Investigating Web Service Account Remediation Advice

Lorenzo Neil
North Carolina State University

Yasemin Acar
Leibniz University Hannover

Bradley Reaves
North Carolina State University

Abstract

Online web services are susceptible to account compromises where adversaries gain access to a user's account. When this occurs, the victim must go through five phases to restore the account; these include: discover the compromise, restore their access, limit the adversary's access, restore the service to its pre-compromise state, and then take action to prevent repeat compromise. This is a technically complex process, and the quality and completeness of the advice that services give is of paramount importance. In this paper, we collect account remediation advice from 13 top US web services. We systematically investigate what advice web services provide about the five phases of account compromise remediation. We find that while most services cover all phases, specific, appropriate, and actionable advice is generally lacking in every service. This preliminary work highlights the need for better guidance both for operators and users at large.

1 Introduction

Account compromises are a pervasive problem, with billions of accounts being compromised in 2019 alone [7]. In response, many web services provide users with documentation on how to recognize a compromise and then recover and restore the account to its original settings. The documentation may also tell users how to regain complete and sole access of their accounts. We term this process "account remediation". How users complete account remediation is essential to the security of their accounts. If they fail to completely remediate their accounts, their accounts may remain compromised or vulnerable. Therefore, the advice given by web services to help users remediate their accounts is of critical importance. Account remediation advice, however, has not received as much consideration from the security community as account recovery advice and mechanisms have. Account recovery is only a fraction of account remediation which encompasses the complete process of restoring an account after compromise.

We note that previous work aimed to research account recovery mechanisms, security advice, and detecting compromised accounts. Past work on online account compromises [11] focused on detecting compromised accounts by building a models to represent normal account behavior and then using that behavior to analyze current account behavior for anomalies or unusual activity [5, 10]. Prior work on account recovery mechanisms [2] investigated different authentication schemes [3] and password reset strategies [6]. In addition, prior research has also focused on the user's mental model in regards to computer security [4, 9] and analyzed advice and warning sources for computer security [1]. We recognize that much prior work has been made on account recovery mechanisms. However, account remediation is not the same as account recovery, and the lack of research in account remediation is the motivation for this work.

In this paper, we investigate account remediation advice given by 13 of the most popular U.S. domestic web services. We analyze the advice by qualitatively coding the account remediation advice web pages from each service. We systematically develop a codebook that identifies five important phases of the account remediation process: compromise discovery, account recovery, limiting account access, service restoration and prevention of future compromises. These phases are represented by categories in our codebook that each possess individual codes. Each individual code represents a separate type of account remediation advice that is found within service's advice web page. Our findings indicate that account recovery and prevention were two out of the three phases that were mentioned on all 13 web services. Also, at least 66% of codes from account recovery and at least 70% of codes from prevention respectively were represented as advice in at least

Who Are You?! Adventures in Authentication (WAY) 2020.
August 7, 2020, Virtual Conference.

half of the web services investigated.

Compromise discovery was the third phase to be mentioned on all 13 web services, however, only a third of the advice from this phase was covered in at least half of the services investigated.

Limiting account access and service restoration were only mentioned by 10 web services and 9 web services respectively. None of the codes from limiting account access were represented as advice in at least half of web services. Also, only 40% of codes from service restoration were represented as advice in at least half of web services.

While all services mention advice for discovering compromises, account recovery, and prevention, the actual coverage of these phases is sparse among the web services. Limiting account access and service restoration advice was not mentioned in at least 3 services and is insufficiently covered on most web services. We discovered that while services handle account recovery advice well, account remediation advice is not fully addressed by web services.

2 Methodology

This section explains our methodology for examining account remediation advice among web services. We first present our codebook which holds five phases, each represented as different categories that collectively consist of 32 individual codes. Then, we describe the process for developing our codebook through a preliminary pilot study. Following our pilot study, we explain how we coded web services. Finally, we conclude this section by explaining how we collected account remediation advice from web services.

Codebook[1]**:** Our codebook is divided into five different categories that each contain individual codes and respective code explanations. We created categories in order to define the complete process of account remediation as a systematic procedure of steps. The phases are: compromise discovery, account recovery, limiting access, service restoration, and prevention. *Compromise discovery* is defined as a user observing suspicious activity from their account or service that indicates a possible compromise. *Account recovery* is defined as 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 total account remediation process. *Limiting access* is defined as preventing current and future unauthorized access from adversaries. *Service restoration* is defined as restoring an account's original settings, content, or state before a compromise. Lastly, *prevention* is defined as preventing future compromises by taking steps to further secure an account.

Codebook Development: To develop our codebook, we first performed a pilot study. The first step consisted of authors collaboratively drafting the first iteration of the codebook from analyzing five web services (Spotify, Netflix, Skype, LinkedIn, and Twitter). With the draft, we identified a systematic process for account remediation. Next, we used the codebook to individually code two more web services (Facebook and Google). All authors then compared their codes to make necessary adjustments to the codebook. The codebook was revised until it contained completely unambiguous codes, and coders could independently arrive at similar codings for web services. We repeated this process but with two more web services (Yelp and Walmart). We then determined our codebook was sufficiently reliable to code the remainder of the web services.

Coding: After the pilot study, a single coder analyzed each web service's advice and coded the results with Nvivo coding software. All of the web services that were coded will be mentioned in the following paragraph. Every web service's account remediation advice was analyzed for the existence of codes from the codebook.

Data Collection: Account remediation advice from web services was collected from April 13th through April 23rd, 2020. In this work, we referred to 13 of the top U.S. domestic web services from the Tranco Website Ranking List (as of March 31, 2020) [8]. We collected pages from the following web services: Apple, Facebook, Google, Instagram, LinkedIn, Microsoft, Netflix, Skype, Spotify, Twitter, Walmart, Yelp, and YouTube. We chose U.S. domestic web services since our authors primarily speak English. We also exclude adult content web services. We collected the account remediation advice web pages from services by both manually navigating to the web service help pages and by Google search querying for them. We used Google search queries to ensure the completeness and accuracy of our data. Google search queries for any remediation advice was simply either: "My [web service] account was compromised" or "My [web service] account was hacked". We collected advice from web pages that included account compromise as the following: accounts that were compromised, hacked, or suspended by the online service itself for suspicious activity. We do not consider accounts that were suspended due to actions of the user or suspensions that were self inflicted. We followed all relevant links and web pages referenced on the main account remediation web page to a depth of one. After finding all relevant web pages and content, we saved PDF versions of the web pages and stored them for analysis. This would ensure we had a static data set that did not change as we were coding. This also allowed us to code collectively for web services as a group by analyzing the same PDF.

3 Results

This section shows our results from analyzing account remediation advice. Figure 1 represents code service counts for every

[1]Our complete codebook can be found at: https://bradreaves.net/codebook.pdf

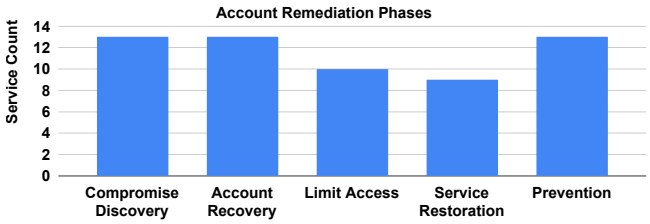

Figure 1: Bar graph of all account remediation phases among web services. All phases are mentioned by every service, except for Limit Access and Service Restoration.

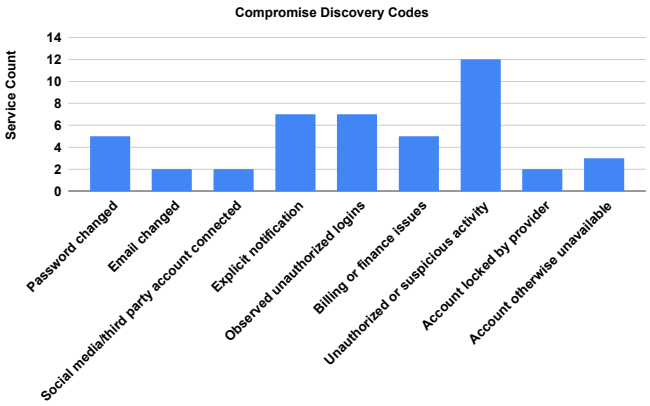

Figure 2: Bar graph of Compromise Discovery codes among web services. Unauthorized or suspicious activity was the highest covered code with 12 web services

phase. The rest of the figures represent code service counts for all of the codes in each category. Code service counts are calculated as the sum of their individual references among all web services. Our findings indicate that account remediation advice from web services is incomplete and numerous important areas are not prioritized. The phases of limit access and service restoration were left out on at least three web services and are insufficient for multiple specific areas. Every web service managed to mention the compromise discovery, account recovery, and prevention phases, but still do not adequately cover all of the relevant information.

Compromise discovery advice is advice about observing activity from an account or service that indicates a possible compromise, and is shown in figure 2. Advice for discovering account compromises is not exhaustively explained to users. For example, advice for discovering password changes, email changes, and new third party account applications were all together only present in 69% of the web services. None of these topics were covered in more than 38% of web services separately. We also 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. However, both of these codes were both separately covered in 54% of web services. Not only should this advice have been universal, but the latter advice should have received a higher coverage since it was not exclusive to its counterpart. It is also reasonable for services to advise users to only notice activity relevant to that web service. For example, services like Twitter and Instagram do not store financial information and therefore don't need advice for noticing billing issues. The only advice within this phase that was close to universal was advice for discovering "unauthorized or suspicious activity", which was mentioned by every service except for Yelp. 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. That being said, there is still an insufficient coverage of compromise discovery advice among web services given that only 33% of codes from this category were mentioned in at least 50% of web services investigated.

Account recovery advice provides a means for users to recover their account after losing access to it or having it compromised, as shown in figure 3 . Account recovery mechanisms were universal among the web services we looked at. 66% of the codes from this phase were covered in at least half of the web services. Every web service gave advice on completing password reset challenges to recover an account. Web services provide users with universal advice and resources for recovering accounts. Some services require 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. Even though we acknowledged the different versions of customer service processes among web services, in this initial study, we did not differentiate when coding them among web services. The code used to represent customer service advice accounted for 54% of web services. While we recognize this topic 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. Lastly, we observed advice for running endpoint security to recover an account was only covered in four web services. The low service count could be the result of authors of account remediation advice not taking endpoint security into consideration. Also, correctly running Anti-virus software is highly technical and possibly

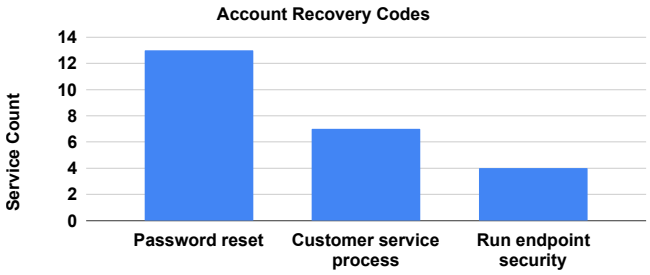

Figure 3: Bar graph of Account Recovery codes among web services. Password reset was mentioned by all web services.

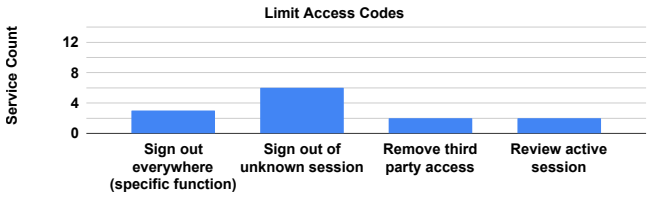

Figure 4: Bar graph of Limit Access codes among web services. No single code was mentioned in more than 46% of web services.

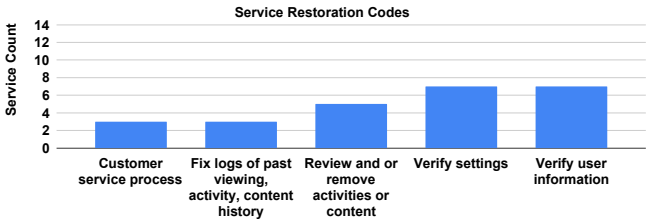

Figure 5: Bar graph of Service Restoration codes among web services. No single code was mentioned in more than 54% of web services.

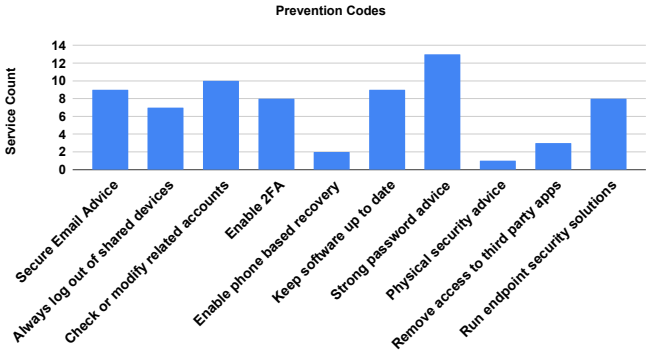

Figure 6: Bar graph of Prevention codes among web services. Seven out of ten codes were mentioned in at least 54% of web services and strong password advice was mentioned in all web services.

beyond the reach of most users. Lastly, it might be unclear to the extent of how much antivirus or other harm remediation measures help remediate online account compromise.

Limiting account access is defined as preventing current and future unauthorized access by unwanted adversaries, as shown in figure 4. Many web services in our study also offer insufficient advice for it. Signing out of unknown sessions or signing out everywhere are important abilities for users to control their account sessions and each were represented by separate codes. Yet, advice for both codes were mentioned in only 46% and 23% of web services respectively. Advice for reviewing active sessions also was represented with a code that was only present in 15% of web services. All three of these codes represent advice that should be universal among web services, given that they are important functionalities to have and are not technically complex. Without the advice to limit or review the access of an account, it is difficult to impossible for users to remediate an account compromise. Lastly, advice for removing third party access was also only present in 15% of web services we investigated.

Service restoration advice involves restoring an account's original settings or information to how it was before the compromise, shown in figure 5. Advice from this phase is also insufficient among web services. Advice for fixing logs of past viewing activity was only present in 23% of web services. Reviewing and removing activities or content was only present in 38% of web services. These are extremely low percentages for advice that should applicable to most if not all of the web services we analyzed. Advice for verifying user information and account settings were each recorded in 54% of web services. All web services here store some amount of user information or settings and therefore all need advice for verifying it. All of the advice in this phase is heavily insufficient throughout web services.

Prevention advice was observed to have the highest rate of coverage among other phases, as shown in figure 6 . This phase is defined as preventing future compromises by taking steps to further secure an account. Out of the total 10 codes, seven were represented in at least 54% of the web services. Yet, all of these codes, with exception to running endpoint security, are relevant and should be universal for all web services given their functionality. Similarly for account recovery, endpoint security can be highly technical for most users. Ideally, prevention advice should be a topic that covers rigorous amounts of information and should be complete for every web service. However, only one of the codes in this phase, strong password advice, was present in all web services. With the exception to physical security advice, all of these codes should have been universal throughout the web services.

Absent explicit account remediation advice: Web services that were also highly ranked but did not have explicit

account remediation advice were characterized by the difficulty of finding their advice. We initially looked at PayPal and Amazon, but did not find sufficient enough content to code. PayPal covers account remediation advice in their help web page under the "Fraud" sub section. Skype gives explicit account remediation advice, but also includes a separate document that gives advice on account remediation that was not included in the initial advice.

Limitations: This project was faced with two limitations which we tried to reasonably counter in our investigation. Firstly, while all authors collaborated for the pilot study, only one single coder coded the rest of the web services. The purpose of conducting the pilot study was to reduce the risk for inaccurate codes for separate coding. Therefore, we iteratively created a codebook reliable enough to allow authors to individually code similar web services and compute similar results. Secondly, our work investigates a small sample size, consisting of the top ranked U.S. web services. Other popular web services ranked lower may better represent the majority of web services people use daily. Investigating these web services may even be more compelling given that even the top ranked web services we analyzed gave insufficient account remediation advice.

4 Conclusion

Advice for limiting account access and service restoration is critical for successfully remediating compromised accounts and yet was not universal among web services. Given the low cost and complexity to implement the advice from these phases, all of the advice from these phases is much lower in coverage than it should be. Also, even the phases that every web service mentioned, web services did not come close to covering all of the important advice for discovering compromised accounts, recovering accounts, or preventing future compromises as they should. Account recovery advice is universal and consists of mechanisms that are very well implemented. Account remediation advice on the other hand is not universal and important advice is being left out on web services. This is a very preliminary analysis into account remediation advice and we want to expand the scope of this work. Our research investigated a small sample of the most popular U.S. domestic web services and discovered that even with their resources and functionality, they do not fully address account remediation advice. Therefore, analyzing lesser ranked or smaller web services that are popular will give more insight into how much account remediation advice is covered among web services. That would also allow us to possibly provide recommendations and suggestions for how account remediation advice can be better covered in web services.

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*, 2013.

[2] 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*, 2015.

[3] 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.

[4] 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*, 2010.

[5] Manuel Egele, Gianluca Stringhini, Christopher Kruegel, and Giovanni Vigna. Towards detecting compromised accounts on social networks. *IEEE Transactions on Dependable and Secure Computing*, 2017.

[6] 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*, 2017.

[7] Megan Leonhart. *The 5 biggest data hacks of 2019*. https://www.cnbc.com/2019/12/17/the-5-biggest-data-hacks-of-2019.html.

[8] 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. https://tranco-list.eu/.

[9] 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)*, 2016.

[10] Vin Ruan, Zhenyu Wu, Haining Wang, and Sushil Jajodia. Profiling online social behaviors for compromised account detection. *IEEE Transactions on Information Forensics and Security*, 2016.

[11] 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*, 2014.