

## Piccolo Manuale Della Sicurezza Informatica Pocket

Tecnologia - saggio (12 pagine) - Può un algoritmo di memorizzazione univoca dei dati cambiare il nostro futuro? Blockchain lo sta già facendo: scoprire cos'è e come funziona è fondamentale Con questo piccolo manuale, grazie a un linguaggio semplice per neofiti, si esplora il mondo della blockchain, cercando di capire cosa sia, che utilizzi se ne posso fare e cosa ci riserva il futuro. Il manuale aiuta il lettore a districarsi in un argomento ostico, supportandolo a fissare bene alcuni concetti fondamentali e portandolo a conoscere il mondo delle criptovalute, in special modo i Bitcoin, applicazione pratica della blockchain e protagonisti dei futuri pagamenti online e reali. Nato a Roma, laureato in Chimica alla Università degli Studi di Roma La Sapienza, G.P. Rossi lavora nel campo delle Telecomunicazioni occupandosi di eSIM e di Digital Identity su progetti in ambito GSMA (GSM Association). È giornalista pubblicista, e scrive su Cor.Com, giornale che tratta di economia e innovazione digitale. Ha già pubblicato diversi racconti per la Giulio Perrone Editore, nelle antologie Il Desiderio, Al Bar, Il Sogno e ha anche scritto due ebook per la collana TechnoVisions di Delos Digital.

Perdere tutti i propri dati perché ci si è dimenticati di fare un backup. Non riuscire ad accedere a un servizio perché non si riesce a recuperare la password. Vedere il proprio account Facebook violato. Trovarsi con il PC inutilizzabile a causa di un virus.Quante volte ci si trova in situazioni simili?Questo libro aiuta i lettori a prevenire, con poche, semplici mosse, i problemi più comuni e li guida con linguaggio semplice e diretto alla soluzione delle situazioni critiche, aiutandoli a tirarsi fuori dai guai. Perché la sicurezza informatica non è qualcosa di astratto e lontano, ma un insieme di pratiche quotidiane che ci semplificano la vita.

Codice penale. Rassegna di giurisprudenza e di dottrina
Internet 2000
Come pesci nella rete
Manuale del contensioso in materia di codice della strada
Piccolo manuale della sicurezza informatica
A Guide for the Penetration Tester

Hacklog, Volume 2: Web Hacking è il secondo volume pensato per l'apprendimento della Sicurezza Informatica ed Ethical Hacking. È stato ideato per far in modo che tutti, sia i professionisti che i principianti, riescano ad apprendere i meccanismi e i metodi che stanno alla base degli attacchi ad Infrastrutture e Applicazioni nel World Wide Web. Hacklog, Volume 2: Web Hacking è un volume stand-alone: non è necessario aver letto il Volume 1, sebbene possa essere molto d'aiuto nelle fasi ritenute ormai consolidate (come l'uso di strumenti di anonimizzazione che precedono un attacco informatico). Non richiede particolari abilità o conoscenze e può essere letto da tutti, sia dall'appassionato che dall'esperto. In questo corso imparerai ad analizzare un'infrastruttura Web, a conoscerne le debolezze che si celano dietro errate configurazioni e a trovare e sfruttare vulnerabilità presenti nelle Web App di ogni giorno, esponendosi giornalmente al cyber-crimine della rete. Sarai in grado di creare un ambiente di test personalizzato in cui effettuare attacchi in tutta sicurezza e studiarne le caratteristiche, scrivere brevi exploit e infettare macchine; quindi, ti verrà insegnato come difenderti da questi attacchi, mitigando le vulnerabilità più comuni, e sanificare l'ambiente infetto. Hacklog, Volume 2: Web Hacking è un progetto rilasciato in Creative Commons 4.0 Italia, volto all'apprendimento e alla comunicazione libera per tutti. La versione cartacea è disponibile con fini promozionali e non ha nulla di diverso da quella presente in formato digitale, distribuita gratuitamente in rete. -- IMPORTANTE -- Leggi prima di acquistare: questo libro è disponibile gratuitamente in rete. La versione qui presente fa riferimento solo alla versione Kindle (obbligatoriamente imposto da Amazon a pagamento) e alla versione cartacea. Se vuoi puoi scaricare gratuitamente questo ebook direttamente sul nostro sito ufficiale. Acquistandolo, finanzierai il progetto e con esso i prossimi volumi. Attenzione: il corso Hacklog, Volume 2: Web Hacking prevede l’uso del Sistema Operativo Debian GNU/Linux. Se non hai mai utilizzato questo Sistema Operativo, ti consigliamo caldamente di seguire il breve corso introduttivo che lo riguarda scaricabile sul sito ufficiale www.hacklog.net. Gratuito, ovviamente.

Una panoramica completa sul mondo della sicurezza e certezza digitale. Qui trovi argomenti forse nuovi o forse no, sui quali tu e i tuoi clienti dovete avere maggiore lucidità. Temi affascinanti quali la conservazione sostitutiva e digitale, la fatturazione elettronica, la firma digitale, le firme elettroniche, la privacy, i processi digitali aziendali e la cartella clinica elettronica. Un libro per te che hai bisogno di comprendere quale sicurezza offra il mondo digitale che ti ruota attorno. Sai come conservare una PEC? Sei sicuro di archiviare correttamente tutti i documenti informatici che armeggia tra computer e smartphone? Come gestisci il tuo rapporto informatico con la sanità? Hai mai gestito una ricetta medica digitale o il tuo fascicolo sanitario elettronico? Nel momento in cui metti una firma elettronica avanzata su una tavoletta grafica alle Poste o in banca, devi essere cosciente dei tuoi diritti digitali. Diritti che probabilmente non sai di avere. Siamo circondati dall’avanguardia digitale ma ne sappiamo poco o nulla: questa guida ti aiuterà ad affrontare correttamente il radicale passaggio dalla carta ai bit. Volta pagina, non puoi più farne a meno!

Manuale delle macchine utensili
Guida per non essere le sardine di Internet
L'arte digitale. Lezioni di lettura informatica delle immagini
Manuale di informatica giuridica e diritto delle nuove tecnologie
Monografie
The Art of Deception

Ciao mi chiamo **Fernando**, sono un **web developer full stack**, **analista in cybersecurity** e laureato in **ing. informatica**, vi guiderò in questo primo percorso di **sicurezza infozmatica** con concetti di **ethical hacking**. **Hackerpunk** è un corso interattivo di **informatica avanzata** che parte da **livello 2** come giusto che sia quando si parla di questa tipologia di percorsi. Nel spiegare concetti di **ethical hacking** si danno spesso per scontato le basi del **network** importantissime per comprendere questi argomenti, io ho cercato ugualmente di racchiuderli all'interno dell'opera editoriale e ho scelto **amazon kindle** per condividere con voi tutta la mia esperienza nel campo, facilitando oltremodo la comprensione, mediante l'utilizzo della tecnologia **Qr**. Per lo scopo ho pensato di collegare i capitoli del manuale con i **videotutorial** sul mio canale **gratuito youtube** che d'altronde è in continuo aggiornamento. Vi basterà scaricare dallo store una semplice applicazione **android/ios** sul vostro **smartphone** e quando richiesto scansionare il codice **Qr** di fine capitolo, per essere reindirizzati subito dopo sul **videotutorial** di riferimento, estendendo la comprensione con la pratica ma anche con la grafica, attraverso le presentazioni animate. **Hackerpunk** è totalmente legale, verranno trattati argomenti etici e altamente professionali che fanno parte della vita lavorativa di figure come quella del **pentester** o dell'It admin aziendale. L' **ethical hacking** è ancora da molti considerato inconsapevolmente come **pirateria** perché utilizza conoscenze informatiche per violare o far crashare i sistemi, purtroppo non è così anzi è il contrario, tutte queste tecniche vengono utilizzate legalmente sotto un contratto per aumentare il grado di sicurezza di questi sistemi benché ci sia l'autorizzazione del proprietario del sistema, in effetti l' **ethical hacker** è una figura lavorativa ben inquadrata nel campo **IT** (**information technology**). **Hackerpunk** è rivolto a coloro che vorranno raffinare le proprie conoscenze nel campo della **sicurezza informatica** o chi vorrà iniziare a farne parte, in questo volume tratteremo i concetti base del **network**, entreremo nelle modalità di **anonimato digitale** e vedremo le prime fasi del **pentesting**, affrontando gia' da subito la fase della ricerca di informazioni sugli obbiettivi da testare. Essa coincide con la prima fase del **pentesting** chiamata "**Information gathering**". Nonostante la mole di argomenti da trattare non verranno tralasciate le sessioni pratiche grazie ai laboratori di **kali linux** che svolgeremo in ambito virtuale. La **playlist youtube** "**#Navigare in incognito**" è associata al primo volume unitamente al secondo che uscirà prossimamente. La collana editoriale si comporrà in totale di 3 volumi: **hackerpunk vol 1** - "**Profiling**" (livello 1) **hackerpunk vol 2** -"**Intrusioni e pentesting** " (livello 2) **hackerpunk vol 3** -"**Exploiting e web hacking**" (livello 3) **Lasciate un like** sul mio canale **youtube**, **iscrivetevi per essere sempre aggiornati** sulle novità delle **Playlist**. sito web: **https://hackerpunk.it** contatti: **ultimock@gmail.com** @instagram **https://www.instagram.com/hackerpunk2019/** @linkedin **https://www.linkedin.com/mwlite/in/fernandoc-364ab419a** @youtube **https://www.youtube.com/channel/UCiAAq1h\_ehRaw3gi09z1RoQ**

**First comprehensive study of Italy's "art police", an organisation devoted to protecting cultural artefacts.**

**Maia**
**Saving the World's Heritage**
**Rete in Sicurezza**

**Manuale interattivo di Ethical Hacker e Sicurezza informatica**
**Manuale di logistica**
**The Carabinieri Command for the Protection of Cultural Property**

**Da una recensione del TGI RAI: «Internet è una realtà in continua evoluzione, logico quindi che il più famoso manuale della rete, edito da Laterza, sia giunto felicemente alla quarta edizione con l'arrivo del 2000. Gli autori sono, come sempre, Marco Calvo, Fabio Ciotti, Gino Roncaglia e Marco Zela. Come per le precedenti edizioni, il testo del manuale è disponibile gratis e in forma integrale sul sito internet della casa editrice Laterza. Ma con Internet 2000 per la prima volta viene anche allegato al libro un CDROM, arricchito da filmati e animazioni che aiutano a capire meglio programmi e procedure. Un libro su tre supporti dunque: carta stampata, CDROM e sito Internet. Una scelta coraggiosa perché sfida i soliti luoghi comuni sulla rivalità tra le rete e la stampa, e anche molto gradita dai lettori che possono così approfondire la propria conoscenza della rete nei tempi e nei modi che più preferiscono».**

**Alessandro Curioni è uno dei maggiori esperti di cybersicurezza in Italia, Bianca è sua fi gli** e, a tutti gli effetti, una “nativa digitale”. Nel 2017 il rapporto tra genitori e fi gli viaggia anche attraverso una connessione wi-fi . **Internet non è mai stato un luogo così poco “virtuale” e così tanto “reale”. Eppure mamme e papà sono spesso all'oscuro delle più banali regole di sicurezza su Internet, mentre i figli, fin troppo abili, restano vittime dell'ingenuità dei loro anni. Al giorno d'oggi, la rete si colloca al centro di un nuovo dibattito dove genitori e fi gli possono condividere le loro esperienze - e le loro debolezze - per affrontare insieme gli spiacevoli inconvenienti della navigazione on line. Dopo Come pesci nella rete e La privacy vi salverà la vita, Alessandro Curioni prosegue il ciclo di pubblicazioni dedicate al tema della sicurezza su Internet e ai pericoli del web con un manuale, scritto con il contributo fondamentale di Bianca, che spiega in modo divertente come unire il meglio delle due visioni - quella degli adulti e quella dei ragazzi - per affrontare in tutta serenità e responsabilmente gli sconfi nati mari del web.**

**Blockchain**
**ECDL Open il manuale. Syllabus 4.0. Linux. OpenOffice.org. Mozilla**
**manuale per l'uso della rete**
**Computer crime. Manuale di criminologia informatica**
**Information security: risk assessment, management systems, the ISO/IEC 27001 standard**
**La privacy vi salverà la vita!**

I numeri dicono molto: in Italia si parla di 25 mila furti d ' identit à e 11 mila reati informatici denunciati ogni anno, oltre 100 mila vittime di virus informatici, mentre un milione di nuovi malware appaiono su Internet ogni giorno. Forse non dobbiamo chiederci se potrebbe capitarci, ma quando. Utilizzando un linguaggio che mette in soffi tta il gergo tecnico e informatico, l ' autore affronta il tema dei rischi connessi all ' utilizzo delle nuove tecnologie. Alternando brevi racconti a consigli pratici, il libro conduce il lettore attraverso un viaggio nel lato oscuro del Paese delle Meraviglie e nella mente dei nuovi criminali del web. Storie che aiutano a evitare il peggio e ci preparano ad affrontarlo con il giusto autocontrollo. Un libro unico nel suo genere, che rende comprensibile la sicurezza informatica ai non addetti ai lavori e potrebbe farvi sorridere degli altri e magari di voi stessi, cosa che accadr à di sicuro se per caso siete " del mestiere " e sapete perfettamente che potreste scoprire da un momento all ' altro di essere diventati una vittima.

Il Manuale Essential Cyber Security è una grande risorsa ovunque tu vada; presenta la ricerca di punta pi ù attuali e di primo piano per la sicurezza e la sicurezza del sistema. Non è necessario essere un esperto di sicurezza informatica per proteggere le informazioni.Ci sono persone l à fuori che ha il compito principale che sta cercando di rubare le informazioni personali e finanziarie. Sei preoccupato per la vostra sicurezza online, ma non sai da dove cominciare? Quindi, questo manuale vi dar à , studenti, studiosi, scuole, imprese, aziende, governi e decisori tecnici le conoscenze necessarie per prendere decisioni informate in materia di sicurezza informatica a casa o al lavoro. 5 Domande CEO deve chiedere rischi informatici, 8 maggior parte dei problemi comuni Internet Security si possono affrontare, evitare violazione del copyright, evitando Social Engineering e attacchi di phishing, evitando le insidie del trading online, banking Online Protette, sicurezza di base Concetti, Fondamenti di Cloud Computing, prima di collegare un nuovo computer a Internet, utili e rischi di servizi di posta elettronica gratuiti, i benefici di BCC, Navigando in sicurezza - intesa contenuto attivo e biscotti, la scelta e la protezione di password, rischi comuni di utilizzo di applicazioni aziendali nel cloud, coordinamento Virus e Spyware difesa, Cybersecurity per dispositivi elettronici, Opzioni di backup dei dati, affrontare i cyber, Sfatare alcuni miti comuni, Difendere telefoni cellulari e PDA contro l'attacco, Eliminazione dei dispositivi di modo sicuro, efficace cancellazione di file, Valutazione delle impostazioni di sicurezza vostro web browser, buona sicurezza abitudini, Linee guida per la pubblicazione di informazioni online, Movimentazione distruttivo malware, vacanza itinerante con i dispositivi di Internet personali, computer di casa e la sicurezza di Internet, come Anonymous Are You, Come fermare la maggior parte del adware cookie traccianti Mac, Windows e Android, Identificazione Hoaxes e Urban Legends, Keeping bambini Safe online, giocare sul sicuro - evitare i rischi di gioco online, Preparati per Heightened Phishing rischio fiscale stagione, prevenire e rispondere al furto di identit à , privacy e sicurezza dei dati, proteggere il vostro posto di lavoro, Protezione dati aggregati, la protezione dei dispositivi portatili - Sicurezza dei dati, Protezione portatile dispositivi - Sicurezza fisica, Protezione della Privacy, i leader Domande Bank, avvertenze del mondo reale a tenervi a salvo linea, riconoscere ed evitare truffe e-mail, riconoscere ed evitare Spyware, riconoscendo Gli antivirus falsi, Ripristino da un cavallo di Troia o virus, Recupero da virus, worm , e cavalli di Troia, riducendo Spam, alla revisione degli accordi con l'utente finale di licenza, i rischi di File-Sharing tecnologia, la salvaguardia dei dati, sicurezza dei dati Iscrizione nelle liste elettorali, reti wireless fissante, Protezione della rete di casa, Shopping sicuro online, piccolo ufficio o router domestico Ufficio Sicurezza, Comunicazione saldamente - Utilizzando Social Networking Services, Contratti di licenza software - ignorare a proprio rischio, spyware casa, protezione in siti di social networking, Integrando le password, i rischi di utilizzo di dispositivi portatili, le minacce per i telefoni cellulari, la comprensione e proteggerci contro sistemi di moneta Mule, Capire Software Anti-Virus, Capire la tecnologia Bluetooth, Capire Denial-of-service, la comprensione Firme digitali, crittografia intesa, sui firewall, comprendere le minacce nascoste - rootkit e botnet, la comprensione minacce nascoste file danneggiati Software, la comprensione di dominio internazionalizzati nomi, Comprendere gli ISP, Capire le patch, intesa Voice over Internet Protocol (VoIP), la comprensione certificati dei siti Web, la comprensione del computer - client di posta elettronica, la comprensione del computer - Sistemi operativi, Conoscere il computer - Browser Web, Usare cautela con allegati e-mail, Usare Attenzione con drive USB, Utilizzo di Instant Messaging e Chat Rooms in modo sicuro, utilizzando la tecnologia senza fill in modo sicuro, perch é è Cyber Security un problema, perch é sicura del browser, e Glossario della sicurezza informatica Termini. un grazie alla mia meravigliosa moglie Beth (Griffo) Nguyen e il mio figli sorprendenti Taylor Nguyen Nguyen e Ashton per tutto il loro amore e sostegno, senza il loro sostegno emotivo e di aiuto, nessuno di questi libri elettronici in lingua educativi e audio sarebbe possibile.

L'Informazione bibliografica
Internet, social, chat e altre mortali amenit à
Internet 2004. Manuale per l'uso della rete
Manuale di commercio elettronico per piccole e medie imprese
Privacy in azienda. Manuale di formazione per titolari, responsabili e incaricati
Questa casa non è un hashtag!
Hacklog, Volume 1: Anonimato è il primo dei nostri corsi pensati per l’apprendimento della Sicurezza Informatica ed Ethical Hacking. È stato ideato per far in modo che tutti, sia i professionisti che i principianti, riescano ad apprendere i meccanismi e i metodi che stanno alla base dell’Anonimato. Abbiamo scelto di iniziare con l’Anonimato appunto perché è un tema molto attuale ed applicabile da chiunque, che non richiede particolari abilità e che si può applicare in ogni realtà, sia privata che aziendale. Attenzione: il corso Hacklog, Volume 1: Anonimato prevede l’uso del Sistema Operativo Debian GNU/Linux. Se non hai mai utilizzato questo Sistema Operativo, ti consigliamo caldamente di seguire il breve corso introduttivo che lo riguarda. Gratuito, ovviamente. Nel corso imparerai a utilizzare metodi di anonimato semplici e complessi, a cifrare le tue informazioni in rete e i tuoi dati nel computer, a navigare nel Deep Web in maniera sicura e a riconoscere i rischi che si corrono navigando in Internet. Conoscerai metodi reali, applicati sia dai professionisti che dai malavitosi, per nascondere le tracce in rete; lo scopo finale di questo corso è quello di fare chiarezza sugli strumenti a disposizione di tutti, liberamente in rete. Con il percorso che ti consigliamo, sarai in grado anche di comandare un intero Sistema Operativo a base GNU/Linux tramite una distribuzione Debian, attualmente la più popolare nei computer ad uso casalingo e server. Ciò aiuterà a formarti in vista dei prossimi volumi e anche nella vita professionale di un esperto del settore Informatico. Dalla rassegna stampa: «Internet, si sa, è un universo sterminato; non è dunque poi così raro che succeda di pensare di conoscerla a fondo e di sapersi muovere al suo interno con agilità, per poi scoprire che in realtà ci si limita a un suo utilizzo superficiale e ripetitivo. Questo manuale - giunto oramai alla sua sesta edizione e divenuto uno strumento diffusissimo e apprezzatissimo - aiuta così a trasformarsi da semplici navigatori a "utilizzatori consapevoli e produttivi della Rete", unendo una trattazione più prettamente tecnica (i software, le risorse della Rete, i meccanismi del suo funzionamento) a un discorso "culturale" più generico che faciliti la comprensione di Internet come veicolo per la "creazione, la distribuzione e la condivisione di conoscenze».

Conosci e proteggli la tua sicurezza informatica: Fai luce sul lato oscuro del digitale e gestisci serenamente i tuoi dati

ECDL il manuale. Syllabus 4.0. Windows XP. Office XP. Con CD-ROM

Manuale pratico delle notificazioni. Con CD-ROM

Controlling the Human Element of Security

Bibliografia nazionale italiana

Manuale di notariato

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.

" Stiamo morendo per eccesso di informazioni " è una frase di Federico Zerì che oggi appare profetica. Al cospetto di una Rete sconfinata che non dimentica nulla, continuiamo a riversare su web, chat on line e social media pezzi della nostra vita, con conseguenze imprevedibili e non di rado tragiche. Ricatti, vendette, umiliazioni pubbliche, furti di identità sono cronaca quotidiana sul web e spesso i colpevoli sono le stesse vittime, incapaci di trattenerne il desiderio di trovare un posto al sole su Internet. Un atteggiamento favorito da un sistema in cui la vera merce sono proprio i dati e le informazioni che vengono venduti e scambiati più o meno legalmente. L ' unica salvezza sembra essere la riscoperta del valore della propria privacy, che diventa il tema centrale di questo libro, in cui l ' autore, attraverso racconti, a volte drammatici altre esilaranti, spiega come e perché tutelare la nostra vita privata non è un diritto, ma un dovere; come esistano leggi e regolamenti in materia e di quelle volte in cui mettiamo in pericolo anche gli altri.

piccolo manuale delle indagini digitali

Linux. Manuale per l'amministratore di sistema

Manuale sulla Sicurezza Informatica e Hacking Etico

Manuale Essenziale di Cyber Security in italiano

Genitori e figli su internet senza rete

Il manuale del giovane hacker. Tutto quello che avreste voluto sapere su internet e nessuno vi ha mai detto

***Modern cars are more computerized than ever. Infotainment and navigation systems, Wi-Fi, automatic software updates, and other innovations aim to make driving more convenient. But vehicle technologies haven’t kept pace with today’s more hostile security environment, leaving millions vulnerable to attack. The Car Hacker’s Handbook will give you a deeper understanding of the computer systems and embedded software in modern vehicles. It begins by examining vulnerabilities and providing detailed explanations of communications over the CAN bus and between devices and systems. Then, once you have an understanding of a vehicle’s communication network, you’ll learn how to intercept data and perform specific hacks to track vehicles, unlock doors, glitch engines, flood communication, and more. With a focus on low-cost, open source hacking tools such as Metasploit, Wireshark, Kayak, can-utils, and ChipWhisperer, The Car Hacker’s Handbook will show you how to: -Build an accurate threat model for your vehicle -Reverse engineer the CAN bus to fake engine signals -Exploit vulnerabilities in diagnostic and data-logging systems -Hack the ECU and other firmware and embedded systems -Feed exploits through infotainment and vehicle-to-vehicle communication systems -Override factory settings with performance-tuning techniques -Build physical and virtual test benches to try out exploits safely If you’re curious about automotive security and have the urge to hack a two-ton computer, make The Car Hacker’s Handbook your first stop.***

***Connessioni attive 24 ore su 24, il mobile come piattaforma primaria per il Web, social network perennemente presenti. Oggi, farsi gli affari altrui è diventato quasi un gioco da ragazzi e poco importa che molti servizi abbiano adottato robusti sistemi di protezione: spesso i principali nemici della nostra privacy siamo noi stessi. Usare motori di ricerca come Google per recuperare informazioni particolari, scoprire la provenienza geografica di un utente della rete Internet, analizzare le relazioni nei social network, sfruttare funzionalità di Facebook per ricerche non convenzionali, capire se un’immagine è artefatta, entrare nel mondo dei software-spia, imparare come monitorare account WhatsApp, mettere in atto trucchi tecno-psicologici per rendere il tutto più credibile: ecco come un malintenzionato può setacciare la nostra vita. Questo manuale insegna questo e molto altro: senza la pretesa di diventare un hacker o un investigatore informatico, il lettore impara alcune delle più efficaci tecniche di spionaggio e soprattutto cosa è possibile fare per proteggersi.***

***Manuale di economia e organizzazione aziendale***

***Manuale pratico dell'ufficiale d'anagrafe. Con CD-ROM***

***Spia nella Rete***

***ECDL il manuale con Atlas. Windows XP. Office XP. Syllabus 4.0. Con CD-ROM***

***Hacklog, Volume 2: Web Hacking***

***Hackerpunk 1 vol. "Profiling"***

In this book, the following subjects are included: information security, the risk assessment and treatment processes (with practical examples), the information security controls. The text is based on the ISO/IEC 27001 standard and on the discussions held during the editing meetings, attended by the author. Appendixes include short presentations and check lists.

CESARE GALLOTTI has been working since 1999 in the information security and IT process management fields and has been leading many projects for companies of various sizes and market sectors. He has been leading projects as consultant or auditor for the compliance with standards and regulations and has been designing and delivering ISO/IEC 27001, privacy and ITIL training courses. Some of his certifications are: Lead Auditor ISO/IEC 27001, Lead Auditor 9001, CISA, ITIL Expert and CBCI, CIPP/e. Since 2010, he has been Italian delegate for the the editing group for the ISO/IEC 27000 standard family. Web: www.cesaregallotti.it.

La posta elettronica,le chat,i motori di ricerca,Windows XP, bambini e genitori in rete,la sicurezza.

Hacklog Volume 1 Anonimato

Applicazioni di qualità, ambiente, sicurezza nelle aziende. Secondo il programma EQDL. La patente europea della qualità. Con CD-ROM

Essential Cyber Security Handbook In Italian

The Car Hacker's Handbook

*Piccolo manuale della sicurezza informatica*Apogeo Editore