates the ways this positive state can be controlled, not just left to chance. Flow: The Psychology of Optimal Experience teaches how, by ordering the information that enters our consciousness, we can discover true happiness, unlock our potential, and greatly improve the quality of our lives. "Explores a happy state of mind called flow, the feeling of complete engagement in a creative or playful activity." —Time

This book is a practical guide to discovering and exploiting security flaws in web applications. The authors explain each category of vulnerability using real-world examples, screen shots and code extracts. The book is extremely practical in focus, and describes in detail the steps involved in detecting and exploiting each kind of security weakness found within a variety of applications such as online banking, e-commerce and other web applications. The topics covered include bypassing login mechanisms, injecting code, exploiting logic flaws and compromising other users. Because every web application is different, attacking them entails bringing to bear various general principles, techniques and experience in an imaginative way. The most successful hackers go beyond this, and find ways to automate their bespoke attacks. This handbook describes a proven methodology that combines the virtues of human intelligence and computerized brute force, often with devastating results. The authors are professional penetration testers who have been involved in web application security for nearly a decade. They have presented training courses at the Black Hat security conferences throughout the world. Under the alias

"PortSwigger", Dafydd developed the popular Burp Suite of web application hack tools.

It is common knowledge that, in rich societies, the poor have worse health and suffer more from almost every social problem. This book explains why inequality is the most serious problem societies face today.

The digital virtual communities have exploded in recent years - this phenomenon is enabled by social media and the changing world we live in. In some cases these communities have created their own currency for exchange of goods and services but it has expanded to outside their own circles and provide a new medium of exchange creating new digital virtual currencies that are changing the world. Bitcoin-Central is now the first Bitcoin exchange to become a bank with guarantee funds insured up to EU$100,000. This book explores the new digital currencies and how they are changing the world. When we were researching -The Deep Dark Web book we saw that some of the criminal elements were using this new currency Bitcoin but we also saw that legit business were also adapting to this new currency. Who uses this currency -What are the financial aspect - governments, business, merchants and criminals. This book will be an invaluable resource for cyber security professionals, financial policy-makers, business experts, lawyers, merchants, scholars, and researchers. Book provides comprehensive research from an international cyber security perspective, technical, and financial implications of the new digital virtual currencies.

Sicilian Elements in Andrea Camilleri’s Narrative Language examines Camilleri’s unique linguistic repertoire and techniques over his career as a novelist. It focuses on the intensification of Sicilian linguistic features in Camilleri’s narrative works, in particular features pertaining to the domains of sounds and grammar, since these have been marginalized in linguistic-centered research on the evolution of Camilleri’s narrative language and remain overall understudied. Through a systematic comparative analysis of the distribution patterns of selected Sicilian features in a selection of Camilleri’s historical novels and novels of the Montalbano series, the author identifies the individual features that have become most widespread and the lexical items that are targeted with highest frequency and consistency. The results of the analysis show that in the earlier novels, Sicilian features are rather sparse and can be attributed to linguistic situational functionality; that is, they function as indices of salient, distinctive aspects of topics, settings, events/situations, and characters. Conversely, in the latest novels, Sicilian elements pervade the entire novels and the texts are written almost entirely in Camilleri’s own Sicilian, vigatese, so that Sicilian is stripped of any linguistic situational functionality.

"Returning to Virginia's post-revolutionary history and to characters introduced in Tail Gait, the story follows the Garth sisters and their husbands, neighbors to a brutal slaveholder whose murder at the hands of one of his slaves is neither unexpected nor unwarranted, especially when the impetus was an attack on that slave's wife. The sisters manage to smuggle the fugitive to safety in York, Pennsylvania, while ensuring that the circumstances underlying the entire ordeal stay long buried. Until now. Harry and her animal companions come closer to drawing a link between the past and the present. And in this centuries-spanning caper, they will discover that hiding who you really are may have mortal consequences ... As the questions surrounding."--

Just as a professional athlete doesn't show up without a solid game plan, ethical hackers, IT professionals, and security researchers should not be unprepared, either. The Hacker Playbook provides them their own game plans. Written by a longtime security professional and CEO of Secure Planet, LLC, this step-by-step guide to the "game" of penetration hacking features hands-on examples and helpful advice from the top of the field. Through a series of football-style "plays," this straightforward guide gets to the root of many of the roadblocks people may face while penetration testing-including attacking different types of networks, pivoting through security controls, privilege escalation, and evading antivirus software. From "Pregame" research to "The Drive" and "The Lateral Pass," the practical plays listed can be read in order or referenced as needed. Either way, the valuable advice within will put you in the mindset of a penetration tester of a Fortune 500 company, regardless of your career or level of experience. This second version of The Hacker Playbook takes all the best "plays" from the original book and incorporates the latest attacks, tools, and lessons learned. Double the content compared to its predecessor, this guide further outlines building a lab, walks through test cases for attacks, and provides more customized code. Whether you're downing energy drinks while desperately looking for an exploit, or preparing for an exciting new job in IT security, this guide is an essential part of any ethical hacker's library-so there's no reason not to get in the game.