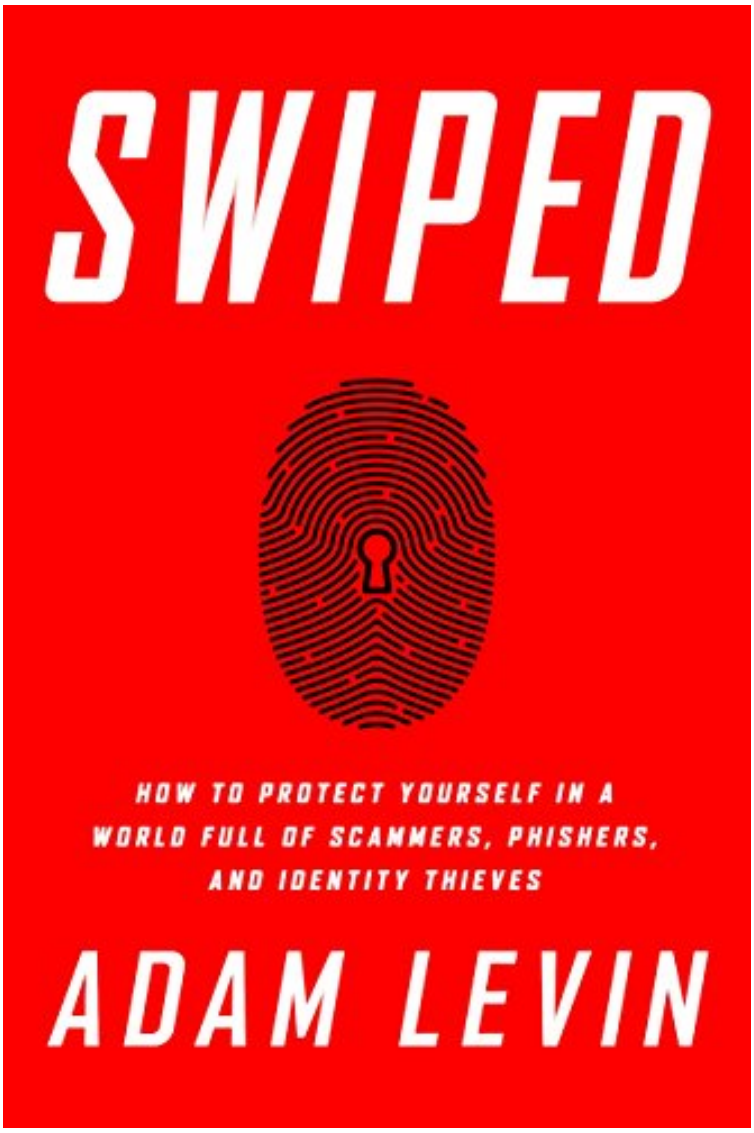
Swiped: How to Protect Yourself in a World Full of Scammers, Phishers, and Identity Thieves

Adam Levin
*ebooks | Download PDF | *ePub | DOC | audiobook*



#371542 in eBooks 2015-11-24 2015-11-24File Name: B012271LV0 | File size: 28.Mb

Adam Levin : Swiped: How to Protect Yourself in a World Full of Scammers, Phishers, and Identity Thieves before purchasing it in order to gage whether or not it would be worth my time, and all praised Swiped: How to Protect Yourself in a World Full of Scammers, Phishers, and Identity Thieves:

56 of 59 people found the following review helpful. Not a useful guideBy EugeneI completely disagree with the positive reviews. The book is very poorly organized. The useful info in this book is buried in pages and pages of dense

text, mostly useless stats (how many times do we need to know what % of people have been victims of various scams? we all know about the problems) and anecdotal stories about scams (these appear in the media every day; why do we need to read more of them, dozens more of them???). The author should have included lots of easily browsable, concise but detailed lists of what you need to do to protect yourself. For example: How to protect yourself on social media. What to do if you're hacked. Etc. Not a few tips buried in 250 pages of text. He barely even mentions credit freezes (and doesn't tell you how to do one), one of the most important things you can do to protect yourself. A complete waste of time for anyone who knows the first thing about the topic. You can learn much more much faster on the any number of web pages. Internet.1 of 1 people found the following review helpful. Is Levin's Advice Hyperbole?By RNJWhen you arenrsquo;t an expert in a particular field, you can be cowed by someone who IS (supposedly) an expert. Thatrsquo;s how I feel as I read Levinrsquo;s book Swiped. Itrsquo;s a clever title. You think at first: Oh, hersquo;s talking about how you swipe your card in a reader when purchasing an item, and then you get caught up in the pun. Hersquo;s really talking about when someone else swipes your card and swipes it in a reader or uses it to swipe your data. As a student of rhetoric, Irsquo;m always suspicious of what seems like hyperbolic speech, oversell, overkill. At the same time, Levin could be Paul Revere, and most of us just arenrsquo;t listening. Although Levinrsquo;s book provides a great deal of usable information, I do believe he could have honed it down to one well-edited magazine article, and it would have been just as effective. You be the judge.Let me share a few of the nuggets I found interesting:ldquo;More than 500 million photographs are uploaded to major websites every day. More than 2 billion pictures are taken on mobile devices every dayrdquo; (Kindle Location 85). Elsewhere Levin cautions against using geotagged photos at websites like Facebook because it can give thieves clues to your PII (personally identifiable information). It probably begins with the settings in your camera or iPhoto. I think it makes sense NOT to geotag.ldquo;Debit cards increase your exposure to fraud. Use a credit cardrdquo; (Kindle Location 578). Levin asserts that ldquo;carefully placed camerasrdquo; (by thieves?) can record PIN numbers as you enter them in an ATM or device at your favorite store. Not sure what his authority or source is on this assertion, and hersquo;s assuming that thieves could EASILY install their own cameras at ATM stations. Seriously?He warns against the free release of your social security number: ldquo;With your Social Security number in the wind, whoever finds itmdash;or, more likely, whoever buys it on one of the many black-market information exchanges on the deep webmdash;holds the keys to every part of your life. What that meansmdash;plain and simplemdash;is that yoursquo;re going to need an efficient way to keep one eye over your shoulder, all the timerdquo; (Kindle Location 591). The paranoiac tone notwithstanding, Levinrsquo;s advice is probably good. Elsewhere in the book, he directs the reader to keep only a COPY of your Medicare card in your wallet with all but the last four numbers blacked out, the ldquo;Mrdquo; or ldquo;F,rdquo; as well. This way, you can still inform someone who needs the number (medical personnel) but protect yourself from unwarranted use if someone should steal your wallet. He also warns against carrying your Social Security card (or copy) for the very same reasons.At one point Levin makes a list: ldquo;We expose our most sensitive personal information any time wePick up a phone, respond to a text, click on a link, or carelessly provide personal information to someone we donrsquo;t know;Fail to properly secure computers or devices;Create easy-to-crack passwords;Discard, rather than shred, documents that contain PII;Respond to an email that directs us to call a number we canrsquo;t independently confirm, or complete an attachment that asks for our PII in an insecure environment;Save our user ID or password on a website or in an app as a shortcut for future logins;Use the same user ID or password throughout our financial, social networking, and email universes;Take [online] quizzes that subtly ask for information wersquo;ve provided as the answers to security questions on various websites.Snap pictures with our smartphone or digital camera without disabling the geotagging function;Use our email address as a user name/ID, if we have the option to change it;Use PINS like 1234 or a birthday;Go twenty-four hours without reviewing our bank and credit card accounts to make absolutely sure that every transaction we see is familiar;Fail to enroll in free transactional monitoring programs offered by banks, credit unions, and credit card providers that notify us every time there is any activity in our accounts;Use a free Wi-Fi network [i.e. cafeacute;s or even airports] without confirming it is correctly identified and secure, to check email or access financial services websites that contain our sensitive datardquo; (Kindle Location 668-678).These tips are all good advice. I only question whether we need to check our accounts EVERY DAY. Perhaps every second or third day, even once a week?ldquo;The deep web is a hidden part of the Internet. It consists of a vast number of sites, most of them thoroughly boring, that canrsquo;t be found by a traditional search engine like Google. To access these sites, you need a password, a specific URL, a sophisticated understanding of how computers communicate, or sometimes all of the above. The deep web is four hundred to six hundred times larger than the lsquo;surface web,rsquo; that is, the familiar sites you can access via search engines and see every dayrdquo; (Kindle Location 781). Hm, yes, okay. On the one hand, I want to run screaming into the street. On the other, I want to laugh. So . . . the deep, dark web is LARGER than our mere regular Internet? But it is also harder to break into? Perhaps the underworld of crime has always been that way, but something about Levinrsquo;s tone makes me wary. Moreover, he repeats many, many times that everyone, EVERYONE, will be hacked or in some way attacked by parties wanting access to our personal digital information. Mathematically, that doesnrsquo;t seem possible. Itrsquo;s like saying EVERYONE will have a car accident in his or her lifetime, or EVERYONE will contract TB or AIDS.

Some people just wonrsquo;t.All these admonitions, in a nutshell, are what Levinrsquo;s entire book is about. If I were to liken his book to a musical form I would say it is a rondo: Theme ABACADA or perhaps Variations on a Theme. He keeps repeating the same themes in slightly different ways. A full quarter of the book consists of five appendices, which repeat oft-harped-on information presented earlier.Again, Levin seems to offer the reader/consumer/citizen-of-the-world valuable data, but his Paul Revere appeal could have been reduced to bite-sized pieces. He could have skipped many of the useless or situaton-specific anecdotes and provided the reader with a little card to keep in the wallet or purse. Sometimes too much information can also be too little.1 of 1 people found the following review helpful. Not only are you the last line of identity theft defense, you are the ONLY defense.By consumser CAIdentity theft is a cottage industry. It almost seems unfathomable to the lengths at which thieves will go about stealing another persons or child's identity and for what purpose. This book explains it all, including why the government is so hesitant to make greater lengths to protect its citizens. The book is written in four parts. Honestly, parts I II can easily be condensed into a two sided trifold and handed out as a consumer protection advert. I recommend the reader gloss through those parts because you will not gain very much otherwise. I would suggest that a reader pay close attention to part III which is where the meat of the book is found. Part IV has some great references and lists current scams and stories to keep in mind. The author's bottom line is that the Cavalry is not coming to save you or protect you anytime soon. The odds of someone trying to use your identity is not and IF, but WHEN. You need to be prepared and this book offers the most up to date advice to prepare for that inevitable day.

Increasingly, identity theft is a fact of life. We might once have hoped to protect ourselves from hackers with airtight passwords and aggressive spam folders, and those are good ideas as far as they go. But the truth is, there are people out there -- a lot of them -- who treat stealing your identity as a full-time job.One such company is a nameless firm located in Russia, which has a trove of over a billion internet passwords. Another set up a website full of live streams of hacked web cameras, showing everything from people's offices and lobbies to the feeds from baby monitors. Even purchases made in person are still logged by retailers like Target, who are famously vulnerable to hackers.Adam Levin, a longtime consumer advocate and identity fraud expert, is your guide to this brave new world. By telling memorable stories and extracting the relevant lessons, he offers a strategy for dealing with these risks. You may not be able to prevent identity theft, but you certainly shouldn't wait until it happens to take action. Levin's approach is defined by the three M's: minimizing risk, monitoring your identity, and managing the damage. The book is also organized around the different problems caused by identity theft: financial, criminal, medical, familial, etc., enabling readers to dip into the sections most relevant to them.Swiped is a practical, lively book that is essential to surviving the ever-changing world of online security. It is invaluable not only for preventing problems but helping cope when they arrive.

"The real value of Levin's book, though, lies not in its diagnosis, alarming as it is, but in its practical advice on how to protect yourself. No one can make themselves completely safe, but much like burglars who target the most vulnerable house on the street, hackers will seek out those with the weakest online defenses. Levin has a wealth of suggestions for making yourself less vulnerable.rdquo; The Sunday Times (UK)In this alarming book, Levin, a consumer advocate and founder of the consulting agency Identity Theft 911, warns about the prominent dangers of identity fraud in the increasingly digital world [SWIPED is] a primer on the potential dangers and what's at stake.rdquo; Publishers Weekly