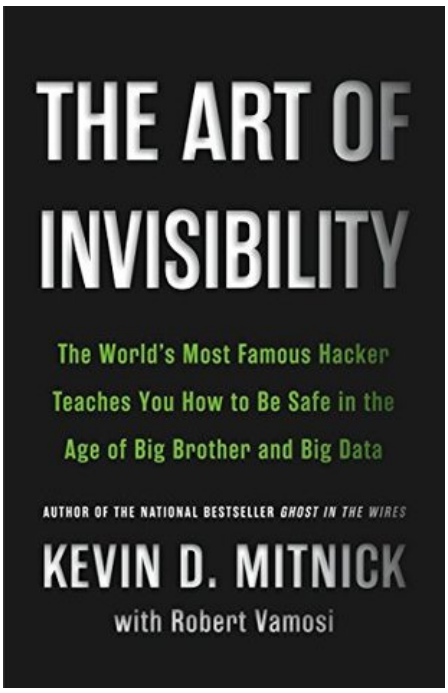

The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data

Kevin D. Mitnick

Download now

Read Online

The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data

Kevin D. Mitnick

The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data Kevin D. Mitnick
Kevin Mitnick, the world's most famous hacker, teaches you easy cloaking and counter-measures for citizens and consumers in the age of Big Brother and Big Data.

Like it or not, your every move is being watched and analyzed. Consumer's identities are being stolen, and a person's every step is being tracked and stored. What once might have been dismissed as paranoia is now a hard truth, and privacy is a luxury few can afford or understand.

In this explosive yet practical book, Kevin Mitnick illustrates what is happening without your knowledge--and he teaches you "the art of invisibility." Mitnick is the world's most famous--and formerly the Most Wanted--computer hacker. He has hacked into some of the country's most powerful and seemingly impenetrable agencies and companies, and at one point he was on a three-year run from the FBI. Now, though, Mitnick is reformed and is widely regarded as *the* expert on the subject of computer security. He knows exactly how vulnerabilities can be exploited and just what to do to prevent that from happening.

In THE ART OF INVISIBILITY Mitnick provides both online and real life tactics and inexpensive methods to protect you and your family, in easy step-by-step instructions. He even talks about more advanced "elite" techniques, which, if used properly, can maximize your privacy. Invisibility isn't just for superheroes--privacy is a power you deserve and need in this modern age.

The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data Details

Date	:	Published February 14th 2017 by Little, Brown and Company
ISBN	:	
Author	:	Kevin D. Mitnick
Format	:	Kindle Edition 285 pages
Genre	:	Nonfiction, Science, Technology, Computer Science, Computers

Download The Art of Invisibility: The World's Most Famous H ...pdf

Read Online The Art of Invisibility: The World's Most Famous ...pdf

Download and Read Free Online The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data Kevin D. Mitnick

From Reader Review The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data for online ebook

Travis says

This is a lot of material, and obviously most of it won't apply to most people, but it's a fascinating look into just how much we take for granted in today's world of electronic devices. This is a good reference for anyone who wants to learn about technology in general, or the internet specifically, and if it teaches even a few people to be a bit less free with their personal information, then I think the author would consider writing the book time well spent.

Youghourta says

???? ????? ?? ??????? ??????? ????? ??????? ??? ??????? ??? ???? ??? ???????? ???? ??? ???? ???? ??????? ??????? ???? ???.

???? ??? ?? ????? ?????? ??? ??"????" ??? ?????? ??? ?? ??????? ????? ????????? ???? ???????? ?????? ??? ?????? ????? ????? ?????? ?? ???????? ???? ?? ?? ????? ????? ??????? ??????? ???? ?????? ?? ??? ???? ?? ???? ?? ???? ???????? ??? ???????? ?? ??? ?????? ??? ???????.
??????? ???? ??????? ?????? ?? ???? ??? ??????? ????? ??????? ??? ?? ???? ????? ?? ??? ??????? ???????? ??? ?? ??? ???? ???? ????? ?????? ??? ??? ???? ???? ???? ??? ?????? ??????? ????? ?????? ???????? ?????? ??????? ?????? ??????? ??????? ?? ??? ??? ??? ???? ???? ????? ????? ?????? ???????? ?? ??? ????? ???? ???????? ?? ???? ?????? ?? ??? ??????? ?? ?????? ???????? ?? ????? ?? ???? ??? (??? ??? ??? ???????) ????? ??????? ???? ?? ????? ????? ????.

??????? ???? ???? ??? ?? ?????? ?? ?? ??????? ?????? ??? ??? ???????? ??? ????? ???? ???? ??? ??? ???? ??????? ????? ?????? ?? ????? ??? ???????? ????????? ?????????? ?? ????????? ????? ?? ??????? ???? ???? ????? ?????????. ?? ???? ????? ????? ???? ?????? ??? ?? ?????? ??? ??? ?????? ??? ???? ???????.

??????? ??????? ?? ?????? ??? ???????? ???????? ???? ????? ?????? ?????? ?? ?????? ???????? ????? ?? ???? ?? ??? ????? ????? ??????? ??????? ??? ????????. ??? ?? ??? ??????? ?? ???? ?????? ??? ???? ????????? ??? ??? ?????? ?? ?????? ???????? ????? ??? ?? ???? ???????? ???? ?? ????? ??? ???????? ??????? ?? ??? ?? ???? ??????????? ????? ?? ?????? ????? ?? ?? ??? ??????? ??????.

????? ?????? ????????? ?????? ?????? ??? ??? ?????? ????????? ???????? ???????? ?? ?? ???? (????? ??????? ??? ???? ??????? ???????) ???????? ????? ????? ?????? ??????? ????? ???????? (?????? ?????? ??????? ???????????) ?????? ??????? ??? ???????? ?? ?? ?? ?? ?????? ????? ??? ????? ?????? ??????? ????? ?? "?????" ???? ????? ???? ???? ??????? ????????? ?????? ?????? ??? ??? ???.
??? ????? ????? ??? ????? ???? ?? ???? ??? ???? ?? ?? ?? ??????? ??????? ???????? "?? ?? ??" ??? ??????? ????????? ?? ????? ????? ?? ????? ????? ??? ??? ?????????? ?? ??? ????? ???? ????? ??? ??? ??? ?????? ?????. ????? ??? ????? ??????? ??????? ??????? ?? ??? ???? ?? ?????? ????????? ???? ??????? ?? ?????.

?????? ???? ?? ??? ???? ??????? ????? ??????? ???? ?????? ?????????? ????????? ??????? ????? ????? ???????? ??????? ??? ?? ????? ???????? ?? ??? ??? ?? "???? ???? ???????" ?? ?? ??? ?????? ??? ?????? ?????? ?????.

Chad Warner says

Packed with strategies and tactics for increasing your digital security and privacy. It instills a privacy mindset. Each chapter raises awareness by explaining some privacy challenges in a not overly-technical way, usually with specific examples or stories, then gives instructions and advice on how to protect your privacy in the face of those challenges.

Average computer and phone users will likely be overwhelmed; this book is most useful to those whose tech-savviness is above average.

You'll quickly learn that the title of Chapter 14 is very true: obtaining anonymity is hard work. Mitnick explains that, "A persistent attacker will succeed given enough time and resources. … All you are really doing by trying to make yourself anonymous is putting up so many obstacles that an attacker will give up and move on to another target."

Mitnick says Rule #1 is "To be invisible online, you more or less need to create a separate identity, one that is completely unrelated to you. … you must also rigorously defend of the separation of your life from that anonymous identity."

Even though the book offers a wealth of privacy-protecting measures, you can still benefit by acting on a subset of them. It's not an all-or-nothing proposition.

I read this because I've been interested in digital security and privacy all my adult life, and that interest has grown lately.

Notes
Your Password Can Be Cracked
Haveibeenpwned.com will tell if you have compromised accounts.

Use passwords of 20-25 random characters.

Use password manager (Mitnick likes Password Safe and KeePass that run locally and aren't cloud-connected).

Use a PIN of more than 4 characters to lock your phone. 7 characters is good. Use letters and numbers if phone allows.

If you use a lock pattern, use a complex, non-obvious pattern.

Phone biometrics are vulnerable, so use as a 2nd, not only, factor.

Provide creative (or false) answers to security questions.

If someone hacks your email: 1) reset password, 2) check Sent folder to see what hacker sent, 3) see if hacker set up any forwards.

Use two-factor authentication (2FA) or multi-factor authentication (MFA). An authentication app (such as Google Authenticator) is more secure than receiving auth codes by SMS (text message).

Use separate device (such as Chromebook or tablet) for working with finances (and maybe medical stuff) online.

Who Else Is Reading Your E-mail?
Use PGP, OpenPGP, or GPG to encrypt email.

When you encrypt a message (email, text, phone call), use end-to-end encryption. There are PGP browser plugins such as Mailvelope.

You can hide your IP address by using a proxy, remailer (such as Mixminian), or Tor (torproject.org, Orbot app for Android, Onion Browser app for iOS).

Use Tor on a separate device.

Wiretapping 101
Signal app is a free VoIP system with end-to-end encryption for iOS and Android.

If You Don't Encrypt, You're Unequipped
Text (SMS) messages aren't private. They're sent unencrypted and are stored by carriers for some amount of time.

All popular messaging apps encrypt data in transit, but not all use strong encryption, and most don't encrypt data at rest. WhatsApp provides end-to-end encryption, and Facebook Messenger provides it if you opt in to "Secret Conversations."

Whisper, Secret, and Telegram apps aren't secure and private enough.

Look for messaging apps that provide off-the-record (OTR) messaging, and perfect forward secrecy (PFS). Mitnick recommends Chat Secure, Signal, Cryptocat, Tor Messenger.

Now You See Me, Now You Don't
HTTPS Everywhere browser plugin forces HTTPS whenever possible, and can secure otherwise insecure connection negotiation.

Beware free proxy services. When using a commercial proxy service, read privacy policy, looking for how it handles data in motion, law enforcement, government requests for info.

Set privacy options in Google account, and/or use DuckDuckGo, which doesn't track users.

Every Mouse Click You Make, I'll Be Watching You
One way to minimize tracking is to browse in a virtual machine (VM).

NoScript and ScriptBlock plugins block ads and third-party referrers, reducing tracking.

Adblock Plus browser plugin blocks potentially dangerous ads, but Adblock tracks you.

Ghostery browser plugin allows you to limit tracking.

Use a variety of email addresses tailored to individual purposes to make it harder for marketers and hackers to build profile of you.

Cookies from normal browsing will apply to private mode browsing.

Consider removing cookies on case-by-case basis to limit tracking. You should delete referrer cookies, super cookies. CCleaner can help.

Don't use social sign-in options (e.g., OAuth) on websites, because if someone hacks your social account they can access all those linked sites.

Browser extensions Facebook Disconnect and Facebook Privacy List for Adblock Plus give you control over what you share with Facebook.

Browser plugins CanvasBlocker and CanvasFingerprintBlock block canvas fingerprinting.

Use cryptocurrency (e.g., Bitcoin) to pay anonymously.

Pay Up Or Else!

If your router has an open/guest network, lock down its settings or disable it.

Update router firmware regularly.

Change WiFi name (SSID) to something that doesn't identify you or the make and model of the router. Change router admin username and password. Use WPA2. Disable WiFi Protected Setup (WPS).

It's easy for malicious software to activate camera and microphone on computers and mobile devices. Put tape over cameras when not in use.

In general, don't respond to unsolicited messages requesting personal info. Instead, contact the alleged sender through a known trustworthy channel (e.g., public phone number) to ensure they actually sent request.

Keep full backups of PCs and mobile devices as precaution against ransomware.

It's difficult to decrypt ransomware, so consider paying ransom if you don't have backup.

Believe Everything, Trust Nothing

Don't use unencrypted public WiFi, at least not for anything involving personal data. Instead, use your cellular connection or personal hotspot.

Disable device's automatic connection to saved WiFi networks, or delete saved WiFi networks when you no longer need them, so device doesn't connect to malicious networks with the same name as saved networks.

Consider using a virtual private network (VPN) when using others' WiFi. Make sure it uses PFS. If the VPN provider keeps logs, make sure it doesn't retain traffic or connection logs, or make data available to law enforcement (as that would mean they log). Mitnick named OpenVPN, TorGuard, ExpressVPN.

Turn off WiFi when you don't need it, to avoid being tracked by your MAC address.

To be invisible, prior to connecting to any WiFi you should change your MAC address to one not associated with you.

Never use public PCs for anything sensitive. Assume they have malware.

You Have No Privacy? Get Over It!

To request that photos of you be removed from a website, email abuse@domain.com, admin@domain.com. If they don't remove photos, email dmca@domain.com, or file a DMCA request with the website's host or ISP.

Limit personal info you put in social media profiles. Set privacy settings. Don't display your birthday.

Be very careful whom you friend or connect with on social media, as they instantly get access to a lot of personal info.

Disable location broadcasting in all apps or for entire phone.

Review Android app permissions before deciding whether to install.

iOS is much more secure than Android (if you don't jailbreak your Apple device).

You Can Run but Not Hide

Periodically delete location history from your phone.

Wearables (fitness bands, smart watches, etc.) can track your location. Lock down privacy settings.

Hey, KITT, Don't Share My Location

Mass transit isn't anonymous unless you pay with cash, or with commuter card you paid for with cash.

Car infotainment systems store info (including your contacts) from paired phones. Don't pair your phone with cars that aren't yours. Delete data from infotainment system before you sell car.

The Internet Of Surveillance

Change default username and password on all Internet of Things (IoT) devices.

Most smart TVs record audio in the room while they're on, and transmit that audio unencrypted to the manufacturer. To stop this, disable voice recognition in settings.

Turning your phone off should prevent it from eavesdropping, but to be sure, pull the battery out.

Listening software and devices (Google Assistant, Siri, Cortana, Alexa, etc.) record audio searches/questions/commands indefinitely.

To avoid eavesdropping, put tape over cameras and put dummy mic plug (cut-off end of headphones) in mic jack.

Delete voice data from Amazon Echo devices before you get rid of them (do in your account).

When possible, turn off voice activation feature in voice-activated devices, to limit eavesdropping.

DIY home security systems that use your home network and home Internet connection are vulnerable to being disabled or triggering false alarms.

Things Your Boss Doesn't Want You To Know

Your employer probably monitors you, so if you're concerned about privacy, don't do anything personal at work, or use a personal device with your own cellular connection.

IMSI catchers (such as StingRay) are used by law enforcement to see which phones were at locations, such as protests.

Skype is monitored by NSA.

Securely wipe drives of printers, copy machines, video conferencing systems, etc. before getting rid of them.

Encrypt files before sharing via file sharing services if you don't want NSA reading them. Even when services encrypt data in transit or at rest, service provider has the keys, and can access or give access to your files.

SpiderOak provides 100% data privacy (they have no knowledge of your password and data).

Obtaining Anonymity Is Hard Work

VeraCrypt can create a visible or hidden encrypted folder.

On iPhone, set a password for encrypted iTunes backups to prevent someone from backing up your phone to their PC without your knowledge.

When traveling, take your laptop with you everywhere. If you must leave it somewhere, power it completely off so an attacker can't dump the memory to get your drive encryption keys.

The Tails OS can be booted up on any modern computer and not leave any forensically recoverable data on the hard drive. Run Tails from a USB drive or DVD.

Windows BitLocker is OK for average user, but isn't ideal because it's privately owned and may contain back doors, and you must share your key with Microsoft unless you pay $250.

Other disk encryption software: PGP Whole Disk Encryption, WinMagic, Apple's FileVault 2.

Don't let encryption software save its keys to the provider's online account, as that grants them access to your data.

Encryption is often enough to foil common thieves, but not dedicated governments.

Hotel safes aren't much safer than keeping items in your suitcase in your room.

Loyalty cards track your purchasing habits. Register with a false name, address, phone number to prevent data from being linked to you.

Don't install software updates when on others' WiFi, unless you use your own cellular connection to verify from the vendor's site that the update is legit. If update isn't critical, wait to install when you're on a trusted network.

Mastering The Art Of Invisibility

Protonmail.com and tutanota.com provide email accounts without identity verification. Use Tor to get to the sites to register anonymously.

Stephen says

So, you want to be invisible online? Great. All you'll need is three separate computers -- one for your top secret business, one for your banking, and one for your everyday use; a few new email addresses, a handful of burner phones, a large pile of cash to buy gift cards and electronics without leaving a credit trace, a slightly larger pile if you intend on paying strangers to buy said cards and electronics for you, an ability to habitually lie, and the concentration of a criminal mastermind to remember which accounts you're using on which computer so you never accidentally blend your Top Secret identity with your real one. Child's play.

Kevin Mitnick knows a thing or two about the necessity and the difficulty of staying invisible. He spent two and a half years as a fugitive from the FBI, wanted for hacking, unauthorized access, and wire fraud. These days he works as a security consultant, and in The Art of Invisibility he provides a point-by-point tour of the surveillance web created by the internet and telecommunications infrastructure. There are also specialized chapters on surveillance in the workplace, and maintaining privacy while traveling abroad. Mitnick's survey and advice have at least two audiences: most of the book can be appreciated by a technologically savvy and privacy-minded individual who wants to know more, while a smaller but not insignificant portion of the book, somewhere between 30 and 40 percent, would be of interest to the truly paranoid.

Although Mitnick does cover material would be a given to those with an interest in security -- don't use public WIFI networks for banking or other sensitive business, even if they're password-protected, that kind of thing -- most of his information is less elementary. He's thorough, explaining how tools like email and hardware encryption work, where they're vulnerable, and why they're useful. The Tor browser is a mainstay of recommendation, as it allows users to be relatively anonymous and evade filters that restrict access in territories controlled by authoritarian states like China by redirecting the user's activity across a series of nodes. The nodes chosen are random, and it's possible to encounter a node controlled by surveying authorities. If a person uses Tor on the same computer and accesses the same accounts as they normally do, however, then if they're under active surveillance by someone their token efforts at anonymity are for naught. People in witness protection can't go to family reunions, and those who want remain invisible can't muddle their identities together. If you want to have an email account and use Tor, Mitnick advises, then use Tor and create a new email account. The same concept applies across communication technologies: Mitnick was caught in the 1990s because despite using multiple cell phones, he was using them in the same location (a motel room), and thereby connecting to the same cell tower every single time -- allowing the FBI to collaborate with the local telecom to get a fix on their man.

The Art of Invisibility is far more comprehensive and helpful than Mitnick's previous books on intrusion and social engineering. Mitnick offers his exhaustive tour of vulnerabilities not to scare readers into retreating to a monastery, but to point out -- this is what you're up against, this is what you can do about it, this is where you'll still be weak. Like a security consultant's tour of your home, The Art of Invisibility shakes expectations, and disturbs the illusion of safety -- while at the same timeVanishingly few people are capable of taking all of Mitnick's advice: even he doesn't. He leaves the decision to the reader how best to integrate this information with their own practices. Everyone can benefit from better cyber-security hygiene, even if it's something as basic as keeping your cellphone locked, running adblock to disable malicious scripts on websites, and keeping SmartTvs that never stop listening to you out of your house.

Related:
10 Don'ts On Your Digital Devices Daniel G. Bachrach, Eric J. Rzeszut. A more entry-level citizen's guide to digital hygiene.
Swiped: How To Protect Yourself in World of Scammers, Phishers, and Identity Thieves, Adam Levin
Future Crime: Everything Is Connected, Everyone is Vulnerable, and What We Can Do About It, Marc Goodman

Bradley says

Scary.

I mean, what non-fiction book about the sheer amount of security loopholes wouldn't be scary? I mean, we're talking about our identities online, in our homes and through all our smart devices, our cars, our workplaces, and everywhere.

It's not even about government abuses. It's about the fact that everyone, everywhere, is at risk. Snowdon may have opened our eyes, but the reality remains that your breasts are still online. Everywhere. Never to be deleted. Always accessible. Forever.

If you're thinking about some other body parts, then keep on thinking, because those will still be there and are being housed on not just government sifter sites, but local and foreign ISPs. And countless private computers.

So what are we doing about it?

We're reading. We're arming ourselves. We're realizing that far from being beset with malicious users and crackers, we're actually beset with a ton of idiots running big businesses saying we're being protected when we really aren't. Security holes are everywhere and they're real and pervasive.

Always on cameras and microphones? Keyloggers as a matter of course on company servers? Regular cracking of your gmail and facebook information? Full breakdowns of any photos you take and post, from location, specific identifiers, etc., right in the metadata? Aren't we worried? Shouldn't we be more worried that what we think are precautionary measures to protect ourselves as we order online or use online banking is only as secure as our weakest link?

Indeed.

And that's why reading books like this should scare you. Not because it tells you how much you should be scared, but because the lax security is as much in our minds as it is in the software. Putting our heads in the sand and saying we're not doing anything wrong is beside the point if we get targeted with ransomware or we're identity hacked or we're just one more in an extremely long list of targeted political somebodies. It's not just about having your private parts online, but that's where most of us will usually get outraged.

So do yourself a favor and arm yourself with some practical knowledge and how-to sets on how to anonymize yourself. :) Mitnick does a pretty damn good job with some of that direct-knowledge stuff. :) Sure, you may know a lot already, and maybe you already use vpn and tor and things like ghostery and HTTPS Everywhere, maybe you practice healthy password management and separate your devices for truly secure transactions. Maybe you don't. But it sure as hell doesn't hurt to know what you're missing. :)

I'm so glad I read this! (It helps to keep up-to-date.) :)

Christopher Lawson says

Trust Me: Even You Are Not Invisible. At Least Not Yet.

THE ART OF INVISIBILITY is a little bit scary. The authors, Kevin Mitnick and Robert Vamosi, document the myriads of ways that others can spy on our activities. You might think no one knows what you are doing, but you are wrong: "Each and every one of us is being watched." If you carry a cell phone, "You are being surveilled."

Mitnick tells the story of how the famous John McAfee, on the lam, was found supposedly by coordinates listed in the meta data of a photo posted online. The authors snicker, "Take it from me: if you're trying to get off the grid and totally disappear, you don't want to start a blog."

Some of the pointers are pretty basic, such as using strong passwords, and being careful to setup your home Wifi using the latest security protocols. A large chunk of the book relates to securing wireless internet access. "Public Wi-Fi wasn't created with online banking or e-commerce in mind. It is merely convenient, and it's also incredibly insecure."

More advanced suggestions are for those who feel they need extreme online privacy. These tactics include things such as using "burner" phones, paid for with cash, and using encryption tools to hide the data on our laptop.

Law enforcement has come a long way in tracking down fugitives. The authors explain how authorities use devices to mimic cellular base stations, and "designed to intercept voice and text messages." Using another tactic, the FBI has successfully tracked criminals by getting the cell tower data, and correlating their cell phone records.

I was surprised to learn of certain recent laws regarding data preservation. In the event of a legal investigation, you must preserve your entire browser history. You can be arrested--and people have been, for clearing the history.

The really meaty parts of the book provide extreme tactics to remain anonymous on the internet. Mitnick advises creating a complete new persona, "one that is completely unrelated to you. . . When you're not being anonymous, you must also rigorously defend the separation of your life from that anonymous identity."

The first thing to do in making yourself anonymous is to get a cheap standalone laptop--used only for your anonymous persona. "Don't ever use the anonymous laptop at home or work. Ever."

Here are a few more tips for becoming anonymous:

* When you travel, don't bring electronics that store sensitive information with you.
* Encrypt the confidential data on your laptop.

The authors present a LOT of different ways to make your online persona more invisible. The authors admit, however, that even with all their precautions, it is still tough to be 100% anonymous. The main idea is to make it much more difficult for the intruder. So, put up "so many obstacles that an attacker will give up and move on to another target. . . Being anonymous in today's digital world requires a lot of work and constant vigilance."

All in all, I found THE ART OF INVISIBILITY to be an interesting, fairly-practical read. It was good to be reminded about the proper setup of networks, and how vulnerable public systems can be. I don't feel the need to go out and buy a "burner" phone anytime soon, but it's good to know.

Advance Review Copy courtesy of the publisher.

Manuel Antão says

If you're into stuff like this, you can read the full review.

This is How the World Will End: "The Art of Invisibility" by Kevin Mitnick, Robert Vamosi

This book calls for a limerick of "me" own:

This is how the world will end.
This is how the world will end.
Not with the roar of a lion
But with the click of a mouse.

Mitnick's and Vamosi's book is for the layman. You won't find here buffer overflows (NOP sled, or overwriting the stack return pointer), network scans/DoS attacks, integer overflow exploitation, details about recent techniques to bypass ASLR, shell-code injection, network sniffing, no kernel hacking/rootkit exploits, i.e., it does not break ground as a book to explain how hacking and software exploits work and how readers could develop and implement their own. It's a breezy read with lots of information, but the deep dives aren't there.

Reading this, it got me thinking once again on IT security aspects. I've done this recently when I read my last security book. Every time I read something like this, I always get in the mood "Oooh spooky, 'cyber security', how hip, how now." Cyber security is what used to be called 'spying' and that goes back to erm...Caesar Augustus as emperor lived in a modest two story home in central Rome. Two floors around an open central area and thin columns sparsely placed to form colonnaded mezzanine ground and top floor and no drapes or hangings - he lived in a modest house with open mezzanines so that NO ONE COULD HIDE BEHIND columns and listen to his conversations. Spying is as old as ancient governments.

If you're into Computer Science and CyberSecurity in particular, you can read the rest of this review elsewhere.

Wayne Marinovich says

Loved this read. It can be a little tech heavy in some places, as is the nature of the beast. Scared the bejeezus out of me in other areas. Orwell was right. Hi there, big brother.

Knigoqdec says

?????? ??? ???? ???? ?????????? ???? ?? ? ????????? ??????? ?? ?????? "??????? ?? ???????????? ? ????????". ????????... ?? ???? ????? ?????? ??????? ???? ?? ??? ?? ???? ?????, ????? ?????? ???? ????? ??

??????? ?????????? ? ???????? ?? ???? ????. ??, ???????? ????? - ?? ?? ????? ?? "?????????????"... ????? ?? ?????? ?? ?? ???????? ????? ?????????? ?? ?? ???? ? ??????.
????????? ??????? ???????????? ?? ? ??? ??????? ? ? ????????? ?? ??????, ???? ????????... ?? ????? ???? ?????? ?? ?? ?????????? ????? xD. ?????? ???????????? ????? ???? ?? ?? ?????????, ??? ???? ?? ??????? AdBlock-?... ? ?????? ?? ?????? ?? ?????? ??? ???? ?????? ? ?????????? ??, ???? ?? ?? ?? ? ??? ????? ??????, ?? ?? ???????? "?????????".
?? ??? ???? ?? ???????, ? ????? ? ???????? ????? ?? ?????? ???? ??????? ?? ????? ?????????? ????????? ???????... ?? ????? ?????????? ??????? ?? ????. ?????? ??? ??????, ?? ?? ???? ?? ????? "?????" (????? ???? ??????????, ???? ??? ???? ??????, ??? ????? ??????), ?? ???????? ??????? ??? ?????? ?? ????? ??????????? ? ?????? ?? ??????? ?? ????? ? ???????????. ????? ?????? ???? ?? ???? ???????????? ???? ?? ????? ???? ????? ??. ???????? ??????? ????? ?????????, ?? ? ?????? ?????? ??? ?????? ? ???????? ?? ???.
??????? ???? ?????? ?? ???, ????????? ?? ???? ?? ???? ??? ?? ? ??? ? ?????... ??? ?????? ??? ????, ?? ???????? ???????????, ?????? ?? ????? ?? ?? ???? ??????? ????????????. ?? ????? ???????? ?? ???????? ????? ????, ??????? ? ??????? ?? ??? ?? ?? ????????. ???? ????????? ????????... ?? ??????, ????? ?? ????????? ?? ?????????????? ??? ???? ??????... ?????. ???? ????? ??????? ?????? ?? ???? ??? ? ??????? ?? ?????? ????? ? ??????????????, ??? ?? ?? ?? ?????, ??? ???? ???? ?? ????? ?????...
????? ?? ????????? ????, ???? ????? ?????? ???? ? ?? ?? ???????? ????? ????? ?? ?? ??????? ? ?????? ?? ????????????? ???? ???? ???? ?????????? ????? ?? ?? ???? ?????, ?? ?? ?? ???? ?????? ??, ??? ?? ? ????? ?? ?? ?????????, ?? ????, ?????? ??????? ?? ? ?????... ???? ?????? ????? ????? ?? ?? ????? ?????, ?? ?? ??????? ???? ?? ?????????? ?? ? ?????? ????????? ?? ?? ?? ????? ?? ??????? ???? ????? ?????? ? ?????? ????? ??????? ?? ??????? ???????? ?? ????.
????? ?? ?? ??????? ?????????!
?????, ??????? ??. ???????? ???? ?? ????????? ?? ??? ??????????. ?????? ?? ??? ????? ??-????? ?? ??? ? ???? ????. ?????? ?? ??? ?? ???? ??????, ????? ?? ????? ? ????????? ?? ??? ???????, ??? ??????, ???? ?? ???? ?????? ?? 300 ???????, ????????? ?????????? ??????? ? ??????.
?????? ?????????? ?????????? ?? ?? ??????? ???????. ?????? ????? ?? ?? ?????????? ?? ???, ??? ?? ? ??????????? ?? ?? ??????????. ?? ???? ?? ?? ???????? ? ????????? ??? ???? ???????. ?? ??? ????????? ?????. ?????? ?? ????? ?? ??????? ?????????? ? ?????????, ?? ?? ?? ???? ? Tor, ????????, ? ???? ????, ?????? ?????? ?? ?????? ?? ????? ?????, ????? ? ??????. ?????? ?? ??? ???????. ?????? ?? ?????????? ????????, ?????? ?????? ?? ??? ????, ????? ?????? ???? ?? ?? ???? ?? ?????????. ?????? ?? ??? ???????? ?? ?????... ??????? ??? ?? ?????????? ? ????????, ???????? ??? "1984" ?? ?????, ??? ??????? ?? ???? ??????. ???????????, ?? ???????? ???? ???? ?????, ?? ?????? ?? ?? ????????... ????? ????? ????????? ????? ?? ???? ?? ?????????? - ?? ???? ???? ?? ???? ?? ???, ?? ???? ???? ? ? ???????????

?????? ????? ? ?????? ???? ???? ?? ???. ??????? ?? ? ???? ???????? ?? ?????? ???????????, ??? ???? ???? ????? ? ???????? ??????. ??? ???, ? ????????, ???? ??? ????? ?????? ?? ???????? ?????? ???? ??????. ????? ???? ? ??? ???? ???? ?????????, ?????????, ????? Tesla? ????? ?????? ? ??? ?????????? ?? ?? ??????? ???????? ???????... ??? ?? ???????? ?? ??????????? ?????? ?? ?? ??? ????????? ?? ????????????? ?????? ????? ???? ?? ???? ???????????? ?? ?? ????? "???-??? ???????? ???????" ? ?? ??????? ? "???????? ?? ?????????? ????????"?
?????, ?? ?? ?? ???????, ?????? ? ?? ?? ???? ????? ?????, ????? ??...

?? ????? ?? ??????? ?????? ??????, ?????? ?? ???? ????????? ? ????????????? ?? ???????? ??????? ? ???????. ???? ???? ?? ?? ?????????, ????? ? ????? ?? ????????? ???????????, ? ??? ????? - ????? ?????????. ?? ????? ?? ??????? ???? ????????? ? ???? ???????? ??? ?? ?????????, ?????? ??. ???? ?? ???????? ???????? ???? ????? ????????? ? ???? ?? ?? ???-??????? ? ????????.
???? ???? ??????? ????????? xD. ??? ??? ?????? ?????, ????? ?? ? ???? ???? ?????, ?? ?????, ?? ????? ???????? ?? ??????? ??????? ???! ???? ?? ????? ?? ??????? ?? ?? ?????????? ????????? ?? ???????????? ??, ??????? ? ????????????? ?????????? ?? ??????? ?? ?????, ?? ??????? ??????? ? ?? ?? ?????? ?? ??????????????????!

Donna says

3.5 stars.

I had many different thoughts and feelings while reading this. The author is an ex-hacker and has done jail time. So some of this felt like it was written by a criminal FOR CRIMINALS.

The author offered a wide range of ideas on how to protect one's identity while on the computer. With some of his ideas, I felt a little pride because I could say, "Did it already." There were also some other useful ideas that I felt I could easily implement. But some of this was so completely over my head. I need to do baby steps. Reading this made me feel an urgency to protect my identity.

Bianca Smith says

You may be questioning why a digital marketer would encourage reading the Art of Invisibility. It’s a book teaching how to hide your online life. Hiding online actions does tend to make our jobs as digital marketers rather difficult.

However, you need to read this book for several reasons. First, I believe in informed choices. Yes, we use audience data for decision making (well, we should). And the data isn’t always anonymized. But our audiences should know and consent to this. Second, this book gives essential tips for protecting yourself online – which also protects your brands and clients. And finally, it’s written by Kevin Mitnick. I probably would have done better in college the first time if I wasn’t following Kevin’s hacking spree and run from the FBI. He definitely influenced my curiosity.

Kevin has now moved on to legal, authorized hacking as a penetration tester. Companies pay him to hack into their systems, except now it’s called testing. It does mean that Kevin sees what companies collate about us, and knows it’s not always used ethically. Is this book, Kevin shares that knowledge.

What’s the Art of Invisibility About?
The book is a how-to guide for avoiding hackers and malicious activities online and offline. It even goes as deep as teaching how to completely be invisible online. This internet-loving introvert thinks that sounds lonely, but recent reports show how much we all need to protect ourselves. For those reading this later, it’s February 2017 and it’s not shaping up to be the safest year in US history.

The Art of Invisibility is essentially divided in two. The first half details how to secure your own life. So choosing secure passwords, which public networks are safe, protecting your online banking, blocking ads and transaction tracking. That kind of thing. It’s very Android and Windows focused. Sometimes the recommendations are on price. Later in the book Kevin references the default security Apple uses, and that probably accounts for the Android and Windows focus. I’m being intentionally vague so I’m not putting words in Kevin’s mouth. In one example Kevin describes a road rage response he gave. If he can social engineer that kind of information on someone while driving down a freeway, I don’t want him grumpy with me. Which leads to a strong point that Kevin makes in the book, social engineering is a huge part of hacking and online security. It’s easy to pretend to be someone and talk a receptionist into handing over details. They may not realize what they’ve actually said. It’s covered in this book. This first 50% (I was reading a Kindle copy courtesy of publishers Little, Brown) could be a book on its own. It covers so much detail that I was wondering what could be left to discuss in the remaining 140 pages.

The second half gets seriously scary. I hope no one is ever in a situation to need to hide this entirely. Actually, it’s February 2017. Sigh, everyone read and follow Kevin’s advice. This second part is where Kevin teaches the art of invisibility. The first part of the book shows some tips, but this shows how to totally disappear. As with the first part, Kevin uses real life examples to illustrate both the points and the need for security. These are mainly his experiences. I found the way Kevin describes these experiences interesting. He’s been detained and searched by US government officials with less than valid reason, but even when describing this and the efforts he does to protect the devices he carries with him, he never allocates blame. I understand by now it’s a fact of life that he’ll be harassed when traveling, but it was interesting the way he turns the stories around. Having cash stolen from a hotel safe was the example of why you shouldn’t trust them and he explains how they are easily broken into.

Who Should Read the Art of Invisibility?
EVERYONE!

Art-of-Invisibility-iMessageI sent this text the night I started reading. The group I reference is highly educated, conscious of current affairs and tech savvy, but there’s more we can do to protect ourselves and our brands and clients. Even though this book is directed at personal actions, we have Facebook accounts and WordPress installs accessible with our phones. We can’t think just of ourselves. Imagine your brand being compromised because you clicked the wrong link. Do you want to be responsible for that?

Consumers also need to make an informed decision on the data they share with us. This book helps them opt out (because we rarely make it easy).

So yes, I say online security and privacy is so important everyone needs to read the Art of Invisibility.

At the very least I urge you to read the first half. It’ll make you more secure than most. Reading the news of the last few weeks, I recommend you read and action the lot.

The Art of Invisibility was released today. Buy it, read it, action it, then share it with your family and friends. Democracy needs you to.

Originally published: http://tapdancingspiders.com/book-rev...

Andy says

A cautionary tale of just how visible you are on the internet and in todays connected society.

First off I am fully aware of the irony of posting a review of this book online on Goodreads, my blog and Facebook after reading a book on how to be invisible on the internet.....

This was a an entertaining read and although I work in the IT field, there were still some security facts in the book that I was not aware so I learnt a fair amount. There are also some useful references for security tools that I had not been previously aware of (although I'm not a security professional).

Despite the above, the book isn't too technical to make the non IT person bored but it may well make them paranoid! There is a huge emphasis on becoming invisible in the book through extreme measures such as paying a complete strange to buy some gift cards at a store that doesn't have cameras in the store OR on the way to the store, then using that to buy bitcoins - twice to ensure they are completely laundered and then using those new coins to purchase various items. Not something that the average person in the street is likely

to ever do .....and I must admit I do wonder if someone needs to go to all that trouble, would they be reading this book?

There are useful hints and tips about using secure messaging, email etc that can be used by everyone just to keep their internet usage secure which are not too extreme for the day to day consumer.

But for the ultra paranoid/nefarious, this book will either help you solve some of your issues or make you even more paranoid as it brings up points you hadn't thought of before....

Fawaz Abdul rahman says

this book gives you a lot of information about the privacy in the virtual world (internet).
what are the things are being tracked, why you're tracked, what are the impacts and much more, and more importantly, how to protect your self from those trackings.
It's better to read the written addition of the book, if you decided to go with the audiobook keep something to take notes while reading, you may need write down some names of add-ons or software.
some information is repeated so many times, but linked in one way or another. the book explains some so advance technics to be invisible, but as a normal user you don't need all that, still what is good is that he explains each process and why you may want that.
Also he mentioned some stories to make clear the importance of some procedures.

Julie says

The Art of Invisibility by Kevin Mitnick: The world’s most famous hacker, teaches you easy cloaking and countermeasures for citizens and consumers in the age of Big Brother and Big Data- is a Little, Brown, and Company publication.

Online privacy is always of concern, but after the Snowden revelation, people became even more aware of how easy it is for companies and the government to spy on us. VPN’s suddenly became mainstream and browsers like DuckDuckGo and programs like Tor became commonplace alternatives, not because everyone was trying to cover up criminal activity, but because what they search online, their photos or videos, emails, etc. are private and we want to keep them that way, no matter how benign.

But, in just the last week, Congress voted to allow our ISP providers to sell our information to the highest bidder, which can mean anything you search online, including symptoms on Webmd, for example.

So, what do you need to do to protect yourself and keep your information safe and most of all, private?

Kevin Mitnick is an expert hacker, which has gotten him in hot water on occasion, but now works to help people ferret out illegal hackers and expose their methods, teaching people how to protect themselves and their clients, otherwise known as a penetration tester.

While some of the suggestions are easy to carry out, and I have already put those measures to good use, others seem a bit extreme, and are a lot of hard work. So, are all these steps absolutely necessary if I’m not doing anything criminal or visiting the ‘dark web’?

If you want to be absolutely invisible, then yes, you do. Even after putting on several layers of protections, I was stunned to learn that even with these safeguards, I only made my information harder to access, but I was still not totally hidden, could still have my activity traced and shared.

So, if you are in a dispute with your boss, going through a messy divorce, or anything of that nature, you will want to make sure there are no traces of your searches left behind that could be used against you, even if you are an ordinary law abiding citizen.

Remember, the slew of celebrity photos that were hacked and posted online a while back?

iPhone users were vulnerable, so although they didn't break any laws, private information about them was hacked and exposed, which means you must protect your smartphones and tablets as well as your home, work, and school desktops and laptops.

Therefore, no matter how safe you think you are, no matter how careful you are, you probably aren't as safe, private, or incognito as you might like to think, which is why everyone should read this book.

It's a real eye opener for sure, and while I probably would never buy a laptop just one purpose, never tap into online currency, or anything like that, at least for now, it's good to have this information, and who knows? If Verizon and AT&T continue to obtain information about my online activity – and here's the real kicker- WITHOUT MY PERMISSION, I may have to resort to such drastic measures, no matter how extreme it might seem.

Overall, this is a very interesting and informative book, but also one that is, unfortunately, necessary. I highly recommend it to anyone using the internet at home, school, or work, as well as anyone using smartphones- which is pretty much everyone.

---

linhtalinhtinh says

A fascinating and tremendously helpful piece of writing. Because of this book, I spent hours changing all my passwords, my online accounts, hours reconfiguring my laptop and cellphone, haha.

The writing isn't that great, and Mitnick's ego gets in the way often, but well, I pick up the book for the other infos that he provides. I have little knowledge in cyber security so this is awesome, but for others with stronger background, it may not be so. I wish the book were more detailed on the exact working of the technologies presented, but well, for practical purpose and its general audience, it serves well.

After the recent few books on technology I have read these days, I realize that the world I'm living in is approaching a dystopian-like realm. I didn't notice it, because from the appearance it's still fine, people still highly value privacy. Yet at the same time, we are unaware of the way we make ourselves vulnerable, of the colossal footprints we leave everyday due to the deeper and deeper integration of technology. Not many people are like Mitnick, a criminal trying to disguise his identity, yet it's disturbing to see how much others, either states or private entities, can tell and pindown who we are with extreme accuracy and with little effort. Legal, ethical, and philosophical systems haven't caught up with the speed that technology has fused into our life, and in the limbo I wonder what to do.

Anyway, the point of the book is more like: becoming invisible is quite impossible, at least for general readers. It is very costly to do so, mentally and financially. What we can do is at best increasing our firewalls, telling the attackers to find easier preys.