Unmasking The Social Engineer The Human Element Of Security

As recognized, adventure as well as experience practically lesson, amusement, as capably as covenant can be gotten by just checking out a book **Unmasking The Social Engineer The Human Element Of Security** with it is not directly done, you could agree to even more as regards this life, roughly speaking the world.

We have enough money you this proper as without difficulty as easy pretension to get those all. We offer Unmasking The Social Engineer The Human Element Of Security and numerous books collections from fictions to scientific research in any way. along with them is this Unmasking The Social Engineer The Human Element Of Security that can be your partner.

The Art of Deception - Kevin D. Mitnick 2011-08-04
The world's most infamous hacker offers an insider's view of the low-tech threats to high-tech security Kevin Mitnick's exploits as a cyber-desperado and fugitive form one of the most exhaustive FBI manhunts in history and have spawned dozens of articles, books, films, and documentaries. Since his release from federal prison, in 1998, Mitnick has turned his life around and established himself as one of the most sought-after computer security experts worldwide. Now, in The Art of Deception, the world's most notorious hacker gives new meaning to the old adage, "It takes a thief to catch a thief." Focusing on the human factors involved with information security, Mitnick explains why all the firewalls and encryption protocols in the world will never be enough to stop a savvy grifter intent on rifling a corporate database or an irate employee determined to crash a system. With the help of many fascinating true stories of successful attacks on business and government, he illustrates just how susceptible even the most locked-down information systems are to a slick con artist impersonating an IRS agent. Narrating from the points of view of both the attacker and the victims, he explains why each attack was so successful and how it could have been prevented in an engaging and highly readable style reminiscent of a true-crime novel. And, perhaps most importantly, Mitnick offers advice for preventing these types of social engineering hacks through security protocols, training programs, and manuals that address the human element of security.
Social Engineering - Christopher Hadnagy 2018-06-25
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.

Social Engineering - Christopher Hadnagy 2010-11-29

The first book to reveal and dissect the technical aspect of many social engineering maneuvers From elicitation, pretexting, influence and manipulation all aspects of social engineering are picked apart, discussed and explained by using real world examples, personal experience and the science behind them to unraveled the mystery in social engineering. Kevin Mitnick—one of the most famous social engineers in the world—popularized the term "social engineering." He explained that it is much easier to trick someone into revealing a password for a system than to exert the effort of hacking into the system. Mitnick claims that this social engineering tactic was the single-most effective method in his arsenal. This indispensable book examines a variety of maneuvers that are aimed at deceiving unsuspecting victims, while it also addresses ways to prevent social engineering threats. Examines social engineering, the science of influencing a target to perform a desired task or divulge information Arms you with invaluable information about the many methods of trickery that hackers use in order to gather information with the intent of executing identity theft, fraud, or gaining computer system access Reveals vital steps for preventing social engineering threats Social Engineering: The Art of Human Hacking does its part to prepare you against nefarious hackers—now you can do your part by putting to good use the critical information within its pages.

Social Psychology - Daniel W. Barrett 2015-12-19

Employing a lively and accessible writing style, author Daniel W. Barrett integrates up-to-date coverage of social psychology's core theories, concepts, and research with a discussion of emerging developments in the field—including social neuroscience and the social psychology of happiness, religion, and sustainability. Social Psychology: Core Concepts and Emerging Trends presents engaging examples, Applying Social Psychology sections, and a wealth of pedagogical features to help readers cultivate a deep understanding of the causes of social behavior.

Zen to Done - Leo Babauta 2011-03

Zen To Done is a simple system to help you get organized and productive--keeping your life saner and less stressed--with a set of simple habits. Zen To Done takes some of the best aspects of popular productivity systems (GTD, Stephen Covey, and others), then combines and simplifies them, giving you just what you need--and no more. Simply put, ZTD teaches you: (1) The key habits needed to be organized and productive. (2) How to implement these habits. (3) How to organize the habits into a simple system that will keep everything in your life in its place. (4) How to simplify what you need to do. (5) How to implement an even simpler version called Minimal ZTD. If you're tired of doing things the hard way and just want a simple, easy, yet effective way to accomplish your goals, Zen To Done is just what you need.

The Human Factor of Cybercrime - Rutger Leukfeldt 2019-10-11

Cybercrimes are often viewed as technical offenses that require technical solutions, such as antivirus programs or automated intrusion detection tools. However, these crimes are committed by individuals or networks of people which prey upon human victims and are detected and prosecuted by criminal justice personnel. As a result, human decision-making plays a substantial role in the course of an offence, the justice response, and policymakers' attempts to legislate against these crimes. This book focuses on the human factor in cybercrime: its offenders, victims, and

parties involved in tackling cybercrime. The distinct nature of cybercrime has consequences for the entire spectrum of crime and raises myriad questions about the nature of offending and victimization. For example, are cybercriminals the same as traditional offenders, or are there new offender types with distinct characteristics and motives? What foreground and situational characteristics influence the decision-making process of offenders? Which personal and situational characteristics provide an increased or decreased risk of cybercrime victimization? This book brings together leading criminologists from around the world to consider these questions and examine all facets of victimization, offending, offender networks, and policy responses.

Social Engineering and Nonverbal Behavior Set - Christopher Hadnagy 2014-03-18

Social Engineering: The Art of Human Hacking From elicitation, pretexting, influence and manipulation all aspects of social engineering are picked apart, discussed and explained by using real world examples, personal experience and the science behind them to unraveled the mystery in social engineering. Examines social engineering, the science of influencing a target to perform a desired task or divulge information Arms you with invaluable information about the many methods of trickery that hackers use in order to gather information with the intent of executing identity theft, fraud, or gaining computer system access Reveals vital steps for preventing social engineering threats Unmasking the Social Engineer: The Human Element of Security Focuses on combining the science of understanding non-verbal communications with the knowledge of how social engineers, scam artists and con men use these skills to build feelings of trust and rapport in their targets. The author helps readers understand how to identify and detect social engineers and scammers by analyzing their non-verbal behavior. Unmasking the Social Engineer shows how attacks work, explains nonverbal communications, and demonstrates with visuals the connection of non-verbal behavior to social engineering and scamming. Clearly combines both the practical and technical aspects of social engineering security Reveals the various dirty tricks that scammers use Pinpoints what to look for on the nonverbal side to detect the social engineer

Finding Truth - Nancy Pearcey 2015-03-01

Christianity Has the Resources to Address Intellectual and Cultural Issues. Do You? Christians can feel overwhelmed at the sheer number of competing worldviews in today’s pluralistic, multicultural society. Thankfully, you don’t have to memorize a different argument to answer every new issue. Instead, you can master a single line of defense, grounded in Scripture, that applies to any theory. In Romans, Paul reveals the strategy for defending the Christian message in a pluralistic culture where many are hearing it for the first time. Finding Truth is the real-world training manual that equips you to confidently address issues you’ll face in the classroom, workplace, and popular culture.

The Triumph of Emptiness - Mats Alvesson 2013-05-30

The book views the contemporary economy as an economy of persuasion, where firms and institutions assign resources to rhetoric, image, and reputation rather than production of goods and services. It examines critically phenomena such as the knowledge society, consumption, higher education, organizational change, professionalization, and leadership.

Social Engineering - Robert W. Gehl 2022-03-08

Manipulative communication—from early twentieth-century propaganda to today’s online con artistry—examined through the lens of social engineering. The United States is awash in manipulated information about everything from election results to the effectiveness of medical treatments. Corporate social media is an especially good channel for manipulative communication, with Facebook a particularly willing vehicle for it. In Social Engineering, Robert Gehl and Sean Lawson show that online misinformation has its roots in earlier techniques: mass social engineering of the early twentieth century and interpersonal hacker social engineering of the 1970s, converging today into what they call “masspersonal social engineering.” As Gehl and Lawson trace contemporary manipulative communication back to earlier forms of social engineering, possibilities for amelioration become clearer. The authors show how specific manipulative communication practices are a

mixture of information gathering, deception, and truth-indifferent statements, all with the instrumental goal of getting people to take actions the social engineer wants them to. Yet the term “fake news,” they claim, reduces everything to a true/false binary that fails to encompass the complexity of manipulative communication or to map onto many of its practices. They pay special attention to concepts and terms used by hacker social engineers, including the hacker concept of “bullshitting,” which the authors describe as a truth-indifferent mix of deception, accuracy, and sociability. They conclude with recommendations for how society can undermine masspersonal social engineering and move toward healthier democratic deliberation.

Human Hacking - Christopher Hadnagy 2021

"Global security expert Christopher Hadnagy applies psychological insights to reveal the secrets of well-intentioned "human hacking." Master the art of social engineering in all areas of your life to win friends, influence people, and get almost anything you want-all by being more empathetic, generous, and kind"--

Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses - M.N. Ogun 2015-10-08

ICT plays a crucial role in the pursuit of modernization in the countries of Slovenia, Croatia, Albania and Bulgaria, which form the South Eastern European (SEE) region., The quest for Euro-Atlantic integration and the undeniable necessity for direct foreign investment have encouraged the SEE countries to invest in the development of cyber technology, and it has become the dominant area for social, economic and political interaction within the region. This has had both positive and negative consequences. This book presents the proceedings of the NATO Advanced Training Course (ATC), held in Ohrid, former Yugoslav Republic of Macedonia, in December 2014. The ATC addressed serious concerns about terrorist use of cyber technology in South Eastern Europe, which not only has the potential to destabilize regional efforts to create a platform for increased development by creating a breeding ground for the training of extremists and the launching of cyber attacks, but also represents a direct and indirect threat to the security and stability of other NATO partner countries. The book will be of interest to all those involved in countering the threat posed by terrorist use of the Internet worldwide.

Phishing Dark Waters - Christopher Hadnagy 2015-03-18

An essential anti-phishing desk reference for anyone with anemail address Phishing Dark Waters addresses the growing and continuingscourge of phishing emails, and provides actionable defensivetechniques and tools to help you steer clear of malicious emails.Phishing is analyzed from the viewpoint of human decision-makingand the impact of deliberate influence and manipulation on therecipient. With expert guidance, this book provides insight intothe financial, corporate espionage, nation state, and identitytheft goals of the attackers, and teaches you how to spot a spoofede-mail or cloned website. Included are detailed examples of highprofile breaches at Target, RSA, Coca Cola, and the AP, as well asan examination of sample scams including the Nigerian 419,financial themes, and post high-profile event attacks. Learn how toprotect yourself and your organization using anti-phishing tools,and how to create your own phish to use as part of a securityawareness program. Phishing is a social engineering technique through email thatdeceives users into taking an action that is not in their bestinterest, but usually with the goal of disclosing information orinstalling malware on the victim's computer. Phishing DarkWaters explains the phishing process and techniques, and thedefenses available to keep scammers at bay. Learn what a phish is, and the deceptive ways they've beenused Understand decision-making, and the sneaky ways phishers reelyou in Recognize different types of phish, and know what to do whenyou catch one Use phishing as part of your security awareness program forheightened protection Attempts to deal with the growing number of phishing incidentsinclude legislation, user training, public awareness, and technicalsecurity, but phishing still exploits the natural way humansrespond to certain situations. Phishing Dark Waters is anindispensible guide to recognizing and blocking the phish, keepingyou, your organization, and your finances safe.

Galileo's Middle Finger - Alice Dreger 2016-04-05

"Galileo's Middle Finger is historian Alice Dreger's eye-opening story of life in the trenches of scientific controversy. Dreger's chronicle begins with her own research into the treatment of people born intersex (once called hermaphrodites). Realization of the shocking surgical and ethical abuses conducted in the name of "normalizing" intersex children's gender identities moved Dreger to become an internationally recognized patient rights activist. But even as the intersex rights movement succeeded, Dreger began to realize how some fellow activists were using lies and personal attacks to silence scientisis whose data revealed uncomfortable truths about humans. In researching one case, Dreger suddenly became a target of just these kinds of attacks. Troubled, she decided to try to understand more -- to travel the country and seek a global view of the nature and costs of these damaging battles. Galileo's Middle Finger describes Dreger's long and harrowing journeys between the two camps for which she felt equal empathy: social justice activists determined to win and researchers determined to put hard truths before comfort. What emerges is a lesson about the intertwining of justice and truth-- and about the importance of responsible scholars and journalists to our fragile democracy." --

Violence at Work - Duncan Chappell 2006

Violence at work, ranging from bullying and mobbing, to threats by psychologically unstable co-workers, sexual harassment and homicide, is increasing worldwide and has reached epidemic levels in some countries. This updated and revised edition looks at the full range of aggressive acts, offers new information on their occurrence and identifies occupations and situations at particular risk. It is organised in three sections: understanding violence at work; responding to violence at work; future action.

Unmasking the Social Engineer - Christopher Hadnagy 2014-01-27

Learn to identify the social engineer by non-verbal behavior Unmasking the Social Engineer: The Human Element of Security focuses on combining the science of understanding non-verbal communications with the knowledge of how social engineers, scam artists and con men use these skills to build feelings of trust and rapport in their targets. The author helps readers understand how to identify and detect social engineers and scammers by analyzing their non-verbal behavior. Unmasking the Social Engineer shows how attacks work, explains nonverbal communications, and demonstrates with visuals the connection of non-verbal behavior to social engineering and scamming. Clearly combines both the practical and technical aspects of social engineering security Reveals the various dirty tricks that scammers use Pinpoints what to look for on the nonverbal side to detect the social engineer Sharing proven scientific methodology for reading, understanding, and deciphering non-verbal communications, Unmasking the Social Engineer arms readers with the knowledge needed to help protect their organizations.

-

Hacker, Hoaxer, Whistleblower, Spy - Gabriella Coleman 2014-11-04

Here is the ultimate book on the worldwide movement of hackers, pranksters, and activists that operates under the non-name Anonymous, by the writer the Huffington Post says “knows all of Anonymous’ deepest, darkest secrets.” Half a dozen years ago, anthropologist Gabriella Coleman set out to study the rise of this global phenomenon just as some of its members were turning to political protest and dangerous disruption (before Anonymous shot to fame as a key player in the battles over WikiLeaks, the Arab Spring, and Occupy Wall Street). She ended up becoming so closely connected to Anonymous that the tricky story of her inside–outside status as Anon confidante, interpreter, and erstwhile mouthpiece forms one of the themes of this witty and entirely engrossing book. The narrative brims with details unearthed from within a notoriously mysterious subculture, whose semi-legendary tricksters—such as Topiary, tflow, Anachaos, and Sabu—emerge as complex, diverse, politically and culturally sophisticated people. Propelled by years of chats and encounters with a multitude of hackers, including imprisoned activist Jeremy Hammond and the double agent who helped put him away, Hector Monsegur, Hacker, Hoaxer, Whistleblower, Spy is filled with insights into the meaning of digital

activism and little understood facets of culture in the Internet age, including the history of “trolling,” the ethics and metaphysics of hacking, and the origins and manifold meanings of “the lulz.”

The Logic of Social Practices - Raffaela Giovagnoli 2020-02-04

This book reports on cutting-edge research concerning social practices. Merging perspectives from various disciplines, including philosophy, biology, and cognitive science, it discusses theoretical aspects of social behavior along with models to investigate them, and also presents key case studies. Further, It describes concepts related to habits, routines, and rituals and examines important features of human action, such as intentionality and choice, exploring the influence of specific social practices in different situations. Based on a workshop held in June 2018 at the 6th World Congress of Universal Logic, UNILOG2018, in Vichy, and including additional invited chapters, the book offers fresh insights into the fields of social practice and the cognitive, computational, and philosophical tools to understand them.

The Cybersecurity Dilemma - Ben Buchanan 2017-02-01

Why do nations break into one another's most important computer networks? There is an obvious answer: to steal valuable information or to attack. But this isn't the full story. This book draws on often-overlooked documents leaked by Edward Snowden, real-world case studies of cyber operations, and policymaker perspectives to show that intruding into other countries' networks has enormous defensive value as well. Two nations, neither of which seeks to harm the other but neither of which trusts the other, will often find it prudent to launch intrusions. This general problem, in which a nation's means of securing itself threatens the security of others and risks escalating tension, is a bedrock concept in international relations and is called the 'security dilemma'. This book shows not only that the security dilemma applies to cyber operations, but also that the particular characteristics of the digital domain mean that the effects are deeply pronounced. The cybersecurity dilemma is both a vital concern of modern statecraft and a means of accessibly understanding the essential components of cyber operations.

How Life Imitates Chess - Garry Kasparov 2010-08-10

Garry Kasparov was the highest-rated chess player in the world for over twenty years and is widely considered the greatest player that ever lived. In How Life Imitates Chess Kasparov distills the lessons he learned over a lifetime as a Grandmaster to offer a primer on successful decision-making: how to evaluate opportunities, anticipate the future, devise winning strategies. He relates in a lively, original way all the fundamentals, from the nuts and bolts of strategy, evaluation, and preparation to the subtler, more human arts of developing a personal style and using memory, intuition, imagination and even fantasy. Kasparov takes us through the great matches of his career, including legendary duels against both man (Grandmaster Anatoly Karpov) and machine (IBM chess supercomputer Deep Blue), enhancing the lessons of his many experiences with examples from politics, literature, sports and military history. With candor, wisdom, and humor, Kasparov recounts his victories and his blunders, both from his years as a world-class competitor as well as his new life as a political leader in Russia. An inspiring book that combines unique strategic insight with personal memoir, How Life Imitates Chess is a glimpse inside the mind of one of today's greatest and most innovative thinkers.

Lauren Ipsum - Carlos Bueno 2014-12-14

Lauren Ipsum is a whimsical journey through a land where logic and computer science come to life. Meet Lauren, an adventurer lost in Userland who needs to find her way home by solving a series of puzzles. As she visits places like the Push & Pop Café and makes friends with people like Hugh Rustic and the Wandering Salesman, Lauren learns about computer science without even realizing it—and so do you! Read Lauren Ipsum yourself or with someone littler than you, then flip to the notes at the back of the book to learn more about logic and computer science in the real world. Suggested for ages 10+

Social Engineering - Adam Podgórecki 1996

Social engineering in the 20th century has brought about some large-scale changes in society, often the result of visionary social projects, and plans designed on a grand and ideal scale. Such plans have often extracted terrible human costs. Numerous failures have marked 20th

century social engineering.

The Mueller Report - Robert S. Mueller 2019-04-26

This is the full Mueller Report, as released on April 18, 2019, by the U.S. Department of Justice. A reprint of the report exactly as it was issued by the government, it is without analysis or commentary from any other source and with nothing subtracted except for the material redacted by the Department of Justice. The mission of the Mueller investigation was to examine Russian interference in the 2016 Presidential election, consisting of possible links, or "collusion," between the Donald Trump campaign and the Russian government of Vladimir Putin as well as any allegations of obstruction of justice in this regard. It was also intended to detect and prosecute, where warranted, any other crimes that surfaced during the course of the investigation. The report consists of a detailed summary of the various investigations and inquiries that the Special Counsel and colleagues carried out in these areas. The investigation was initiated in the aftermath of the firing of FBI Director James Comey by Donald Trump on May 9, 2017. The FBI, under Director Comey, had already been investigating links between Russia and the Trump campaign. Mueller submitted his report to Attorney General William Barr on March 22, 2019, and the Department of Justice released the redacted report one month later.

Hacking the Human - Mr Ian Mann 2012-09-28

Ian Mann's Hacking the Human highlights the main sources of risk from social engineering and draws on psychological models to explain the basis for human vulnerabilities. Offering more than a simple checklist to follow, the book provides a rich mix of examples, applied research and practical solutions for security and IT professionals that enable you to create and develop a security solution that is most appropriate for your organization.

Human-Machine Reconfigurations - Lucy Suchman 2007

Publisher description

Handbook of Research on Policies, Protocols, and Practices for Social Work in the Digital World - Özsungur, Fahri 2021-05-28

Social work plays an important role in reintegrating individuals into society, educating, raising awareness, implementing social policy, and realizing legal regulations. The emergence of digital innovations and the effects of health problems including the COVID-19 pandemic on individuals and society have led to the development of innovations, virtual/digital practices, and applications in this field. The contributions of the recent pandemic and digital transformation to social work and practices should be revealed in the context of international standards. Policies, Protocols, and Practices for Social Work in the Digital World presents the current best practices, policies, and protocols within international social work. It focuses on the impact of digital applications, the effects of the COVID-19 pandemic, and digital transformation on social work. Covering topics including burnout, management, social engineering, anti-discrimination strategies, and women's studies, this book is essential for social workers, policymakers, government officials, scientists, clinical professionals, technologists, practitioners, researchers, academicians, and students.

Phishing Dark Waters - Christopher Hadnagy 2015-03-18

An essential anti-phishing desk reference for anyone with anemail address Phishing Dark Waters addresses the growing and continuingscourge of phishing emails, and provides actionable defensivetechniques and tools to help you steer clear of malicious emails.Phishing is analyzed from the viewpoint of human decision-makingand the impact of deliberate influence and manipulation on therecipient. With expert guidance, this book provides insight intothe financial, corporate espionage, nation state, and identitytheft goals of the attackers, and teaches you how to spot a spoofede-mail or cloned website. Included are detailed examples of highprofile breaches at Target, RSA, Coca Cola, and the AP, as well asan examination of sample scams including the Nigerian 419,financial themes, and post high-profile event attacks. Learn how toprotect yourself and your organization using anti-phishing tools,and how to create your own phish to use as part of a securityawareness program. Phishing is a social engineering technique through email thatdeceives users into taking an action that is not in their bestinterest, but usually with the goal of disclosing information

orinstalling malware on the victim's computer. Phishing DarkWaters explains the phishing process and techniques, and thedefenses available to keep scammers at bay. Learn what a phish is, and the deceptive ways they've beenused Understand decision-making, and the sneaky ways phishers reelyou in Recognize different types of phish, and know what to do whenyou catch one Use phishing as part of your security awareness program forheightened protection Attempts to deal with the growing number of phishing incidentsinclude legislation, user training, public awareness, and technicalsecurity, but phishing still exploits the natural way humansrespond to certain situations. Phishing Dark Waters is anindispensible guide to recognizing and blocking the phish, keepingyou, your organization, and your finances safe.

Strengthening Forensic Science in the United States - National Research Council 2009-07-29

Scores of talented and dedicated people serve the forensic science community, performing vitally important work. However, they are often constrained by lack of adequate resources, sound policies, and national support. It is clear that change and advancements, both systematic and scientific, are needed in a number of forensic science disciplines to ensure the reliability of work, establish enforceable standards, and promote best practices with consistent application. Strengthening Forensic Science in the United States: A Path Forward provides a detailed plan for addressing these needs and suggests the creation of a new government entity, the National Institute of Forensic Science, to establish and enforce standards within the forensic science community. The benefits of improving and regulating the forensic science disciplines are clear: assisting law enforcement officials, enhancing homeland security, and reducing the risk of wrongful conviction and exoneration. Strengthening Forensic Science in the United States gives a full account of what is needed to advance the forensic science disciplines, including upgrading of systems and organizational structures, better training, widespread adoption of uniform and enforceable best practices, and mandatory certification and accreditation programs. While this book provides an essential call-to-action for congress and policy makers, it also serves as a vital tool for law enforcement agencies, criminal prosecutors and attorneys, and forensic science educators.

Hidden Cities - World Health Organization. Centre for Health Development 2010

"The joint WHO and UN-HABITAT report, Hidden cities: unmasking and overcoming health inequities in urban settings, is being released at a turning point in human history. For the first time ever, the majority of the world's population is living in cities, and this proportion continues to grow. Putting this into numbers, in 1990 fewer than 4 in 10 people lived in urban areas. In 2010, more than half live in cities, and by 2050 this proportion will grow to 7 out of every 10 people. The number of urban residents is growing by nearly 60 million every year. This demographic transition from rural to urban, or urbanization, has far-reaching consequences. Urbanization has been associated with overall shifts in the economy, away from agriculture-based activities and towards mass industry, technology and service. High urban densities have reduced transaction costs, made public spending on infrastructure and services more economically viable, and facilitated generation and diffusion of knowledge, all of which have fuelled economic growth"--Page ix.

Beyond Bias and Barriers - Institute of Medicine 2007-05-04

The United States economy relies on the productivity, entrepreneurship, and creativity of its people. To maintain its scientific and engineering leadership amid increasing economic and educational globalization, the United States must aggressively pursue the innovative capacity of all its people—women and men. However, women face barriers to success in every field of science and engineering; obstacles that deprive the country of an important source of talent. Without a transformation of academic institutions to tackle such barriers, the future vitality of the U.S. research base and economy are in jeopardy. Beyond Bias and Barriers explains that eliminating gender bias in academia requires immediate overarching reform, including decisive action by university administrators, professional societies, federal funding agencies and foundations, government agencies, and Congress. If implemented and coordinated across public, private, and government sectors, the

recommended actions will help to improve workplace environments for all employees while strengthening the foundations of America's competitiveness.

Leveling the Playing Field - Rod Scher 2016-08-01

Leveling the Playing Field explores the technologies that “trickle down” to the rest of us, those that were once the domain of the wealthy and powerful--and which therefore tended to make them even more wealthy and powerful. Now, though, these technologies--from books to computers to 3D printing and beyond--have become part of a common toolkit, one accessible to almost anyone, or at least to many more than had heretofore had access. This is what happens with most technologies: They begin in the hands of the few, and they end up in the hands of the many. Along the way, they sometimes transform the world.

Gap Junctions - James E. Hall 1993

Gap junctions are present in nearly all tissues, regardless of their embronic origin and have long been of great interest to scientists from many different disciplines. The international meeting on which this book is based brought together 157 scientists from 12 countries and almost as many scientific disciplines. The papers presented at the meeting were reviewed and updated prior to publication in this book. The seven parts of the book progress from general topics to the more specific ones (role of gap junctions in various tissues, regulation and biochemistry, and cancer).

Social Engineering - Vince Reynolds 2016-02-06

The Art of Psychological Warfare, Human Hacking, Persuasion, and Deception Are You Ready To Learn How To Configure & Operate Cisco Equipment? If So You've Come To The Right Place - Regardless Of How Little Experience You May Have! If you're interested in social engineering and security then you're going to want (or need!) to know and understand the way of the social engineer. There's a ton of other guides out there that aren't clear and concise, and in my opinion use far too much jargon. My job is to teach you in simple, easy to follow terms how to understand social engineering. Here's A Preview Of What This Social Engineering Book Contains... What Is Social Engineering? Basic Psychological Tactics Social Engineering Tools Pickup Lines Of Social Engineers How To Prevent And Mitigate Social Engineering Attacks And Much, Much More! Order Your Copy Now And Learn All About Social Engineering!

Reinvent Your Personal Safety - Matt Tamas 2017-10-03

In Reinvent Your Personal Safety, Matt Tamas takes women through a proactive approach to personal safety, one that isn’t about honing technical moves or perfecting technique, but more about showing them how to work with their own body and mind, considering realistic scenarios, and training them to take appropriate action. Matt’s job, as a personal safety coach, is to not only give women the tools to fight back during an assault, but also to help them prevent themselves from being assaulted in the first place. The right action to take is often in advance of a likely violent encounter in order to avoid it altogether. The best way to protect one’s self is avoiding the situation in which she is forced to defend herself. Reinvent Your Personal Safety talks about the different ways this is possible, as well as about the best way to handle one’s self when violent confrontation simply cannot be avoided. This is for the high-school girl, for the grandmother, for the young professional, for the working mother – anyone who is willing to overcome their limiting beliefs about what they’re capable of and key into what self-protection is really about. In reality, knowledge of the appropriate action to take in any given situation is worth scores more than athleticism.

Revolution and War in Contemporary Ukraine - Olga Bertelsen 2016-10-01

What are the reasons behind, and trajectories of, the rapid cultural changes in Ukraine since 2013? This volume highlights: the role of the Revolution of Dignity and the Russian-Ukrainian war in the formation of Ukrainian civil society; the forms of warfare waged by Moscow against Kyiv, including information and religious wars; Ukrainian and Russian identities and cultural realignment; sources of destabilization in Ukraine and beyond; memory politics and Russian foreign policies; the Kremlin’s geopolitical goals in its 'near abroad'; and factors determining Ukraine’s future and survival in a state of war. The studies included in this

collection illuminate the growing gap between the political and social systems of Ukraine and Russia. The anthology illustrates how the Ukrainian revolution of 2013–2014, Russia's annexation of the Crimean peninsula, and its invasion of eastern Ukraine have altered the post-Cold War political landscape and, with it, the regional and global power and security dynamics.

The Unmasking Style in Social Theory - Peter Baehr 2019-05-20

This book examines the nature of unmasking in social theory, in revolutionary movements and in popular culture. Unmasking is not the same as scientific refutation or principled disagreement. When people unmask, they claim to rip off a disguise, revealing the true beneath the feigned. The author distinguishes two basic types of unmasking. The first, aimed at persons or groups, exposes hypocrisy and enmity, and is a staple of revolutionary movements. The second, aimed at ideas, exposes illusions and ideologies, and is characteristic of radical social theory since the eighteenth-century Enlightenment. The Unmasking Style in Social Theory charts the intellectual origins of unmasking, its shifting priorities, and its specific techniques in social theory. It also explores sociology's relationship to the concept of unmasking through an analysis of writers who embrace, adapt or reshape its meaning. Such sociologists include Vilfredo Pareto, Karl Mannheim, Raymond Aron, Peter Berger, Pierre Bourdieu, Luc Boltanski and Christian Smith. Finally, taking conspiracy theories, accusations of social phobia and new concepts such as micro-aggression as examples of unmasking techniques, the author shows how unmasking contributes to the polarization and bitterness of much public discussion. Demonstrating how unmasking is baked into modern culture, yet arguing that alternatives to it are still possible, this book is, in sum, a compelling study of unmasking and its impact upon modern political life and social theory.

The Hacker Ethos - True Demon 2015-12-20

Herein, you will find a comprehensive, beginner-friendly book designed to teach you the basics of hacking. Learn the mindset, the tools, the techniques, and the ETHOS of hackers. The book is written so that anyone can understand the material and grasp the fundamental techniques of hacking. Its content is tailored specifically for the beginner, pointing you in the right direction, to show you the path to becoming an elite and powerful hacker. You will gain access and instructions to tools used by industry professionals in the field of penetration testing and ethical hacking and by some of the best hackers in the world. ---------- If you are curious about the FREE version of this book, you can reed the original, first-draft of this book for free on Google Drive!
https://drive.google.com/open?id=0B78IWlY3bU_8RnZmOXczTUFEM1U

Social Engineering Penetration Testing - Gavin Watson 2014-04-11

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

The Cybersecurity Body of Knowledge - Daniel Shoemaker 2020-04-23

The Cybersecurity Body of Knowledge explains the content, purpose, and use of eight knowledge areas that define the boundaries of the discipline of cybersecurity. The discussion focuses on, and is driven by, the essential concepts of each knowledge area that collectively capture the cybersecurity body of knowledge to provide a complete picture of the field. This book is based on a brand-new and up to this point unique, global initiative, known as CSEC2017, which was created and endorsed by ACM, IEEE-CS, AIS SIGSEC, and IFIP WG 11.8. This has practical relevance to every educator in the discipline of cybersecurity. Because the specifics of this body of knowledge cannot be imparted in a single text, the authors provide the necessary comprehensive overview. In essence, this is the entry-level survey of the comprehensive field of cybersecurity. It will serve as the roadmap for individuals to later drill down into a specific area of interest. This presentation is also explicitly designed to aid faculty members, administrators, CISOs, policy makers, and stakeholders involved with cybersecurity workforce development initiatives. The book is oriented toward practical application of a computing-based foundation, crosscutting concepts, and essential knowledge and skills of the cybersecurity discipline to meet workforce demands. Dan Shoemaker, PhD, is full professor, senior research scientist, and program director at the University of Detroit Mercy's Center for Cyber Security and Intelligence Studies. Dan is a former chair of the Cybersecurity & Information Systems Department and has authored numerous books and journal articles focused on cybersecurity. Anne Kohnke, PhD, is an associate professor of cybersecurity and the principle investigator of the Center for Academic Excellence in Cyber Defence at the University of Detroit Mercy. Anne's research is focused in cybersecurity, risk management, threat modeling, and mitigating attack vectors. Ken Sigler, MS, is a faculty member of the Computer Information Systems (CIS) program at the Auburn Hills campus of Oakland Community College in Michigan. Ken's research is in the areas of software management, software assurance, and cybersecurity.