A Transcontinental Analysis of Account Remediation Protocols of Popular Websites

Philipp Markert
Ruhr University Bochum
philipp.markert@rub.de

Andrick Adhikari
University of Denver
andrick.adhikari@du.edu

Sanchari Das
University of Denver
sanchari.das@du.edu

***Abstract*—Websites are used regularly in our day-to-day lives, yet research has shown that it is challenging for many users to use them securely, e.g., most prominently due to weak passwords through which they access their accounts. At the same time, many services employ low-security measures, making their users even more prone to account compromises with little to no means of remediating compromised accounts. Additionally, remediating compromised accounts requires users to complete a series of steps, ideally all provided and explained by the service. However, for U.S.-based websites, prior research has shown that the advice provided by many services is often incomplete. To further understand the underlying issue and its implications, this paper reports on a study that analyzes the account remediation procedure covering the 50 most popular websites in 30 countries, 6 each in Africa, the Americas, Asia, Europe, and Oceania. We conducted the first transcontinental analysis on the account remediation protocols of popular websites. The analysis is based on 5 steps websites need to provide advice for: compromise discovery, account recovery, access limitation, service restoration, and prevention. We find that the lack of advice prior work identified for websites from the U.S. also holds across continents, with the presence ranging from 37% to 77% on average. Additionally, we identified considerable differences when comparing countries and continents, with countries in Africa and Oceania being significantly more affected by the lack of advice. To address this, we suggest providing publicly available and easy-to-follow remediation advice for users and guidance for website providers so they can provide all the necessary information.**

I. Introduction

We use websites in everyday life for various purposes, including necessities of life, healthcare, education, business, and information dissemination [75]. Several of these websites require users to create an account to access the content, which causes them to include several individual details [35]. Hence, accounts can hold sensitive and critical information of users, some of which is related to health, social affairs, or political affairs [36]. Technological capabilities and the wealth of data stored through these websites make it lucrative for attackers to steal, destroy, or modify data. Research has shown that every 39 seconds, a website is attacked, and on average, 30,000 websites are attacked every day. Furthermore, such attacks on websites increase at a rate of 13% each year and can be executed in various ways [10].

Symposium on Usable Security and Privacy (USEC) 2023
27 February 2023, San Diego, CA, USA
ISBN 1-891562-91-6
https://dx.doi.org/10.14722/usec.2023.235078
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

Due to the described risks, websites can become insecure and easy to compromise, out of which the user accounts become a primary target. Once an account is compromised, it must be restored to its pre-compromise state, referred to as "account remediation" [53]. In general, account remediation is a set of protocols to transform a compromised account into one that is again entirely under the user's control. This process includes several aspects, e.g., the mechanisms of resetting the password, turning on two-factor authentication, security verification checks, or account deletion [53]. Hence, it can be technically complex and, in several cases, is left to user choices and discretion [47], [76]. Thus, lacking information about account remediation is one of the most critical factors that often keep users un/misinformed about actions to perform if an account is compromised. Moreover, users depend on a thorough provision of advice by the website owners to protect their accounts from hacks. Unfortunately, prior research has shown that among U.S.-based websites, these instructions are often incomplete making it cumbersome or even impossible for users to complete the process [53].

To further explore this, we report on an analysis covering the remediation advice of the 50 most popular websites in 30 countries across 5 continents, Africa, America, Asia, Europe, and Oceania. We selected 6 countries from each continent based on each country's ranking in Global Cybersecurity Index (GCI) 2020 [33], the 3 countries with the best and 3 with the worst rating. Afterward, we assembled a list of the 50 most popular websites in each country based on the Tranco list [40]. Several of these websites are popular across countries, hence, the final list for the analysis consisted of 158 unique websites. In the analysis, we checked each website for the presence of account remediation advice using an updated model from prior work [53], which defines account remediation in 5 phases: *Compromise Discovery*, *Account Recovery*, *Limit Access*, *Service Restoration*, and *Prevention*. Finally, we compared the 5 different continents based on the results of the analysis.

We believe automation of all possible steps is key to unburdening users and limiting an account compromise's adverse effects. Consequently, the research object was to analyze the current remediation process to identify missing, redundant, or unclear steps on a global scale. Ultimately, through this research and with future extension of this work we aim to create an account remediation protocol that is optimized both regarding maximizing the technical assistance and the guidance of steps where such assistance is not possible. Through our analysis, we noted the following issues in the account remediation protocols of websites popular in different places of the world which is the contribution of this work:

- Lack of information: We found that most websites have pages with policies, including the privacy policy. However, they often lack instructions, e.g., on how to create a strong password and how to delete an account including information on what will be removed. In addition, websites should address the means of protecting accounts from hacking, the procedures the user must follow if the account was hacked, or the user's desire to restore the account with its contents.
- Lack of security measures: Most websites do not use multiple security checks to verify the user's authentication. For example, they do not offer two-factor authentication and are limited to verification only by sending an email to the user. Frequently, they also do not check if a newly set password is related to the one being replaced—a test possible without any risk as knowledge of the old password also needs to be checked.
- Difference between countries: We found that remediation advice is missing on websites popular across continents, yet, users in countries with lower security standards are more prone to missing advice. While most of these differences appear manageable, users in countries which are part of the global south in Africa and Oceania are significantly more affected by the absence of crucial remediation advice. We want to mention that in this work, we are intentionally not using phrases such as "developed and developing nations" or "Third World"; instead we are using the terms "Global South" and "Global North." These phrases mark a shift from a focus on development or economic differences toward an emphasis on geopolitical power relations [11]. Moreover, prior work suggests that the concepts or phrasing such as "Third World" is no longer a viable concept from a political perspective and can be patronizing [38], [50]. We understand that these terms may still provide an inspiration for similar discussions, which can be presently represented with the phrasing of global south and global north into a force in the reconfiguration of global relations [13].
- Identification of the impact of third parties on account remediation: The presence of third parties means data is shared between services for commercial purposes, which threatens the users' privacy and the security of their accounts. Some websites name third parties they share data with, but many websites say that they sent data to third parties but do not provide easy-to-find and sometimes any information at all which parties particularly.
- Ignorance of recommendations from research: numerous recommendations have evolved from research in the field of (usable) security throughout the years, still, it depends on the website to also adopt them [18]. We noted that several pieces of advice are not implemented even by these highly used websites. For example, 2FA is a recommendation by experts to protect user accounts [64], [70], yet, most websites do not offer 2FA at all, and those which do often only send one-time passwords (OTP) via email.

In Section II, we detail related work focusing on how the account compromise and remediation protocols came into existence and how users become the primary actors in making these protocols a success. Section III depicts the process of collecting the websites and developing the codebook to analyze the account remediation procedures of websites. Next, Section IV depicts an overview of the collected data and the analysis across different continents and countries. Section V discusses and contextualizes the results, which forms the basis for our recommendation in Section VI. Finally, we provide an overview of the limitations of this study, which we plan to address through the future extension of this work in Section VII, and conclude the paper in Section VIII.

II. Related Work

Account remediation is a critical process for online interaction to protect user data; however, it can be complicated. For our analysis, we selected the account remediation protocol developed by Neil et al. [53] to understand the account remediation aspects. They investigated the account remediation procedures of 57 U.S.-based websites and identified 5 phases that compose the process: (1) compromise discovery, (2) account recovery, (3) limit access, (4) service restoration, and (5) prevention. We extended their methodology for a transcontinental analysis of 158 website covering the top 50 websites visited in 5 continents and across 6 countries from each continent in combination to get a broader understanding of the protocol impacts and application for account remediation. Below we also want to address the work in the 3 most related research areas: the process of discovering an account compromise, risk mitigation, and users' decision-making process.

A. Account Compromise Discovery

Researchers have emphasized account compromise discovery to improve the timeliness and ability of websites to effectively detect compromised accounts [15], [16], [25], [31], [43]. Additional work on prevention mechanisms drew attention to best practices that can mitigate the risk of account compromise, e.g., a risk analysis [9]. With our study, we focus on the general protocols provided by the websites.

Halawa et al. suggested an early warning system based on machine learning to detect compromised and vulnerable accounts by identifying suspicious account usage behavioral patterns [25]. Egele et al. have also leveraged machine learning techniques to detect compromised accounts in social networks by introducing a tool called *COMPA*. COMPA creates behavioral profiles for Facebook and Twitter users, trains a model with a small manually labeled dataset of compromised and non-compromised user accounts, and uses this model to detect compromised Twitter and Facebook accounts [15].

B. Risk Mitigation

Work on prevention mechanisms draws attention to best practices that can mitigate the risk of account compromise—Bursztein et al. advocate for defense strategies such as using second-factor authentication [9]. Doerfler et al., on the other hand, investigated the effectiveness of these prevention mechanisms and their impact on users [14]. Other research analyzed different fallback authentication mechanisms that can serve as tools for users that have lost access to their accounts [5], [45]. These forms which have been analyzed, both in terms of security and usability, can be separated into four different types: email-based resets [22], SMS-based systems [4], personal knowledge questions [37], [56], [57], [66], and social authentication measures [6], [67].

Of all those methods, Li et al. identified the email-based reset as the most popular [44]. Furthermore, they propose an improved method called *Secure Email Account Recovery* to prevent malicious activities when the registered email account is compromised. However, in addition to the technical implementation, it is also essential to understand the user perspective. At the same time, expert advice is valued for privacy, cybersecurity auditing, and research. Nevertheless, since advice also needs to be provided at the appropriate places, the utilization of websites and applications is as important [62]. Through our study, we intend to explore and check this.

C. Users' Decision-Making Process

Along these lines, regarding the decision-making procedures of account remediation and online account compromise reactions, researchers have also focused on users' mental models [7], [21]. While discussing decision-making procedures of account remediation and online account compromise reactions, researchers have also focused on mental models in the face of a hacked account. The key finding here was that understanding security measures is incomplete [59], [68].

Zangerle and Specht further analyzed the user behavior after a discovered account compromise [77]. 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 relying on the account remediation process to regain control and prevent future compromises.

III. Method

This section describes the method used for the transcontinental analysis of account remediation protocols. We collected the top 50 websites from 6 countries and across 5 continents worldwide to conduct our evaluation of the account remediation protocol. We intended to get a holistic overview of the account remediation protocols adapted by several websites. Therefore, our study design includes the following 2 steps: First, we describe the collection of the relevant websites in Section III-A, which we composed such that they represent the most popular websites in each of the continents. Followed by that, Section III-B depicts how we updated the codebook for our analysis, which was initially developed by Neil et al. [53].

A. Website Collection

Previous work [53] found that the information about account remediation procedures on U.S.-based websites is oftentimes incomplete. Through our study, we aim to evaluate the account remediation for 50 websites from 6 countries on 5 continents globally. This was done to provide an overview of how expert-suggested account remediation protocols are implemented by the different websites in different geographical locations. The purpose of the analysis is to gain an in-depth evaluation of those websites in several areas for account remediation.

To achieve this, we took 5 continents, Africa, America (North and South), Asia, Europe, and Oceania. We eliminated Antarctica from the analysis, given its low population. To determine the 3 best and worst countries on each continent regarding their cybersecurity proficiency, we used the Global Cybersecurity Index (GCI) [33]. Note that the GCI combines South and North America; hence, we also kept them together for the analysis [8]. We chose GCI as a reference since it assesses nations through expertise of different organizations across legislative measures, technical measures, organizational measures, capacity development, and collaboration - and then aggregates this assessment into an overall score.

TABLE I. List of the analyzed countries for each of the 5 continents. The Global Cybersecurity Index [33] was used for the classification of best and worst countries.

Continent	Best Countries	Worst Countries
Africa	Mauritius Tanzania Ghana	Equatorial Guinea Eritrea Burundi
America	USA Canada Brazil	Honduras Dominica Haiti
Asia	Saudi Arabia South Korea Singapore	Maldives Timor-Leste Afghanistan
Europe	United Kingdom Estonia Spain	San Marino Andorra Bosnia and Herzegovina
Oceania	Australia New Zealand Fiji	Marshall Islands Solomon Islands Vanuatu

The cybersecurity proficiency of a country is estimated based on the ability to protect its infrastructure, including systems, applications, hardware, software, and data. The GCI also evaluates a country's legal measures, such as legislation and laws, technical measures, such as the deployment of incident response teams; organizational measures that examine the governance and coordination mechanisms addressing cybersecurity within a country; capacity development measures to counteract large-scale attacks, cooperative measures among multiple stakeholders or countries, and child protection measures. Taking the GCI ranking, we ended up with 30 countries, the 3 best and 3 worst for each continent, as depicted in Table I.

After selecting the countries, we used the Tranco list [40] to identify the 50 most popular websites for each country. The top websites are calculated based on the number of people who visit the website per month, as listed in Tranco's List. The list was verified and calculated based on a combination of Alexa, Umbrella, and Majestic websites. The second-ranking to classify the websites was the "Alexa rank," a global popularity ranking [72]. It uses web traffic data to make an ordered list of each country's most popular sites on the Internet. We used multiple categories and rankings to ensure we got the most visited and searched websites for the selected countries. By doing this, we ended up with a list of 1394 websites, 300 each from America, Europe, and Asia, 253 websites from Africa, and 241 websites from Oceania. The numbers being lower for Africa and Oceania is due to the sparsity of data. Hence, the Tranco list for Eritrea, the Marshall Islands, the Solomon Islands, and Vanuatu consists of less than 50 websites. We merged the lists from all nations and deleted duplicates, yielding a list of 158 unique websites. They are depicted in Table III and IV along with their number of occurrences in the top 50 list in each country.

B. Codebook Composition

A first step toward analyzing the account remediation procedure on websites was done by Neil et al. They developed a codebook with a total of 32 codes and identified 5 phases they can be grouped into: (1) compromise discovery, (2) account recovery, (3) limit access, (4) service restoration, (5) prevention. The first phase is where the account owner identifies the compromise to initiate the remediation procedure. Afterwards, access to the account may need to be restored, e.g., if the attacker changed the password. The next step is to remove any malicious access to the account, e.g., by stopping unknown sessions. Step four is to identify and restore any unwanted changes, followed by step 5, which aims at reducing the chances of future compromise by following a set of security advice. By completing all 5 phases, a compromised account becomes again an account fully under control by the actual account owner.

To analyze the account remediation protocols of the 158 websites we collected based on the method described in Section III-A, we first updated the codebook by removing and adding 3 codes. We then distributed the websites among 5 coders, who used the updated codebook to examine them. To ensure the quality and correctness of the data, we performed a cross-check for a randomly selected 10% of the websites.

The first two codes we removed are *Run Endpoint Security* and *Run Endpoint Security Solutions*. They are part of the second (*Account Recovery*) and fifth (*Prevention*) phase, respectively, and advise users to run their antivirus software to prevent any potential attacks. We removed both codes as the benefit of such software on computers is disputable [34], [49], [71] and on mobile devices with their dedicated sandbox environments and app stores, the situation is similar [1]. The third code we removed is *Physical Security* which is part of phase 5 *Prevention* and intends to prevent undesired access by strangers. However, it is a code that was barely found in prior work [53], and it only applies to specific use cases, e.g., when using a computer in a café. On the other hand, mobile devices, presumably the most used public, are usually locked after usage [26], [27], [28].

The first code we added is *Password Rotation* which became part of phase two *Account Recovery*. It describes if the website informs the user (and assures) that when changing the password, it must not be related to the old one. If this check is missing, an attacker with credentials may still be able to use them even though the password itself was changed [3]. The following code, added to the third phase *Limit access*, is *Instructions for Account Deletion*. Deleting the account itself is also a way to limit access, primarily if users have not used the account for a while and realize they no longer need it [77]. Finally, we added a code *Regular Security Checkups/Advice* to phase 5 *Prevention*. It depicts if websites inform their users to check the security of their accounts regularly because once the account is remediated, users may shift their focus away from security aspects which is why this long-term advice is essential. Furthermore, to also cover the modality in which certain functionalities are offered, we additionally collected information about the communication channel for notifications (email, SMS, push) and how users can contact customer support (email, chat, phone, form).

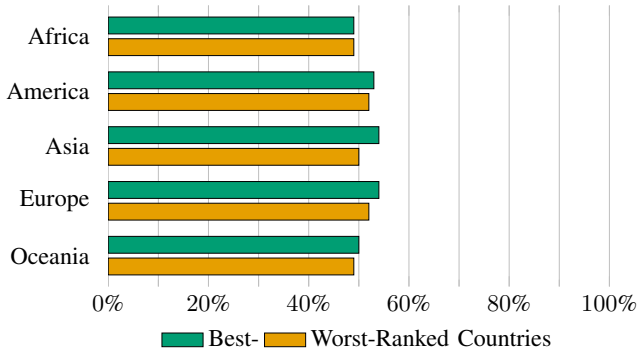

Fig. 1. Average presence of advice for *Phase 1: Compromise Discovery* in each of the 5 analyzed continents.

IV. Results

We now present the results for the analysis of the 158 unique websites, representing the top 50 websites for each of the 6 countries in Africa, America, Asia, Europe, and Oceania. The full details for the best and worst countries from each continent are presented in Table II, where each entry reflects the percentage of websites with established advice on a given account remediation phase. In addition, the averages for each phase are shown in Figures 1–5, and an accumulated overview is given in Figure 6. To compare the presence of account remediation advice across different groups, we used a χ^2 test ($\alpha = 0.05$) with the Benjamini-Hochberg procedure applied for posthoc pairwise comparisons [39], [42], [78].

Phase 1: Compromise Discovery

The first phase, in which a user must detect the compromise, consists of 9 steps. As can be seen in Figure 1, about half of the required advice is present across all continents and countries. Most advice (54%) is present on the most popular websites for the highest-ranked countries in Europe and Asia. Conversely, the least advice (49%) is given on websites that are popular in Africa (best and worst) or the Marshall Islands, Solomon Islands, and Vanuatu, i.e., the lowest-ranked countries according to the GCI [33] in Oceania.

The one type of advice which is present on most websites, irrespective of the continent, is *Explicit Notification*, i.e., websites notify users about a new login. Interestingly, the highest number appears in America (91%) for the popular websites of the lowest-ranked countries according to the GCI [33] in the form of Honduras, Dominica, and Haiti. Conversely, this number goes down to 73% for websites popular in the worst-ranked countries in Oceania (Marshall Islands, Solomon Islands, and Vanuatu). The χ^2 test also suggested some significant differences in the data for this code ($p = 0.023$). However, the post-hoc analysis did not confirm this initial assumption.

We observe the lowest scores for this first phase for websites informing users about a connected social media or third-party account. The percentages range from 18% for websites popular in the worst-ranked countries in Europe to 38% for popular websites in Oceania, again the lowest-rated countries. While this finding may seem counter intuitive, it could be partially explained by the overall lower popularity of this feature across websites popular in the Marshall Islands,

TABLE II. PERCENTAGE OF WEBSITES THAT PROVIDE ADVICE FOR THE 5 PHASES OF ACCOUNT REMEDIATION AMONG THE TOP 50 WEBSITES OF THE 3 BEST AND WORST RANKED COUNTRIES ACCORDING TO THE GCI [33] IN AFRICA, AMERICA, ASIA, EUROPE, AND OCEANIA.

		Africa		America		Asia		Europe		Oceania	
		Best	Worst	Best	Worst	Best	Worst	Best	Worst	Best	Worst
Compromise Discovery	Account Locked by Provider	50%	58%	55%	57%	58%	57%	58%	57%	49%	63%
	Account Otherwise Unavailable	51%	57%	58%	52%	60%	52%	60%	53%	49%	47%
	Billing/Finance Issues	57%	43%	63%	58%	63%	54%	64%	58%	59%	32%
	Email Changed	37%	35%	39%	39%	41%	37%	38%	41%	37%	38%
	Explicit Notification	83%	80%	82%	91%	82%	80%	82%	89%	78%	73%
	Observed Unauthorized Logins	49%	42%	55%	54%	58%	52%	58%	51%	54%	39%
	Password Changed	42%	56%	43%	47%	43%	48%	42%	48%	46%	63%
	Social Media or Third-Party Account Connected	22%	25%	23%	19%	23%	19%	22%	18%	25%	38%
	Unauthorized/Suspicious Activity	48%	48%	55%	51%	58%	50%	58%	50%	51%	47%
Account Recovery	Customer Service Process	83%	78%	82%	78%	85%	78%	84%	80%	79%	84%
	Password Reset	88%	92%	88%	92%	88%	88%	90%	92%	89%	92%
	Password Rotation	45%	38%	55%	45%	58%	44%	58%	46%	46%	38%
Limit Unwanted Access	Instructions for Account Deletion	79%	70%	87%	80%	87%	78%	87%	78%	80%	71%
	Remove Third Party Access	55%	48%	58%	51%	60%	50%	59%	50%	57%	47%
	Review Active Session	42%	38%	45%	43%	48%	43%	48%	42%	43%	40%
	Sign Out Everywhere (Specific Function)	28%	19%	28%	29%	27%	26%	27%	28%	29%	26%
	Sign Out of Unknown Sessions	28%	35%	35%	29%	36%	31%	36%	29%	31%	43%
Service Restoration	Customer Service Process	46%	50%	48%	44%	48%	45%	47%	45%	46%	60%
	Fix Logs of Past Viewing/Activity/Content History	18%	18%	20%	19%	20%	19%	19%	18%	21%	22%
	Review and/or Remove Activities/Content	26%	27%	28%	25%	28%	22%	27%	23%	28%	34%
	Verify Settings	64%	65%	66%	59%	69%	57%	68%	57%	60%	71%
	Verify User Information	60%	58%	63%	61%	66%	57%	65%	60%	59%	74%
Prevention	Advice About Secure Email	58%	62%	58%	60%	61%	58%	61%	58%	57%	56%
	Always Log Out on Shared Devices	27%	38%	33%	29%	33%	31%	33%	30%	30%	44%
	Check/Modify Related Accounts	25%	17%	25%	24%	25%	23%	25%	24%	22%	26%
	Enable 2FA	63%	65%	73%	65%	76%	63%	75%	67%	67%	62%
	Keep Software Up To Date	36%	32%	38%	36%	41%	35%	41%	36%	34%	32%
	Password Advice: Strong, Unique, Change	75%	56%	76%	79%	79%	73%	78%	74%	75%	47%
	Regular Security Checkups/Advice	5%	5%	8%	5%	8%	5%	8%	6%	4%	10%
	Remove Access to Third-Party Apps	34%	22%	35%	33%	35%	32%	34%	31%	35%	19%
	Sign Out of Devices	30%	24%	33%	29%	32%	31%	32%	28%	30%	36%

Solomon Islands, and Vanuatu. Hence, the few websites that give this form of advice, such as Facebook, Instagram, and LinkedIn, stand out more. Finally, we could not confirm the significance of these differences ($p = 0.115$).

We observed significant differences for *Billing/Finance Issues* where websites inform their users, e.g., about irregular charges. Percentages range from 64% for websites popular in the best-ranked countries in Europe to 32% for websites in the lowest-ranked countries in Oceania. The difference between these two groups is significant ($p < 0.05$), as is the difference between the best-ranked countries in America (63%) and Asia (63%) compared to the lowest-ranked countries in Africa (43%) and Oceania (32%). While this difference is problematic in itself, the fact that it is reflected between high-income and low-income countries further adds to the seriousness of the problem. We will further discuss this issue, which we observed throughout all 5 phases in Section V.

Phase 2: Account Recovery

The average presence of advice for the *Account Recovery* phase is shown in Figure 2. Overall, the percentages are the highest across all 5 steps, ranging from 69% for the worst-ranked countries in Africa to 77% for the best-ranked countries in Asia and Europe. In addition, popular websites in the best-ranked countries score higher, or at least identical in the case of Oceania, compared to the worst-ranked countries.

A more in-depth analysis based on the results depicted in Table II shows that *Customer Service Process* and *Password Reset* account for the overall high presence of advice. Both range from ∼80% to ∼90%, showing that most websites instruct their users to change their passwords and contact them in case of difficulties. In contrast, many services do not check if users try to use their potentially breached password again, nullifying any security increase. Numbers range from 38% for websites popular in the worst-ranked countries in Africa and Oceania to 58% for the best-ranked countries in Asia and Europe. Generally, this check is less prevalent across the worst-ranked countries than their best-ranked counterparts on each continent. The initial χ^2 test confirmed this observation ($p < 0.05$), yet we could not observe any actual significance for the pairwise comparisons.

Phase 3: Limit Unwanted Access

The third phase of account remediation intends to limit unwanted access. Here the average presence of advice depicted in Figure 3 ranks from 42% for the most popular website in

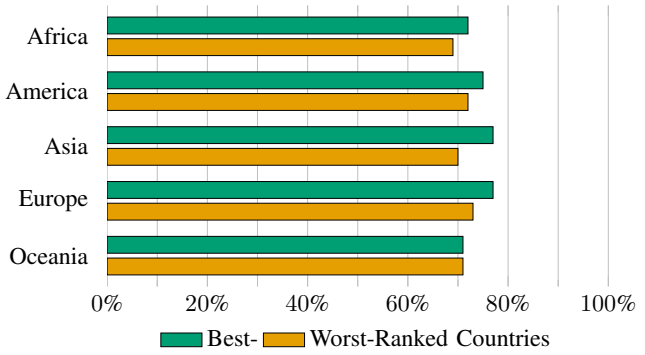

Fig. 2. Average presence of advice for *Phase 2: Account Recovery* in each of the 5 analyzed continents.

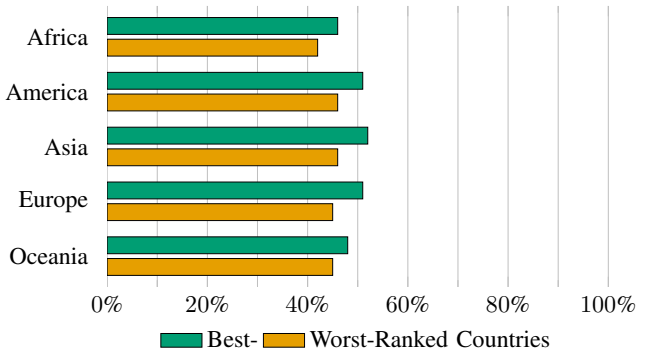

Fig. 3. Average presence of advice for *Phase 3: Limit Unwanted Access* in each of the 5 analyzed continents.

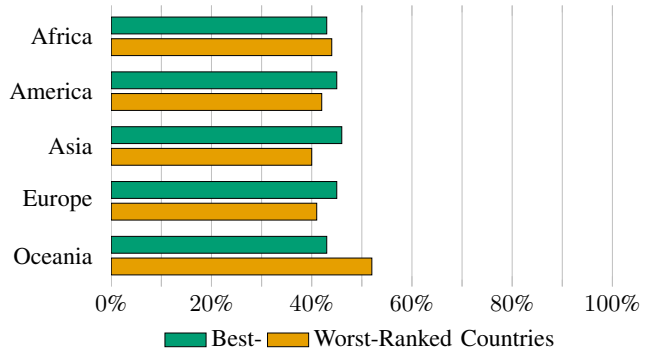

Fig. 4. Average presence of advice for *Phase 4: Service Restoration* in each of the 5 analyzed continents.

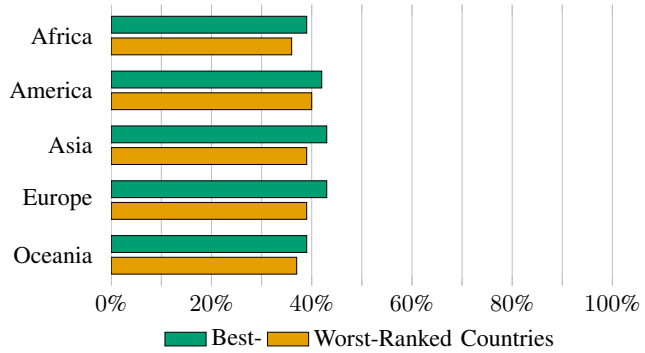

Fig. 5. Average presence of advice for *Phase 5: Prevention* in each of the 5 analyzed continents.

Equatorial Guinea, Eritrea, and Burundi, i.e., the worst-ranked countries in Africa, to 52% for websites popular in the best-ranked countries in Asia. Nevertheless, advice is more present across popular websites in better-ranked countries, up to a difference of 6% between the two groups of countries in Asia (52% vs. 46%) and Europe (51% vs. 45%).

Regarding the 5 codes for this phase, *Instructions for Account Deletion* is the most popular, ranging from 70% to 87%. For this code, the χ^2 test also revealed some significance ($p < 0.01$), however, the subsequent pairwise tests did not confirm this. Advice from this phase which is less present on websites is the instruction to sign out everywhere to ensure no malicious session stays active. In the worst-ranked countries in Africa, only 19% of the website provide this advice; for better-ranked countries, this goes up to 29%. We observed a similar presence for advice telling users to log out from unknown sessions, which is a less invasive way of dealing with the problem. However, it makes users responsible for the complex task of telling malicious and benign sessions apart.

Phase 4: Service Restoration

Phase four *Service Restoration* provides users with instructions on how to restore the initial status of their account. As seen in Figure 4, advice in this phase is given by 40% to 46% of the websites with one exception: the worst-ranked countries in Oceania, the Marshall Islands, Solomon Islands, and Vanuatu. This stark contrast of 52%, especially in comparison to the previous analysis, can be traced back to a comparatively high presence of advice for four of the 5 types of advice in this phase. However, we could not observe any significance for these differences, which is why the sole presence of this outlier does not change the overall picture.

Phase 5: Prevention

The final phase, which intends to prevent further malicious activity, consists of nine different types of advice. In general, guidance in this phase is the least prominent ranging from 37% to 43%, as depicted in Figure 5. However, this is primarily due to one type of advice where services regularly inform users to make security checks ranging from only 4% to 10%. Again we observe the highest presence of this advice for popular websites in the Marshall Islands, Solomon Islands, and Vanuatu, the worst-ranked countries in Oceania. Nevertheless, we could not observe any significant differences here as it was already the case for the *Service Restoration* phase.

In contrast, helping users create a secure password is the most popular advice. At the same time, it also has the most substantial differences being present in 47% of the websites popular in the worst-ranked countries in Oceania, whereas 79% of those in the best-ranked countries in Asia and the worst-ranked in America provide this information. The χ^2 test also confirmed this: advice for a secure password is significantly less present among popular websites in the worst-ranked countries in Africa and Oceania compared to both the worst- and the best-ranked countries in America, Asia, and Europe.

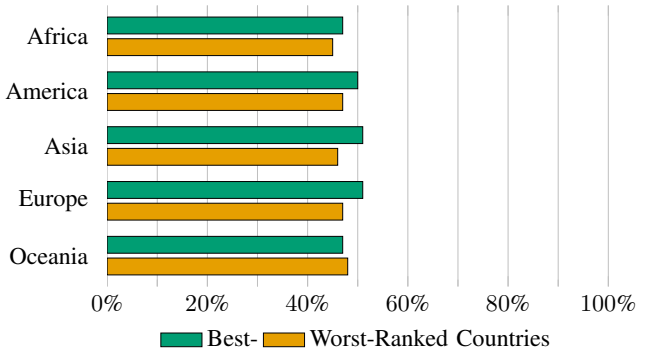

Fig. 6. Average presence of advice across all 5 phases in each of the 5 analyzed continents.

Overall

Now that all 5 phases have been analyzed separately, we also want to look at general trends. For this, Figure 6 presents the average across all 5 phases, i.e., all 31 codes. Here, the worst-ranked countries in Africa list the lowest with only 45% while the best-ranked countries in Asia and Europe have the highest presence of advice with 51%. When comparing the two groups within a continent, we see that the better-ranked countries usually also have a higher presence of advice, with the difference ranging from 2% in Africa (47% vs. 45%) to 5% in Asia (51% vs. 46%). Only in Oceania, the 3 lowest ranked countries have a slightly higher presence of advice, 48% compared to 47%.

While the described observations are mostly marginal, there is a general tendency for countries which are part of the Global South to be more affected by the absence of account remediation advice. In our analysis, we also found multiple case where this discrepancy becomes apparent, two of which were even significant: *Billing/Finance Issues* in the first and *Password Advice* in the fifth phase. We will discuss these findings and their implications in the subsequent sections.

V. Discussion

Our research aims to analyze account remediation for the most popular websites in Africa, America, Asia, Europe, and Oceania. In this section, we discuss the general outcome that we found in most websites in terms of the procedures and protocols of account remediation with a special focus on the differences between countries and continents

A. Situation of the Global South

Throughout our analysis, there is one prevailing aspect: the lack of advice on websites popular in the Global South is more distinct than in industrialized nations forming the Global North. For advice on financial or billing issues and on how to create a secure password the difference is even significant when comparing the worst-ranked countries in Africa and Oceania to the other groups. Ultimately, this lack makes it harder for users to recover from a compromise which adds to the already existing inequality between countries. On top of that, solving this problem is also more complex. Countries in the Global South may not have the same level of access to technology and internet connectivity as industrialized nations, which could impact the ability of organizations to adjust their website. Due to the prevalence of security advice in the English language, barriers may also pose a problem.

Increasing the presence of advice requires communicating the necessity for it, especially across continents, to also improve the situation in countries other than, e.g., the U.S., Canada, and those in Europe. Unfortunately, the process of communicating results and leading to a change can be cumbersome. Probably one of the most prominent examples of such a transition is the deprecation of password complexity rules. The British National Cyber Security Centre (NCSC) changed their guideline in 2016 [52], the National Institute of Standards and Technology (NIST) in the USA followed in 2017 [48], but still, only 13% of websites adhered to them in 2022 [41]. Moreover, most other countries do not have federal agencies at all to communicate such changes, which makes conveying the importance of account remediation advice even more difficult.

B. Account Deletion

Nowadays, people have become aware of privacy and security problems, making them sometimes want to delete their accounts on websites they are no longer using. However, we found that websites make deleting accounts difficult. In our analysis, most websites do not provide enough information about the deletion mechanism, and on average, 20% do not provide information at all. Comparing websites that are popular in the best and worst-rated countries, we find that of the latter, 10% contain fewer account deletion notices, regardless of the continent. Likewise, the websites do not clearly mention what data will be deleted, whether it applies to the entire account, only personal data, or the user's activities. At the same time, some websites indicate not to delete any user data. Finally, there is a problem in determining the time of deletion because websites do not mention when the data will be removed from their databases.

C. Service Restoration

Restoration protocols are among the essentials that must be available on websites in case the account has been hacked or deleted. For most websites, we did not find any information or clear steps for how to restore an account in such a case. Usually, it falls back to a "contact us if there are any problems." Furthermore, some websites only depend on sending a code to the email to verify the authentication and do not provide any alternatives, e.g., confirming a prompt on a linked device [23], providing a one-time or backup code [65], or proving knowledge about the account such as the creation date or last login location [14]. This makes it impossible to restore the account if the email account is unavailable.

VI. Implications and Recommendations

Account remediation is not only a protocol that websites should follow; it is a complex way that brings in the socio-technical components to ensure data protection and prevent further data leakage for an account compromise. Additionally, the proper account remediation process enables users to protect their accounts as a preventive measure through secure behavior such as prevention of password rotation [55], [66]. Our transcontinental analysis for the 158 websites measures

the account remediation for different aspects like changing passwords, reviewing past activities, enabling 2FA, and others. Such a large-scale study in this area is not done per our background research. With the study, we aim to add valuable feedback for evaluating the implementation of the account remediation steps, measuring the security of the websites across different countries, and assessing how websites follow the expert advice in various countries. Based on our evaluation, we provide several recommendations, which we outline below.

The results we obtained confirm that most websites provide insufficient account remediation advice even across the globe and especially in the Global South. In the long term, this highlights the need for more tailored solutions, information campaigns, and more focused research. To address the described issues, we suggest to provide an easy-to-follow checklist for web developers to assure that they provide all account remediation steps. Similarly, a checklist for users could be an alternative to missing or an addition to incomplete advice on websites. We discuss some of these recommendation in the following subsections:

A. Customer Support

Most websites do not provide proper customer support, and even if they do, they are primarily form-based without an immediate response. Yet, it is crucial to provide customer support with immediate responses, not only to keep users satisfied but also to quickly respond to security-related and thus presumably also time-critical issues, especially when users assign a high value to the account [74]. If websites do not provide customer support, this is even more concerning because locked-out users cannot report an account compromise, take necessary steps to secure their account, or do a simple task such as changing the password.

Hence, we encourage national and international policy-makers to mandate account remediation procedures for all websites that maintain user accounts. This could be similar to breach notification obligations like the data breach notification laws in the US [51] or GDPR in the EU [17] which intend to give users the right to be made aware of data breaches they are affected by. However, it is essential to note that this requires substantial focus on improving the security workforce by the organization owning the website [54]. Therefore, it is crucial to focus on this workforce and provide proper customer support for the users to contribute to the account management activities.

B. Compromise Discovery Protocol

We noticed room for improvement in compromise discovery and mitigation protocols, including flexibility of changing email and passwords or up-to-date password requirements. The central problem of the attacks is discovering the compromise concerning user data. For example, Acker et al. analyzed the top Alexa $100,000$ pages to identify login pages and measure their security. As a result, they found that possibilities for password leaks to third parties and password eavesdropping on the network without the knowledge of the website owners [73]. This is concerning as without such knowledge or a discovery mechanism in place, it is difficult for the users to identify a compromise and act accordingly [12], [29].

Therefore, websites should inform users about unusual activity although this comes with its own challenges. Too many false positives, i.e., sending notifications for legit activity, can give misleading warnings to the users and create an illusion for the users' mental models to ignore the actual warning signs. Thus, websites need to be precise about what constitutes an "unusual activity" by giving concrete examples such as changed passwords or emails [46], [61]. A second aspect of this is an interface to review account activities, such as logins and actions that alter an account's status (purchases, password or preference changes, settings, user information) [19] Through this interface, a user should be able to terminate any or all active sessions. Our results show that only very few websites currently provide this functionality: 33% allow to sign out of certain sessions, 27% allow to sign out everywhere, and again numbers vary across countries and continents. Along with the idea of revealing account activity, there should also be an interface that allows users to delete undesired items and reverse changes made to their settings as also suggested by prior work [4], [30].

C. Robust Security Requirements

As part of this study, we checked password requirements on websites and found that on average 53% of them do not check for a proper password rotation [55], [66]. This check is possible without any security infringement, as knowledge of the old password also needs to be double-checked at that point. Otherwise, someone could change the password who does not know the old one but has access to the account, e.g., via a stolen session cookie or an existing session on a shared device.

Furthermore, 29% do not advise users about strong passwords and even more provide outdated requirements which is in line with findings by Lee et al. [41]. For example, we have noted that banking websites such as JPMorgan Chase prevent password rotation. However, the same is not followed by the most common websites. Therefore, the usage of up-to-date password requirements as provided by the NIST SP800-63B [24] or the NCSC [52] needs to promoted even more. Strong passwords can be helpful to secure the websites from many attacks like phishing, key logging, and brute-force attack [20]. Hence, passwords or, in general, authentication requirements should align with the expert advice like usage of 2FA [58], [79]. Still, even those websites with 2FA enabled mostly activated it once during account creation and often did not have any mechanism in place to protect user data after a change of the device.

D. Account Deletion, Recovery, and Restoration

A proper data deletion protocol is necessary to review which data was removed from user accounts [60]. We found that many websites do not have enough information on what data will be removed when the users delete their accounts. So, we recommend that websites have information about deleting users' data, how users can delete their accounts, and how long it would take to delete the entire accounts from the database.

Regarding recovering and restoring the service for any account compromise, we found that email is the most used communication channel. Note that phone calls are susceptible to phishing attacks [2]. Thus, email can also be considered

to be the more secure communication channel [32] unless dealing with financial institutions or when critical information is exchanged where a high level of security is necessary, e.g., in-person or physically mailing to the user address. In addition, we considered security verification checks that can be a second step to confirm the user's identity to restore an account. Again, we found that email is the most used channel for this type of check. Hence, we also want to stress the importance of assuring the security of this connection by using state-of-the-art configurations including DNSSEC, SPF, DKIM, DMARC, DANE, and STARTTLS [69].

E. Proper Documentation and Better Guidance

In general, we noted a lack of information and documentation provided by the websites which became even more evident for the Global South. Still, even when the instructions for account remediation were available, it was not easy to obtain certain information, e.g., about how to delete the account or reset the password. Additionally, we discovered significant heterogeneity in the preventative documentation and guidance offered by these websites, indicating that many offer insufficient prevention guidance, which can be harmful to the users. Prior research has shown that such guidance and proper documentation are invaluable for user data protection [62], [63], however, several websites disregard that. In fact, various websites do not provide some of the features of their web application counterparts. Though this was out of the scope of our current research study, we plan to explore this disparity as a future extension of this work.

VII. Limitations and Future Work

Account remediation is an essential aspect of assessing the protocols used in the websites to protect the users' data and accounts. However, despite our best efforts, we needed help analyzing the websites for the following reasons. First, we analyzed websites from different continents. Consequently, the first language for many of these websites is not English, and some are not offered in English at all. Therefore, to analyze non-English pages, we used translation services, e.g., the built-in feature in Google Chrome. Still, not all of these translations were perfect, which may have influenced the analysis. Secondly, some websites do not allow account sign-up, such as online news, sports news, online platforms, games, and streaming websites. As a result, we limited ourselves to websites that allow account sign-up.

Moreover, we found that some websites do not allow us to access them from our location. We tried to circumvent any location-based blocks by using a VPN, still, some websites remained unavailable. Finally, to facilitate replication we did not analyze websites which required a national ID, credit card number, phone number, or company name to register. As such websites occurred for each country, we also expect any potential differences due to this constraint to be negligible.

Based on our analysis of the top 50 websites for each country, we already observed significant differences for certain account for remediation steps when comparing different countries and continents. However, we assume the differences to be even more noticeable when including more and less popular websites. To confirm this assumption, a broader analysis covering more countries and websites is needed. Finally, we plan to do a time-based analysis to provide a detailed evaluation of the account remediation protocols. Through such an analysis, we can provide both the perspective of account remediation protocols offered by the website and how seamlessly it is implemented in everyday usage.

VIII. Conclusion

Account Remediation is the protective mechanism that ensures the account access is restricted and the data leakage is prevented by following the protocols defined. Thus, the account remediation process is technically complex, requiring several procedures to ensure legitimate access is not restricted and illegitimate access and data leakage are prevented. Thus, in most cases, this procedure is left to the end-user knowledge and proactive behavior. However, many websites either do not create the technical feasibility to conduct a proper account remediation protocol or provide adequate documentation for users to be aware of the procedure they need to do to secure their accounts.

Therefore, our goal for this study was to conduct an intercontinental analysis of the account remediation protocols of the top 50 websites from 6 countries on 5 continents: Africa, America, Asia, Europe, and Oceania. Of the websites, 3 of the 6 were the best performing, and the remaining 3 were the worst countries based on the cybersecurity index from GCI. We analyzed the websites based on the 5 phases of account remediation: compromise discovery, account recovery, limit access, service restoration, and prevention. As part of this, we note features such as the flexibility of changing passwords, identifying unwanted activities, deleting accounts, and enabling 2FA. Our analysis showed that websites across the globe do not follow expert advice as part of the account remediation schema. For example, initially identifying a compromise is difficult, websites require their users to be able to log in to take countermeasures, and password advice needs to be updated or included. When comparing countries and continents, this need for adequate information is even more prevalent in the Global South which shows a technological disparity when compared with the Global North. This highlights the need for easy-to-follow advice that reaches users and website providers alike, which we intend to prepare, test and provide as part of future work.

Acknowledgment

We would like to thank the Inclusive Security and Privacy-focused Innovative Research in Information Technology (InSPIRIT) Laboratory at the University of Denver. We would also like to thank Hebah Alafari, Ahmed Khormi, Shatha Surayyi, and Alyssa Zinn for their initial contribution in this research. Any opinions, findings, conclusions, or recommendations expressed in this material are solely those of the authors. They do not necessarily reflect the views of any organization with which the authors may be affiliated.

REFERENCES

[1] AV-Comparatives, "Independent Tests of Anti-Virus Software," Mar. 2019, https://www.av-comparatives.org/wp-content/uploads/2019/03/avc_android_201903_en.pdf, as of January 27, 2023.

[2] S. B. Barnes, "A Comprehensive Study of Phishing Attacks," *First Monday*, vol. 11, no. 9, Sep. 2006.

[3] S. Bhagavatula, L. Bauer, and A. Kapadia, "(How) Do People Change Their Passwords After a Breach?" in *Workshop on Technology and Consumer Protection*, ser. ConPro '20. Virtual Conference: IEEE, May 2020.

[4] J. Bonneau, E. Bursztein, I. Caron, R. Jackson, and M. Williamson, "Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google," in *The World Wide Web Conference*, ser. WWW '15. Florence, Italy: ACM, May 2015, pp. 141–150.

[5] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," in *IEEE Symposium on Security and Privacy*, ser. SP '12. San Jose, California, USA: IEEE, May 2012, pp. 553–567.

[6] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, "Fourth-Factor Authentication: Somebody You Know," in *ACM Conference on Computer and Communications Security*, ser. CCS '06. Alexandria, Virginia, USA: ACM, Oct. 2006, pp. 168–178.

[7] C. Bravo-Lillo, L. F. Cranor, J. S. Downs, and S. Komanduri, "Bridging the Gap in Computer Security Warnings: A Mental Model Approach," *IEEE Security & Privacy*, vol. 9, no. 2, pp. 18–26, Mar. 2011.

[8] R. Bruggemann, P. Koppatz, M. Scholl, and R. Schuktomow, "Global Cybersecurity Index (GCI) And the Role of Its 5 Pillars," *Social Indicators Research*, vol. 159, no. 1, pp. 125–143, Jan. 2022.

[9] E. Bursztein, B. Benko, D. Margolis, T. Pietraszek, A. Archer, A. Aquino, A. Pitsillidis, and S. Savage, "Handcrafted Fraud and Extortion: Manual Account Hijacking in the Wild," in *Internet Measurement Conference*, ser. IMC '14. Vancouver, British Columbia, Canada: ACM, Nov. 2014, pp. 347–358.

[10] S. S. Costigan, "Sovereign or Global Internet? Russia and China Press for Cybercrime Treaty," *Connections: The Quarterly Journal*, vol. 20, no. 2, pp. 9–13, Mar. 2021.

[11] N. Dados and R. Connell, "The Global South," *Contexts*, vol. 11, no. 1, pp. 12–13, Feb. 2012.

[12] Y. Diogenes and E. Ozkaya, *Cybersecurity – Attack and Defense Strategies: Counter Modern Threats and Employ State-Of-The-Art Tools and Techniques to Protect Your Organization Against Cybercriminals*, 2nd ed. Birmingham, United Kingdom: Packt Publishing, 2019.

[13] Dirlik, Arif, "Global South: Predicament and Promise," *The Global South*, vol. 1, no. 1, pp. 12–23, May 2007.

[14] P. Doerfler, K. Thomas, M. Marincenko, J. Ranieri, Y. Jiang, A. Moscicki, and D. McCoy, "Evaluating Login Challenges as a Defense Against Account Takeover," in *The World Wide Web Conference*, ser. WWW '19. San Francisco, California, USA: ACM, May 2019, pp. 372–382.

[15] M. Egele, G. Stringhini, C. Kruegel, and G. Vigna, "COMPA: Detecting Compromised Accounts on Social Networks," in *Symposium on Network and Distributed System Security*, ser. NDSS '13. San Diego, California, USA: ISOC, Feb. 2013.

[16] ——, "Towards Detecting Compromised Accounts on Social Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 4, pp. 447–460, 2015.

[17] T. European Parliament and the Council of the European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," Official Journal of the European Union, L 119/1, Apr. 2016.

[18] M. Fagan and M. M. H. Khan, "To Follow or Not to Follow: A Study of User Motivations Around Cybersecurity Advice," *IEEE Internet Computing*, vol. 22, no. 5, pp. 25–34, Sep. 2018.

[19] A. N. Fernandes, P. Markert, and S. Das, "Where You're Logged In: Analyzing the Usability of Device Activity Pages (Work-in-Progress)," in *Annual Computer Security Applications Conference*, ser. ACSAC '22, Austin, Texas, USA, Dec. 2022.

[20] D. Florêncio, C. Herley, and B. Coskun, "Do Strong Web Passwords Accomplish Anything?" in *Workshop on Hot Topics in Security*, ser. HotSec '07. Boston, Massachusetts, USA: USENIX, Aug. 2007, pp. 1–6.

[21] K. R. Fulton, R. Gelles, A. McKay, Y. Abdi, R. Roberts, and M. L. Mazurek, "The Effect of Entertainment Media on Mental Models Of Computer Security," in *Symposium on Usable Privacy and Security*, ser. SOUPS '19. Santa Clara, California, USA: USENIX, Aug. 2019, pp. 79–95.

[22] S. L. Garfinkel, "Email-Based Identification and Authentication: An Alternative to PKI?" *IEEE Security & Privacy*, vol. 1, no. 6, pp. 20–26, Nov. 2003.

[23] Google, "Strengthening 2-Step Verification by Showing Phone Prompts to More Users," Jun. 2020, https://workspaceupdates.googleblog.com/2020/06/stronger-google-account-verification-phone-prompts.html, as of January 27, 2023.

[24] P. A. Grassi, J. L. Fenton, and W. E. Burr, "Digital Identity Guidelines – Authentication and Lifecycle Management: NIST Special Publication 800-63B," Jun. 2017.

[25] H. Halawa, M. Ripeanu, K. Beznosov, B. Coskun, and M. Liu, "An Early Warning System for Suspicious Accounts," in *ACM Workshop on Artificial Intelligence and Security*, ser. AISec '17. Dallas, Texas, USA: ACM, Nov. 2017, pp. 51–52.

[26] M. Harbach, A. De Luca, and S. Egelman, "The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens," in *ACM Conference on Human Factors in Computing Systems*, ser. CHI '16. San Jose, California, USA: ACM, May 2016, pp. 4806–4817.

[27] M. Harbach, A. De Luca, N. Malkin, and S. Egelman, "Keep on Lockin' in the Free World: A Multi-National Comparison of Smartphone Locking," in *ACM Conference on Human Factors in Computing Systems*, ser. CHI '16. San Jose, California, USA: ACM, May 2016, pp. 4823–4827.

[28] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception," in *Symposium on Usable Privacy and Security*, ser. SOUPS '14. Menlo Park, California, USA: USENIX, Jul. 2014, pp. 213–230.

[29] B. Hosack, "Businesses Still Unaware of Risks of Account Data Compromise," *Computer Fraud & Security*, vol. 2011, no. 1, pp. 17–19, Jan. 2011.

[30] J. H. Huh, H. Kim, S. S. Rayala, R. B. Bobba, and K. Beznosov, "I'm Too Busy to Reset My LinkedIn Password: On the Effectiveness of Password Reset Emails," in *ACM Conference on Human Factors in Computing Systems*, ser. CHI '17. Denver, Colorado, USA: ACM, May 2017, pp. 387–391.

[31] R. A. Igawa, A. M. G. de Almeida, B. B. Zarpelao, and S. Barbon, "Recognition of Compromised Accounts on Twitter," in *Brazilian Symposium on Information Systems: Information Systems: A Computer Socio-Technical Perspective*, ser. SBSI '15. Goiânia, Goiás, Brazil: ACM, May 2015, pp. 9–14.

[32] T. Innocenti, S. A. Mirheidari, A. Kharraz, B. Crispo, and E. Kirda, "You've Got (A Reset) Mail: A Security Analysis of Email-Based Password Reset Procedures," in *Conference on Detection of Intrusions and Malware & Vulnerability Assessment*, ser. DIMVA '21. Virtual Conference: Springer, Jul. 2021, pp. 327–346.

[33] International Telecommunication Union, "Global Cybersecurity Index 2020," Jun. 2021, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E, as of January 27, 2023.

[34] I. Ion, R. W. Reeder, and S. Consolvo, ""...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices," in *Symposium on Usable Privacy and Security*, ser. SOUPS '15. Ottawa, Ontario, Canada: USENIX, Jul. 2015, pp. 327–346.

[35] R. C. Jammalamadaka, T. W. Van Der Horst, S. Mehrotra, K. E. Seamons, and N. Venkasubramanian, "Delegate: A Proxy Based Architecture for Secure Website Access From an Untrusted Machine," in *Annual Computer Security Applications Conference*, ser. ACSAC '06. Miami Beach, Florida, USA: IEEE, Dec. 2006, pp. 57–66.

[36] A. Jøsang, B. AlFayyadh, T. Grandison, M. AlZomai, and J. McNamara, "Security Usability Principles for Vulnerability Analysis and Risk Assessment," in *Annual Computer Security Applications Conference*,

ser. ACSAC '07. Miami Beach, Florida, USA: IEEE, Dec. 2007, pp. 269–287.

[37] M. Just and D. Aspinall, "Personal Choice and Challenge Questions: A Security and Usability Assessment," in *Symposium on Usable Privacy and Security*, ser. SOUPS '09. Mountain View, California, USA: ACM, Jul. 2009, pp. 8:1–8:11.

[38] B. E. Kolko and C. Putnam, "Computer Games in the Developing World: The Value of Non-instrumental Engagement With ICTs, or Taking Play Seriously," in *International Conference on Information and Communication Technologies and Development*, ser. ICTD '09. Doha, Qatar: IEEE, Apr. 2009, pp. 46–55.

[39] L. Lassak, A. Hildebrandt, M. Golla, and B. Ur, ""It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn," in *USENIX Security Symposium*, ser. SSYM '21. Virtual Conference: USENIX, Aug. 2021, pp. 91–108.

[40] V. Le Pochat, T. Van Goethem, S. Tajalizadehkhoob, M. Korczyński, and W. Joosen, "Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation," in *Symposium on Network and Distributed System Security*, ser. NDSS '19. San Diego, California, USA: ISOC, Feb. 2019.

[41] K. Lee, S. Sjöberg, and A. Narayanan, "Password Policies of Most Top Websites Fail to Follow Best Practices," in *Symposium on Usable Privacy and Security*, ser. SOUPS '22. Boston, Massachusetts, USA: USENIX, Aug. 2022, pp. 561–580.

[42] S. Lee and D. K. Lee, "What Is the Proper Way to Apply the Multiple Comparison Test?" *Korean Journal of Anesthesiology*, vol. 71, no. 5, pp. 353–360, Oct. 2018.

[43] L. Li, B. Pal, J. Ali, N. Sullivan, R. Chatterjee, and T. Ristenpart, "Protocols for Checking Compromised Credentials," in *ACM Conference on Computer and Communications Security*, ser. CCS '19. London, United Kingdom: ACM, Nov. 2019, pp. 1387–1403.

[44] Y. Li, H. Wang, and K. Sun, "Email as a Master Key: Analyzing Account Recovery in the Wild," in *IEEE Conference on Computer Communications*, ser. INFOCOM '18. Honolulu, Hawaii, USA: IEEE, Apr. 2018, pp. 1646–165.

[45] P. Markert, M. Golla, E. Stobert, and M. Dürmuth, "Work in Progress: A Comparative Long-Term Study of Fallback Authentication," in *Workshop on Usable Security*, ser. USEC '19. San Diego, California, USA: ISOC, Feb. 2019.

[46] P. Markert, L. Lassak, M. Golla, and M. Dürmuth, ""It Knew It Was Me": Understanding Users' Interaction with Login Notifications," *CoRR*, vol. abs/2212.07316, pp. 1–24, Dec. 2022.

[47] J. L. McClelland, *Failures to Learn and Their Remediation: A Hebbian Account*, 1st ed. London, United Kingdom: Psychology Press, 2001, ch. 4, pp. 97–121.

[48] R. McMillan, "The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1nd!" Aug. 2017, https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118, as of January 27, 2023.

[49] C. Mihalcik, "Antivirus Firm Avast Is Reportedly Selling Users' Web Browsing Data," Jan. 2020, https://cnet.co/3NztnF4, as of January 27, 2023.

[50] J. T. Murphy, "Economic Geographies of the Global South: Missed Opportunities and Promising Intersections With Development Studies," *Geography Compass*, vol. 2, no. 3, pp. 851–873, May 2008.

[51] National Conference of State Legislatures, "Security Breach Notification Laws," Jan. 2022, https://www.ncsl.org/technology-and-communication/security-breach-notification-laws, as of January 27, 2023.

[52] National Cyber Security Centre, "Password Guidance: Simplifying Your Approach," Jan. 2016, https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach, as of January 27, 2023.

[53] L. Neil, E. Bouma-Sims, E. Lafontaine, Y. Acar, and B. Reaves, "Investigating Web Service Account Remediation Advice," in *Symposium on Usable Privacy and Security*, ser. SOUPS '21. Virtual Conference: USENIX, Aug. 2021, pp. 359–376.

[54] W. Newhouse, S. Keith, B. Scribner, and G. Witte, "Workforce Framework for Cybersecurity (NICE Framework): NIST Special Publication 800-181," Nov. 2020.

[55] S. Parkin, S. Driss, K. Krol, and M. A. Sasse, "Assessing the User Experience of Password Reset Policies in a University," in *International Conference on Passwords*, ser. PASSWORDS '15. Cambridge, United Kingdom: Springer, Dec. 2015, pp. 21–38.

[56] J. L. Pinchot and K. L. Paullet, "What's in Your Profile? Mapping Facebook Profile Data to Personal Security Questions," *Issues in Information Systems*, vol. 13, no. 1, pp. 284–293, Mar. 2012.

[57] A. Rabkin, "Personal Knowledge Questions for Fallback Authentication: Security Questions in the Era of Facebook," in *Symposium on Usable Privacy and Security*, ser. SOUPS '08. Pittsburgh, Pennsylvania, USA: ACM, Jul. 2008, pp. 13–23.

[58] E. Rader and R. Wash, "Identifying Patterns in Informal Sources of Security Information," *Journal of Cybersecurity*, vol. 1, no. 1, pp. 121–144, 2015.

[59] E. Rader, R. Wash, and B. Brooks, "Stories as Informal Lessons About Security," in *Symposium on Usable Privacy and Security*, ser. SOUPS '12. Washington, District of Columbia, USA: ACM, Jul. 2012, pp. 1–12.

[60] J. Reardon, D. Basin, and S. Capkun, "SoK: Secure Data Deletion," in *IEEE Symposium on Security and Privacy*, ser. SP '13. San Francisco, California, USA: IEEE, May 2013, pp. 301–315.

[61] E. M. Redmiles, ""Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response," in *IEEE Symposium on Security and Privacy*, ser. SP '19. San Francisco, California, USA: IEEE, May 2019, pp. 920–934.

[62] E. M. Redmiles, A. R. Malone, and M. L. Mazurek, "I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security," in *IEEE Symposium on Security and Privacy*, ser. SP '16. San Jose, California, USA: IEEE, May 2016, pp. 272–288.

[63] E. M. Redmiles, N. Warford, A. Jayanti, A. Koneru, S. Kross, M. Morales, R. Stevens, and M. L. Mazurek, "A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web," in *USENIX Security Symposium*, ser. SSYM '20. Virtual Conference: USENIX, Aug. 2020, pp. 89–108.

[64] R. W. Reeder, I. Ion, and S. Consolvo, "152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users," *IEEE Security & Privacy*, vol. 15, no. 5, pp. 55–64, Oct. 2017.

[65] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, "A Usability Study of Five Two-Factor Authentication Methods," in *Symposium on Usable Privacy and Security*, ser. SOUPS '19. Santa Clara, California, USA: USENIX, Aug. 2019, pp. 357–370.

[66] S. Schechter, A. J. B. Brush, and S. Egelman, "It's No Secret. Measuring the Security and Reliability of Authentication via "Secret" Questions," in *IEEE Symposium on Security and Privacy*, ser. SP '09. Oakland, California, USA: IEEE, May 2009, pp. 375–390.

[67] S. Schechter, S. Egelman, and R. W. Reeder, "It's Not What You Know, But Who You Know: A Social Approach to Last-Resort Authentication," in *ACM Conference on Human Factors in Computing Systems*, ser. CHI '09. Boston, Massachusetts, USA: ACM, Apr. 2009, pp. 1983–1992.

[68] R. Shay, I. Ion, R. W. Reeder, and S. Consolvo, ""My Religious Aunt Asked Why I Was Trying to Sell Her Viagra": Experiences with Account Hijacking," in *ACM Conference on Human Factors in Computing Systems*, ser. CHI '14. Toronto, Ontario, Canada: ACM, Apr. 2014, pp. 2657–2666.

[69] K. Shen, C. Wang, M. Guo, X. Zheng, C. Lu, B. Liu, Y. Zhao, S. Hao, H. Duan, Q. Pan, and M. Yang, "Weak Links in Authentication Chains: A Large-scale Analysis of Email Sender Spoofing Attacks," in *USENIX Security Symposium*, ser. SSYM '21. Virtual Conference: USENIX, Aug. 2021, pp. 3201–3217.

[70] M. Shirvanian and S. Agrawal, "2D-2FA: A New Dimension in Two-Factor Authentication," in *Annual Computer Security Applications Conference*, ser. ACSAC '21. Virtual Conference: ACM, Dec. 2021, pp. 482–496.

[71] J. Temperton, "AVG Can Sell Your Browsing and Search History to Advertisers," Sep. 2015, https://www.wired.co.uk/article/avg-privacy-policy-browser-search-data, as of January 27, 2023.

[72] A. Thakur, A. Sangal, and H. Bindra, "Quantitative Measurement and Comparison of Effects of Various Search Engine Optimization Parameters on Alexa Traffic Rank," *International Journal of Computer Applications*, vol. 26, no. 5, pp. 15–23, Jul. 2011.

[73] S. Van Acker, D. Hausknecht, and A. Sabelfeld, "Measuring Login Webpage Security," in *Symposium in Applied Computing*, ser. SAC '17. Marrakech, Morocco: ACM, Apr. 2017, pp. 1753–1760.

[74] D. Wilson, T. Bridge, P. Deasy, and A. Whelan, "That's the Ticket! Redesigning an Online Customer Support System in an Internet Company," in *Americas Conference on Information Systems*, ser. AMCIS '01. Boston, Massachusetts, USA: AIS Electronic Library, Dec. 2001, pp. 913–916.

[75] P. Wohlmacher and P. Pharow, "Applications in Health Care Using Public-Key Certificates and Attribute Certificates," in *Annual Computer Security Applications Conference*, ser. ACSAC '00. New Orleans, Louisiana, USA: ACM, Dec. 2000, pp. 128–137.

[76] W. Wu, R. Kang, and Z. Li, "Risk Assessment Method for Cybersecurity of Cyber-Physical Systems Based on Inter-Dependency of Vulnerabilities," in *IEEE International Conference on Industrial Engineering and Engineering Management*, ser. IEEM '15. Virtual Conference: IEEE, Dec. 2015, pp. 1618–1622.

[77] E. Zangerle and G. Specht, ""Sorry, I Was Hacked": A Classification of Compromised Twitter Accounts," in *ACM Symposium on Applied Computing*, ser. SAC '14. Gyeongju, Republic of Korea: ACM, Mar. 2014, pp. 587–593.

[78] V. Zimmermann, K. Marky, and K. Renaud, "Hybrid Password Meters for More Secure Passwords – A Comprehensive Study of Password Meters Including Nudges and Password Information," *Behaviour & Information Technology*, pp. 1–44, Mar. 2022.

[79] M. E. Zurko, "User-Centered Security: Stepping up to the Grand Challenge," in *Annual Computer Security Applications Conference*, ser. ACSAC '05. Tucson, Arizona, USA: IEEE, Dec. 2005, pp. 184–202.

APPENDIX

TABLE III. THE NUMBER OF TIMES EACH OF THE 158 WEBSITES APPEARS IN THE TOP 50 OF THE 3 BEST AND WORST RANKING NATIONS, AS DETERMINED BY THE GCI [33] IN EACH OF THE CONTINENTS. WEBSITES WITH THE SAME TOTAL WERE ORDERED ALPHABETICALLY.

		Africa		America		Asia		Europe		Oceania		
No.	**Website**	Best	Worst	Best	Worst	Best	Worst	Best	Worst	Best	Worst	**Total**
1	amazon.com	3	2	3	3	3	3	3	3	3	3	29
2	google.com	2	3	3	3	3	3	3	3	3	3	29
3	youtube.com	2	3	3	3	3	3	3	3	3	3	29
4	facebook.com	2	2	3	3	3	3	3	3	3	3	28
5	imdb.com	3	2	3	3	2	3	3	3	3	3	28
6	pinterest.com	3	2	3	3	3	3	3	3	3	2	28
7	twitter.com	2	2	3	3	3	3	3	3	3	3	28
8	wikipedia.org	2	2	3	3	3	3	3	3	3	3	28
9	linkedin.com	2	2	3	3	3	3	3	3	3	2	27
10	yahoo.com	3	2	3	3	3	3	3	3	3	1	27
11	instagram.com	2	2	3	3	3	3	3	3	3	1	26
12	live.com	3	2	3	3	3	2	3	3	3	1	26
13	microsoftonline.com	3	2	3	3	3	3	3	3	1	2	26
14	reddit.com	3	1	3	3	3	3	3	3	3	1	26
15	whatsapp.com	3	2	3	3	3	3	3	3	3	0	26
16	github.com	3	1	3	3	3	2	3	3	3	1	25
17	microsoft.com	2	2	3	3	3	3	3	3	3	0	25
18	netflix.com	2	2	3	3	3	3	3	3	1	2	25
19	bing.com	3	2	3	3	3	2	3	2	3	0	24
20	zoom.us	3	1	3	3	3	2	3	3	2	1	24
21	adobe.com	3	0	3	3	3	2	3	3	3	0	23
22	nih.gov	3	1	3	3	3	2	3	2	3	0	23
23	nytimes.com	3	1	3	3	3	2	3	2	3	0	23
24	paypal.com	2	1	3	3	3	2	3	3	3	0	23
25	spotify.com	3	0	3	3	3	2	3	3	3	0	23
26	apple.com	2	0	3	3	3	2	3	3	3	0	22
27	office.com	3	0	3	3	3	2	3	2	3	0	22
28	vimeo.com	3	0	3	3	3	1	3	3	3	0	22
29	vk.com	3	1	3	2	3	2	3	2	3	0	22
30	blogspot.com	3	1	3	2	3	2	3	2	2	0	21
31	msn.com	3	1	0	3	3	2	3	3	3	0	21
32	medium.com	3	0	3	3	2	2	2	2	3	0	20
33	tiktok.com	0	2	3	3	3	2	3	3	0	1	20
34	stackoverflow.com	2	1	3	2	2	2	3	3	1	0	19
35	mozilla.org	3	0	3	2	3	1	3	2	1	0	18
36	tumblr.com	3	0	3	1	3	2	3	1	2	0	18
37	soundcloud.com	3	2	0	3	0	2	0	1	3	2	16
38	ebay.com	3	1	0	3	0	2	0	2	3	1	15
39	sohu.com	3	0	3	0	3	0	3	0	2	1	15
40	aliexpress.com	3	2	0	3	0	2	0	3	1	0	14
41	baidu.com	2	0	3	0	3	0	3	1	1	1	14
42	qq.com	1	0	3	0	3	0	3	1	2	1	14
43	taobao.com	1	0	3	0	3	0	3	1	2	1	14
44	yandex.ru	0	0	3	1	3	2	3	2	0	0	14
45	cnn.com	3	0	0	3	0	2	0	2	3	0	13
46	flickr.com	3	0	2	1	3	1	1	2	0	0	13
47	theguardian.com	2	1	0	2	0	3	0	1	3	1	13
48	twitch.tv	3	0	0	3	0	2	0	3	2	0	13
49	weibo.com	1	0	3	0	3	0	3	0	2	1	13
50	dropbox.com	3	0	0	2	0	2	0	2	3	0	12
51	wordpress.org	0	0	3	1	3	1	3	1	0	0	12
52	amazonaws.com	0	0	3	1	3	0	2	0	2	0	11
53	bilibili.com	0	0	3	0	3	0	3	1	0	1	11
54	csdn.net	1	0	3	0	3	0	3	0	0	1	11
55	sina.com.cn	1	0	3	0	2	0	3	0	2	0	11
56	zhihu.com	0	0	3	0	3	0	3	0	0	1	10
57	canva.com	0	1	0	3	0	2	0	3	0	0	9
58	jd.com	0	0	3	0	3	0	3	0	0	0	9
59	etsy.com	1	0	0	2	0	0	0	2	3	0	8
60	europa.eu	2	0	0	1	2	1	1	1	0	0	8
61	forbes.com	2	1	0	2	0	1	0	1	1	0	8
52	quora.com	0	1	0	2	0	2	0	1	0	2	8
63	alibaba.com	0	2	0	0	0	1	0	1	0	3	7
64	bit.ly	0	0	3	0	1	0	2	0	0	0	6
65	healthline.com	0	2	0	0	0	1	0	0	0	3	6
66	icloud.com	0	0	0	2	0	2	0	2	0	0	6
67	wordpress.com	3	0	0	0	0	1	0	0	2	0	6
68	archive.org	1	0	0	0	0	2	0	0	2	0	5
69	imgur.com	1	0	0	0	0	0	0	0	3	0	5
70	mediafire.com	0	2	0	0	0	1	0	0	0	2	5
71	skype.com	2	0	0	1	0	1	0	1	0	0	5
72	weather.com	0	1	0	0	0	1	0	1	0	2	5
73	bbc.com	0	3	0	0	0	0	0	0	0	1	4
74	cloudflare.com	1	0	0	1	0	2	0	0	0	0	4
75	fandom.com	0	0	0	1	0	1	0	2	0	0	4
76	mayoclinic.org	0	1	0	0	0	1	0	0	0	2	4
77	researchgate.net	0	1	0	1	0	1	0	0	0	1	4
78	slideshare.net	0	1	0	0	0	1	0	0	2	0	4
79	sourceforge.net	2	0	0	1	0	0	0	0	1	0	4

TABLE IV. THE NUMBER OF TIMES EACH OF THE 158 WEBSITES APPEARS IN THE TOP 50 OF THE 3 BEST AND WORST RANKING NATIONS, AS DETERMINED BY THE GCI [33] IN EACH OF THE CONTINENTS. WEBSITES WITH THE SAME TOTAL WERE ORDERED ALPHABETICALLY. (CONTINUED)

No.	Website	Africa		America		Asia		Europe		Oceania		Total
		Best	Worst	Best	Worst	Best	Worst	Best	Worst	Best	Worst	
80	accuweather.com	0	1	0	0	0	1	0	0	0	1	3
81	bbc.co.uk	1	0	0	1	0	0	0	0	1	0	3
82	booking.com	0	1	0	1	0	0	0	1	0	0	3
83	gsmarena.com	0	1	0	0	0	1	0	0	0	1	3
84	godaddy.com	2	0	0	0	0	0	0	0	1	0	3
85	ilovepdf.com	0	1	0	0	0	1	0	1	0	0	3
86	macromedia.com	0	0	1	0	1	0	1	0	0	0	3
87	myshopify.com	2	0	0	1	0	0	0	0	0	0	3
88	samsung.com	0	1	0	0	0	1	0	1	0	0	3
89	savefrom.net	0	2	0	0	0	1	0	0	0	0	3
90	sciencedirect.com	0	1	0	2	0	0	0	0	0	0	3
91	telegram.org	0	1	0	0	0	1	0	1	0	0	3
92	washingtonpost.com	1	0	0	0	0	0	0	0	2	0	3
93	webmd.com	0	0	0	0	0	1	0	0	0	2	3
94	academia.edu	0	1	0	0	0	1	0	0	0	0	2
95	bongacams.com	1	0	0	0	0	0	0	0	1	0	2
96	dailymail.co.uk	0	1	0	1	0	0	0	0	0	0	2
97	discord.com	0	0	0	1	0	0	0	1	0	0	2
98	ecer.com	0	1	0	0	0	0	0	0	0	1	2
99	indeed.com	0	1	0	1	0	0	0	0	0	0	2
100	iqbroker.com	0	1	0	0	0	0	0	0	0	1	2
101	issuu.com	0	0	0	0	0	0	0	1	1	0	2
102	livemint.com	0	0	0	0	0	0	0	0	0	1	2
103	marca.com	0	1	0	0	0	0	0	0	0	1	2
104	medicalnewstoday.com	0	1	0	0	0	0	0	0	0	1	2
105	mega.nz	0	1	0	0	0	0	0	1	0	0	2
106	messenger.com	0	0	0	0	0	0	0	0	0	2	2
107	scribd.com	0	1	0	0	0	1	0	0	0	0	2
108	t.me	0	1	0	0	0	0	0	0	0	1	2
109	wetransfer.com	0	1	0	0	0	0	0	1	0	0	2
110	wikihow.com	0	1	0	0	0	1	0	0	0	0	2
111	wix.com	0	0	0	0	0	0	0	0	2	0	2
112	xinhuanet.com	0	0	0	0	0	0	0	0	2	0	2
113	ytmp3.cc	0	0	0	0	0	0	0	0	0	2	2
114	abc.net.au	0	0	0	0	0	0	0	0	0	1	1
115	as.com	0	1	0	0	0	0	0	0	0	0	1
116	bet365.com	0	0	0	0	0	0	0	1	0	0	1
117	britannica.com	0	0	0	0	0	0	0	0	0	1	1
118	businessinsider.com	0	1	0	0	0	0	0	0	0	0	1
119	cdc.gov	0	0	0	0	0	0	0	0	0	1	1
120	cnbc.com	0	1	0	0	0	0	0	0	0	0	1
121	cnblogs.com	0	0	0	0	0	0	0	0	0	1	1
122	deepl.com	0	1	0	0	0	0	0	0	0	0	1
123	detik.com	0	0	0	0	0	1	0	0	0	0	1
124	duckduckgo.com	0	0	0	0	0	1	0	0	0	0	1
125	elpais.com	0	1	0	0	0	0	0	0	0	0	1
126	eluniverso.com	0	1	0	0	0	0	0	0	0	0	1
127	genius.com	0	0	0	0	0	0	0	0	0	1	1
128	grid.id	0	0	0	0	0	1	0	0	0	0	1
129	hindustantimes.com	0	0	0	0	0	0	0	0	0	1	1
130	ikea.com	0	0	0	0	0	0	0	1	0	0	1
131	infobae.com	0	1	0	0	0	0	0	0	0	0	1
132	jianshu.com	0	0	0	0	0	0	0	0	0	1	1
133	kompas.com	0	0	0	0	0	1	0	0	0	0	1
134	kumparan.com	0	0	0	0	0	1	0	0	0	0	1
135	made-in-china.com	0	0	0	0	0	0	0	0	0	1	1
136	merdeka.com	0	0	0	0	0	1	0	0	0	0	1
137	naver.com	1	0	0	0	0	0	0	0	0	0	1
138	noodlemagazine.com	0	0	0	0	0	1	0	0	0	0	1
139	okezone.com	0	0	0	0	0	1	0	0	0	0	1
140	pikiran-rakyat.com	0	0	0	0	0	1	0	0	0	0	1
141	primevideo.com	0	0	0	0	0	0	0	1	0	0	1
142	proiezionidiborsa.it	0	0	0	0	0	0	0	1	0	0	1
143	remove.bg	0	0	0	0	0	1	0	0	0	0	1
144	shein.com	0	1	0	0	0	0	0	0	0	0	1
145	speedtest.net	0	0	0	0	0	0	0	1	0	0	1
146	suara.com	0	0	0	0	0	1	0	0	0	0	1
147	tencent.com	0	0	0	0	0	0	0	0	0	1	1
148	tokopedia.com	0	0	0	0	0	1	0	0	0	0	1
149	tribunnews.com	0	0	0	0	0	1	0	0	0	0	1
150	trustpilot.com	0	0	0	0	0	0	0	1	0	0	1
151	tokopedia.com	0	0	0	0	0	1	0	0	0	0	1
152	un.org	0	1	0	0	0	0	0	0	0	0	1
152	usgs.gov	0	0	0	0	0	0	0	0	0	1	1
153	usps.com	0	0	0	0	0	0	0	0	0	1	1
154	who.int	0	0	0	0	0	0	0	0	1	0	1
155	wikimedia.org	0	1	0	0	0	0	0	0	0	0	1
156	xe.com	0	0	0	0	0	0	0	0	0	1	1
157	y2mate.com	0	1	0	0	0	0	0	0	0	0	1
158	zara.com	0	1	0	0	0	0	0	0	0	0	1