Password Logbooks and What Their Amazon Reviews Reveal About Their Users' Motivations, Beliefs, and Behaviors

Vijay Kothari
Department of Computer Science
Dartmouth College
vijayk@cs.dartmouth.edu

Ross Koppel
Department of Sociology
University of Southern California
rkoppel@sas.upenn.edu

Jim Blythe
Information Sciences Institute
University of Southern California
blythe@isi.edu

Sean Smith
Department of Computer Science
Dartmouth College
sws@cs.dartmouth.edu

***Abstract*—The existence of and market for notebooks designed for users to write down passwords illuminates a sharp contrast: what is often prescribed as proper password behavior—e.g., never write down passwords—differs from what many users actually do. These *password logbooks* and their reviews provide many unique and surprising insights into their users' beliefs, motivations, and behaviors. We examine the password logbooks and analyze, using grounded theory, their reviews, to better understand how these users think and behave with respect to password authentication. Several themes emerge including: previous password management strategies, gifting, organizational strategies, password sharing, and dubious security advice. Some users argue these books enhance security.**

I. Introduction

User behavior often conflicts with advice and policies prescribed by security practitioners. To name a few examples of such behavior:

- users write down passwords on sticky notes and affix them to computers,
- users use the same password for different services, and
- users ignore certificate warnings.

Recognizing and understanding such behavior is critical to improving security solutions. More generally, better understanding of user motivations, perceptions, constraints, and behaviors empowers security practitioners both to set more effective security policies and mechanisms and to offer better security guidance, which increases user compliance and mitigates the risks posed by circumvention, ultimately improving both individual and aggregate security.

Security decisions based on false assumptions—stemming from disconnects between what security practitioners believe about the users and the users as they actually are—will almost always be ineffective. Thus, it is imperative to learn what users do and why they do it, and then to tailor security policies, security mechanisms, and security advice based on this understanding. Indeed, this has been a major aim of usable security research, much of which relies on more traditional, controlled data acquisition methods, such as surveys and behavioral experiments.

In this paper, we build on and complement existing research by studying the numerous password logbooks, notebooks designed for users to record passwords and other information, that are available on Amazon.[1] We also analyze their reviews. Of the several hundred password logbooks available on Amazon, we examine 116 unique password logbooks, and we analyze 4,330 unique reviews for them. These reviews provide remarkable insights into reviewers' motivations, pre-purchase and post-purchase behaviors, and perceptions and misperceptions about security, among other findings.

We first discuss related work in section II and then provide an overview of our study in section III. We analyze password logbooks and their reviews in sections IV and V. In section VI we discuss our findings. We detail our methodology and note both limitations and advantages of the approach in sections VII and VIII. We conclude with suggestions for future work in sections IX and X.

II. Related Work

Gaw and Felten [1], as well as other researchers, studied password management strategies such as writing down

[1]These are also known by other names, e.g., password notebooks, password journals

EuroUSEC '17, 29 April 2017, Paris, France

http://dx.doi.org/10.14722/eurousec.2017.23018

passwords on paper and sticky notes and reusing the same password or small variations of a core password across services. Scholars have commented negatively on the use of dedicated logbooks to record passwords, and view any writing down of passwords as detrimental and a symptom of the poor authentication usability, e.g., [2], [3], [4]. While conventional wisdom and many security experts deplore the practice of writing down passwords, many experts have also advocated such practices so long as the passwords are securely stored, e.g., [5]. Irrespective of whether these practices are secure, researchers have shown the viability and rationality of user adoption of such practices, e.g., Herley [6] showed that many "incorrect" password management strategies users employ are rational.

Many researchers have used variants of grounded theory and other methods to better understand user password decisions and behaviors. Stobert and Briddle [7] interviewed users to learn how they manage their account credentials. They then applied grounded theory to explain the password lifecycle, i.e., the behaviors users employ to keep track of a password throughout its use. Fagan and Khan [8] conducted a survey on Amazon Mechanical Turk to understand why users make security-related decisions. Inglesant and Sasse [9] gave users a diary to record their password behaviors for a week and conducted interviews afterward, findings that users want to comply with security policies but struggle to do so. They suggested policies should be designed using HCI principles.

Ha and Wagner [10], have used product reviews to learn more about user behaviors, perceptions, and attitudes. Alkadi and Renaud [11] analyzed user reviews of password managers on the Google Play Store and the iTunes App Store, and they conducted a survey to understand user attitudes. In this paper we also analyze user reviews, but we do so on a larger scale with a significantly different subpopulation of users who circumvent often recommended security practices by using password logbooks.

Our work builds on previous efforts by a focused analysis of reviews and development of a typology of explanations (hereafter called *themes*). We illustrate each theme with examples from the products, their marketing, and their reviews. Other researchers—e.g., [12], [13]—have employed automatic user reviews analysis methods for products other than password logbooks. We, however, use grounded theory, blending manual and computerized text analysis to extract themes from reviews.

III. Study Overview

We define a *password logbook* as any printed book marketed for users to record passwords and related account information (e.g., names of services, usernames, security hints), as well as other computer and internet-related information (e.g., network settings, ISP telephone numbers).

We create a data set comprising password logbooks that have one or more Amazon Verified Purchase reviews, along with their reviews.[2] The final dataset comprises 116 password logbooks and 4,330 reviews for them with duplicate reviews removed. We analyze the products and used grounded theory methods to inductively construct common themes in the reviews using two coders. A complete discussion of the methodology and limitations is provided in sections VII and VIII.

IV. Product Findings

We reviewed 116 password logbooks. The most-reviewed book had 1,811 reviews, of which 1,687 were Verified Purchase reviews; on the other end of the spectrum, many password logbooks in our set had only a single Verified Purchase review. Indeed, as seen in Figure 1, a few password logbooks accounted for a large fraction of reviews. Once duplicate reviews were removed, we found that the first five products accounted for 2,973 of the 4,330 reviews or equivalently, 68.7% of the reviews.[3]

Figure 2 is a histogram of reviews by review date. As we gathered the final set of reviews on March 7, 2017, we have only a fraction of the reviews from 2017. Therefore, we derived a projection for the total number of reviews in 2017 by scaling the number of reviews we had seen in 2017 by the number of reviews posted in the previous three years over the fraction of reviews posted before or on March 7 in the previous three years. The graph reveals that password logbooks listed on Amazon have received more reviews in recent years. This may be due to a number of factors, e.g., more demand for password logbooks, more password logbooks available on Amazon, and people opting to buy books via online stores like Amazon instead of brick and mortar stores.

Password logbooks were generally highly rated with the average rating being 4.56 out of 5. As a few popular books covered most reviews, this is expected.

Front covers of ten of the password logbooks appear in Figure 3. Additionally, pictures from the interiors of four password logbooks are provided in Figure 4.

Our analysis revealed a number of features that differentiate the password logbooks:

- *Inconspicuousness:* Would an adversary not be able to recognize a password logbook as such? Some password logbooks had non-removable covers that said "password logbook" or had other indicators that enable people to easily identify it as a password logbook when closed. Others had similar covers and labels, but they could be easily removed and were intended to be removed. Some other books went one step further in that they masqueraded as a novel (e.g., see Figure 3g).
- *Password Security Tips:* Password logbooks provided various password security and book usage tips regarding keeping the password logbook in a safe place and not traveling with it, writing down password hints instead of passwords, not sharing passwords with others, using a pencil so passwords can easily

[2] "An 'Amazon Verified Purchase' review means [Amazon] verified that the person writing the review purchased the product at Amazon and didn't receive the product at a deep discount." [14]

[3] These numbers depend on which of the duplicate reviews to remove or rather, more precisely, which review of a collection of identical reviews for different books to keep. Still, as there were only a few duplicate reviews, the numbers would only vary slightly (less than 1%) depending on this choice. Please see VII for further details on how we handled duplicate reviews.

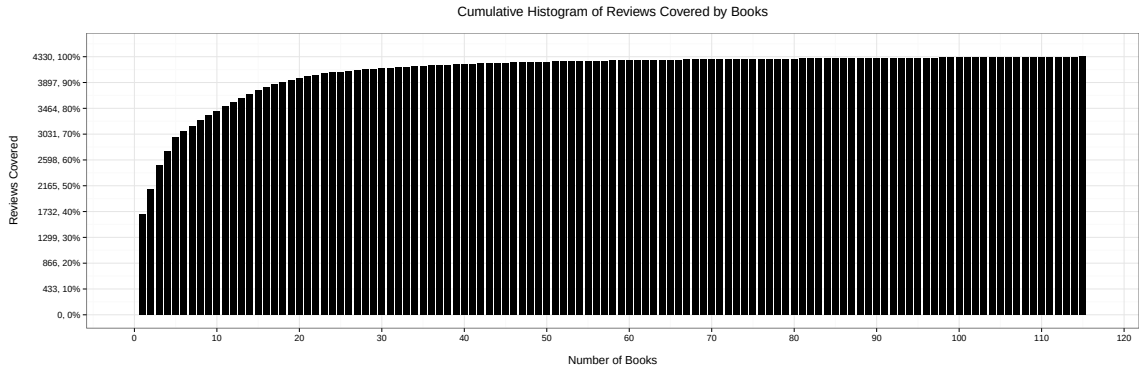


Fig. 1: *Cumulative Histogram of Reviews Covered by Books. This histogram shows the number of reviews covered by a subset of books, selected in non-increasing order of number of reviews. For example, the graph shows that the 10 most reviewed password logbooks account for 3,418 (*78.9%*) of the reviews.*

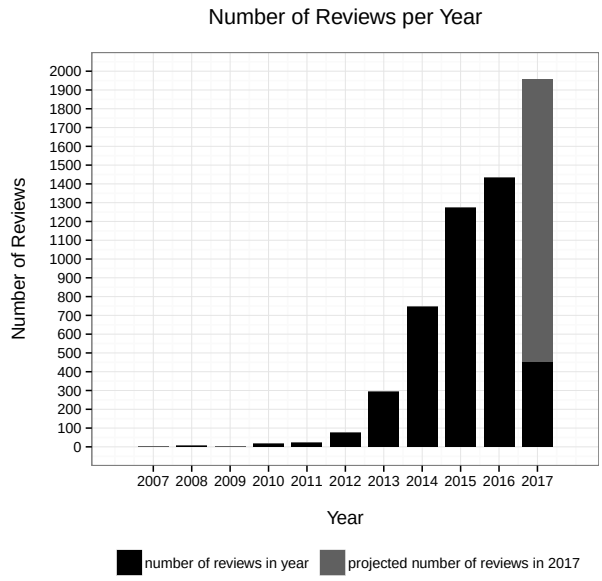


Fig. 2: *Number of (Amazon Verified Purchase) Reviews per Year. We collected reviews on March 7, 2017. The 2017 projection was obtained by multiplying the number of reviews seen in 2017 by a scaling factor; this scaling factor is the number of reviews in the years 2014-2016 divided by the number of reviews before or on March 7 in 2014-2016.*

and neatly be erased, and so forth. Some even gave instructions on how to create a strong password. Some tips contradicted the design and marketing of other password logbooks, even ones sold by the same vendor. For example, one password logbook advised the user not to travel with the book; however, the same vendor was selling a password logbook that was marketed as pocket-sized.

- *Durability:* Books varied in the durability of the binding, flimsiness of the cover, page thickness and ability to withstand ink and erasures, and other factors.
- *Aesthetics:* Books had a variety of different designs. A few books had unique aesthetics to target select demographics (e.g., children, women) and state such in their descriptions. For an example, the book seen in Figure 3c was marketed as "a fun kids' password journal with 'Top Secret' and 'Keep Out' on the front and back covers."
- *Size:* Books ranged in dimensions from 2.875" x 4.75" to 6.5" x 8.5". In general, smaller books could easily fit in pockets, purses, and briefcases, whereas larger books provided more space and were easier to read.
- *Tabs:* Some password logbooks had tabs that allowed the user to more quickly find their passwords by service name. Many books devoted the same number of pages to every pair of consecutive letters, corresponding to a tab, though other tab layouts existed. Most users appreciated tabs, but some were frustrated due to a misalignment between the number of pages dedicated to tabs and user needs, granularity of tabs, durability of tabs, and visibility of tabs (some tabs protruded for greater visibility).
- *Elastic Band:* Some logbooks had an elastic band attached to the back cover to keep track of the owner's place during use and to keep the book shut during non-use. An example of such an elastic band can be found in Figure 3d.
- *Contact Information:* Some books had space for the owner to enter their name, email address, and phone number. Of course, in the event that the password logbook is misplaced or lost, if this information is filled in, it may pose an additional privacy risk.
- *Other Entries:* Password logbooks ranged significantly in what information they allowed users to record. All password logbooks allowed users to record basic account credentials, i.e., site name, username, and password. However, many also allowed for other password-related information, e.g., multiple password entries per service with attached date fields, password question answers, notes. Moreover, many books had space to record other information that might be

(a) 1441303251 (b) 0996009825 (c) 1515382265 (d) 0735344620 (e) 1505432995

(f) 1631061941 (g) 1500863548 (h) 1441319441 (i) 152372398X (j) 1515246825

Fig. 3: *Front covers of 10 of the 116 password logbooks examined in this paper. Each image is located at https://amazon.com/dp/ASIN/ (ASINs specified in subcaptions).*

important to a computer user , e.g., home network information, software license keys. Figure 4 provides a few examples of entries within these books.

Numerous other password-related products are also available on Amazon, but they fall outside the scope of our study. Nevertheless, we briefly mention them here for completeness. These products include electronic password storage devices, books that give tips on creating and remembering passwords (including a unique flavor of self-help book entitled "Password Therapy"; see Figure 5a), books that suggest how to organize one's records, including passwords, and alternative password management solutions. A few of these products are provided in Figure 5.

V. Themes

Our analysis revealed numerous themes:

A. *Love This Book!*

Reviewers were often joyous about the logbooks they purchased. Some reviewers wished that they had known about password logbooks sooner. Others used words and phrases such as "essential," "vital," and "can't live without this" to express, often hyperbolically, their love for their password logbook.

Many reviewers considered the use of password logbooks (and similar circumventions) as an inescapable risk or reasonable tradeoff. Some argued that the requirement to track associations among services, usernames, and passwords, along with answers to security questions and other challenges (e.g., complex password composition requirements and frequent password resets) was overwhelming and that a password logbook was the best solution available.

B. *Inconspicuousness*

Reviewers generally valued inconspicuous password logbooks and, conversely, disparaged conspicuous ones. Some password logbooks had jackets or labels that said "password" on them. Some of these conspicuous covers were easily removable, but some others were not, which frustrated users. For example, one reviewer wrote:

> "It would be great if it didn't say 'Password Log' on the cover."

Some password logbooks resembled novels and blended in with other books. Reviewers generally found this clever. In reviewing a password logbook that masqueraded as a novel about a cat, a reviewer wrote:

> "No one thinks to look on the bookshelf or in a cat book for passwords."

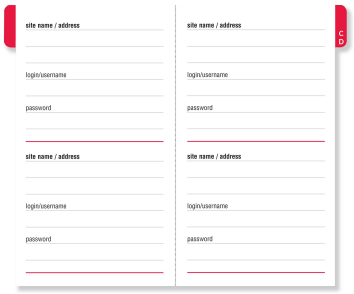
C. *Gifting & Spread of Circumventive Behavior*

Numerous reviewers purchased or planned to purchase additional password logbooks for friends and family. Some

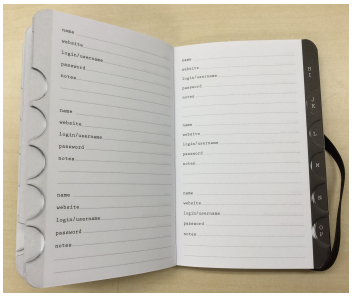
(a) 1441319077

(b) 1441319077

(c) 1441319077



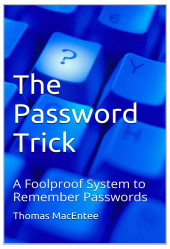
(d) 1441315969



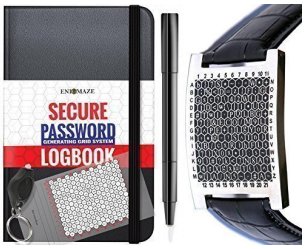
(e) 0735344620

(f) 1441319441

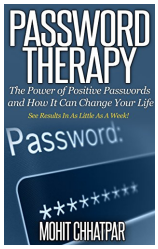
Fig. 4: *Images of interiors of 4 of the 116 password logbooks we examined in this paper. The first 3 images display pages from different sections of the same book. Each image is located at https://amazon.com/dp/ASIN/ (ASINs specified in subcaptions).*



(a) 2136504160



(b) B01I94N9TC



(c) B00REGSI6G

Fig. 5: A few other password-related products.
Each image is located at https://amazon.com/dp/ASIN
(ASINs specified in subcaptions).

purchases were gifts based on projected utility, whereas others were made upon request. Also, some reviewers mentioned that they purchased password logbooks after they saw friends or family use them. One reviewer wrote:

> "My mom bought one first and I saw how useful it can be so I got one too."

Gifting of password logbooks can be viewed as a way of spreading circumventive password behavior. This extends previous work that finds users obtain security advice from friends, families, and coworkers (e.g., [15], [16]). It also corroborates our earlier findings in enterprise settings [17]. That is, it's insufficient to only consider security advice prescribed by the enterprise; rather, it's just as important to consider security advice and behaviors spread by co-workers, family, friends and other enterprises.

D. Maintaining Passwords for Family Members

Reviewers explained that they used their password logbooks to keep track of their family members' passwords. For example, one reviewer wrote:

> "How about when your elderly parents keep having to change their password because they swear they are putting in the right one but it's not working... Yes, I put my [mom's] and [dad's] passwords in too, plus I did buy my mom one."

Another reviewer mentions:

> "Bought this for my father. Love how it is alphabetical. He was recently in the hospital and I found 3 sheets of ripped paper/notes with all his internet sites and passwords...some listed 2 or 3 times with different passwords. I had to take over bill paying while he was sick and this is working like a charm."

Another wrote:

> "I'm trying to get everyone organized. This is for my mother so I can find her passwords when she gets into trouble on the computer and I have to try and fix it. Before she had a confused and garbled note pad."

Indeed, many reviewers were concerned about how their family would get by in the event that they were no longer accessible. For example, one reviewer wrote:

> "If I were unavailable for any reason, my husband can now get into all the accounts for our kids

> activities, and not miss a beat! He can also get into all our bill paying areas if there is ever an issue. Must be kept under lock and key, but has given me a piece of mind!"

Another reviewer wrote:

> "Even though I use a password manager, I used this book in case something happens to me, my kids can get to the accounts."

This last quote is particularly interesting because the reviewer uses a password manager, which is often stated to be a good password management strategy, but keeps a password logbook as well.

Reviews also suggested that these concerns were prompted by life experiences. One reviewer stated:

> I'm sure this will also be useful for the dreaded "just in case" moment. A friend of mine's husband passed away a few years ago. To this day I don't know if she was ever able to access any of his sites on his computer because she didn't know any of his passwords. Always something to think about.

Another wrote:

> Great little logbook to have handy. My husband recently passed away and I had a hard time finding a couple of things. This made me realize just how much I handled of the household finances and things. If something happened to me, my son would be left trying to [decipher] my mess. Keeps things organized and in one place and easy to secure where no one can stumble across it if need be.

E. Repeat Purchases and Multiple Logbooks

Some reviewers stated they had purchased a password logbook prior to the one for which they were writing a review. Reasons for doing so included: the previous password logbook lacked durability, the previous one lacked sufficient entries to store all passwords, and the reviewer wished to keep two or more password logbooks in different locations, e.g., one at home and one at work.

F. Age

Indicators of age were prevalent in a number of reviews. Reviewers often used old age and perceived memory loss as justification for using password logbooks, e.g., one reviewer wrote:

> "We are seniors with short term memory loss."

In contrast, as we noted earlier, some password logbooks were designed for children and were marketed as inculcating good security habits.

G. Size, Portability, and Storage

Many reviewers commented on the size and portability of password logbooks. Some reviewers preferred smaller, easily transportable books. Others preferred larger books capable of holding more passwords. Similarly, there was a tradeoff with the font size between readability and quantity of passwords that could be stored within the book.

Some reviewers routinely carried their password logbook in a briefcase, purse, or other carrying bag. Some left them on top of their desk or in their desk drawer. Others took effort to keep it in a safer place, e.g., a lockbox. These behaviors pertaining to carrying and storing the password logbooks often affected user preferences of the size of the password logbook.

H. Organization and the Centrality of Digital Life

Many reviewers stated these password logbooks helped them organize their accounts. In addition to just website addresses and passwords, users sought books that allowed them to store other information to access their accounts, e.g., usernames, answers to security questions. For example, one reviewer wrote:

> "There is not enough room for related information to passwords such as secret codes and question."

Another said:

> "[This is] perfect for those of us who are either brave to risk our information by signing up for numerous websites and we can't remember the password nor the website because there were so many, and for those that are new to the internet age and can't remember their name let alone a password to the only website they signed up for, this is the perfect book to use."

Moreover, many reviewers stated they used password logbooks as major organizing tools for their lives and their families. The books became a centerpiece of critical information about all of their accounts, wills, addresses, and other essential information.

I. Alternative and Previous Password Management Strategies Inadequate

A number of reviews reveal that alternative password management strategies, whether classified under the umbrella of circumvention or not, were inadequate. For example, one reviewer wrote:

> "Usually I would have just kept them in a file on a flash drive but....well...we did that and it got [corrupted] and now there are 4 accounts I am still trying to have shut down cause I don't remember ANY of the info I used to start the account."

Reviewers eagerly shared their previous password management strategies. These included writing down passwords on sticky notes, index cards, backs of envelopes, scattered sheets, and scraps of paper; more organized solutions including storing passwords in an envelope containing paper scraps, a binder containing sheets of paper, and notebooks; storing passwords in text files and Excel spreadsheets; storing passwords on phones; and, as noted earlier, storing passwords on flash drives.

J. Risks

Many reviewers acknowledged the risk of keeping a password logbook, specifically, that it could be lost or stolen and wind up in the hands of an unscrupulous character. However, most, but not all, believed that password logbooks were better than other password management strategies. A few sub-themes emerged here:

1) Perception that Password Logbooks Improve Security: Some reviewers suggested that even though password logbooks pose risk, using an alternative password management aid would pose even greater risk, while not using any aid would cause them to struggle with remembering passwords, driving them to reuse passwords or to use weaker passwords. One reviewer wrote:

> "Not only do I have too many passwords now to remember, but I just know reusing the same password for multiple sites is a big no-no, even if they are really good passwords! This solves both issues."

Another wrote:

> "I use this almost every day. Having everything in one spot has made my life much easier. Without my passwords in the computer, I feel they are much more secure."

2) Risks are Negligible or Could Be Mitigated: Some reviewers recognized that there are risks associated with using password logbooks. However, they felt these risks were insignificant. For example, one reviewer wrote:

> "Yes, obviously, if your book gets stolen that's a problem but it's a problem if your password app account is compromised or someone reads your thoughts, too, so everything is a risk and I will take a risk for convenience."

Others believed that naive usage might be risky, but taking appropriate precautions would mitigate these risks. For example, one reviewer wrote:

> "Okay. I have read the objections to this means of keeping one's passwords–and I get it–but there need not be any problems! I would not travel with this anyway, so that risk is eliminated. Still, there are ways to enter the info into this book that make it impossible for anyone to sabotage you, by stealing your info. I do not write out the full names of the websites I frequent; I find creative ways to abbreviate the names, so that no one other than myself could guess what the site is. I select passwords/phrases that I will still know, even after I substitute x's or underscores (_) for some of the characters. So, again, unless someone is psychic, they will not be able to get my pass codes. There is plenty of room to write–perhaps, too much, as my only complaint about this book is that it is too big. I would have preferred one no larger than a 3 x 4, but decided to go with it, given all the other positive reviews. Size makes it easily hide-able enough in your home. Use your common sense and this will be just fine. :)"

3) User Perceptions of Risks of Using Password Managers.: Almost all reviewers valued the password logbooks they purchased, but there were a small fraction of reviewers who were dissatisfied with their purchase, and a minuscule fraction who disapproved of password logbooks altogether. Given the subpopulation we're considering of reviewers who had purchased password logbooks on Amazon, this skew makes sense. One reviewer said they purchased and sent a password logbook as a gag gift to a friend who works in security. The reviewer then cautioned against using password logbooks, suggesting password managers as a more secure alternative. As stated above, this reviewer was an anomaly amongst verified purchasers.

To explore this theme further and to see how other users would respond, we temporarily broadened the scope of our reviews to include a small set of unverified purchase reviews, in which we saw more criticism of password logbooks. Many reviewers suggested password managers to be a lower-risk solution. Some justified their statements. Some rebuked users for using password logbooks. These reviews led to interesting and surprising dialogue that shed light on why some users choose to use password logbooks even when they're aware of password managers. For example, one individual no longer trusted their password manager because the antivirus software they were using classified it as a Trojan. Another stated:

> "I purchased LastPass a year ago and was dismayed to get an alert from them that their system had been compromised. My data wasn't compromised, but decided then and there nothing is really safe. I prefer to have something that I have control of, like this small book, than give my information over to a service where I have no control of where information is stored or how it is protected.

Curiously, one individual stated that the book was a bad idea, but then suggested a method to generate what they deemed strong, memorable passwords; however, the suggested method is easily susceptible to a password reuse attack by an adversary who notices the pattern.

K. Tricks and Advice

Reviewers were very willing to share what they thought of as clever tricks and prudent advice. This included writing down passwords in pencil so they could easily be erased, writing in what is effectively a password hint in lieu of the actual password, storing the password logbook securely, leaving out contact information so an adversary cannot identify who the book belongs to (though some purchasers appreciated space for listing contact information), etc.

For one example, a reviewer wrote:

> "Write your entries in pencil! Even if it is for an account that you suspect will always have the same information, there are plenty of reasons that entries in pencil are beneficial. Your account could be hacked forcing you to change a password, you could change banks or email accounts, the website address to the business may even change. Much simpler and cost effective to erase/edit an entry, rather than buy a new book."

Another reviewer wrote:

> "I sometimes consult with people who have problems remembering their passwords. First, I teach them a 'reminder' method, then I gift to them this little book, where they write their password 'reminders.' Using a 'reminder' method (where you don't put the actual password, but instead something that reminds you of the password), this book is invaluable. And if it goes missing, it's not the end of the world because nobody will understand how to use it. And, if you're smart, you won't put your name (or any other identifying info) in the book. This should not be the ONLY place you have passwords, because that would be like not backing up at all, and we've all heard those horror stories. But for quick reference at home or in the office, it's a great idea. Like the 'little black address book,' it's indispensable."

Yet another wrote:

> "To make your passwords in your book even more secure, add an extra special character that you never use in any password. Then ignore that special character whenever you enter your password. For example, put @ into each password just as a ruse. Or use some variation, such as ignoring the eighth character in each password."

VI. Discussion

We acknowledge the irony of users writing down account credentials in password logbooks, some of which are even labeled "Password Logbook," violating the often prescribed security advice that you should never write down your passwords. Adoption of these books is at least partially rooted in well-intentioned, but potentially counterproductive, password policies and password authentication protocols. The cognitive burden of having to remember associations between service names, usernames, and passwords, along with other challenges such as having to remember answers to security questions or remembering a password to an old account after a mandatory password reset, leads users to use these password logbooks. For example, one reviewer wrote:

> "My memory is not bad but every website now wants passwords and security questions. I am so tired to trying to remember every one."

That is, we may be seeing an *uncanny descent*: increasing the complexity of password policies with the expectation of improving security may actually make things worse by driving users to engage in riskier practices, such as writing down and reusing passwords, to alleviate the increased cognitive burden of managing their passwords under the new password policies.

There's also the reverse irony that these password logbooks may provide better security than the alternative password management strategies users employ. The knee-jerk reaction of discrediting the use of password logbooks as an unacceptable form of circumvention that only worsens security may be premature or not sufficiently nuanced to reflect the reality of regular users' lives. Password logbooks often supplant other, more risky forms of circumvention and alternative password management strategies. Moreover, many users don't believe they're capable of memorizing many strong, unique passwords which is why they turn to password logbooks; many view password logbooks as a convenient tool that provides more convenience, better security, and/or better organization than their current password management strategy. For example, one user wrote:

> "I also like that I don't have to use the same password for every site because it's all I can remember."

A number of reviewers expressed awareness of the risks associated with using password logbooks, but used them despite the risks. The reviews suggest that many users employ a rational decision-making process to settle on password logbooks; they determine alternatives provide less value in terms of convenience or security and, in many cases, both. This is in agreement with the literature, e.g., [6].

While we make no claim that password logbooks are optimal or even good options for password management, we are suggesting— as has been suggested by reviewers— that in the absence of password logbooks, some users would be at greater risk. Prescribing good security behavior that users don't adopt may be worse than giving users suboptimal advice that is still pretty good, which can easily be followed. That is, we should not expect users to engage in the most secure behaviors, but we should instead nudge users toward the best security solution amongst those they're willing to put up with. We must also acknowledge the limitations of proposed security solutions. For example, while some password managers may be more secure than password logbooks, in the event that the user is unexpectedly incapacitated, they provide no mechanism to transfer account credentials to family. Indeed, earlier we quoted a reviewer who used a password manager, but still had a backup password logbook for this very reason.

VII. Methodology

To conduct our analysis, we downloaded both the product pages for each password logbook, as well as Amazon Verified Purchase reviews for them.

We searched amazon.com for the key phrase "password logbook." We then constrained the search to include only those products classified under the category of "Books." From the results, we obtained a list of 132 password logbooks in sorted order of reviews with at least one review, with the most reviewed book appearing first. However, five of these did not adhere to our descriptive definition of a password logbook, narrowing our dataset to 127 books.[4].

We downloaded both the product pages for the 127 password logbooks, as well as all 4,778 Amazon Verified Purchase reviews for them. Next, we removed duplicate reviews; if we found two or more reviews that had the same author, review title, and review text, we kept only one copy of the review. Duplicate reviews appeared for various reasons. Some password logbooks were listed as different products but were

[4]The five discarded books roughly fell under two categories: regular address books, e.g., https://www.amazon.com/dp/1593593899, and books that served as guides to organize one's records with space to record things like tax records, property records, and even passwords, e.g., https://www.amazon.com/dp/1413323154/.

just a different edition of another book, which had the exact same set of reviews; 7 of the 127 password logbooks were doubly-listed, accounting for 413 duplicate reviews. 35 more duplicate reviews were found using a script. Additionally, 4 more password logbooks were removed from our dataset: 1 logbook was removed because it only had a single review, which was a duplicate; the 3 other logbooks were removed because they only had non-Verified Purchase reviews. These steps and manual inspection of reviews reveal most duplicate reviews were attributable to doubly listed logbooks and instances of reviewers buying multiple logbooks and leaving the same review for all of them, e.g., because the review involves a comparison of them or because the reviewer bought multiple editions as gifts and left the same review for each edition as they are essentially the same other than cosmetic differences, although we did see a few fraudulent reviews. Please see Section VIII for further details.

Our final dataset comprised 116 password logbooks and 4,330 reviews for these password logbooks, with duplicates removed. We extracted relevant data from the reviews and two of us applied grounded theory to determine common themes from the reviews.

VIII. Limitations and Advantages

The study has the following limitations:

- **Some Reviews May Be Fake or Biased:** Any study on a corpus of Amazon reviews may suffer from the presence of illegitimate reviews. For example, the reviewer may have bought the product at a discounted rate in exchange for leaving a review; the reviewer may have been paid to leave a positive review; the reviewer may even have been paid to leave a negative review for a competitor product; the reviewer may have left a review to gain credibility. To address this problem, we restricted the data set to comprise solely Amazon Verified Purchase reviews for products. However, we still came across some reviews that we believe to be fake, although we believe they constitute only a small fraction of all reviews. Moreover, the primary motivation behind this study is to glean insights into how some users think about password authentication; the existence of a few fake reviews has negligible impact on this pursuit.
- **The Sample Set:** Any study on a corpus of Amazon reviews also inherently limits its sample set to authors of Amazon reviews. In our case, this meant that (aside from a few reviewers–e.g., one review purchased a password logbook as a gag gift for a friend), reviewers were drawn from the subpopulation of general users who willfully circumvented recommended security practices, bought a password logbook on Amazon, and wrote a review for said password logbook. While this sample undoubtedly does not reflect the entire population of users, we believe there's valuable information to be had in these reviews— and, indeed, the sample reveals the existence a subpopulation who engages in the practice of using password logbooks.

Despite these limitations, our approach— and ones similar to it— have a number of benefits:

- **The Sample Set:** Our approach is less susceptible to some other selection biases common to other studies. For example, many academic studies involve a disproportionately large fraction of college students. Some themes we saw simply would not emerge with such a sample set. For this reason, our findings in this study nicely complement those in the existing literature.
- **Scale:** Our data set of reviews comprises 4,330 reviews and has no monetary cost. In general, approaches like this, i.e., ones that looks at user product reviews, posts in forums, comments on articles, and so forth, provide great scale for minimal cost.
- **Reviews are Volunteered:** Perhaps the strongest aspect of this approach is that the information contained in these reviews is provided to us directly from the user without any request for information. A number of the biases present in face-to-face interactions, surveys, or other solicited feedback, is not present here. Moreover, we speculate that the reviewer's state of mind is different in writing these reviews than it would be if their feedback were solicited, regardless of such biases. That is, the user isn't primed to deliberate about their motivations, beliefs, and behaviors regarding passwords, as they likely would be in a survey.

IX. Future Work

While this work provides valuable qualitative data about certain users, due to the limitations mentioned in Section VIII, we cannot provide meaningful quantitative data about users in general. Follow-up studies, such as surveys and behavioral experiments conducted on a representative sample of a broader subpopulation of users that further explore the themes mentioned in this paper may provide valuable quantitative data to further assist in suggesting security policies and mechanisms to employ and to suggest how we should communicate with and advise users regarding security.

Similar approaches to this, that involve analyzing other reviews, forum posts, and comments on articles, may serve useful in developing a better and understanding of the user. Data sources like Amazon customer reviews also provide valuable metadata. For example, review dates may enable researchers to study how user perceptions and attitudes change over time, which is hard to attain retroactively via other means. Similarly, comparisons between reviews on, say, amazon.com and amazon.co.uk, would enable researchers to study regional variations in beliefs and behaviors. It would also be enlightening to explore data sources that provide dialogue amongst users.

X. Conclusion

We examined a subset of available password logbooks on Amazon and their reviews. The sheer existence and diversity amongst password logbooks and the magnitude of reviews available for them was illuminating in its own right. Moreover, a number of interesting themes emerged in the process of analyzing reviews, some of which provide new insights into user beliefs and behaviors.

ACKNOWLEDGEMENTS

This material is based upon work supported by the Maryland Procurement Office under Contract No. H98230-14-C-0141. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Maryland Procurement Office. Koppel's work was supported in part by NSF CNS-1505799 & the Intel-NSF Partnership for Cyber-Physical Systems Security & Privacy.

REFERENCES

[1] Shirley Gaw and Edward W Felten. Password Management Strategies for Online Accounts. In *Proceedings of the Second Symposium on Usable Privacy and Security*, pages 44–55. ACM, 2006.

[2] Eiji Hayashi and Jason Hong. A Diary Study of Password Usage in Daily Life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2627–2630. ACM, 2011.

[3] Anne Adams and Martina Angela Sasse. Users are Not the Enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[4] Alexa Huth, Michael Orlando, and Linda Pesante. Password Security, Protection, and Management. *United States Computer Emergency Readiness Team*, 2012.

[5] Bruce Schneier. Schneier on Security. Write Down Your Password. https://www.schneier.com/blog/archives/2005/06/write_down_your.html. Accessed: 03-11-2017.

[6] Cormac Herley. So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *Proceedings of the 2009 New Security Paradigms Workshop*, pages 133–144. ACM, 2009.

[7] Elizabeth Stobert and Robert Biddle. The Password Life Cycle: User Behaviour in Managing Passwords. In *Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 243–255. USENIX Association, 2014.

[8] Michael Fagan and Mohammad Maifi Hasan Khan. Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 59–75. USENIX Association, 2016.

[9] Philip G Inglesant and M Angela Sasse. The True Cost of Unusable Password Policies: Password Use in the Wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 383–392. ACM, 2010.

[10] Elizabeth Ha and David Wagner. Do Android Users Write about Electric Sheep? Examining Consumer Reviews in Google Play. In *Consumer Communications and Networking Conference (CCNC), 2013 IEEE*, pages 149–157. IEEE, 2013.

[11] Nora Alkaldi and Karen Renaud. Why Do People Adopt, or Reject, Smartphone Password Managers? In *1st European Workshop on Usable Security, Darmstadt*, volume 18, pages 1–14, 2016.

[12] Marios Kokkodis. Learning from Positive and Unlabeled Amazon Reviews: Towards Identifying Trustworthy Reviewers. In *Proceedings of the 21st International Conference on World Wide Web*, pages 545–546. ACM, 2012.

[13] Minqing Hu and Bing Liu. Mining and Summarizing Customer Reviews. In *Proceedings of the Tenth ACM SIGKDD International conference on Knowledge Discovery and Data Mining*, pages 168–177. ACM, 2004.

[14] About Amazon Verified Purchase Reviews. Amazon. https://www.amazon.com/gp/help/customer/display.html?nodeId=201145140. Accessed: 03-11-2017.

[15] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *Security and Privacy (SP), 2016 IEEE Symposium on*, pages 272–288. IEEE, 2016.

[16] Emilee Rader, Rick Wash, and Brandon Brooks. Stories as Informal Lessons about Security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, page 6. ACM, 2012.

[17] Jim Blythe, Ross Koppel, and Sean W Smith. Circumvention of Security: Good Users Do Bad Things. *IEEE Security & Privacy*, 11(5):80–83, 2013.