My Account Is Compromised – What Do I Do? Towards an Intercultural Analysis of Account Remediation for Websites

Kathryn Walsh*, Faiza Tazi*, Philipp Markert†, and Sanchari Das*
Department of Engineering and Computer Science
*University of Denver, † Ruhr-Universität Bochum
Email: *FirstName.LastName@du.edu, †FirstName.LastName@rub.de

***Abstract*—Account remediation is the process users perform in case an online account gets compromised. It can be particularly challenging for users as it involves multiple steps, starting from the initial detection until a compromised account is fully recovered. To understand further, we collected and analyzed account remediation protocols from a total of top 50 websites from seven different countries: the United States of America, Canada, United Kingdom, Australia, India, South Korea, and China. Our results suggest that the instructions often miss essential steps. Besides, information is not always easily accessible because web services do not provide central information pages. This absence implies that in the case of an account compromise, users may need to turn to third party sources which can have malicious or incorrect information. Based on these issues, we outline the studies we plan to conduct as a future extension of this work.**

***Index Terms*—Social Media, Account Remediation, Web Services.**

I. Introduction

People have become increasingly aware of internet-related crime and started to recognize the importance of their online privacy [5]. These privacy concerns have led many users to reconsider the importance of some of their web accounts [17], [6]. When users decide to start protecting their privacy online, they might choose to delete some of their online accounts for various reasons [20]. Hence, providing information on account remediation is critical to adhere to the user privacy preferences for any web-based services. Despite the need for a transparent account remediation procedure, it can be challenging for the users. To fully recover a hacked account, a user needs to follow several steps determined by web service providers. In some cases, even getting access to these steps can be arduous [11]. Thus, it is critical to have a more secure and easily implementable account remediation protocols.

To this aid, we conducted an in-depth analysis of the account remediation protocols from different websites. We start by identifying the 50 most popularly used websites in total across seven different countries: the United States, Canada, United Kingdom, Australia, India, South Korea, and China. Due to various factors, such as language barriers or duplicate web services across different countries, we discarded 22 web services. For our analysis, we extended the work by Neil et al. [15], [16] by adding multiple nations to explore the cross-cultural aspects.

II. Related Work

Prior research has focused on different aspects of account remediation [8], [10]. For our study, we selected the account remediation protocol analyzed by Neil et al. [15]. They investigated 13 US web services' account remediation procedures and identified five phases that compose the account remediation: compromise discovery, account recovery, limit access, service restoration, and prevention. In a subsequent work [16], Neil et al. extended this analysis to 57 US-based web services. We extended their methodology for cross-cultural analysis, including 50 top websites visited in seven different countries in combination, to get a more global impression. Based on this examination of the status quo, we planned our in-depth analysis of the account remediation process.

Previous works placed the focus on account compromise discovery with an emphasis on methods that could improve the timeliness and ability for web services to effectively detect compromised accounts [13]. Work on prevention mechanisms also draws attention to best practices that can be used to mitigate the risk of account compromise. Here, Bursztein et al. advocate for defense strategies such as using second-factor authentication [4]. Doerfler et al., on the other hand, investigated the effectiveness of these prevention mechanisms and their impact on users [7].

In terms of work on account recovery, research analyzed various authentication mechanisms that can serve as tools for users that have lost access to their accounts [2], [14]. These forms which have been analyzed, both in terms of security and usability, can be separated into 4 different types: email-based resets [9], SMS-based systems [1], personal knowledge questions [18], and social authentication measures [3]. Zangerle and Specht on service restoration analyzed the user behavior in the aftermath of a discovered account compromise [22]. They found that 27.3 % of users whose accounts were exposed chose to change to a new account. This result is interesting as it sees users possibly adding or circumventing a new category in account remediation — choosing to create a new account entirely instead of solely relying on completing the account remediation process of regaining control and preventing future account compromise. Thus, for our future extension of the work as mentioned in Section V, we propose user studies.

III. Method

As mentioned earlier, for this study, we analyzed the account remediation protocols of the top 50 websites in total from seven countries: Australia, Canada, China, India, South Korea, the United Kingdom, and the United States. We did this by extending a methodology introduced by Neil et al. [15], [16]. For our research, we further expanded the analysis to include other countries in addition to the US. The list of countries was chosen by selecting the top countries with the highest total amount of data breaches by records and the highest ratios of data breaches to population size, as identified by Varonis [21].

Websites were initially selected by choosing the top 20 websites from Tranco [12], using the configure request and the selection "only include domains included in the Chrome User Experience Report of September 2020." After selecting the top 20 websites, we discovered many duplicates or non-English websites, thus we expanded to include the top 50 websites obtained. Expanding the dataset also added smaller web services in the analysis. The final data set, including the 50 websites given the traffic analysis of the websites. This data set was pulled from Tranco on November 7, 2020.

After removing duplicates from the dataset, 15 websites were excluded from analysis because their account remediation process redirected or was a subsidiary of a website already included in the analysis. Four websites redirected or overlapped with Google's account remediation steps or were part of Google's infrastructure: googleusercontent.com, goo.gl, youtube.com, and blogspot.com. Six websites redirected or overlapped with Microsoft's account remediation steps or were part of Microsoft's infrastructure: windowsupdate.com, live.com, office.com, msn.com, bing.com, and skype.com. One website coincided with Amazon: amazonaws.com, and one overlapped with WordPress: gravatar.com. Two websites were excluded because there was no option to create an account on the website: okezone.com, europa.eu.

We found 12 websites which included a default language other than English: tmall.com, baidu.com, sohu.com, Taobao.com, 360.cn, weibo.com, sina.com.cn, Alipay.com, csdn.net, vk.com, jd.com, xinhuanet.com. Of those 12 websites, 11 are international; however, they have Mandarin Chinese as their default language used upon initial website access. vk.com, a social media site predominately used by Russians, is included in this category. Although the default language when visiting the United States website is English, some parts of the remediation process are only available in Russian. Thus, our final dataset resulted in 28 websites with English as the default language for our evaluation. For future work, we will remove this limitation by translating the pages for the analysis.

IV. Analysis and Findings

In our analysis, in general, we noted four common points of interest across different platforms:

- Lack of information about the account remediation process
- Absence of a central information page to initiate the account remediation process
- Presence of a third-party source of advice in the absence of a central page provided by the web service
- Presence of crowd-sourced advice or solution provided by the web service in the absence of a central page

A. Lack of Proper Information

1) Compromise Discovery: For each of the web services, we searched for the presence of information for account remediation. Figure 1a exemplary shows the results in terms of the presence of advice from the websites' central page or a second click point on the websites. We selected the compromise discovery phase as it plays an important role in initiating the account remediation process. We found three of the compromised discovery categories in 16 of the web services: "Account Locked by Provider", "Explicit Notification", and "Email Changed". Moreover, two of the compromised discovery categories, "Social Media or Third-Party Account Connected" and "Billing/Finance Issues", were included in only five of the web services, indicating that these information factors received the lowest amount of attention from web service providers. Part of the reasons for a low occurrence of "Billing/Finance Issues" is that uploading financial information was not always a common practice for users of all web services. A similar reason may exist for the low occurrence of "Social Media or Third-Party Account Connected." However, it is also notable that not all web services clearly defined the relationship or possibility of third party accounts to users.

2) Active Session Overview: The most common way the websites used to limit account access was to review the active sessions, occurring in 12 of the web services analyzed. This action provides users with the capability to review active account sessions, giving them the ability to see unauthorized activity in real-time. However, this implies that less than half of the 28 websites had this option for the users. The least common account remediation strategy, occurring in four web services, was to remove third-party access. However, not all web service accounts had a clear option to grant access to third party accounts, limiting the presence of this option in both the limiting account and account compromise phases of account remediation.

3) Service Restoration: Service restoration was the most well represented phase of account remediation across, with 11 websites including information about all steps of the service restoration procedure. Fourteen websites had some mechanism to verify user information and the customer service process, but three of them did not mention any additional details of the service restoration. The least common feature mentioned was the monitoring of logs of past viewing/activity/content history.

4) Preventing Future Account Compromises: An important part of the account remediation procedure is preventing future account compromises. However, only 17 of the web services followed or provided options to the user with any tangible recommendations such as: "Enable 2FA", "Advice About Secure Email", and "Password Advice." Two of these categories are components of increasing login security choices made by users: passwords and 2FA. For five of the websites, more

detailed security measurements were advised such as: "Run Endpoint Security Solutions", "Keep Software up to Date", "Check/Modify Related Accounts", and "Always Log Out on Shared Devices."

B. Lack of Central Page

For a total of seven web services we marked that they do not provide a central page for account remediation advice as none of these websites contained a central page in response to "account hacked" or "account compromised." These websites include: amazon.com, adobe.com, zoom.us, bit.ly, nytimes.com, flickr.com, and cnn.com. A lack of a central page is significant, as it does not provide users with guidance or a starting point to present their account remediation advice. If users experience an account compromise, they may seek additional sources of guidance in the absence of a clear central page on the web service with the compromised account, which can lead to trusting unauthorized web pages with possible incorrect information.

C. Third-Party Sources

During the Google search portion of the account remediation process, some of the top search results included resources for the account remediation process specific to that website from third-party sources. For example, when a user searches for the term "yahoo account compromise" the first result directs users to a page on the yahoo website. However, the first page of results also includes six pages that include third-party resources offering advice and next steps for users to take in the account remediation process. These third-party resources are especially significant when the original web services lack a central page for users to initiate the account remediation process, as it may be the primary source users have available to guide them in the event of an account compromise. Of the seven web services that did not have a central page, five of them had third-party sources readily available through a Google search. Some of these third-party sources can also be malicious websites, which can be harmful to account security.

D. Crowdsourcing Advice

Investigating the account remediation process also revealed another source of account remediation advice available to users within a website such as: help forums and postings from users that can provide answers and advice during an account compromise. Of the seven web services that did not have a central page, two of them had crowd-sourced advice readily available through a Google search. adobe.com did not contain a central page for a hacked or compromised account, however, searching for the term "account hacked" within the website did provide 51 results of users seeking help from others. Additionally, flickr.com contains advice in a help forum on their primary site. Interestingly, one of the most common and well-received responses to these forum responses is to contact the support, indicating that this is likely the most effective course of action for users seeking guidance through the account remediation process.

E. Intercultural Analysis

All of the websites analyzed during this study have an international aspect, in fact all of these websites appear in the top 50 websites in the Tranco lists of the seven countries. Out of the 28 websites, only two were headquartered outside of the United States (details in Table I). Additionally, we were only able to analyze the account remediation process of the websites when it was written in English. This is a limitation of our analysis that will be addressed in our future work (Section V), by translating the pages, comparing and contrasting them to what is being offered in the English version.

V. Future Research Proposal

Through the study, we found that there are some areas of account remediation which can be explored further. We note that no web service analyzed contained account remediation advice in every category; however, there did seem to be a trend that less popular sites contained fewer remediation steps or information about it. We also found seven web services that lack a central web page for account remediation advice entirely. This absence implies that in the case of an account compromise, users may need to turn to sources other than the primary web service for guidance on how to complete the remediation process, putting the power outside of the hands of the initial web service. Hence, the first research direction is to investigate how users react to and cope with incomplete or missing information.

Closely related to this is the question of how users behave if a web service provides information about all remediation steps. While thoroughness may be the intended result at the end, some form of prioritization may be necessary for the immediate reaction or in the short term. Hence, the second direction is to learn more about how many of the remediation steps are completed by users and at which point in time. Moreover, many account remediation guidance lack prioritization of steps or narrative and visual devices to guide and motivate users through the account remediation process. We also want to include the influence of these aspects in our research.

For a third research direction, we will follow the five account remediation phases' order and investigate how we can enable the user to discover account breaches more efficiently. In detail, we will look at account activity pages, i.e., pages that display all logins to a user's account. Account activity pages play a central role in the account remediation as they enable the user to identify compromises in the first place.

Our approach to improving the design of account activity pages is two-fold: first, we will analyze the status quo. To do this, we will select a representative sample from the service providers who provide such a page. We will test the sample by conducting a study using a method from Rader et al. [19]. In a user study, we will first ask participants if they have an account with the services from our sample. Afterward, we will ask users to visit the account activity page of one of those services, to download the source code of the page, and to upload it to our study web service. This will allow us to embed the page, analyze, and extract information from it.

VI. Conclusion

Account remediation is an essential procedure to identify malicious login attempts for a web service Neil et al. provide a foundation for understanding the presence of account remediation advice available throughout web services [15], [16]. This paper extended their methodology and conducted an in-depth analysis of the account remediation protocols from 28 top websites in total across seven countries: USA, UK, Canada, Australia, India, South Korea, and China. In line with the findings about US-based web services from Neil et al., we found that the absence of sufficient information for successful account remediation is also very prominent in most web services evaluated across the nations. In cases where information is present, websites do not offer enough advice for a successful account remediation process, especially when it comes to helping users prevent future account compromises. Given the results from our initial analysis, we propose a future research direction. The efforts will focus on users' behavior towards available account remediation steps and improve account activity pages through detailed studies.

Acknowledgments

We would like to thank the Security and Privacy Research Lab at the University of Denver to provide resources for this study. We would also like to thank the students of the Human-Centered Data Security and Privacy course for their initial feedback on the project. Any opinions, findings, conclusions, and recommendations expressed in this material are solely those of the authors and do not necessarily reflect the views of the University of Denver nor the Ruhr-Universität Bochum.

References

[1] 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 *The World Wide Web Conference*, WWW '15, pages 141–150, Florence, Italy, May 2015. ACM.

[2] 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 *IEEE Symposium on Security and Privacy*, SP '12, pages 553–567, San Jose, California, USA, May 2012. IEEE.

[3] John Brainard, Ari Juels, Ronald L. Rivest, Michael Szydlo, and Moti Yung. Fourth-Factor Authentication: Somebody You Know. In *ACM Conference on Computer and Communications Security*, CCS '06, pages 168–178, Alexandria, Virginia, USA, October 2006. ACM.

[4] Elie Bursztein, Borbala Benko, Daniel Margolis, Tadek Pietraszek, Andy Archer, Allan Aquino, Andreas Pitsillidis, and Stefan Savage. Handcrafted Fraud and Extortion: Manual Account Hijacking in the Wild. In *Internet Measurement Conference*, IMC '14, pages 347—-358, Vancouver, British Columbia, Canada, November 2014. ACM.

[5] Sanchari Das, Jayati Dev, and Kaushik Srinivasan. Modularity is the key a new approach to social media privacy policies. In *Proceedings of the 7th Mexican Conference on Human-Computer Interaction*, pages 1–4, 2018.

[6] Sanchari Das, Robert S Gutzwiller, Rod D Roscoe, Prashanth Rajivan, Yang Wang, L Jean Camp, and Roberto Hoyle. Humans and technology for inclusive privacy and security. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 64, pages 461–464. SAGE Publications Sage CA: Los Angeles, CA, 2020.

[7] Periwinkle Doerfler, Kurt Thomas, Maija Marincenko, Juri Ranieri, Yu Jiang, Angelika Moscicki, and Damon McCoy. Evaluating Login Challenges as a Defense Against Account Takeover. In *The World Wide Web Conference*, WWW '19, pages 372–382, San Francisco, California, USA, May 2019. ACM.

[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] Simson L. Garfinkel. Email-Based Identification and Authentication: An Alternative to PKI? *IEEE Security & Privacy*, 1(6):20–26, November 2003.

[10] Rodrigo Augusto Igawa, Alex Marino Goncalves de Almeida, Bruno Bogaz Zarpelao, and Sylvio Barbon. Recognition of Compromised Accounts on Twitter. In *Brazilian Symposium on Information Systems: Information Systems: A Computer Socio-Technical Perspective*, SBSI '15, pages 9–14, Goiânia, Goiás, Brazil, May 2015. ACM.

[11] Sowmya Karunakaran, Kurt Thomas, Elie Bursztein, and Oxana Comanescu. Data Breaches: User Comprehension, Expectations, and Concerns With Handling Exposed Data. In *Symposium on Usable Privacy and Security*, SOUPS '18, pages 217–234, Baltimore, Maryland, USA, August 2018. USENIX.

[12] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński, and Wouter Joosen. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In *Symposium on Network and Distributed System Security*, NDSS '19, San Diego, California, USA, February 2019. ISOC.

[13] Lucy Li, Bijeeta Pal, Junade Ali, Nick Sullivan, Rahul Chatterjee, and Thomas Ristenpart. Protocols for Checking Compromised Credentials. In *ACM Conference on Computer and Communications Security*, CCS '19, pages 1387–1403, London, United Kingdom, November 2019. ACM.

[14] Philipp Markert, Maximilian Golla, Elizabeth Stobert, and Markus Dürmuth. Work in Progress: A Comparative Long-Term Study of Fallback Authentication. In *Workshop on Usable Security*, USEC '19, San Diego, California, USA, February 2019. ISOC.

[15] Lorenzo Neil, Yasemin Acar, and Bradley Reaves. Investigating Web Service Account Remediation Advice. In *Who Are You?! Adventures in Authentication Workshop*, WAY '20, pages 1–6, Virtual Conference, August 2020.

[16] Lorenzo Neil, Elijah Bouma-Sims, Evan Lafontaine, Yasemin Acar, and Bradley Reaves. Investigating Web Service Account Remediation Advice. In *Symposium on Usable Privacy and Security*, SOUPS '21, Virtual Conference, August 2021. USENIX.

[17] Abu Saleh Md Noman, Sanchari Das, and Sameer Patil. Techies Against Facebook: Understanding Negative Sentiment Toward Facebook via User Generated Content. In *ACM Conference on Human Factors in Computing Systems*, CHI '19, pages 468:1–468:15, Glasgow, Scotland, United Kingdom, May 2019. ACM.

[18] Ariel Rabkin. Personal Knowledge Questions for Fallback Authentication: Security Questions in the Era of Facebook. In *Symposium on Usable Privacy and Security*, SOUPS '08, pages 13–23, Pittsburgh, Pennsylvania, USA, July 2008. ACM.

[19] Emilee Rader, Samantha Hautea, and Anjali Munasinghe. "I Have a Narrow Thought Process": Constraints on Explanations Connecting Inferences and Self-Perceptions. In *Symposium on Usable Privacy and Security*, SOUPS '20, pages 457–488, Virtual Conference, August 2020. USENIX.

[20] Brady Robards. Leaving MySpace, Joining Facebook: 'Growing up' on Social Network Sites. *Continuum*, 26(3):385–398, 2012.

[21] Rob Sobers. The World in Data Breaches, March 2020. https://www.varonis.com/blog/the-world-in-data-breaches/, as of July 1, 2021.

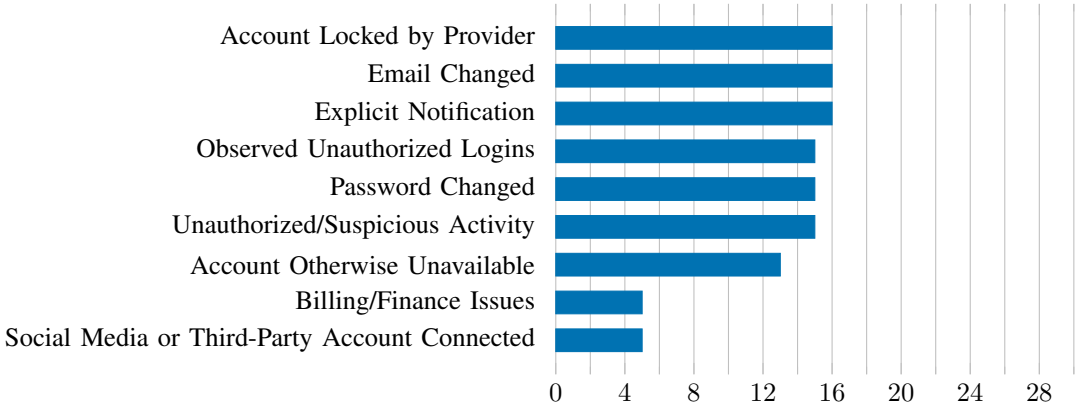
[22] Eva Zangerle and Günther Specht. "Sorry, I Was Hacked": A Classification of Compromised Twitter Accounts. In *ACM Symposium on Applied Computing*, SAC '14, pages 587–593, Gyeongju, Republic of Korea, March 2014. ACM.

APPENDIX

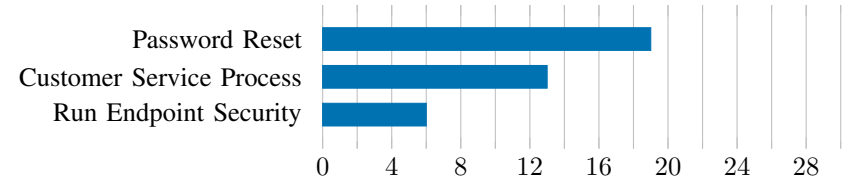
TABLE I: List of the 28 analyzed websites, including headquarters and rank according to the national Tranco lists [12].

			National Tranco Rank							
No.	**Website**	**Headquarter**	**Australia**	**Canada**	**China**	**India**	**South Korea**	**UK**	**USA**	**Average**
1	google.com	Menlo Park, CA, USA	1	1	1	1	1	1	1	1.0
2	facebook.com	Menlo Park, CA, USA	2	2	2	2	2	2	2	2.0
3	microsoft.com	Redmond, WA, USA	4	4	4	4	4	4	4	4.0
4	twitter.com	San Francisco, CA, USA	5	5	5	5	5	5	5	5.0
5	instagram.com	Menlo Park, CA, USA	7	7	7	7	7	7	7	7.0
6	linkedin.com	Sunnyvale, CA, USA	9	9	9	9	9	9	9	9.0
7	apple.com	Cupertino, CA, USA	12	12	11	12	12	12	12	11.9
8	wikipedia.org	San Francisco, CA, USA	13	13	12	13	13	13	13	12.9
9	netflix.com	Los Gatos, CA, USA	15	15	14	15	15	15	15	14.9
10	amazon.com	Seattle, WA, USA	17	17	16	17	17	17	17	16.9
11	yahoo.com	Sunnyvale, CA, USA	18	18	17	18	18	18	18	17.9
12	pinterest.com	San Francisco, CA, USA	20	20	19	20	20	20	20	19.9
13	adobe.com	San Jose, CA, USA	21	21	20	21	21	21	21	20.9
14	vimeo.com	New York, NY, USA	23	23	22	23	23	23	23	22.9
15	reddit.com	San Francisco, CA, USA	25	25	24	25	25	25	25	24.9
16	zoom.us	San Jose, CA, USA	26	26	25	26	26	26	26	25.9
17	wordpress.com	San Francisco, CA, USA	29	29	28	29	29	29	29	28.9
18	github.com	San Francisco, CA, USA	33	33	31	33	33	33	33	32.7
19	bit.ly	New York, NY, USA	–*	–*	–*	36	35	36	36	35.8
20	vk.com	Saint Petersburg, Russia	37	38	34	39	38	39	39	37.7
21	tumblr.com	New York, NY, USA	40	41	37	42	41	42	42	40.7
22	mozilla.org	Mountain View, CA, USA	41	42	38	43	42	43	43	41.7
23	nytimes.com	New York, NY, USA	43	44	40	45	44	45	45	43.7
24	whatsapp.com	Menlo Park, CA, USA	44	45	41	46	45	46	46	44.7
25	flickr.com	San Francisco, CA, USA	45	46	42	47	46	47	47	45.7
26	dropbox.com	San Francisco, CA, USA	47	48	43	49	48	49	49	47.6
27	soundcloud.com	Berlin, Germany	50	52	46	52	51	52	52	50.7
28	cnn.com	Atlanta, GA, USA	51	53	47	53	52	53	53	51.7

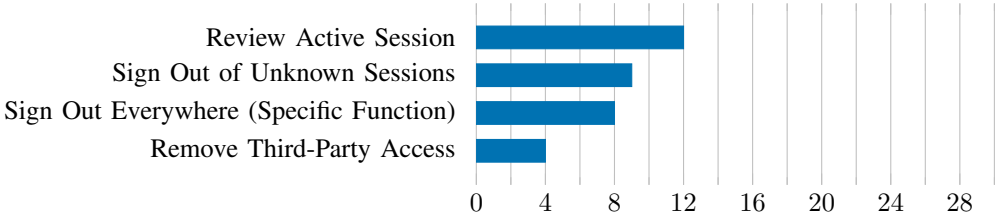
$\star$: bit.ly was not included in the respective Tranco lists.



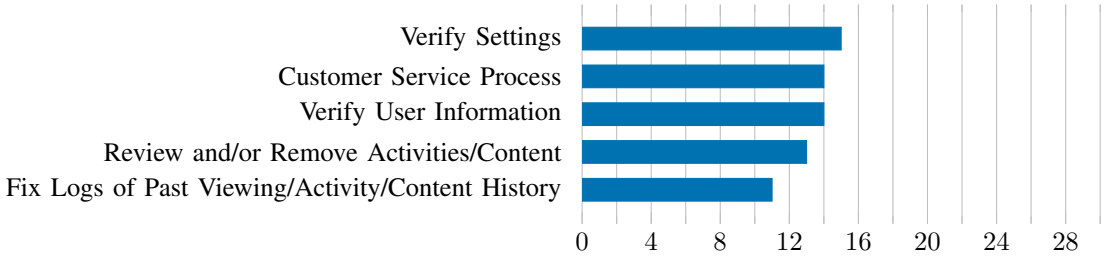
(a) Presence of advice to discover account compromise.



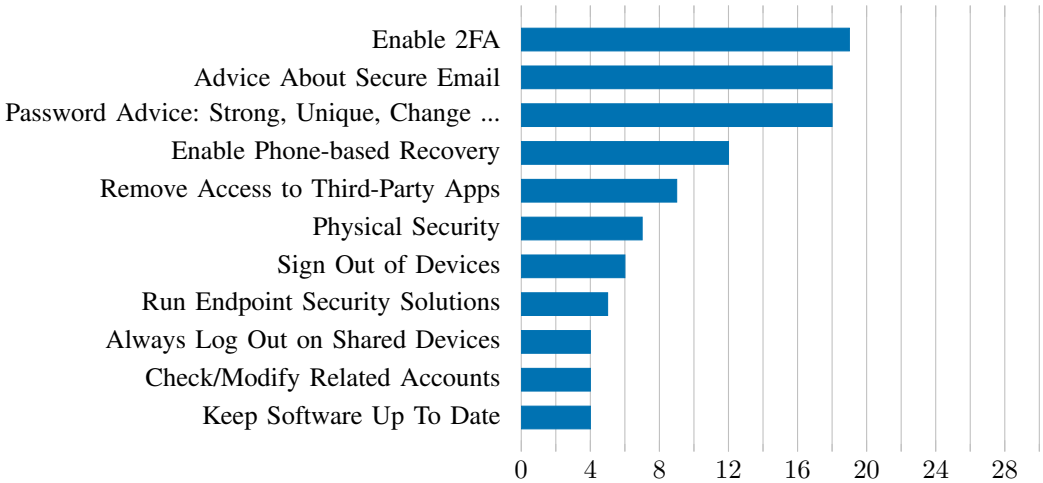
(b) Presence of advice to recovery the user's account.



(c) Presence of advice to limit or restrict unauthorized access.



(d) Presence of advice to restore the user's service.



(e) Presence of advice to prevent future account compromises.

Fig. 1: Presence of advice among the 28 analyzed web services.