

1. Record Nr.	UNISA990000411140203316
Autore	GRIFFIN, David Ray
Titolo	11 settembre : cosa c'è di vero nelle "teorie del complotto" / David Ray Griffin ; prefazione all'edizione statunitense di Richard Falk ; prefazione all'edizione inglese di Michael Meacher ; traduzione di Giuseppina Oneto
Pubbl/distr/stampa	Roma, : Fazi, 2004
ISBN	88-8112-554-4
Descrizione fisica	XII, 288 p. ; 23 cm
Collana	Le terre ; 85
Disciplina	973.931
Soggetti	Terrorismo - Stati Uniti d'America - 2001 Strage - New York - 2001
Collocazione	X.3.B. 3663
Lingua di pubblicazione	Italiano
Formato	Materiale a stampa
Livello bibliografico	Monografia

2. Record Nr.	UNINA9910734821803321
Autore	Dudek Micha (Lawyer)
Titolo	Courtroom Power Distance Dynamics // by Micha Dudek, Mateusz Stpie
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
ISBN	3-030-66984-X
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (xii, 295 pages) : illustrations
Collana	Law and Visual Jurisprudence, , 2662-4540 ; ; 3
Disciplina	347.012
Soggetti	Law - Philosophy Law - History Theories of Law, Philosophy of Law, Legal History Philosophy of Law
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	1 Introduction -- 2 Courts, Courtrooms and Power Distance -- 3 Judge-Witness Courtroom Power Distance Dynamics -- 4 Subjective Power Distance and Opinions on Judges -- 5 Conclusion.
Sommario/riassunto	The book presents a comprehensive reconceptualization of Geert Hofstede's well-known concept of power distance, applying the theory to the specific case of judge–witness courtroom interactions in Polish regional courts. In the light of the detailed critique of Hofstede's original approach to power distance, the book first carefully develops a three-level concept of power distance, including personal preferences concerning the realization of power relations (subjective level); rules, practices and spatio-architectural arrangements underlying power relations (organizational level); and individual demeanors that can, in practice, increase or decrease the asymmetry between parties to a power relation (interactional level). This reconceptualization provides a universal conceptual apparatus that is applicable to various social settings, but the authors have used it in extensive qualitative and quantitative research focused on courtroom interactions. After laying the theoretical foundations, the book details the elements of judge–witness courtroom interactions (both verbal and non-verbal) that contribute to establishing power distance between judge and witness.

These were identified over 6 months of observational research conducted in 2018 in the Kraków regional courts. Lastly, the book addresses the issue of the relationship between the subjective level of power distance and opinions that laypeople can have concerning a judge's demeanor in the courtroom environment. To do so, it describes specific quantitative research that involved the creation of original film clips depicting witness questioning by the judge in a courtroom in three power distance situations. Offering a coherent framework for examining various interpersonal relations in legal contexts and illustrating how the framework can be applied on the courtroom interactions example, the book will appeal to a wide range of legal practitioners and academics. It also allows scientists outside the legal field to gain a new and broad understanding of power distance that they can easily apply in their respective fields. Furthermore, it provides non-academics with insights into courtroom interactional dynamics, as exemplified by the discussion of Polish judicial practice.

3. Record Nr.

Autore

Titolo

Pubbl/distr/stampa

UNINA9910300464403321

Bachrach Daniel G.

10 don'ts on your digital devices : the non-techie's survival guide to cyber security and privacy / / Daniel G. Bachrach, Eric J. Rzeszut

[New York, NY] : , : Apress, , [2014]

New York, NY : , : Springer Science+Business Media

©2014

ISBN

9781484203675

1484203674

Descrizione fisica

1 online resource (xxvi, 150 pages) : illustrations

Disciplina

004

005.82

Soggetti

Data protection

Data encryption (Computer science)

Lingua di pubblicazione

Inglese

Formato

Materiale a stampa

Livello bibliografico

Monografia

Note generali

Includes bibliographical references and index.

## Nota di contenuto

Contents; Introduction; Chapter 1: Don't Get Phished; A Closer Look at "Phishing"; "Target"-ed Phishing; Other Forms; What Should You Do?; Additional Reading; Chapter 2: Don't Give Up Your Passwords; Where Did Passwords Come From?; Password Threats and New Solutions; Alternatives to the "Simple" Password: Biometrics and Two-Factor Authentication; Bigger Can Be Better. . .; Mix It Up; Protecting Passwords; What Should You Do?; Additional Reading; Chapter 3: Don't Get Lost in "The Cloud "; What Is "The Cloud"?; Cloud Controversy and Risks; Formalizing an Informal Relationship; Data Breaches Not Just for Storage AnymoreReliability; Accessibility; What Should You Do?; Additional Reading; Chapter 4: Don't Look for a Free Lunch; Software-Consider the Source; Issues with Warez; Hidden Agenda; Lesser Threats; How to Protect Yourself; Additional Reading; Chapter 5: Don't Do Secure Things from Insecure Places; Background: Wireless Networking at Home, at Work, and on the Road; Home Sweet Home. . .; Back at the Office. . .; On the Road Again. . .; Encryption Standards; VPN; Workplace Security, on the Road; Extra Layers of Protection; Other Uses for VPNs; Additional Reading Chapter 6: Don't Let the Snoops InWho Are the "Snoops"?; Boundless Informant; PRISM; Tempora; MUSCULAR; FASCIA; Dishfire; Optic Nerve; So, Who Else Is Snooping?; For-Profit Corporations; Employers; Where Your Data Are...; Data on the Move; Taking an Active Role in Protecting Your Data; Data at Rest; Additional Reading; Chapter 7: Don't Be Careless with Your Phone; Mobility in the 21st Century; When It's the Employee's Device, but the Company's Resources-BYOD; When It's the Company's Device, but Used at the Employee's Discretion-COPE; Know Your Rights; Physically Securing Your Phone Start Me Up-but Not Without a PasswordWhen a Password Isn't Enough; Losing (and Finding!) the Key to Your Digital Life; Mobile Law; Insecure Background Wireless Networks; Don't Trust a Wireless Network Based on Its Name; Don't Trust Your Phone to Connect for You; Bluetooth Hacking; Malware Apps; Operating System Updates; Additional Reading; Chapter 8: Don't Use Dinosaurs; Software: It Has an Expiration Date; The "Good Old Days" of Software; New Software for a New Era; Don't Forget About Mobile Apps; Windows XP; Not Just Windows; Not Just Operating Systems; Not Just Desktops and Laptops What Can You Do?Additional Reading; Chapter 9: Don't Trust Anyone Over... Anything; What Is Social Engineering?; Keep Your Eye on the Ball; Hooking the Phish; Social Engineering via Social Networking; Knowledge Is Power; Big Companies, Big Problems; Ransomware; In-Person Tricks; Not Your Mother's Kind of Tailgating; How to Combat Social Engineering; Additional Reading; Chapter 10: Don't Forget the Physical; Physical Security: An Overview; Physical Security at Home; Letting Outsiders In; Removing Temptation; Don't Blanket the Neighborhood with Wi-Fi; Physical Security at Work Limit Your Paper (or Whiteboard) Trails

## Sommario/riassunto

In nontechnical language and engaging style, 10 Don'ts on Your Digital Devices explains to non-techie users of PCs and handheld devices exactly what to do and what not to do to protect their digital data from security and privacy threats at home, at work, and on the road. These include chronic threats such as malware and phishing attacks and emerging threats that exploit cloudbased storage and mobile apps. It's a wonderful thing to be able to use any of your cloud-synced assortment of desktop, portable, mobile, and wearable computing devices to work from home, shop at work, pay in a store, do your banking from a coffee shop, submit your tax returns from the airport, or post your selfies from the Oscars. But with this new world of connectivity and convenience comes a host of new perils for the lazy,

the greedy, the unwary, and the ignorant. The 10 Don'ts can't do much for the lazy and the greedy, but they can save the unwary and the ignorant a world of trouble. 10 Don'ts employs personal anecdotes and major news stories to illustrate what can—and all too often does—happen when users are careless with their devices and data. Each chapter describes a common type of blunder (one of the 10 Don'ts), reveals how it opens a particular port of entry to predatory incursions and privacy invasions, and details all the unpleasant consequences that may come from doing a Don't. The chapter then shows you how to diagnose and fix the resulting problems, how to undo or mitigate their costs, and how to protect against repetitions with specific software defenses and behavioral changes. Through ten vignettes told in accessible language and illustrated with helpful screenshots, 10 Don'ts teaches non-technical readers ten key lessons for protecting your digital security and privacy with the same care you reflexively give to your physical security and privacy, so that you don't get phished, give up your password, get lost in the cloud, look for a free lunch, do secure things from insecure places, let the snoops in, be careless when going mobile, use dinosaurs, or forget the physical—in short, so that you don't trust anyone over...anything. Non-techie readers are not unsophisticated readers. They spend much of their waking lives on their devices and are bombarded with and alarmed by news stories of unimaginably huge data breaches, unimaginably sophisticated "advanced persistent threat" activities by criminal organizations and hostile nation-states, and unimaginably intrusive clandestine mass electronic surveillance and data mining sweeps by corporations, data brokers, and the various intelligence and law enforcement arms of our own governments. The authors lift the veil on these shadowy realms, show how the little guy is affected, and what individuals can do to shield themselves from big predators and snoops.

---