Investigating Web Service Account Remediation Advice

Lorenzo Neil
North Carolina State University

Elijah Bouma-Sims
North Carolina State University

Evan Lafontaine
North Carolina State University

Yasemin Acar
Max Planck Institute for Security and Privacy

Bradley Reaves
North Carolina State University

Abstract

Online web services are susceptible to account compromises where adversaries gain access to a user's account. Once compromised, an account must be restored to its pre-compromise state in a process we term "account remediation." Account remediation is a technically complex process that in most cases is left to the user, though some web services provide guidance to users through help documentation. The quality of this account remediation advice is of paramount importance in assisting victims of account compromise, yet it is unclear if this advice is complete or suitable. In this paper, we analyze account remediation advice from 57 popular U.S.-based web services. We identify five key phases of account remediation, use this five-phase model to develop a codebook of account remediation advice, then analyze topic coverage. We find that only 39% of the web services studied provided advice for all phases of account remediation. We also find that highly-ranked websites and sites with a previously disclosed data breach have more complete coverage than other sites. Our findings show that account remediation should be more carefully and systematically considered by service providers, security researchers, and consumer advocates, and our detailed analysis will aid in creating better guidelines for users and services.

1 Introduction

Online web services allow people to create accounts that store information and communicate with others. Compromises of these accounts are a pervasive problem, with billions of accounts being compromised in 2019 alone [21]. Account compromises allow the attacker to steal service, surveil the activities of the victim, abuse the system, or otherwise compromise the confidentiality, integrity, or availability of the account. When compromised, an account must be re-secured in a process we term *account remediation*. In this work, we determine that there are five key phases for account remediation. In order, these are: detecting the compromise, recovering access to the account, limiting access by the attacker, restoring the account state and associated data to the pre-compromise state, and taking action to prevent future compromises.

After having accounts compromised, the authors discovered first-hand how technically complex and frustrating the task of account remediation can be. We found anecdotally that help documentation provided by web services differs drastically in terms of completeness. When documentation on remediating compromises is lacking, it is much more difficult for users, even technically-savvy users, to remediate a compromise. Therefore, the advice given by web services to help users remediate their accounts is of critical importance. We realized that not only is the advice given to users critical for navigating the process correctly and effectively, but the advice also acts as a proxy for understanding how the organization responsible for creating it views the process.

In this paper, we make the following contributions:

- **Model Account Remediation:** We develop a five-phase model to capture each phase of account remediation, from initial compromise discovery to remediation. We then use this five-phase model to fully represent the range of activities a user may engage in during account remediation in a qualitative codebook.
- **Characterize Webservice Account Remediation Advice:** We use our codebook to evaluate the account remediation advice of 57 popular web services in the United States, providing a window into the resources available to users as well as acting as an implicit measure of web services' own understanding of the issue. We find this advice is sparse and underspecified, especially when we

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Virtual Conference.

examine activities unique to account remediation. For example, fewer than half of the services studied provide *any* guidance to limit further access by an attacker.

- **Broad Trends and Recommendations:** We find that average phase coverage is higher for services that either are very popular or that have a previously disclosed data breach. We also provide recommendations for web service owners and future researchers.

We note that *account recovery,* defined as the process of restoring a legitimate user's access to an account if credentials are lost or changes, has received substantial research coverage, as we discuss in Section 2. However, account recovery is only a single phase of account remediation. Areas such as limiting an account's access and restoring an account's original state are crucial for account remediation, but have received little research attention.

2 Related Work

A user's mental model on security ultimately informs their security decisions with their devices and online services [12]. Prior research has focused on the user's security mental model [5,29] and how they interpret security advice and warnings [1]. Improving a user's basic knowledge in security limits the chances of their online services being compromised [5], though users may reject the advice if it presents a poor cost-to-benefit ratio or it threatens their privacy [15, 29, 29, 30]. Previous work has found that it is hard for end users, and even experts to prioritize security advice [30]. User advice can cover all five phases of account remediation, though a significant body of work has focused on detecting compromise and account recovery.

Many account compromises stem from stolen credentials. Prior work has measured how the risk of stolen credentials varies between phishing, malware, or data breaches and predicts the chances for total online account takeover from stolen credentials [24, 27, 34]. Billions of stolen usernames and passwords are also widely available in underground forums [25, 35–37]; these data sets have been used to create systems that alert users if their usernames or passwords are vulnerable and have been publicly exposed [25, 35, 37]. Other work on detecting compromised accounts [33] focused on building models to represent normal account behavior and then using that behavior to analyze current account behavior for anomalies or unusual activity [6, 8, 19, 31]. Recent work has investigated whether users are informed about data breaches, how they feel about them, and whether they have taken or plan on taking action [22]. In our work, we go beyond compromise discovery and account recovery, also focusing on remediating harm to the compromised accounts.

Account recovery mechanisms restore access to an account after credentials are lost or changed by an attacker after a compromise. Virtually all widely used password recovery mechanisms, including secret questions and e-mail reset links, have well-understood vulnerabilities and deployment limitations [26]. Many major webmail providers employ security questions that can be solved through data mining, are easily guessable, or have low memorability over time [3, 32]. Prior work on account recovery mechanisms investigated different authentication schemes [4] and password reset strategies [16]. Password recovery schemes may also be vulnerable to man-in-the-middle (MitM) attacks [13, 14]. Compromise detection and account recovery have both been widely studied topics, yet to the best of our knowledge, we are the first to study account *remediation* from a holistic perspective.

3 Methods

In this section, we describe our methods (see Figure 1): codebook development (3.1), account remediation model creation (3.2), ensuring inter-rater reliability among coders (3.3), coding account remediation advice from 57 web services (3.4), and our analysis of differences in the coverage of account remediation advice among web services based on their popularity and disclosure of data breaches (3.5).

3.1 Codebook Development

Three authors created the codebook deductively based on nine popular web services' account remediation advice, inductively informed by authors' personal and professional experience with account remediation, and existing research on account recovery, data breach notification and behavior, and authentication. We first annotated nine popular web services' account remediation advice, [1] then iteratively built and revised our codebook and operationalized the codes. We finalized our codebook when we were able to unambiguously apply it to assess account remediation advice for the initial nine web services. This was evidenced by high agreement when applying the codebook (Krippendorff's Alpha > 0.75 for all three coders for independent coding [9, 10]). In line with recommendations for qualitative coding, we used this score not only to assess our level of agreement, but also to investigate where and how we disagreed [2, 23]. If that coefficient was not met when we compared our codes, we used it as an opportunity to better define and disambiguate codes, as well as discuss what causes confusion or disagreement.

The final codebook contains five top-level codes, *compromise discovery*, *account recovery*, *limiting access*, *service restoration*, and *prevention*, which we call the five phases of account remediation, as well as sub-codes that represent concrete advice, For example, in *prevention*, we have a sub-code "enable 2FA", which describes advice to enable 2-FA for an account to prevent a *future* compromise.

[1] Facebook, Netflix, Skype, Spotify, Twitter, LinkedIn, Google, Yelp, Walmart

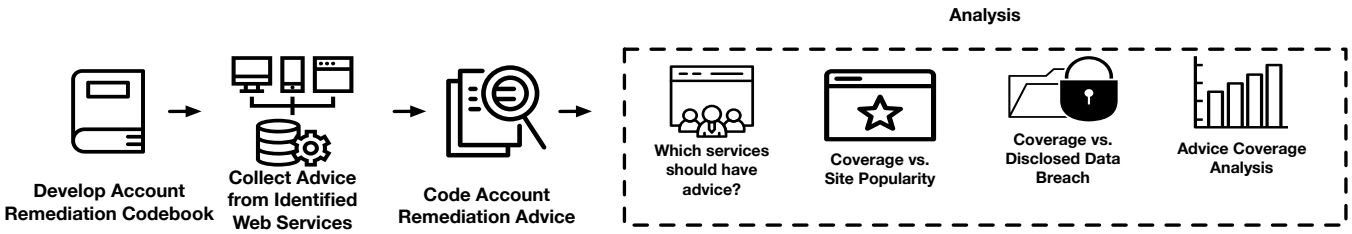

Figure 1: Methodology: codebook and model development, data collection and analysis.

3.2 Account Remediation Model

We explain the account remediation process as five phases of account remediation: *compromise discovery*, *account recovery*, *limiting access*, *service restoration*, and *prevention*, corresponding to our codebook's top-level categories.

Compromise discovery describes a user observing suspicious activity from their account or service that indicates a possible compromise, for example: "If you notice unfamiliar activity on your Google Account, someone else might be using it without your permission." (Google).

Account recovery describes the process for users to regain access to their account after losing access to it or having it compromised. We differentiate account remediation from account recovery in the sense that account recovery is only one phase in the account remediation process. An example of advice for *account recovery* is: "Change your password or send yourself a password reset email." (Instagram)

Limiting access describes preventing current and future unauthorized access from adversaries, for example: "Sign out of all devices connected to your account unless you believe your device has been stolen." (Netflix)

Service restoration describes restoring an account's original settings, content, or state before a compromise. An example of advice for *service restoration* is: "After signing in, you'll want to review the recent activity on your account." (Microsoft)

Prevention describes preventing future compromises by taking steps to further secure an account, like "Never click suspicious links, even if they appear to come from a friend or a company you know" (Facebook).

While advice coverage was not uniform across services, we found that the concept of the top-level categories (our five phases) was present across services. While we theorize that these five phases conceptualize account remediation in general, we do not imply that each specific subcode in each phase has to be covered by all services to provide complete advice, as service offerings may differ. We established this model to account for a wide range of advice and describe the majority of account remediation steps.

3.3 Training and Reliability

Following the development of the codebook, the main author trained two supporting coders on the nine initial web services, again measuring inter-rater reliability to pinpoint and resolve disagreement and to determine the successful conclusion of the training phase. The agreed-upon coding by the three codebook developers was used as ground-truth for training, and once Krippendorff's Alpha consistently exceeded 0.75, we considered the new coders competent to apply the codebook [10].

After the training phase concluded, the supporting coders then coded the rest of the web services individually. The primary coder independently double-coded a select subset of web services from each supporting coder, usually those that had been subjectively the hardest to code. After each week of independent coding, the primary coder met with each supporting coder separately to resolve disagreements, errors, and confusion, as well as to make sure that coding strategies did not diverge over time.

3.4 Collecting Advice from Web Services

In this section, we explain our process for web service selection, how we collect and store the advice, and how we established groups of web services for research questions.

Service Selection Criteria: We referred to two lists generated from the Tranco Website Ranking Service [28] to identify web services of interest. The lists were generated on March 31, 2020 and August 18, 2020. Using these Tranco lists as a reference, we examined web services that were U.S.-based, allowed user online account creation, and provided publicly available account remediation advice. We chose U.S.-based web services since all authors are fluent in English. We excluded adult-content web services from the study, as our research was performed on computers owned by a public university. Finally, we excluded services that were unreachable at the time of data collection.

Finding Advice: To ensure the totality of advice collection, we collected account remediation advice from web services by both manually browsing their help pages and through search queries on the website and Google. When navigating the web

service, we searched both the help center sections and security settings (if available). We queried the help center with the template phrases: "My account was compromised" and "My account was hacked". Once we found a web service's main page for account remediation advice, we also collected every relevant link mentioned on that page for account remediation. We further extended our collection of advice by Google search querying for any account remediation advice from the target web service based on text snippets we found on advice sites, our own experiences, and anticipating the spectrum of possible user queries. Our Google search queries were the following: "My [web service] account was compromised" and "My [web service] account was hacked". We added any new account remediation advice that was not found when navigating the web service. This multi-step process ensured that we identified all relevant account remediation advice from a web service. We note that many large companies have separate web services served by the same account management; one example is Google and YouTube. In such cases, we only include an advice policy once.

Content Exclusion Criteria: For our analysis, not all information is appropriately considered account remediation advice. For example, we do not consider advice for accounts that were suspended due to actions of the user or suspensions that were self-inflicted. Secondly, we did not include advice within forums or posts by other users on the service or on third-party sites, because such information may be inaccurate, outdated at the time of collection, or from an untrustworthy source. We also exclude advice documents when they consisted *solely and entirely* of a suggestion to contact the service.

We also only collect advice available without requiring a logged-in web service account to replicate the process a user would take if they could not access their compromised account and needed guidance. This strategy also allowed us to collect all relevant advice regardless of the login status. After our initial data collection, we observed that financial services and universities had been almost entirely excluded by this strict criteria. Owing to the importance of these two industries as targets of compromise, we revisited these services to collect publicly available remediation advice. Out of an abundance of caution, in Section 4.3 we include results with and without the financial service and university data.

Collected Datasets: We divide our collected data into two groups, shown in detailed tables in the Appendix. Both groups account for 57 total web services. The *very popular* web services dataset consisted of the top 31 web services (as ranked by Tranco) that were U.S.-based and offered account remediation advice. To this dataset, we added one additional service (Yelp) slightly outside of the Top 31 that had been chosen arbitrarily as a case study during codebook creation. We note that after filtering by our criteria and excluding combined web properties from the list (e.g., Google and YouTube) our first 31 services span from Google (ranked #1) to Walmart (ranked #184), with our last service (Yelp) ranked 209 at the time of data collection. Therefore, this group consists of 32 web services and we will refer to them as our *very popular* set of web services throughout the paper. We explain in Section 3.5 how we define popularity.

Our second dataset, termed the *less popular* web services dataset, consisted of a random selection of 25 services meeting our full criteria with a Tranco rank in the range of 500–1000. Initially, we aimed to collect advice from 32 web services in this range in order to have two equal sets of web services. However, upon coding these web services in the full study, the coders had trouble coding the advice specifically in regards to advice from the phase compromise discovery. The confusion came from the fact that it was hard to differentiate whether advice to discover a compromised account was either solely billing/financial issues or actually other codes related to compromise discovery. Due to this confusion, we decided to discard banking web services in this group of web services, which left us with 25 *less popular* services, as we will refer to them throughout the paper. This specific range was chosen to select a group of web services that were not obscure but was also noticeably different from the very popular web services ranked at the top. Rankings like Tranco in general are rarely linear in correlation with the phenomena measured (or implied). For example, consider the case of Youtube, Netflix, and Crunchyroll. Youtube and Netflix were ranked 3^{rd} and 9^{th} respectively, while Crunchyroll was ranked 837^{th}. Though Youtube is ranked 3 times higher than Netflix, it is unlikely that YouTube has three times the resources for security than Netflix; nor is it likely the case that Youtube has nearly a three-orders of magnitude larger security budget than Crunchyroll. Consequently, to see if site popularity has an effect on remediation advice coverage, we choose to look at group distances between the rough equivalence classes formed by the broad rank range.

Recording Existence of Account Remediation Advice: Using the same selection and exclusion criteria, we analyze all web services that were ranked between 500- -1,000 on Tranco [28] for existence of publicly available account remediation advice. We are not coding web services here; we simply check if web services provide public account remediation advice. Therefore, we examine all web services in this range, not just web services with account remediation advice. Once we calculated how many web services fit our selection criteria and provided public account remediation advice, we divided that number by the total number of web services that fit our selection criteria.

We perform this method on two different data sets, each data set however consists of web services ranked between 500- -1,000. Both data sets consisted of web services that were U.S.-based and allowed for account creation. The difference is that the first data set will also include financial or university-based web services that were ranked between 500- -1,000. We refer to this data set throughout the paper as the *include financial/university* services group. The second

data set is identical but excludes financial or university-based web services ranked between 500- -1,000. We define this data set throughout the paper as the *exclude financial/university* services group. We include two data sets since we cannot confirm if financial-based or university web services provide different account remediation advice to users with a login or belonging to that community. Since our criteria were to only collect advice that was publicly available without a login, we separate our findings for this question. These results will be shown in Section 4.3.

Storing Advice: When we found all relevant account remediation advice from a web service, we saved PDF versions of the web pages and stored them for analysis. This helped ensure we had a static dataset that did not change as we were coding. This also allowed us to code web services both collectively or individually by analyzing similar PDFs for web service's account remediation advice.

Coding: After the training phase was complete, each new coder coded 22 web services (totaling 44 more web services). Each coder coded the PDF pages from the web service's advice with Nvivo, in increments of five to nine web services at a time. Once each week, the first author met with both coders separately to go over the overlapping coding results and resolve confusion or disagreements about the coding results. Each coder then corrected their codes or added codes that they missed. Our coding results are in Sections 4.1 and 4.2.

3.5 Differences in Coverage of Account Remediation Advice

In this paper, we seek to understand whether there are significant differences in the coverage of account remediation advice between *very popular* web services and *less popular* web services, and whether there are significant differences in the coverage of account remediation advice between web services with a disclosed data breach and web services without a disclosed data breach. To address these questions, we need to operationalize aspects of these questions, including coverage, popularity, breach history, and group differences. This subsection presents the methods we use for each of these issues.

We operationalize the coverage of account remediation advice as a web service covering all five phases of account remediation in their advice. The range of the coverage of advice is measured from one phase coverage up to five phases coverage. For example, if a web service gives advice that covers only compromise discovery, account recovery, and limiting access, the coverage of the advice for that web service will be a three since it mentioned advice from three phases. We define the coverage of advice for account remediation in this manner because every phase for account remediation is important in successfully remediating a compromised account. However, not every individual code in every phase will be relevant or important for every web service. For example, codes for advice on noticing billing/finance issues will not be relevant for web services that do not handle money transactions or store financial information. Also, web services that do not give users the functionality to install third-party applications will not need advice on how to remove potentially malicious third-party applications. For this reason, if a web service has advice that mentions at least one code from a given phase, that phase will be counted to the coverage of account remediation advice for that web service. While this may overestimate a service's advice (i.e., coverage does not imply a high quality of advice), we can confidently assess services with low coverage and services with high coverage of advice.

We define the popularity of a web service by its ranking on the Tranco Website Ranking Service [28]. This ranking service was developed mainly for research purposes and consists of data from many ranking services over a period of 30 days. Tranco lists web services based on their popularity. The top 32 ranked web services we analyze are at the very top of this list, called here the *very popular* group of services. Lower ranked web services on the list such as the 25 randomly sampled web services in the 500-1,000 range are the *less popular* group of services. Our results for comparing the differences in coverage between *very popular* web services and *less popular* web services are shown in Section 4.4.

We operationalize "public disclosure of data breaches" by using a well-known database maintained by Troy Hunt on his website "haveibeenpwned" [17]. Haveibeenpwned consists of a database of publicly disclosed data breach incidents that have been consolidated and displayed on the website. The database also contains hundreds of database dumps and paste bins containing billions of leaked account credentials. Users then can query this website to search if their credentials such as their emails, usernames, or passwords have been compromised or "pwned." Users can also check an overview of web services that haveibeenpwned has listed as being breached, and sign up for breach notification. When we define web services to have publicly disclosed a data breach, we refer to web services that are listed on haveibeenpwned; the *data breach disclosed* group contains 16 web services. The remaining 41 web services that were not mentioned in the breached list of web services [17] make up our *non-data breach disclosed* group. Our results for comparing the differences in coverage between *data breach disclosed* and *non-data breach disclosed* web services are shown in Section 4.5.

In order to statistically evaluate the differences in our two research questions, we perform a Mann-Whitney U Test for both questions. Specifically, we investigate if the means of the distribution of the number of phases within the groups involved in the research questions is significant in difference. Using the Mann-Whitney U scores, we then calculate the magnitude in differences between each group of web service's coverage of advice by calculating their respective ef-

fect size [11,20]. This effect size is also quantified in Cohen's confidence interval r [7]. We follow the interpretations as guidelines provided by Fritz [11], which describe r = 0.1 as "small", r = 0.3 as "medium", and r = 0.5 as "large". The Mann Whitney U Test and other related statistical measures were performed with SPSS software [18]. We then used these results to calculate the effect size [11].

3.6 Limitations

As with any study that involves qualitative coding, this study is subject to the authors' biases, as well as possible differences in coding strategies between coders. We tried to reasonably address these in our investigation by having coders with diverse research backgrounds on our team to allow multiple perspectives to inform the creation of our codebook, and, eventually, the five phase model of account remediation. We also diligently refined our codebook and the codes' explanations in order to allow independent coders to arrive at similar assessments, and regularly controlled for divergent strategies, discussed differences and resolved disagreements.

Additionally, due to the nature of our study, we cannot provide ground truth about the differences in the coverage of account remediation advice between different groups of web services. Our definition in the coverage of advice does not take into account the length or depth of the advice, rather a metric for how many phases in account remediation it covers. We also do not provide ground truth for the applicability of all of the codes in our codebook to web services. Most of the codes in our codebook represent advice that can be broadly applied to all web services. However, some codes that we developed during our codebook development like "observe billing" or "finance issues" or "observe a third party account connected" do not apply to all web services. Therefore, we explain the results for specific codes like this with the caveat that they may not be broadly applicable to all web services.

We only collect advice from web services when it was publicly available without an account login. Some web services may provide additional account remediation advice once a user is logged in. We collected advice in this manner to replicate the process of finding account remediation advice, in the case where the account owner cannot access their account. For our coding results in Sections 4.1, 4.2, 4.4, and 4.5, we only include web services that provide publicly available account remediation. In Section 4.3, we include two versions of results in which we exclude web services that may provide additional account remediation advice given an account login.

Lastly, we only included U.S-based web services in this study. We wanted to ensure that all coders could fully interpret and code the web services we selected for this work. Since the only language that every author could fluently speak is English, we limited ourselves to U.S.-based web services.

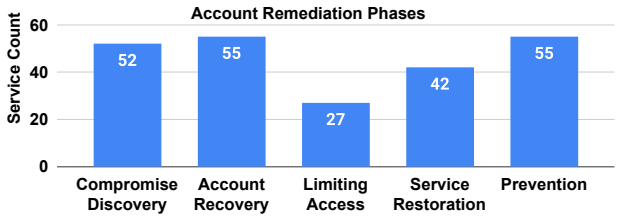

Figure 2: Bar graph of all account remediation phases among web services. Limiting Access advice is mentioned in less than half of the web services we analyzed. Service Restoration advice was mentioned in 74% of the web services. All other phases were mentioned by at least 90% of the web services we analyzed.

4 Results

In this section, we discuss the results of our codes and implications behind the results. In Section 4.1, we provide the overall coverage of the phases for account remediation advice from the web services. In Section 4.2, we look at each phase individually and examine the coverage of their respective codes within the web services. In Section 4.3, we report how many of bottom 500 ranked web services provided users with publicly available account remediation advice. We present this report with the inclusion of financial web services and university web services and also without financial web services and university web services. In Section 4.4, we present our results for investigating the differences in the coverage of account remediation advice between *very popular* and *less popular* web services. Similarly in Section 4.5, we present our results for investigating the differences in the coverage of account remediation advice between *data breach disclosed* services and *non-data breach disclosed* services.

4.1 Overall Phase Coverage

Sections 4.1 and 4.2 reflect results from coding all 57 web services. Advice for compromise discovery, account recovery, and prevention was mentioned by 91%, 96%, and 96% of all web services, respectively. These were the only phases that were covered in at least 80% of account remediation advice from web services. On the other hand, advice for limiting access was mentioned by 46% of web services and advice for service restoration was mentioned by 75% of web services. Figure 2 represents web service counts for every phase in the account remediation model. The service count in the graph indicates how many web services mentioned at least one code from a specific phase.

The phases of compromise discovery, account recovery, and prevention are not only widely addressed by most web services, but also represent areas that have been heavily re-

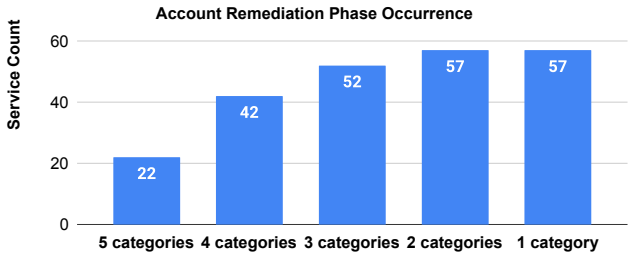

Figure 3: How many web services mentioned at least n amount of web services, where n is either at least 5,4,3,2,or 1 phase. Only 39% web services gave advice for all five phases.

searched by the security community. These three phases, however, do not fully cover the process of account remediation. Limiting the access of an account and restoring an account's original settings are fundamental for account remediation. Without it, the account remediation process is not complete, and a compromised account may still remain vulnerable. Still, more than half of the web services we investigated did not mention any advice for limiting an attacker's access.

Out of the total 57 web services we analyzed for account remediation advice, only 39% managed to mention advice from all five phases. 74% of web services mentioned at least four account remediation phases. 91% of web services mentioned at least three account remediation phases. Lastly, all 57 web services mentioned at least two account remediation phases. Figure 3 shows these results from coding all 57 web services.

The consequences of these results require careful consideration. On the one hand, our results for security advice most unique to account remediation (limiting access and service restoration) would seem to indicate that web services are neglecting these two phases. On the other hand, while we believe our model is sufficiently general to capture the account remediation process, there may be cases where it is not necessary to cover all five phases explicitly. Consider a hypothetical service that recommends completing the account recovery process, and it happens to log out all logged-in sessions. The service's advice may not reflect any limiting access content because it is automatically handled. Without ground-truth knowledge about each web service's internals, it is difficult to determine which case applies to a particular web service. Taken together, it is clear that future work should determine if remediation phase coverage is low because it is neglected or if it is simply not necessary.

4.2 Content Analysis by Phase

Compromise discovery: Compromise Discovery involves observing activity from an account or service that indicates a possible compromise. Our results for the compromise discovery codes are shown in Figure 4. *Only 11% of the codes in this phase were covered by at least half of the web services.*

Advice for discovering unauthorized or suspicious activity was recorded in 68% of the web services. This was the only advice in compromise discovery however that was mentioned in at least half of the web services. A possible reason for this could be that all of the advice in this phase can be related to unauthorized or suspicious activity, and the code itself is much less specific compared to other codes in this phase. This is a broad interpretation of compromise discovery since there are multiple methods of compromise discovery.

Advice to discover an email change or password change was mentioned in 12%, and 21% of web services, respectively. The majority, if not all, of web services with account creation store a user's email address and password and allow users to change them as well. Observing that either of these identifiers changed within an account is a strong indication of a possible compromise. Still, even the union of the coverage of advice for discovering a changed password and changed email address reached no more than 33% of web services we investigated. This is a clear oversight of advice coverage on the part of web services.

Advice noticing an explicit notification and observing unauthorized logins was mentioned in 30% and 35% of the web serviced we investigated, respectively. We wanted to code advice for users discovering account compromises from explicit notifications from the service, or by observing unauthorized logins on their accounts. From this, we also concluded that users could observe unauthorized logins due to an explicit service notification, or by examining their account as well. Therefore, we created a code for noticing explicit service notifications about a compromise and a code for observing unauthorized logins that includes coverage from the explicit service notification code, while not being exclusive to it. With these results, we present the caveat that we do not confirm if all web services give users the functionality to observe log-ins on their accounts. Therefore, the results for our code "observe an unauthorized login" may not be broadly applied to all web services.

Advice to discover a social media/third party account connected and billing/finance issues were mentioned in only 5% and 35% of web services, respectively. While these results do reflect low coverage across web services, we can not confirm how many web services in our study implement billing or finances into their functionality for users. We also can not confirm if all web services in our study allow users to connect a social media or third-party account to their main account.

We look to our results in coding limiting access advice later in this section and compare the results of the code "Remove third party access." This specific code, "Remove third party access", was mentioned in 18% of web services. The difference in coverage between this code and our code in this category, "social media/third party account connected," shows that at least 12% of web services that allow users to connect a

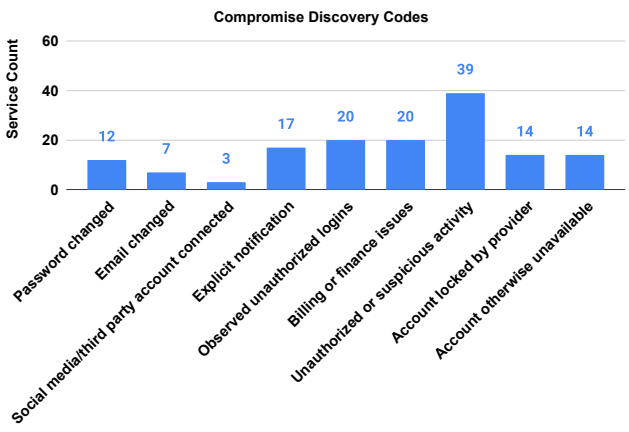

Figure 4: Bar graph of Compromise Discovery codes among web services. Unauthorized or suspicious activity was the highest covered code with 39 web services. No other code was mentioned in more than half of the web services.

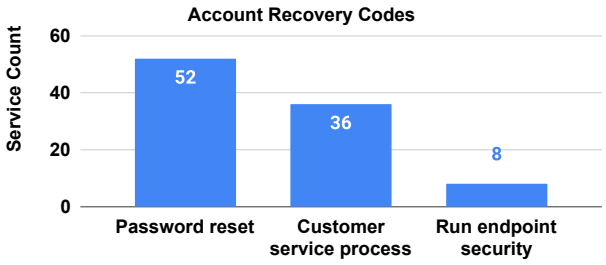

Figure 5: Bar graph of Account Recovery codes among web services. Password reset was mentioned by 91% of services and customer service support was mentioned by 63% of services.

social media or third account are not advising users to notice a new social media or third-party account when discovering a compromise.

Overall, compromise discovery advice was sparsely covered. Only one code in this phase was covered by at least half of the web services. Most of the codes in this phase can either be broadly applied or covered at a higher usage given other results we recorded in other phases. Most of the advice in this phase is also cheap in implementation but important to discovering a compromised account. Web services have much room for improvement in their coverage of compromise discovery advice.

Account recovery: Account recovery provides a means for users to recover their account after losing access to it or having it compromised. Our results for coding this phase are shown in Figure 5. *66% of the codes from this phase were covered in at least half of the web services.* This phase is highly covered by web services and continues to be prioritized, even as a means to remediate compromised accounts.

Advice to initiate a password reset or to change a password was covered in 91% of web services. This advice was also the highest covered code out of all phases in this study. It was the most common method for advising users to recover their compromised accounts.

Advice to advise users to engage in customer service to recover a compromised account was covered by 63% of web services. Some services require contacting customer service for account recovery processes. Customer service for account recovery involves assisting users in recovering a compromised account with a guided process or interaction with a service client. This is different from other customer service processes that services may offer outside of account recovery. While we recognize this advice was not covered universally among web services, it may not be reasonable to have users go through customer service every time to recover their account or reset their password. However, keeping customer service as an optional route may be more beneficial to users.

Advice to reset passwords and to engage in customer service to recover an account were both covered in over half of the web services. These results can imply that not only is account recovery prioritized in account remediation advice, but mainly in the forms of password reset advice and customer service support

We observed advice for running endpoint security to recover an account was only covered in 14% of web services. The low service count could be the result of authors of account remediation advice not considering endpoint security. Also, correctly running anti-virus software is highly technical and possibly beyond the reach of most users. It might be unclear to the extent of how much antivirus or other harm remediation measures help remediate online account compromise. This can imply that web services may not view endpoint security options as a viable solution or prioritize it for account recovery purposes.

Limiting access: Limiting account access is defined as preventing current and future unauthorized access by adversaries. *Limiting Access advice was the lowest covered phase in the study, reaching only 47% of web services.* Less than half of the web services in our study advised users to manage the access of their account, and thus not prioritizing an important step in account remediation. Advice for limiting an account's access includes signing out of instances of an account, reviewing active sessions, and removing access from third-party applications. The results for coding this phase are shown in Figure 6.

Advice for signing out of an individual instance or all instances of an account were covered by only 26% and 14% of web services, respectively. All services allow users to sign out of an account and many allow to sign out of multiple account instances, yet the union of these two codes was only covered

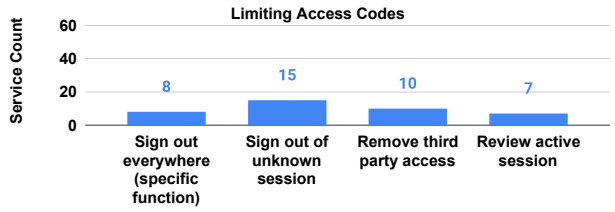

Figure 6: Bar graph of Limiting Access codes among web services. No single code was mentioned in more than a third of the web services.

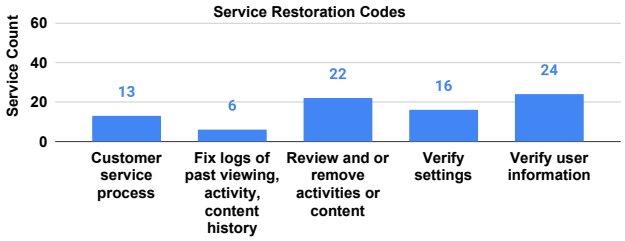

Figure 7: Bar graph of Service Restoration codes among web services. No single code was mentioned in more than 42% of web services.

by 40% of web services. This coverage is insufficient given that all web services allow users to sign out of an instance or multiple instances of their account and it is an important step in managing the access of an account.

Advice for reviewing active sessions also was represented with a code that was only present in 12% of web services. We also record this finding with the caveat that we lack ground truth for how many web services provide users the ability to check for active sessions of their account. However, we explain in Section 5, why we recommend this functionality be implemented in web services and then provided in account remediation advice.

Advice for removing third party access was only present in 18% of web services we investigated. This is important to note since advice for discovering a new social media or third-party account connected to an account in the compromise discovery category was only mentioned in 5% of web services. All of the advice in this phase is underwhelmingly covered given its importance to secure the access of a compromised account.

Service restoration: Service Restoration advice involves restoring an account's original settings or information to how it was before the compromise. *74% of web services mentioned advice for service restoration, yet none of the specific codes in service restoration were covered by at least half of the services.* The results for coding this phase are shown in Figure 7. Advice from this phase is also insufficient in coverage among web services.

Advice for verifying user information, verifying account settings, and reviewing and/or removing activities or content were each recorded in 42%, 28%, and 39% of web services, respectively. These are extremely low percentages for advice that should apply to most, if not all, of the web services we analyzed. All web services in this study store information about the user, settings for the user, and activity by the user. Therefore, there should be advice to verify all of this information. Yet, none of the codes that represent this advice are mentioned beyond 42% of web services investigated.

Lastly, advice to seek customer service support in this phase received a low percentage: 23% of web services. This percentage differs significantly in coverage than the service count for customer service support for account recovery which was mentioned in 63% of web services. This could imply that most services are more likely to prioritize customer service support advice for account recovery, or they do not prioritize customer service for service restoration purposes.

Prevention: Prevention is defined as taking further steps to further secure an account. *Out of the total 11 codes in Prevention, four were represented in at least 60% of the web services investigated.* This category also held six of the top ten most covered codes in the codebook (strong password advice, secure email advice, enable 2FA, check/modify related accounts, enable endpoint security options, and keep software updated). Results for coding this phase are presented in Figure 8.

Advice to maintain strong passwords was the highest mentioned code in this category with 88% coverage. This was the second individual highest covered code right behind the advice to initiate a password reset to recover an account (91% coverage). This means that advice for password security amounted to the two highest codes and therefore the highest coverage out of any advice for account remediation. This could be a result of the vast industry and academic work on password security. It could also mean that web services believe strong password advice is very crucial to account remediation.

Advice on securing emails, enabling two-Factor Authentication, and checking or modifying related accounts was covered in 72%, 70%, and 61% of web services, respectively. Similar to strong password advice, secure email advice and two-factor authentication advice also represent areas that are heavily researched by the research community and are popular among web services.

Running endpoint security options and keeping software up to date advice were both mentioned in 47% of web services investigated. Interestingly, the coverage in this phase for running endpoint security was significantly higher than advice for running endpoint security for account recovery (14%). This shows authors of advice for account remediation were more likely to advise users to run endpoint security options to prevent an account compromise instead of recovering an account from compromise. However, given that it is unclear

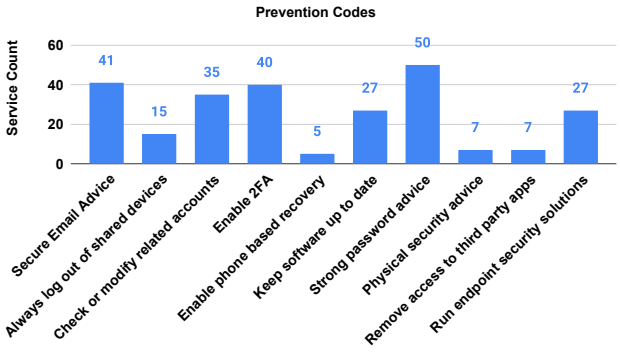

Figure 8: Bar graph of Prevention codes among web services. Four out of 11 codes were mentioned in at least 60% of web services and strong password advice was mentioned in 88% of web services.

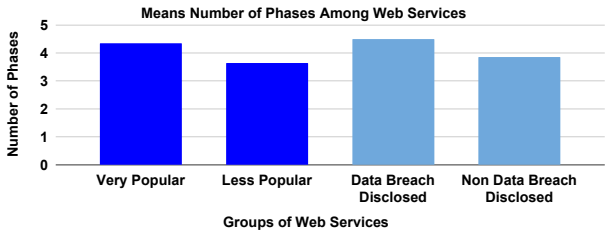

Figure 9: Graph of the mean number of phases covered in account remediation by all experimental groups. *Very popular* web services had a higher mean count of phases mentioned in their account remediation advice than *less popular* web services. *Data breach disclosed* services had a higher mean count of phases mentioned in their account remediation advice than *non-data breach disclosed* web services.

how effective running endpoint security options are towards recovering a compromised account, it is also unclear as to how effective it is in preventing a future compromise.

Notably, prevention advice generally focused on shifting responsibility to other services or the user. While not explicitly coded for, very few services discussed reporting breaches or security flaws in their own service. For example, Netflix states that "If [users] believe [they've] found a security vulnerability on a Netflix property or app, we strongly encourage [them] to inform [Netflix] as quickly as possible and to not disclose the vulnerability publicly until it is fixed." In the worst case, Fandom.com prefaces its prevention advice with the statement that "there is a possibility that if your account is hacked you will need to create a new account" and implies that security is solely the responsibility of the user.

4.3 85% of Web Services did not provide Account Remediation Advice

In our *include financial/university* web service data set, 220 web services allowed users to create public accounts and were U.S.-based. *Of these 220 web services, only 15% of these web services gave publicly available account remediation advice.* In our *exclude financial/university* web service data set, 195 web services allowed users to create a public accounts and were U.S.-based. *Of these 195 web services, only 12% of these web services gave publicly available account remediation advice.*

The majority of web services in our study that were U.S.-based and allowed for user account creation did not provide users with public advice for account remediation. This is alarming since we made sure to only collect account remediation advice from a web service if the advice was publicly available and did not require users to log in. A user with a compromised online account needs to have access to such advice even if they cannot access their account. If this advice is not made publicly available, let alone created at all, then users are left with significantly less help in successfully remediating their compromised accounts.

4.4 Coverage of Advice versus Popularity

In this section, we give our results from investigating the differences in the coverage of account remediation advice between *very popular* web services and *less popular* web services. As stated in Section 3.5, we define the coverage of account remediation advice as the number of account remediation phases that are discussed by a web service.

Our objective is to see if there are differences in the number of phases covered within account remediation advice for web services of vastly different popularity. We performed a Mann-Whitney U Test in which we define the following null hypothesis: the distribution of the number of phases mentioned in account remediation advice is similar across *very popular* web services and *less popular* web services. We perform this test to discover if the number of phases between the two groups of web services is significant in difference.

The mean number of phases mentioned by *very popular* web services was 4.3 with a standard deviation of 0.90. While the mean number of phases mentioned by *less popular* web services was 3.6 with a standard deviation of 0.90. Using a Mann-Whitney U test, we find a statistically significant difference in the mean number of phases covered by the two groups (U = 224, z = -2.994, $p = 0.003$). Using these test scores, we calculate an effect size $r = 0.397$, which is considered to be a "medium" effect size [11, 20].

It is plausible that *very popular* web services have more incentive to provide users with account remediation advice since they have more users creating accounts than less popular web services. Not only would they have more users, but there

may also be a higher importance or usage of accounts with very popular web services. However, there are important web services that are not *very popular*, but are likely to also provide extensive account remediation advice. Financial and banking web services are also important to users, and compromised accounts from these web services can impact a user's finances or potentially compromise their identity. Many banks provide both advice for account remediation and identity theft and also give users resources to contact for further assistance.

4.5 Coverage of Advice versus Disclosed Data Breach

In this section, we show the differences in the coverage of account remediation advice between *data breach disclosed* web services and *non-data breach disclosed* web services.

Our objective is to see if there are differences in the number of phases covered within account remediation advice for web services that have or have not publicly disclosed a data breach. We performed a Mann-Whitney U Test in which we define the following null hypothesis: the distribution of the number of phases mentioned in account remediation advice is similar across *data breach disclosed* web services and *non-data breach disclosed* web services. We perform this test to discover if the number of phases between the two groups of web services is significant in difference.

The mean number of phases mentioned by *data breach disclosed* web services was 4.5 with a standard deviation of 0.63. While the mean number of phases mentioned by *non-data breach disclosed* web services was 3.8 with a standard deviation of 1.0. Using a Mann-Whitney U test, we find a statistically significant difference in the mean number of phases covered by the two groups (U = 210, z = -2.217, $p = 0.027$). Using these test scores, we calculate an effect size $r = 0.294$, which is considered to be approximately a "medium" effect size [11, 20].

These findings may suggest that *data breach disclosed* web services have updated their account remediation advice once their compromised data was publicly known. The breach may have influenced a service to improve their systems and the resources they provide to users to secure their accounts. Interestingly, despite having the experience of a data breach, none of the web services which had disclosed a breach on haveibeenpwned explicitly mention reporting security flaws in the service to mitigate or prevent breaches.

Finally, we note that the analyses of differences of advice based on popularity and history of disclosing data breaches are preliminary and correlational. More work would be needed to confirm a causal relationship between a web service's coverage of account remediation advice and its popularity or history of disclosing data breaches.

5 Discussion

In this section, we discuss recommendations for implementing account remediation advice for web services. We also discuss what future work can be done to further this investigation.

Account Remediation Model: While remediation for each web service may have domain-specific concerns like fixing a playlist or recovering documents in cloud storage, our validated codebook provides evidence that the majority of account remediation steps are general, if not universal. Each phase in our codebook was constructed by analyzing multiple popular web services and creating codes that be broadly applied. We note that if one defines account remediation as "reversing the consequences of compromise," one must have all five phases for successful account remediation. One cannot claim an account is remediated until the compromise is discovered, user access is regained, the attacker has lost access, the account is restored to its pre-compromise state, and re-compromise is prevented. If any step is neglected, either a compromise is not remediated or the account will simply be re-compromised.

Our codebook also provides flexibility for domain-specific concerns as well. As discussed in Section 2, specific phases of account remediation such as discovering compromised accounts [6, 8, 19, 31, 33], recovering compromised accounts [3, 4, 16, 26, 32], and preventing compromises through general security practices [22, 30] have been researched and implemented. However, we are the first to conceptually define account remediation into a five-phase structured process. While the variations between services mean that account remediation advice cannot be totally centralized, we believe our codebook could be used for consumer advocates (such as the FTC) as the basis of public information campaigns and guides to help users in the complex task of account remediation.

On Service Responsibility: As mentioned in Section 4.2, much of the remediation advice given by services focus exclusively on account compromise resulting from other services or user error. They suggest that compromises may result from poor password choice, password reuse, falling victim to phishing, compromise of a "master" account like an email account, or malware infection. An example of advice following this tone is the following: "Don't worry, we have no indication that the Walmart systems have ever been compromised, but there are steps you should take to protect your personal information if you suspect unauthorized access or a phishing attempt". Services very rarely mention the possibility of a security flaw in their own service, even when they have previously disclosed a breach. While it may be the case that the source of most compromises is from external sources, companies should not completely shift responsibility onto individuals. Additionally, in some cases, users are limited in their ability to remediate an account. For example, banks do not allow users to unilaterally revoke a transaction after completion, and many web services automatically lock accounts based on indicators of compromise. An argument could be made that if

web services have the best visibility and ability to detect compromise, they should also be able to assist users proactively, if not automatically, in remediating the effects of that compromise. On the other hand, if it is true that account compromises mostly originate from external security problems, it would be unfair to put this burden solely on the web service. Similarly, the web service may have an incomplete perspective on what actions around the time of an account compromise were authorized or not. By analogy, credit card companies have regular monitoring for anomalous transactions, and in many cases can automatically block fraudulent transactions, even when caused by an external breach. Still, credit card companies often have to contact their users to confirm or deny specific anomalous charges. We recommend that web services consider to what extent they can automate remediating compromised accounts in order to balance responsibility with best serving users. We also suggest that language should be added to account remediation advice to encourage users to report security flaws with the service rather than focusing only on external causes of hacking.

Another question is what role, if any, law enforcement agencies have to play in identifying and prosecuting account compromises (especially in the furtherance of other criminal activities). We noted that 15 web services mention some form of evidence gathering of an account compromise alongside account remediation advice. However, we also note that computer crime is notoriously difficult to bring to prosecution, so it is arguable to what extent this would be helpful to current or even future victims.

Recommendations: Web services should, as a best practice, provide a mechanism to review account activity, including logins and actions that change the state of an account (purchases, password or preference changes, settings, user information.) Services should also provide better guidance on what "unusual activity" means through specific examples such as changed passwords, changed usernames, or changed emails. Owing to the large amount of prior work on account recovery, we recommend readers see the recommendations of prior work [3, 16, 26, 32]. All web services should also provide an interface to show all active log-in sessions and/or access permissions. This interface should also allow a user to revoke access for any or all current sessions. Along with the recommendation to show account activity, there should be an interface allowing users to revert changes made to their settings or remove unauthorized content. While not specifically coded for in our study, we observed that only six services provided a method to restore content deleted in an account compromise.

Enforcing mandatory customer service for account remediation purposes will inform the web service directly while also potentially discovering a large scale data breach. On the other hand, it potentially increases the effort on part of both the user and web service. Also, if mandatory customer service is not staffed 24/7, there may be consequential delays in preventing further damage from the compromise. This is why optional customer service may be a better feature to have, especially for complex remediation cases, because users without significant technical understanding of the compromise may need additional support. Finally, we observed a high variance in the prevention advice given by web services for what is largely the same problem, implying that many individual web services have incomplete prevention guidance. Similar to the work done by Redmiles et al. [29,30], there is an abundance of general prevention advice but a lack of advice prioritization.

Future Work: Future work should explore more usable or contextual guidance. Some of the steps in account remediation are technically complex to perform for users. Making the process of account remediation more usable and easier to follow will better aid users in remediating their accounts. For example, Facebook actually implements a chatbot-style wizard for guiding users through account remediation. It consists of easy to read diagrams that prompts users if they recognize information or settings on their account that is presented to them by the chatbot wizards. Future work could evaluate these approaches and explore ways of generalizing this approach to be usable for other types of web services beyond social media. Additionally, it is worth exploring to what extent a service could certify that an account has been remediated, or what assurances could be provided to users that their accounts have become "safe."

6 Conclusion

Online account compromises have become rampant, and anyone with an online account is susceptible to having their account compromised. The resources that help users remediate a compromised account should cover all the necessary procedures to help users re-secure their accounts. We investigated publicly available advice for account remediation from both top-ranked web services and lower-ranked web services. We identified important phases for account remediation that are not only sparse in coverage but also are not addressed by a significant amount of popular web services that provide account remediation advice. Also, the amount of web services we studied that even provide users with publicly available account remediation advice is critically low and did not surpass at least 15% of the total web services we analyzed that allow users to create accounts. Lastly, we discovered that highly ranked web services and web services with a previously disclosed data breach presented more complete coverage of their account remediation advice than other web services. Our analysis of the coverage of account remediation advice presented important areas that are lacking in attention, to which we explain credible recommendations to both bolster the advice and the process of account remediation.

References

[1] Devdatta Akhawe and Adrienne Porter Felt. Alice in warningland: A large-scale field study of browser security warning effectiveness. In *Presented as part of the 22nd USENIX Security Symposium*, pages 257–272, 2013.

[2] Rosaline S. Barbour. Checklists for improving rigour in qualitative research: a case of the tail wagging the dog? *British Medical Journal*, 322(7294):1115–1117, 2001.

[3] Joseph Bonneau, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike Williamson. Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google. In *Proceedings of the 24th International Conference on World Wide Web*, pages 141–150, 2015.

[4] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy*, 2012.

[5] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2):18–26, 2010.

[6] Asaf Cidon, Lior Gavish, Itay Bleier, Nadia Korshun, Marco Schweighauser, and Alexey Tsitkin. High precision detection of business email compromise. In *28th USENIX Security Symposium*, pages 1291–1307, 2019.

[7] J Cohen. Statistical power analysis for the behavioural sciences. Hillsdale, NJ: Laurence Erlbaum Associates, 1988.

[8] Manuel Egele, Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna. Towards detecting compromised accounts on social networks. *IEEE Transactions on Dependable and Secure Computing*, 14(4):447–460, 2015.

[9] Deen Freelon. *ReCal2: Reliability for 2 Coders*.

[10] Deen Freelon. *ReCal3: Reliability for 3+ Coders*.

[11] C Fritz. E Morris P, J Richler J. Effect Size Estimates: Current Use, Calculations, and Interpretation. *J Exp Psychol Gen*, 8:2–18, 2011.

[12] Kelsey R Fulton, Rebecca Gelles, Alexandra McKay, Yasmin Abdi, Richard Roberts, and Michelle L Mazurek. The effect of entertainment media on mental models of computer security. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, 2019.

[13] Nethanel Gelernter, Senia Kalma, Bar Magnezi, and Hen Porcilan. The password reset MitM attack. In *2017 IEEE Symposium on Security and Privacy*, pages 251–267. IEEE, 2017.

[14] Mordechai Guri, Eyal Shemer, Dov Shirtz, and Yuval Elovici. Personal information leakage during password recovery of internet services. In *2016 European Intelligence and Security Informatics Conference (EISIC)*, pages 136–139. IEEE, 2016.

[15] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, pages 133–144, 2009.

[16] Jun Ho Huh, Hyoungshick Kim, Swathi SVP Rayala, Rakesh B Bobba, and Konstantin Beznosov. I'm too busy to reset my linkedin password: On the effectiveness of password reset emails. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 387–391, 2017.

[17] Troy Hunt. *Pwned websites*. https://haveibeenpwned.com/PwnedWebsites.

[18] IBM. *IBM SPSS software*. https://www.ibm.com/analytics/spss-statistics-software.

[19] Hamid Karimi, Courtland VanDam, Liyang Ye, and Jiliang Tang. End-to-end compromised account detection. In *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, pages 314–321. IEEE, 2018.

[20] Daniël Lakens. Calculating and reporting effect sizes to facilitate cumulative science: a practical primer for t-tests and anovas. *Frontiers in psychology*, 4:863, 2013.

[21] Megan Leonhardt. *The 5 biggest data hacks of 2019*, Dec. 17, 2019. https://www.cnbc.com/2019/12/17/the-5-biggest-data-hacks-of-2019.html.

[22] Peter Mayer, Yixin Zou, Florian Schaub, and Adam J Aviv. " Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. In *30th USENIX Security Symposium*, 2021.

[23] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. In *ACM on Human-Computer Interaction*, page 72, 2019.

[24] Jeremiah Onaolapo, Enrico Mariconti, and Gianluca Stringhini. What happens after you are pwnd: Understanding the use of leaked webmail credentials in the

wild. In *Proceedings of the 2016 Internet Measurement Conference*, pages 65–79, 2016.

[25] Bijeeta Pal, Tal Daniel, Rahul Chatterjee, and Thomas Ristenpart. Beyond credential stuffing: Password similarity models using neural networks. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 417–434. IEEE, 2019.

[26] Simon Parkin, Samy Driss, Kat Krol, and M Angela Sasse. Assessing the user experience of password reset policies in a university. In *International Conference on Passwords*, pages 21–38. Springer, 2015.

[27] Peng Peng, Chao Xu, Luke Quinn, Hang Hu, Bimal Viswanath, and Gang Wang. What happens after you leak your password: Understanding credential sharing on phishing sites. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, pages 181–192, 2019.

[28] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński, and Wouter Joosen. Tranco: A research-oriented top sites ranking hardened against manipulation. *arXiv preprint arXiv:1806.01156*, 2018.

[29] 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 *2016 IEEE Symposium on Security and Privacy (SP)*, pages 272–288. IEEE, 2016.

[30] Elissa M Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L Mazurek. A comprehensive quality evaluation of security and privacy advice on the web. In *29th USENIX Security Symposium*, pages 89–108, 2020.

[31] Xin Ruan, Zhenyu Wu, Haining Wang, and Sushil Jajodia. Profiling online social behaviors for compromised account detection. *IEEE transactions on information forensics and security*, 11(1):176–187, 2015.

[32] Stuart Schechter, AJ Bernheim Brush, and Serge Egelman. It's no secret. measuring the security and reliability of authentication via "secret" questions. In *30th IEEE Symposium on Security and Privacy*, pages 375–390. IEEE, 2009.

[33] Richard Shay, Iulia Ion, Robert W Reeder, and Sunny Consolvo. " My religious aunt asked why I was trying to sell her viagra" experiences with account hijacking. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2657–2666, 2014.

[34] Kurt Thomas, Frank Li, Ali Zand, Jacob Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, Oxana Comanescu, Vijay Eranti, Angelika Moscicki, et al. Data breaches, phishing, or malware? Understanding the risks of stolen credentials. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1421–1434, 2017.

[35] Kurt Thomas, Jennifer Pullman, Kevin Yeo, Ananth Raghunathan, Patrick Gage Kelley, Luca Invernizzi, Borbala Benko, Tadek Pietraszek, Sarvar Patel, Dan Boneh, et al. Protecting accounts from credential stuffing with password breach alerting. In *Proceedings of the 28th USENIX Security Symposium*, pages 1556–1571, 2019.

[36] Courtland VanDam, Jiliang Tang, and Pang-Ning Tan. Understanding compromised accounts on twitter. In *Proceedings of the International Conference on Web Intelligence*, pages 737–744, 2017.

[37] Ke Coby Wang and Michael K Reiter. Detecting stuffing of a user's credentials at her own accounts. In *29th USENIX Security Symposium*, pages 2201–2218, 2020.

7 Codebook

Compromise Discovery		
Codes	**Code Explanations**	**Examples**
Billing/finance issues	Unwanted changes in financial or billing settings/standings or unauthorized credit card charges.	You see charges or notices for purchases that you didn't make.
Email changed	Observe any email associated with account has been changed.	What do I do if someone changed my email address?
Explicit notification	Service notifies you of login or possible compromise by email or other factor. Check this if the service sends emails about new logins.	You receive an email or notification that your Apple ID was used to sign in to a device you don't recognize or did not sign in to recently (for example, "Your Apple ID was used to sign in to iCloud on a Windows PC").
Account locked by provider	Cannot access account due to account being locked or disabled.	For your protection, we may place a temporary hold on your account.
Account otherwise unavailable	Account is not accessible due to circumstances outside of provider locking account.	You can't sign in for another reason.
Observed unauthorized logins	Includes if "observation" is due to a notification from the service, but not exclusively.	You see logins from unexpected locations on your recent activity page.
Password changed	Observe password associated with account has been changed.	Someone changed the password on my Etsy account.
Social media or third party account connected	Unwanted social media becomes associated with account.	A malicious application has been given access to your account.
Unauthorized/supicious activity	Including changed content on streaming sites, but must be more than login. For example messages, friend requests, playlists, etc.	If you notice unfamiliar activity on your Google Account, someone else might be using it without your permission. Use the info below to help spot suspicious activity.

Account Recovery		
Codes	**Code Explanations**	**Examples**
Customer service process	Engage with service customer support (chat client, form, email, etc) to regain access/reset password.	If you can't access your account and believe that someone else has accessed it, complete the form and after receiving it we'll verify that it's your account and then help you regain access.
Password reset	Initiate a password reset challenge or go through password change process.	Change your password immediately.
Run endpoint security	Run external security applications on computer to stop a suspected *ongoing* attack.	If you see any successful sign-in that you do not recognize, run a scan with your security software and remove any malware you find.

Limiting Access		
Codes	**Code Explanations**	**Examples**
Remove third party access	Disallow external third party applications (including social media) from accessing account.	Revoke access to any suspicious third-party apps.
Review active session	Review activity/logs for currently active sessions to see if compromise is ongoing.	Review your active sessions to see all the places you're signed into LinkedIn right now.
Sign out everywhere (specific function)	Logs out *all* instances of account (not just one or a few).	We recommend to log out of all computers from your phone.
Sign out of unknown session	Logs out of individual unrecognized instances of account.	If your account does get hacked, you can remove any trusted devices that you didn't log in to yourself.

Service Restoration		
Codes	**Code Explanations**	**Examples**
Customer service process	Engage with service customer support (chat client, form, email, etc.) to help restore data etc.	Contact us for help removing unauthorized bids or listings.
Fix logs of past viewing/activity/content history	For example, viewing history, input to recommendations, past purchases.	Review Order history for unrecognized charges.
Review and/or remove activities/content	For example, deleting friends you didn't add, messages you didn't write.	Delete any resources on your account that you didn't create, such as EC2 instances and AMIs, EBS volumes and snapshots, and IAM users.
Verify settings	User should verify security, privacy, or account settings.	Review your general account settings to make sure all other information is correct.
Verify user information	User should check the identifying information for users (email, name, address, or payment info like credit card number).	Verify that the email address and mobile number associated with your account are accurate in Snapchat settings.

Prevention		
Codes	**Code Explanations**	**Examples**
Advice about secure email	Describes advice on suspicious emails, phishing, etc.	Phishing is when someone tries to trick you into giving up your Twitter username, email address or phone number and password, usually so they can send out spam from your account.
Always log out on shared devices	Always log out shared instances of account.	Sign out of public computers- - -Always sign out of your accounts when you're done.
Check/modify related accounts	For example, email accounts, shared passwords, etc.	Check your personal email account(s) tied to your account to ensure their security.
Enable 2FA	Enable any 2FA for every login attempt.	Enable Two-Factor Authentication (2FA).
Enable phone-based recovery	Enable ability to *recover* account/credentials by using a phone number as a second factor.	Add a recovery phone number to your account so that you can get back into your account faster and keep your account more secure.
Keep software up to date	Catchall: any application/program/devices/software up to date with current updates.	Regularly patch, update, and secure the operating system and applications on your instance.
Password advice: strong, unique, change frequently	Catchall for any password advice (good bad or otherwise).	Create a strong password. Make it unique: Do not reuse an existing password when setting up an account for PlayStation Network.
Physical security	Catchall for any advice to maintain physical security of devices, environment, etc.	Don't leave your devices unlocked or unattended where anyone can use it.
Remove access to third party apps	Prompted to disallow external third party applications from accessing account.	Remove suspicious applications or browser add-ons.
Run endpoint security solutions	Run external security programs/applications on computer to prevent *future* attacks.	Always use an antivirus program to check the files you receive from other people.
Sign out of devices	Log out of *individual* devices that have instances of account.	Log out when you are done.

8 Web Services Studied

Very Popular Websites		Less Popular Websites	
Ranking	Website	Ranking	Website
1	google.com	524	hootsuite.com
2	facebook.com	542	ox.ac.uk
3	youtube.com	547	umn.edu
4	microsoft.com	559	uci.edu
5	twitter.com	568	ucla.edu
7	instagram.com	575	att.com
9	netflix.com	578	snapchat.com
10	linkedin.com	608	uchicago.edu
13	wikipedia.org	620	playstation.com
14	apple.com	635	xfinity.com
18	yahoo.com	658	parallels.com
23	pinterest.com	669	epicgames.com
25	vimeo.com	682	fidelity.com
28	reddit.com	730	ning.com
40	amazonaws.com	776	verizon.com
44	tumblr.com	785	uber.com
45	godaddy.com	795	msu.edu
51	skype.com	806	ea.com
55	whatsapp.com	836	northwestern.edu
56	dropbox.com	837	crunchyroll.com
58	soundcloud.com	886	arizona.edu
61	myshopify.com	904	wattpad.com
67	twitch.tv	917	stripe.com
79	spotify.com	932	namecheap.com
81	paypal.com	942	xbox.com
93	cloudflare.com		
94	ebay.com		
117	etsy.com		
170	aol.com		
183	fandom.com		
188	walmart.com		
209	yelp.com		

9 Data

Our annotated advice is available at: https://github.ncsu.edu/lcneil/Investigating-Web-Service-Account-Remediation-Advice