Too Many Zombies: Exploring Challenges and Motivations for (Not) Deleting Unused Online Accounts

Franziska Bumiller
franziska.bumiller@fau.de
Friedrich-Alexander-Universität Erlangen-Nürnberg
Erlangen, Germany

Sarah Delgado Rodriguez
sarah.delgado@unibw.de
University of the Bundeswehr Munich
Munich, Germany

Lukas Mecke
lukas.mecke@ifi.lmu.de
LMU Munich
Munich, Germany

Verena Distler
verena.distler@aalto.fi
Aalto University
Espoo, Finland

Florian Alt
florian.alt@ifi.lmu.de
LMU Munich
Munich, Germany

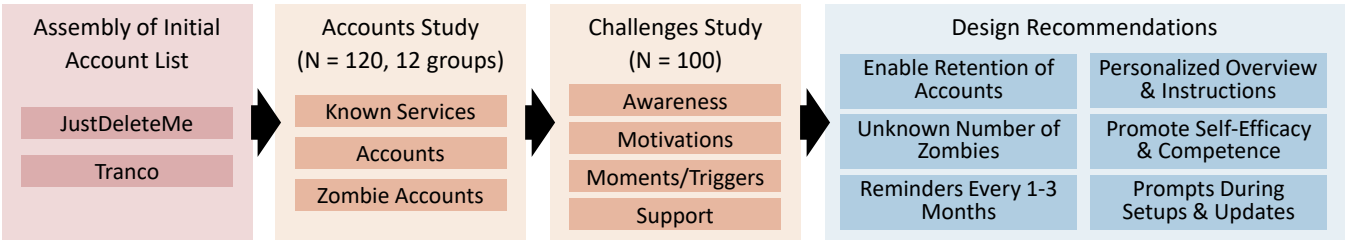


Figure 1: We explored the challenges users face with unused online accounts (zombie accounts) and their deletion. In particular, we investigated the number and types of zombie accounts users currently have through an initial online survey with 120 participants. Participants selected online services they knew or had accounts with (past or present), and identified unused accounts from a predefined list. We then conducted a second online survey to explore related challenges. This included participants' awareness of zombie accounts, their motivation for deleting them, suitable moments and triggers for account deletion, and how they wished to be supported in the process. We finally derived design recommendations for future zombie account deletion support tools from our results.

Abstract

Unused online accounts ("zombie accounts") pose avoidable privacy and security risks by retaining personal data that may be exposed in breaches. Yet, little is known about when and how to effectively prompt users to delete them. This work investigates the challenges users encounter when attempting to delete zombie accounts. We conducted two online studies with U.S. participants via Prolific: the accounts study (N = 120) to identify common zombie account categories, and the challenges study (N = 100) to examine users' motivations, perceived abilities, and preferred moments for deletion. Participants reported high self-efficacy but underestimated the number of zombie accounts they had. We identify promising opportune moments — such as when updating account information or setting up a new device — and evaluate potential triggers, including breach notifications and data sensitivity. This work contributes an empirical characterization of end-users' diverse challenges related to zombie accounts and design recommendations for future deletion-support tools.

CCS Concepts

• **Security and privacy** → **Social aspects of security and privacy**; • **Human-centered computing** → Empirical studies in HCI.

Keywords

Unused Online Accounts, Zombie Accounts, Opportune Moments, Account Deletion

CHI '26, Barcelona, Spain

ACM ISBN 979-8-4007-2278-3/2026/04
https://doi.org/10.1145/3772318.3790497

ACM Reference Format:
Franziska Bumiller, Sarah Delgado Rodriguez, Lukas Mecke, Verena Distler, and Florian Alt. 2026. Too Many Zombies: Exploring Challenges and Motivations for (Not) Deleting Unused Online Accounts. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/3772318.3790497

1 Introduction

Data breaches are a common security issue affecting billions of users. For example, in June 2024, Ticketmaster[1], a vendor for event tickets, confirmed a database hack potentially affecting 560 million users. The attacker claimed "the stolen data includes names, addresses, phone numbers, and partial credit card details"[2]. As Sood and Cor [55] highlight, at least 82% of Americans have been affected by a data breach at least once.

The Global Password Health Score Report 2023[3] stated that the average internet user has over 227 online accounts that require a password. Each of these accounts stores potentially sensitive data, such as contact information, postal addresses, or even payment data, on servers accessible from the Internet. Therefore, users are at risk of identity theft, financial loss, and further invasions of their privacy if their login details are leaked [33, 34]. As users often reuse passwords, a single breached account can potentially put multiple others at risk of being taken over or leaked [4].

Users often keep online accounts they no longer need. Liu et al. [30] established the term "zombie accounts" to describe this type of account. These accounts can still hold potentially sensitive information, which poses an avoidable threat. Therefore, zombie accounts should be deleted to reduce the risk of personal data being affected by a data breach. However, Liu et al. [30] found that users did not delete zombie accounts in mobile apps even though they were partially aware of the associated threat.

Users face various challenges when dealing with zombie accounts. On one hand, users may not be aware of all their zombie accounts. On the other hand, service providers discourage users from deleting zombie accounts by using deceptive design patterns due to commercial interests [28, 52]. While this power asymmetry in the form of manipulation through deceptive design patterns and differences in the available knowledge between providers and users is already known [44], prior work has, to our knowledge, neither examined the challenges and motivations for deletion of zombie accounts in depth nor investigated opportune moments for supporting such deletion.

To address this gap, we conducted two complementary online studies with U.S. participants via Prolific[4]. In the accounts study (N = 120), we identified common categories of zombie accounts and compiled a set of exemplary services. In the challenges study (N = 100), we examined users' motivations, perceived abilities, and preferred moments for account deletion, as well as potential triggers and support mechanisms. Participants reported high self-efficacy and confidence, yet underestimated the number of zombie accounts they had. Moments such as updating account information or setting up a new device were rated as particularly suitable for interventions, while triggers involving sensitive data or breach notifications increased willingness to delete.

Contribution Statement. This paper makes two primary contributions. (1) Our work offers the first empirical characterization of opportune moments for deleting unused online accounts ("zombie accounts"), based on two online studies (N = 120, N = 100) detailing the prevalence and categories of such accounts, users' self-reported motivations and abilities, and the triggers and contexts most conducive to deletion. (2) We provide actionable design recommendations for timing-aware, user-centered interventions that can translate awareness into everyday digital practices.

2 Background and Related Work

In this section, we review prior work on unused online accounts ("zombie accounts"), their legal and practical challenges, and related concepts such as opportune moments for security interventions.

2.1 Zombie Accounts

We build on Liu et al. [30]'s work regarding zombie accounts in mobile apps. They used the term "zombie accounts" to refer to unused mobile app accounts that still contain user data, whereas Deng et al. [15] used the term to refer to fake accounts created for fraudulent or manipulative purposes.

For the purpose of the present article, we define a *zombie account* as a real account created by a user (as opposed to a fake or automated account) that may never have been used but is *no longer in active use*. Such an account *still contains user data* that has not been deleted or anonymized. Users may be aware of some of these accounts, while others may have been forgotten over time.

Liu et al. [30] postulated a model for a mobile account deletion process and showed how diverse and often complicated account deletion is across different mobile apps. The researchers presented insights from both an online survey and an on-site experiment. Their findings suggested that participants had zombie accounts and wanted to delete them, but were unable to do so because they lacked an overview of these accounts and experienced issues with the deletion process. The authors suggested improving the situation by increasing the users' consciousness and confidence on the topic and unifying the deletion process according to user needs. Although Liu et al. [30] incorporated users' expectations regarding the deletion process into their research, they did not investigate opportune moments, motivation, or potential user support.

Legal regulations like the General Data Protection Regulation (GDPR)[5] or the California Consumer Privacy Act (CCPA)[6] grant users the right to erasure (right to be forgotten), meaning that users can request the deletion of their data and the provider generally has to comply with this wish. However, it is often difficult for users to exercise their right to delete their data. Schaffner et al. [52] and Kelly and Rubin [28] identified several strategies and designs employed by service providers to motivate or manipulate users into keeping their accounts. Other researchers also reported and criticized the poor usability of deletion procedures [25, 30, 45].

[1]Ticketmaster: https://www.ticketmaster.com/, last accessed February 17, 2026
[2]Ticketmaster confirms hack which could affect 560m: https://www.bbc.com/news/articles/cw99ql0239wo, last accessed February 17, 2026
[3]A Global Look at Password Health Scores in 2023: https://www.dashlane.com/resources/global-password-health-2023, last accessed February 17, 2026
[4]Prolific: https://www.prolific.com/, last accessed February 17, 2026

[5]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): https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679, last accessed February 17, 2026
[6]California Consumer Privacy Act (CCPA): https://oag.ca.gov/privacy/ccpa, last accessed February 17, 2026

Habib et al. [26] investigated data protection settings and the deletion of data on websites utilizing a content analysis. They argued that the GDPR improved the situation, despite the deceptive patterns, as many websites now offer options to delete data and configure privacy settings. Nevertheless, Habib et al. [25] demonstrated in a user study with several tasks, including deleting data online, that users were skeptical about whether the actions were actually carried out by the service provider. Along the same lines, Ramokapane and Rashid [44] described a fundamental power asymmetry between service providers and users concerning data deletion, criticizing a lack of transparency and explainability. They suggested that users require more support for effectively deleting their data and argued for explainable deletion. They also pointed out that users could not be certain that their data had been permanently deleted, as they lack access to the service provider's relevant systems. Furthermore, it was often possible to restore presumably deleted data [44].

There are various motivations for deleting unused accounts. Schaffner et al. [52] showed that not using an account anymore is the most common reason for users to delete social media accounts. Murillo et al. [35] examined the mental models of the deletion process for e-mails and social media content. They demonstrated that the reasons for deleting content vary by user and scenario, and highlighted that there is no one-size-fits-all solution for designing a deletion process. Considering the deletion of data in the cloud, Ramokapane et al. [45] also highlighted the crucial role of motivation and showed that, depending on the reasons users have for deleting files in cloud storage, users employ different coping strategies when unsuccessful.

Aside from scientific research, advice about zombie accounts aimed at end users has been published in several news articles and blog entries[7]. Databases like JustDeleteMe[8] and AccountKiller[9] provide instructions on deleting specific accounts, while search engines such as WhatsMyName[10] and Have I Been Pwned[11] assist with finding accounts and data breaches, respectively. These tools already offer limited support to users trying to delete an account.

2.2 Opportune Moments

The concept of opportune moments is rooted in research on interruptions. Parkin et al. [39] conceptualized opportune moments as a context in which a security intervention is well-timed, explicitly incorporating both the user's motivation and ability to act. Other work on interruption timing [21, 27] emphasized cognitive load and task boundaries, but without explicitly considering these motivational and ability-related aspects.

For the purpose of the present article, we define an *opportune moment* as a point in time when a user is both *motivated* to change their security-related behavior and *able* to carry out the intended action, and when a *suitable trigger* is present to prompt that action. While the ultimate goal is to achieve the desired action, its success is not part of the definition; rather, opportune moments can be evaluated through the likelihood that a given combination of motivation, ability, and trigger leads to successful execution.

Motivation Motivation refers to the willingness or desire to perform the behavior in question [6]. In our context, it captures why a user would choose to delete a zombie account at a particular moment. It is here understood as the force that "drives all intentional behavior" [8], and can arise from various sources, such as perceived risk, personal values, or social influence. To capture the diversity of motivational processes that may influence opportune moments, we draw on established psychological theories. Following Chen et al. [11] who suggest to explore the influence of psychological needs and motivation factors rather than focusing on deterrence alone, we incorporated complementary perspectives on motivation by employing the Protection Motivation Theory (PMT) [47, 48] and the Organismic Integration Theory (OIT) [49] from the Self-Determination Theory (SDT) [12]. Appendix A provides details on these theories.

Ability Ability describes the user's capacity to execute the intended behavior at that moment. This includes both the necessary knowledge (e.g., knowing how to navigate deletion menus) and the resources available (e.g., having credentials or the time to complete the process). Without sufficient ability, even high motivation may not translate into action.

Trigger A trigger is an event or cue that prompts the user to perform the intended behavior at the appropriate time. In the context of zombie accounts, examples include receiving a breach notification, updating account information, or encountering a relevant reminder while performing related tasks. Effective triggers are timely, contextually relevant, and aligned with users' current mental workload.

Addressing mental workload in combination with opportune moments, Iqbal and Bailey [27] conducted a study to methodically evaluate different interruption moments, including the perceived annoyance of the interruption and respect for the disrupted task. The authors highlighted that workload is an effective predictor of opportune moments. This implies breaks between tasks, as moments with reduced workload are especially promising. Fischer et al. [21] also provided insights into the correlation between mental workload and opportune moments, implying that the context between the interrupted task and the wanted behavior should be as similar as possible. Furthermore, they found that the best moment for an interruption was after finishing a task, while the worst moment was when planning or initiating a new task, leaving a tight time frame for an opportune moment.

Opportune moments appear to be a promising concept for researchers of usable security, as Alt et al. [2] argued, proposing a new paradigm that utilizes more behavioral data in security. Nevertheless, research on the intersection remains rare. Murtezaj et al.

[7]Exemplary Blogs and Articles: How to Delete Online Accounts You No Longer Need: https://www.consumerreports.org/electronics-computers/privacy/how-to-delete-online-accounts-you-no-longer-need-a1194263953/; Privacy Fix: How to Find Old Online Accounts: https://www.consumerreports.org/electronics/digital-security/how-to-find-old-online-accounts-a1266305698/; Saying Goodbye: Tips for Closing Hard-to-Delete Online Accounts: https://www.consumerreports.org/digital-security/tips-for-closing-hard-to-delete-online-accounts-a6499479986/; Delete Your Old Accounts (If You Can): https://www.nytimes.com/wirecutter/blog/delete-your-old-accounts/; all last accessed February 17, 2026

[8]JustDeleteMe: https://justdeleteme.xyz/, last accessed February 17, 2026

[9]AccountKiller: https://www.accountkiller.com/en/home, last accessed February 17, 2026

[10]WhatsMyName Web: https://whatsmyname.app/, last accessed February 17, 2026

[11]Have I Been Pwned: https://haveibeenpwned.com/, last accessed February 17, 2026

[36] mentioned opportune moments in their concept of public security user interfaces as part of their ideas. But, to our knowledge, only Parkin et al. [39] investigated security-related opportune moments so far. The authors examined purchasing a new technical device on-site as an opportune moment for cybersecurity intervention, utilizing qualitative in-situ interviews. They demonstrated the potential of a device transition as a mediator for more secure behavior when interventions were provided in a timely manner by a trustworthy salesperson.

2.3 Summary

Zombie accounts are unused online accounts that retain personal data and pose avoidable privacy and security risks; prior work has focused on the specific domain of mobile apps [30]. Deleting accounts is legally supported (e.g., GDPR) but often hindered by deceptive design patterns [28, 52] (previously also called dark patterns[12]), poor usability [25, 30, 45], and uncertainty about actual data removal [44]. Opportune moments—times when users are receptive to behavioral prompts—are influenced by cognitive load [27] and task context [21], but have rarely been studied in usable security, and not at all for account deletion.

Against this backdrop, our work examines how users perceive zombie accounts, what motivates their deletion, and which moments and triggers are most suitable for supporting this process.

3 Research Approach

Little is known about users' perspectives on *zombie accounts*, including the number and types of such accounts they have, and their motivations and abilities to delete them. To date, no work has empirically identified contextually suitable moments and triggers that could prompt users to delete their zombie accounts.

3.1 Research Questions

We take an exploratory approach to address the following questions:

- **RQ1** What types and categories of zombie accounts do users have, and how aware are they of them?
- **RQ2** What intrinsic and extrinsic motivations influence users' decisions to delete zombie accounts?
- **RQ3** Which moments and triggers can enable or encourage account deletion?
- **RQ4** What forms of support or resources can help users successfully delete their zombie accounts?

3.2 Methodology

Figure 1 shows an overview of our methodology. We conducted two studies using online questionnaires.

The *accounts study* (cf. Section 5) focused on identifying common zombie accounts. Here, we systematically derived a list of potential zombie accounts based on two distinct online sources (i.e., JustDeleteMe and Tranco [29], see Section 4) to estimate the amount and kind of services that are zombie accounts.

[12]Words Matter: https://www.acm.org/diversity-inclusion/words-matter, last accessed February 17, 2026

In the *challenges study* (cf. Section 6) we explored participants' awareness of their zombie accounts, their motivation, suitable moments and triggers for account deletion, and how they wished to be supported in the process.

4 Assembling the Initial Account List

To identify and categorize common zombie accounts, we first needed an extensive list of online services that allow users to create accounts. As no such list was available in existing research or public datasets, we assembled one ourselves by combining two complementary sources. The first source was *JustDeleteMe*, a community-maintained directory of services with account deletion instructions. We retrieved all available entries on August 20, 2024, resulting in 1,964 distinct services. The second source was the *Tranco list* [29]. The Tranco list aggregates multiple existing popularity rankings (e.g., from Alexa, Majestic, Cisco Umbrella) over a 30-day period and then scores domains using the Dowdall rule [23] to yield a stable, reproducible top-domains list for research. We used the list snapshot generated on October 23, 2024, and restricted it to the top 1,000 domains to complement the JustDeleteMe dataset. We did this to capture any popular or high-impact accounts that may not be included in JustDeleteMe. We focused on the top 1,000 entries as a tradeoff between page relevance and the burden we would put on participants in rating the items. That said, our approach does not incorporate low-ranking domains as potential candidates. Future research could therefore specifically target these accounts to determine the connection between the popularity of a service over time and its likelihood of becoming a zombie account.

We then merged the two lists by standardizing the entries (by removing all text after the first dot in each domain name and capitalizing the first letter) and dropping duplicates. In a second step, we manually reviewed the merged list to correct spelling inconsistencies (e.g., *Bankofamerica* to *Bank of America*) and to merge entries referring to the same service under different names or domains (e.g., *office* and *office365* into *Microsoft Office 365*). We also removed services where user accounts are not possible. To ensure the plausibility of the merging and cleaning process, we randomly sampled 5% of entries from the final merged list and 5% from the removed entries, checking each manually against the original sources.

The final list comprised 2,559 entries: 207 appeared in both the JustDeleteMe dataset and the Tranco top 1,000. A further 1,604 entries were present in JustDeleteMe and in lower-ranked positions in Tranco, 151 entries appeared only in JustDeleteMe, and 597 entries appeared only in the Tranco top 1,000. This list served as the sampling frame for the accounts (Section 5) and the challenges study (Section 6) and can be found in the supplementary material.

5 Accounts Study

We conducted the accounts study to identify which services from the assembled account list (Section 4) most frequently appeared in participants' self-reported zombie accounts. This step addresses RQ1 (*What types and categories of zombie accounts do users have, and how aware are they of them?*) and produces a refined set of services most commonly flagged as zombie accounts for use in the challenges study (Section 6).

5.1 Questionnaire Design

We divided the complete account list into 12 non-overlapping subsets (each containing roughly 216 services[13]), as it was too large for one participant to review in a single session. Participants were randomly assigned to one of the 12 groups, each receiving a distinct subset of services but otherwise completing the same questionnaire. An overview of the questionnaire is shown in Figure 2, and the complete instrument and the subsets for the 12 groups are provided in the supplementary material.

The questionnaire begins by providing the participant with information and verifying their age to ensure all participants are of legal age. After consenting to the data collection, the main task of the study is divided into 3 steps: As shown in Figure 3, in the first step, we ask participants to select all services that they know at least by name. Next, participants are asked to indicate whether they have ever had an account with these services. Finally, participants are asked which of those they would consider a zombie account. For this, an explanation is provided that describes a zombie account as one that has not been actively used for at least a year.

We added two attention checks [37] to assess the data quality. For this, each participant saw the entries "Google" and "Prolific" as we assumed that all participants should be familiar with them.

After the main task, participants were asked to rate their technology affinity and security attitudes through the Affinity for Technology Interaction Scale (ATI) [24] and SA-6 [20] scales. By including these standard scales, we aimed to assess how our sample's technical affinity and security attitudes compare to the general US population, as these personal attributes can influence participants' data-protection–related perceptions [3, 14, 17]. We used these particular scales because they are (1) widely adopted in usable security and privacy research (e.g., [10, 65] and [46, 53, 63]) and (2) are short, adding little workload for participants, especially since they are not directly related to our research questions.

Demographic questions complemented the questionnaire. Finally, a text box for feedback allowed the participants to share their thoughts and impressions on the questionnaire.

We conducted a pilot test [18, 54] to evaluate the questionnaire and assess the different display options for the account lists with 11 pilot testers We compared three different format options (single-column, 3-column, and 4-column) for the account list. Finally, the pilot testers had to select in an additional feedback question which option between 1 and 5 columns they preferred. As a result, the 4-column design of the account list was chosen for the questionnaire. A mobile version with account lists in a single-column design was added to enable the questionnaire completion on a smartphone. The Ethics Committee of our University approved our study design and certified that it adheres to all relevant ethics guidelines.

5.2 Recruitment

We distributed the questionnaire to participants in the United States via Prolific in December 2024. Crowdworking platforms have been widely used in various areas of research [16, 40, 56, 59], as they offer a convenient method for recruiting a diverse sample of participants within a reasonable timeframe. In particular, we chose Prolific over other crowdworking platforms because it is designed specifically for research, providing unique features tailored to such studies [38]. We selected a Prolific standard sample and did not apply quotas. We recruited 120 participants, targeting 10 participants per group. We chose this group size inspired by typical sample sizes in formative HCI studies [9]. Note that we do not assume it to be sufficient to identify all possible zombie accounts. Instead, it is intended to capture a broad subset of common zombie accounts to inform the design of our challenge study. On average, participants needed 10 minutes and 7 seconds (median = 8 minutes and 27 seconds, std = 6 minutes 12 seconds) to complete the study and received £1.70 as compensation. This is in line with local ethics guidelines, and exceeds U.S. minimum wage. We checked potential outliers manually for data quality and consistency.

5.3 Analysis

Demographics, ATI, and SA-6 are analyzed descriptively, following the specifications outlined in the respective publications. For the account list, we calculated the clicks for each service in the three categories (known by name, account at any point in time, and zombie account) in absolute numbers as well as relative to the group size and in comparison to the selection in previous categories. Furthermore, the number of accounts selected by each participant in each category was also determined. We also analyzed potential correlations between these values and the demographic attributes of our participant sample, in order to present the trends in our dataset thoroughly and provide more context for interpreting our findings. In particular, we used the Spearman coefficient [64] to assess correlations between the number of selected accounts and demographics. Inspired by Braun and Clarke [7], one researcher first familiarized themselves with the entire dataset and then inductively derived themes from the free-text answers by grouping similar statements. To ensure the integrity of our findings, all themes were discussed with a second researcher while revising the related participant quotes. Both researchers discussed potential ambiguities and differences in understanding during this meeting.

To assess data quality, we calculated an agreement rate based on the proportion of accounts that all participants in each group rated identically. This yielded three values per group – one for each category (known account, account, zombie account). Looking at zombie accounts only, the participants reached an agreement rate of over 85%. We then summarized these values by computing their mean for each group. The resulting agreement rate for all groups exceeds 60%, with 8 groups even reaching over 70%. These high agreement rates indicate that, despite the small group sizes, comprising only 9 to 11 participants, the sample size was sufficient to yield meaningful results.

5.4 Limitations

Even though the initial account list was carefully compiled using two sources (JustDeleteMe and the Tranco list [29]) it may still omit some zombie accounts participants had. Moreover, our findings may not be replicable in the future due to the fluid nature of the digital landscape. Therefore, we view our results as a snapshot of the current state that helps estimate the scale of the underlying challenges, rather than as a comprehensive list of zombie accounts.

[13] Pilot self-tests indicated that approximately 250 services could be reviewed without excessive fatigue

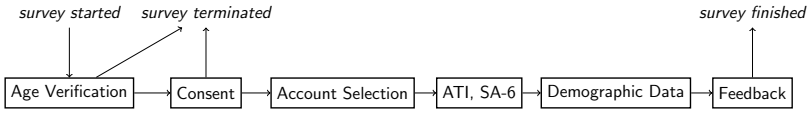


Figure 2: Overview of the structure of the questionnaire for the account study. During account selection as the main task of the survey, the participants have to check for 216 services on up to 3 pages if they (1) know a service by name, (2) have/had an account there, and (3) currently have a zombie account there.

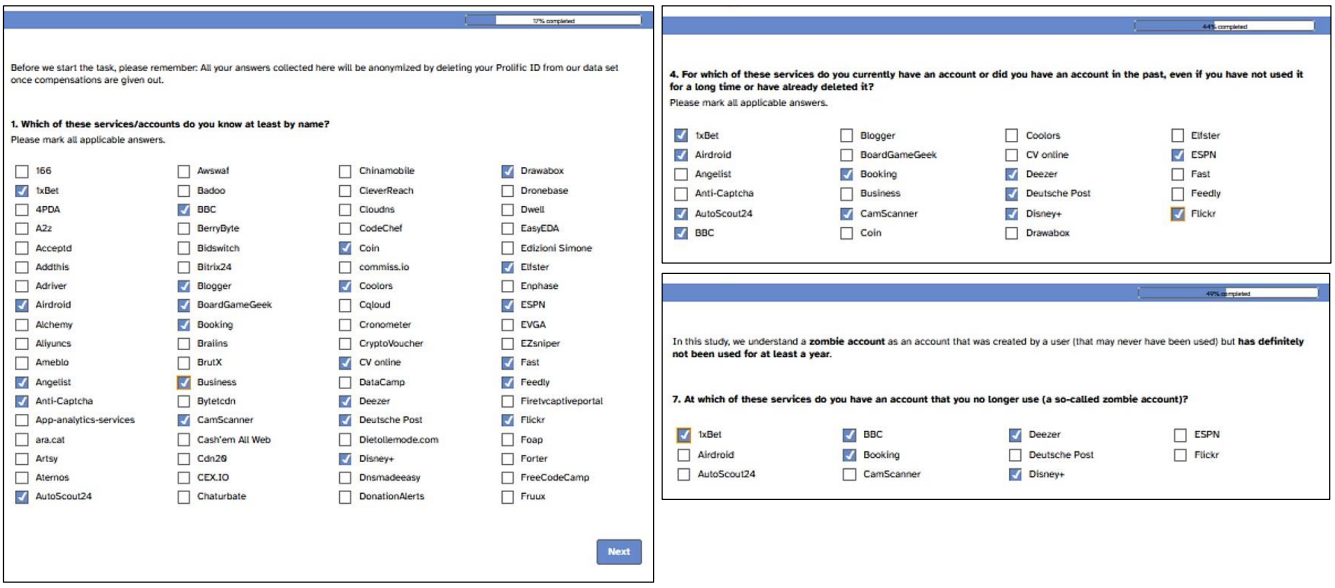


Figure 3: Illustration of the main task of the account study: First, the selection of accounts known by name (left), second, the services one ever had an account at (top right), and third, the corresponding zombie accounts (bottom right). Only services selected in the previous step were presented in the next.

Our results only include zombie accounts that participants recalled when prompted. Completely forgotten accounts are not captured. Our sample size per group is also not sufficient to comprehensively capture all possible zombie accounts. Instead, our aim was to reduce the initial list of accounts to a manageable subset with a high probability of containing a large number of potential zombie accounts, in order to inform the design of the challenge study. Future research could complement our findings with objective measures (e.g., by analyzing email accounts) and larger sample sizes to better estimate the true number of zombie accounts.

We recruited participants from the United States to minimize any cultural differences within the sample. Hence, other services might be more popular in other regions [30].

Finally, we used the ATI and SA-6 scales to assess technical affinity and overall security attitudes, to describe our participant sample and facilitate insights into its comparability with the overall U.S. population. We chose these two scales because they are short and frequently adopted in related research. We did not use further standard scales, such as the Internet Users' Information Privacy Concerns [31] or the Security Behavior Intentions Scale [19]. This could have caused us to overlook the influence of additional factors on the topic. Future research could therefore assess whether these might provide additional or more detailed insights or correlations with participants' zombie accounts.

5.5 Sample

The cleaned sample consists of 120 participants who contributed to this study's results. All participants passed at least one of our attention checks and most (N = 94) passed both. When a participant had missed an attention check, we assumed that one possible reason might have been fatigue due to the extensive questionnaire. In this case, their data was checked for plausibility and quality in the other questions by examining patterns as well as the content of the feedback question if an answer was provided. The participant was included in the sample if these criteria were met. Moreover, six of the 12 groups consisted of 10 participants. Three groups had 9 participants, and three had 11 participants.

5.5.1 Demographics. The sample consists of 62 females, 57 males, and one participant indicating a different unspecified/non-binary option. Participants were aged between 19 and 75 years, with a mean of 37.15 years (median = 36, std = 12.87). The sample is highly educated, as 79 participants have a university degree. More than half of the sample (63 participants) is employed full-time. Multiple occupations were mostly selected by students who, in addition to their studies, work full or part-time.

5.5.2 Technical Affinity and Security Attitudes. The ATI within the sample has a mean of 3.95, a standard deviation of 1.36, and a Cronbach's Alpha of 0.85, indicating that the participants are rather

Table 1: Overview of categories and sub-categories of accounts reported as zombie accounts by at least 20% of participants, with examples. Total of categorized accounts: 89

Category	Sub-Category	Example	Amount
Communication		AOL / Instant Messenger	10
	Social Media	Instagram, MySpace	6
	Dating	Tinder	2
Entertainment		iHeart, 1xBet	2
	Streaming	Disney+, ESPN, Peacock	7
	Gaming	Pokemon GO	2
	Adult Content	PornHub, OnlyFans	2
(Softw.) Product		Adobe, Apple, LogoMaker	14
	Security	Avast!, McAfee	4
	Search Engine	Yahoo!, Bing	3
	Education	Photomath, Quizlet	2
Shopping		Temu, Ticketmaster, McDonald's	17
	Service/Product Offer	Uber, eBay	5
Recommendation/ Discount		TripAdvisor, Quora, Groupon (Worldwide)	6
Finance		Coinbase, Bank Of America	7

technically inclined. The SA-6 has a mean of 3.72, a standard deviation of 1.06, and a Cronbach's Alpha of 0.88. With this SA-6 score, the sample is "close to the average score for the U.S. population" ($3.57 < X < 3.99$) [20]. Furthermore, Cronbach's Alpha between 0.8 and 0.9 shows the good internal consistency of both scales[14].

5.6 Results

5.6.1 Common Zombie Accounts. For each service in the assigned subset of the initial account list, participants indicated whether they (a) knew the service by name, (b) had ever held an account there, and (c) currently held a zombie account there. Figure 4 shows the distribution of services across these three categories. The number of services considered decreases in each step because only services selected in the previous step were presented in the next.

Half of all services in the initial list (1,304 of 2,559; 50.96%) were not known by name to any participant in their group (Figure 4a). In the zombie account category, 2,202 services were never selected (Figure 4c), confirming that a large proportion of the initial list was irrelevant to most users and justifying a reduction to the most relevant services. We retained 89 services with a zombie account click rate of at least 20% within their group for further investigation in the challenges study. Table 1 summarizes their categories and subcategories; shopping, (software) product access, and communication services were most common.

The ten services most frequently reported as zombie accounts (in descending order of mentions) were *Pinterest*, *Coinbase*, *Starbucks*, *Google Pay*, *eBay*, *Robinhood*, *Yahoo!*, *Hotmail*, *LinkedIn*, and *Roku*. A complete list of the 89 services, with click rates and categories, is provided in Appendix B.

5.6.2 Users' Zombie Accounts. Out of 120 participants, 110 reported at least one zombie account. Participants identified up to 27 zombie accounts, with an average of 4.41 mentions (median = 3, std = 4.57) in their assigned subset, indicating that most users could recall at least some unused accounts. Extrapolating from group means to the full account list, a typical user would know appr. 341 services by name, have had an account on 134 of them, and hold about 53 zombie accounts – nearly 40% of all created accounts.

Correlations between demographic and attitudinal variables revealed no significant relationships between the number of accounts (in any category) and gender, age, or education. A moderate positive correlation was observed between ATI and SA-6 scores ($r = .45, p < .001$). The ATI also correlated moderately with the number of accounts held ($r = .31, p < .001$) and weakly with known services ($r = .20, p = .026$) and zombie accounts ($r = .21, p = .022$), suggesting that higher technology affinity is associated with greater exposure to, and accumulation of, online accounts.

5.6.3 Participants' Feedback. 50 participants used the feedback text box provided in the questionnaire to share their thoughts on the study. Five participants noted that they learned something from the questionnaire or had the chance to reflect on their online behavior. One participant stated:

"I never really thought about zombie accounts, but thinking about it, I have quite a lot."

Three wondered about the presented services. Four participants suggested improvements to the questionnaire, such as displaying more services or including additional examples. Overall, the feedback was very positive, highlighting the clarity of the study and showing participants' interest in the topic and its relevance.

6 Challenges Study

Building on the accounts study, we conducted the challenges study to gain insights into challenges users face when deleting zombie accounts, understanding their motivation and (self-assessed) skills, and identifying opportune moments for interventions.

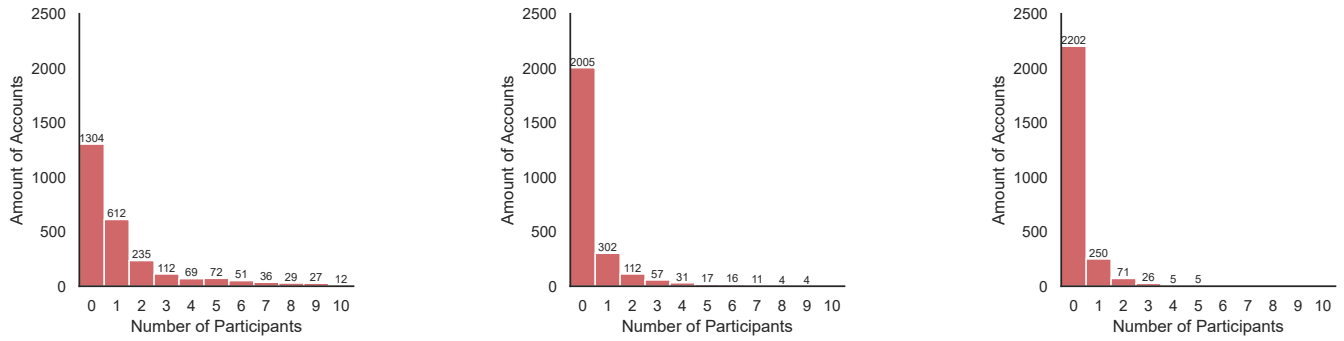
6.1 Questionnaire Design

The questionnaire for the challenges study was developed to address the research questions (Section 3.1) and was refined through several iterations. It combined self-developed items with established scales from the literature to explore the topic from multiple perspectives. Whenever possible, items used a 5-point Likert scale ranging from "strongly disagree" to "strongly agree"; for questions not fitting this scale, response formats were adapted from Brown[15]. An overview of the questionnaire flow is provided in Figure 5, and the complete instrument is included in the supplementary material.

6.1.1 Introductory Section and Prior Experience. The questionnaire began with an age verification and consent form. Participants then answered questions about the approximate period in which they created their first online account, the devices they most frequently used to access online accounts, and their self-rated internet proficiency, following the approach of Liu et al. [30]. They were also asked to provide open-text descriptions of reasons for wanting to, or not wanting to, delete an account in the past. The frequency of wanting to delete and actually deleting accounts was assessed. Participants who reported to have deleted at least one account completed an additional page about their experiences, success rate, and challenges, including a mandatory open-text description of challenges they encountered.

[14]https://datatab.net/tutorial/cronbachs-alpha, last accessed February 17, 2026

[15]Likert Scale Examples for Surveys: https://www.extension.iastate.edu/documents/anr/likertscaleexamplesforsurveys.pdf, last accessed February 17, 2026



(a) Known by name **(b) Account** **(c) Zombie Account**

Figure 4: Distribution of services that participants in the questionnaire (a) knew by name, (b) have at any point in time had an account with (although it could be already deleted), and (c) have identified as zombie accounts. As visualized, many services are not known by name to any participant within the corresponding group and, therefore, are irrelevant for the search for zombie accounts that the participants can recall.

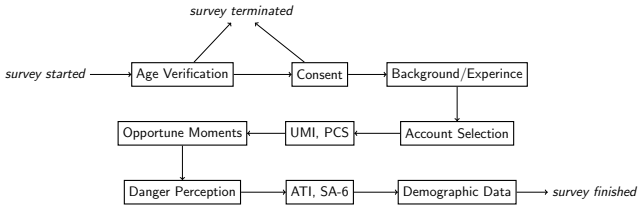


Figure 5: Overview of the structure of the questionnaire for the challenges study. During account selection, the participants have to check for 86 services if they (1) know a service by name, (2) have/had an account there, and (3) currently have a zombie account there.

6.1.2 Initial Perceptions and Zombie Account Identification. Before being shown any account lists, and to avoid priming, participants were asked whether they believed they actively used all their current accounts, whether they could recall all their zombie accounts, and to estimate the number of zombie accounts relative to their active accounts. They were then presented with a refined list of common zombie accounts identified in the accounts study (Section 5.6.1). Three entries were removed from the list because of potentially sensitive content. For each remaining service, participants indicated whether they knew it by name, had ever had an account, and currently had a zombie account there.

6.1.3 Motivation and Ability. To measure motivation and perceived competence in relation to zombie account deletion, the questionnaire included the User Motivation Inventory (UMI) [8] and the Perceived Competence Scale (PCS) [61, 62], both of which were adapted to the topic of deleting zombie accounts. The UMI measured types of motivation in line with the Organismic Integration Theory from the Self-Determination Theory, while the PCS captured participants' self-reported ability to delete such accounts.

6.1.4 Opportune Moments and Triggers. Participants evaluated potential triggers for deletion, including the type of data stored in an account (financial, identity, health, business, or personal media), information about data breaches from various sources, and their trust in the service provider or in other individuals with whom the account might be shared. One question assessed participants' confidence in finding forgotten zombie accounts, whether they knew strategies for doing so, and whether they would require assistance. Participants were also shown potential strategies for locating such accounts, like searching saved login credentials or browsing registration e-mails, and indicated which ones they would use. To assess suitable moments for deletion, participants rated different times of day, online activities (e.g., browsing, shopping, banking), and account-related tasks (e.g., updating account information, setting up a new device).

6.1.5 Aids, Threat Perception, and Final Measures. Participants then indicated whether they would like different types of information in a reminder to delete zombie accounts, such as a personalized list of accounts, and stated the maximum amount of time they were willing to spend on deleting a single account, as well as their preferred reminder interval.

Threat perception was measured using severity ratings for possible negative consequences of having zombie accounts, such as having accounts hacked or an identity stolen, adapted from Zou et al. [65]. We also incorporated Protection Motivation Theory-based items adapted from Prange et al. [43] with one item representing each construct of the theory[16]. We fitted these to the topic of zombie accounts, and placed the items toward the end of the questionnaire to minimize priming effects.

As in the accounts study (Section 5.1), the questionnaire concluded with the ATI and SA-6 scales, demographic questions (age, gender, education, occupation), and an open-text feedback field. Two instructed attention checks [37] were placed approximately 10 and 20 minutes into the survey. Because the PCS could not be adapted for smartphone display, participation was restricted to tablet, laptop, or desktop devices.

[16]Namely, vulnerability, severity, maladaptive intrinsic and extrinsic rewards, response efficacy, self-efficacy, and response costs.

6.1.6 Pilot Testing and Ethical Approval. A pilot test conducted in April 2025 with 13 participants confirmed the clarity and usability of the questionnaire. The pilot test data was not included in further analysis. Minor wording adjustments were made to two items, and the pilot provided an estimate of completion time. The final design was approved by our university's ethics committee.

6.2 Recruitment

Using Prolific once again, we recruited 100 participants from the United States in May 2025. Participants needed on average 28 minutes and 25 seconds (median = 24 minutes and 38 seconds, std = 11 minutes 30 seconds) to complete the questionnaire and were compensated with £4.18 (in line with our university's ethics guidelines and higher than the US federal minimum wage). All participants passed two attention checks. Again, we checked potential outliers manually for data quality and consistency.

6.3 Analysis

The analysis of the challenges study utilizes the same tools as for the accounts study (cf. Section 5.3) and follows the same process regarding data cleaning.

We used the account list presented to the participants to calculate the number of services selected by each participant for each category as well as to calculate the number of participants who selected a specific service within the given category. The UMI and PCS, along with the ATI and SA-6, are analyzed according to the provided instructions by the respective authors. We used the Spearman coefficient [64] to calculate various correlations between the number of selected accounts per category, utilized scales, and demographics (incl. SA-6 and ATI scores) for further insight.

In line with Döring and Bortz [18] on the topic of quantitative analysis for explorative studies, first, visualizations of the results, mostly in the form of (stacked) bar plots, are built and analyzed. Furthermore, we conducted a Friedman test [41] on central items of the questionnaire to determine whether the difference between the items is statistically significant. Text responses on experience and challenges, as well as the feedback provided by participants, were exported and analyzed individually by question. The qualitative analysis approach applied here follows the same method inspired by Braun and Clarke [7] as specified for the accounts study. First, one researcher familiarized themselves with the data and inductively derived themes. All themes were then discussed with a second researcher while revising the related participant quotes.

6.4 Limitations

Our study relies on self-reported data, measuring intentions rather than actual user behavior [65]. Furthermore, self-reported data might be subject to self-report bias, social desirability bias, and availability bias. The applicability of our findings to non US-populations needs to be also investigated in the future, as we intentionally restricted our sample to minimize cultural differences. Replicating the design of our accounts study, we again used the ATI and SA-6 to describe the sample and enable comparability with the overall U.S. population. We envision future work examining potential correlations with other standard scales.

6.5 Sample

The challenges study received 106 clicks, and 100 participants completed interviews. The sample consists of 51 females, 48 males, and one non-binary participant. Participants were aged 20-75 years, with a mean age of 43.75 years (median = 43.5, std = 13.79). The sample is highly educated (82 participants have a university degree). 70 participants are employed full-time. Five participants selected more than one occupation. Most were students or employed part-time.

The ATI of the sample has a mean of 4.16, a standard deviation of 1.48, and a Cronbach's Alpha of 0.76. The SA-6 has a mean of 4.03, a standard deviation of 0.98, and a Cronbach's Alpha of 0.89. The sample shows a score that is considerably higher than the average score for a U.S. population sample ($X > 3.99$) [20].

6.6 Results

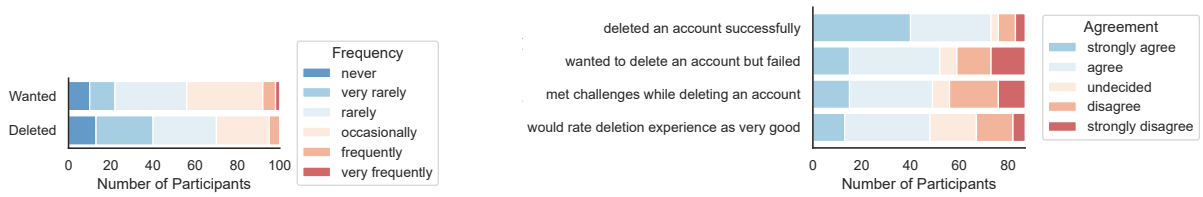
6.6.1 Experience. Most participants described themselves as familiar with being online (73 participants), while 23 identified as professional/developer and 4 as basic users. The time at which participants first created an online account spanned the last three decades, with a peak between 2010 and 2014.

Many participants reported both wanting to delete and successfully deleting an account in the past, although actual deletion was less frequent than the desire to delete (Figure 6a). Fourteen participants had never deleted an account, leaving 86 to answer questions about their deletion experiences.

Among those 86 participants, most had successfully deleted an account, but over half reported having failed in at least one attempt or encountering challenges (Figure 6b). While the majority would rate their deletion experiences positive (median = *agree*), reported *challenges* included complicated procedures (n=36), hidden or hard-to-find deletion settings (n=25), and service providers offering only deactivation instead of deletion (n=4). Other difficulties were extensive verification requirements (n=10), lost credentials (n=8), problems recovering credentials (n=5), and the need to contact customer support (n=17). Although some participants found support helpful, others preferred to avoid it. A lack of confirmation of deletion (n=12) and uncertainty about whether data were truly removed also reduced motivation (n=8) and caused frustration (n=11). Data loss was reported rarely (4 participants).

Participants cited multiple *reasons for wanting to delete accounts*, most often because the account was no longer used or needed (n=32). Other reasons included decluttering an online presence (n=12), loss of interest (n=9), switching to alternatives (n=6), privacy protection (n=22), security concerns (n=11), prevention of data leaks (n=5), accounts being hacked (n=8), avoidance of unwanted messages (n=10), and distrust or ethical objections to the provider (n=5). Personal motivations included removing embarrassing information or starting anew (n=8), and reducing distractions (n=6).

Reasons for keeping accounts included no perceived need to delete (n=15), continued (n=13) or planned use (n=10), fear of data loss (n=8), maintaining access to stored information (n=6), and retaining important or valuable data (n=9). Some participants avoided deletion due to cumbersome procedures (n=7), lack of motivation (n=2), or convenience (n=3). Emotional attachment was also cited, such as saved memories (n=6), staying connected with friends and family (n=12), and following news or organizations (n=4).



(a) Deletion: wanted vs. deleted

(b) Deletion experience

Figure 6: Participants' previous experience with deleting online accounts. (a) Comparison between the frequency of wanting to delete an account and actually doing it, and (b) participants' rating of different experiences related to account deletion.

Table 2: Overview of services selected most by participants as zombie accounts with corresponding ratings of knowing the service and having an account there, and descriptives of the ratings for all 86 presented accounts.

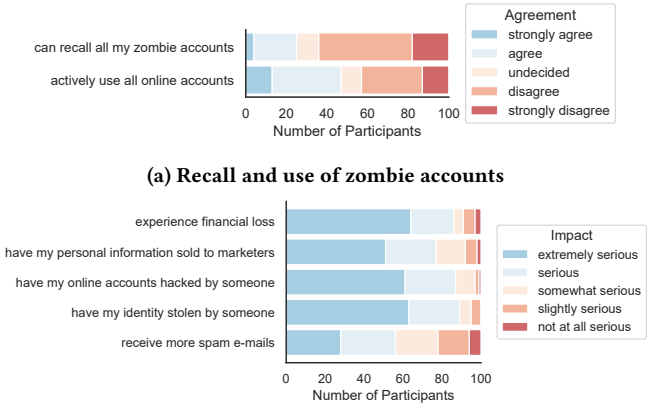
	known	account	zombie account
Skype	77 %	49 %	23 %
Tinder	66 %	36 %	20 %
Hotmail	63 %	35 %	19 %
MySpace	44 %	26 %	18 %
Yahoo!	80 %	58 %	18 %
Facebook Messenger	81 %	64 %	16 %
AOL / Instant Messenger	32 %	22 %	16 %
Adobe	71 %	39 %	15 %
Dropbox	49 %	25 %	14 %
AT&T	59 %	31 %	14 %
AliExpress	61 %	32 %	14 %
mean	39.38	19.58	5.63
median	36.50	17.50	3.00
range	2-80	0-57	0-28
std	24.33	14.56	5.81

6.6.2 Zombie Accounts. Building on the account list gathered in the accounts study, the challenges study provides a more detailed picture of current zombie accounts. As presented in Table 2, the most common zombie account in the list is Skype, which was selected 23 times by participants. Although the presented list resembled the accounts selected most as zombie accounts in the accounts study, three services were not selected by a single participant as zombie accounts. One of these 3, Dashlane[17], a provider of a password manager and digital wallet, was the only service selected by zero participants to ever have an account there.

From the 86 entries in the account list, the participants marked on average 5.63 as zombie accounts. Seven of the 100 participants marked no account as a zombie account, while 20 participants marked 10 or more accounts on the list as zombie accounts. A summary of the participants' responses on all three categories queried is given in Table 2.

We tested for correlation between the number of selected services per category, the participants' age, their affinity for technology (ATI score), and their security attitude (SA-6 scale) using a Spearman test. No correlation was found between age and ATI with the number of selected services of the three categories. The number of services known by a participant correlated lightly negatively with their SA-6 ($r = -.24, p = .015$) as well as the number of services selected as zombie accounts with the SA-6 ($r = -.27, p = .007$), indicating

[17]Dashlane: https://www.dashlane.com, last accessed February 17, 2026



(a) Recall and use of zombie accounts

(b) Potential impact of threats from zombie accounts

Figure 7: Participants' agreement on statements regarding their zombie accounts: (a) Participants' awareness and use of (zombie) accounts and (b) their assessment of the potential impact of threats from zombie accounts.

that a higher security attitude correlates with a lower number of services known and less zombie accounts. Furthermore, we found a moderate correlation between the SA-6 and ATI ($r = .47, p < .001$).

As shown in Figure 7a, almost half of the participants reported using all of their accounts actively (median = *undecided*) and, therefore, having no zombie accounts. Note that this assessment was made before we confronted participants with potential zombie accounts. Fewer participants believed that they could find all their zombie accounts (median = *disagree*). In line with these statements, most participants believed they have either fewer zombie accounts than regularly used ones (median = *little less*).

Answering RQ1 – Categories and Awareness of Zombie Accounts

Participants had zombie accounts mostly for shopping, communication, and to access software products (Section 5.6.1). They were not aware of their number of zombie accounts and partially thought they would use all their accounts.

With regard to the *perception of danger* around zombie accounts, Figure 7b shows that a majority of participants thought that nearly all proposed threats would impact them seriously or extremely seriously. Identity theft was being assessed as the most severe (median = *extremely serious*), followed by accounts getting hacked (median = *extremely serious*), financial loss (median = *extremely serious*), and

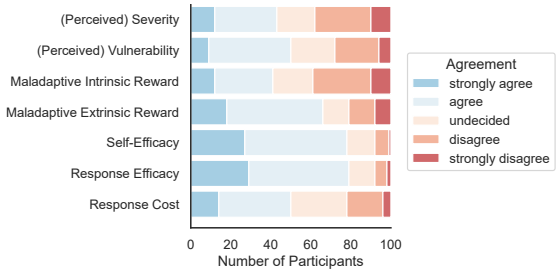
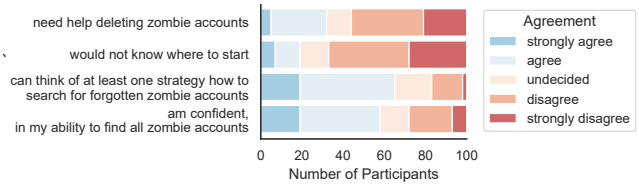


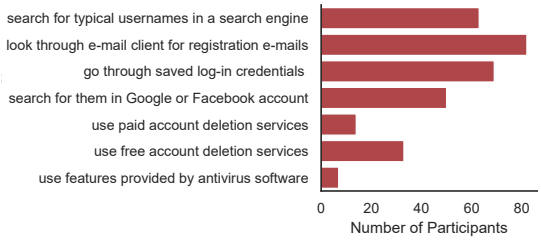
Figure 8: Participants' motivation to delete zombie accounts based on the Protection Motivation Theory (PMT) [47, 48]

Table 3: Mean, standard deviation, and Cronbach's alpha for each of the constructs within the User Motivation Inventory (UMI) [8] measured to capture participants' motivation to delete zombie accounts.

Construct	mean	std	Cronbach's alpha
amotivation	3.36	1.88	0.80
external regulation	2.16	1.39	0.88
introjected regulation	2.47	1.57	0.83
identified regulation	4.07	1.91	0.74
integrated regulation	3.36	1.86	0.85
intrinsic motivation	2.97	1.72	0.86



(a) Participants' perceived ability to find and delete zombie accounts



(b) Strategies for finding zombie accounts

Figure 9: Participants' estimate of needing help to delete their zombie accounts, and their ability to find zombie accounts (a) as well as their strategies to do so (b). Participants could select multiple strategies.

having sold personal information to marketers (median = *extremely serious*). Participants expected the least personal impact from receiving more spam e-mail (median = *serious*). A Friedman test shows that the items are significantly different (X^2 (4) = 54.787, $p < .001$), indicating that the participants' perception of the danger from the presented threats varies severely. A Wilcoxon signed-rank test with a Bonferroni correction specifies that the participants ranked the threat of receiving more spam e-mail significantly lower than experiencing financial loss ($z = 312.50, p < .001$), personal information sold to marketers ($z = 246.00, p < .001$), getting accounts hacked ($z = 198.00, p < .001$) or identity theft ($z = 201.5, p < .001$).

6.6.3 Motivation. Regarding the users' motivation to delete their zombie accounts, we asked participants to agree or disagree with different motivational beliefs. As shown in Figure 8, the theoretical constructs of the Protection Motivation Theory (PMT) [47, 48] have different impacts. The highest rate of agreement among the constructs of the PMT is achieved with the item on response efficacy (median = *agree*), followed by self-efficacy (median = *agree*). The maladaptive intrinsic reward received the most disagreement from the participants (median = *undecided*). This suggests that intrinsic rewards, such as saving time and energy, do not deter participants from deleting zombie accounts.

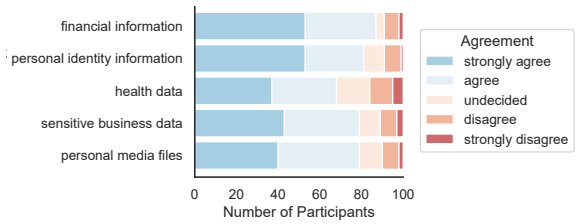
The results from the User Motivation Inventory (UMI) [8] regarding the motivation to delete zombie accounts are given in Table 3 for each of the six motivation types. With all values between 2 and 5 (values from 1 to 7 are possible due to the utilized scale), external regulation received the lowest mean, with a lower score indicating less motivation in this area. The identified regulation had the highest mean, the largest standard deviation, and the lowest Cronbach's alpha, indicating significant variations.

Answering RQ2 – Influence of Intrinsic and Extrinsic Motivation

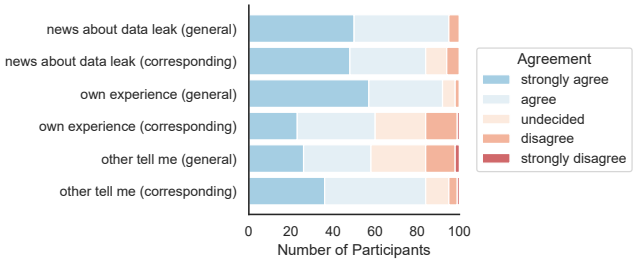
Regarding factors influencing users' decision to delete zombie accounts, we found little intrinsic motivation, but extrinsic motivation and amotivation. Extrinsic motivation is mostly regulated by identification, meaning that users accept the worth of this task for themselves. For the Protection Motivation Theory, participants reported substantial response efficacy and self-efficacy. This indicates that the participants believe they have effective strategies for dealing with their zombie accounts and can implement them.

6.6.4 Ability. Considering the perceived competence in identifying and deleting zombie accounts, the participants were overall rather confident. The Perceived Competence Scale (PCS) [61, 62] has a mean of 5.4, a standard deviation of 1.53, and a Cronbach's alpha of 0.89. Utilizing a Spearman test, we found no correlation between the number of selected accounts in either category or the participants' age with the PCS. A moderate correlation was found between the ATI and PCS ($r = .48, p < .001$) and between the SA-6 and PCS ($r = .34, p < .001$). In line with this confidence were the participants' ratings of statements about their perceived ability to find and delete zombie accounts (see Figure 9a). Participants did not feel they would need help deleting zombie accounts, nor were they unsure where to start (medians = *disagree*). A majority of participants indicated that they could think of at least one strategy to find forgotten zombie accounts (median = *agree*), and were confident in their ability to find all their zombie accounts (median = *agree*).

Regarding strategies to find forgotten zombie accounts, Figure 9b shows that most participants would look through their email client

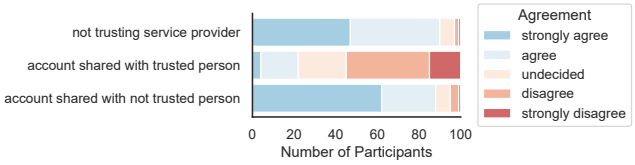


(a) Likelihood of deletion based on saved information

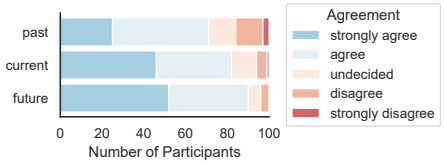


(b) Likelihood of deletion after receiving information about a leak

Figure 10: Ratings of participants' likelihood to delete zombie accounts based on (a) the specific type of information saved there, and (b) the notice on a data leak. Here we distinguish between a scenario where the notice was not connected to a certain zombie account (general) and where it was related to a specific account (corresponding).



(a) Likelihood of deleting a zombie account based on trust in service providers and people who an account is shared with.



(b) Likelihood of keeping a zombie account based on its perceived usefulness in the past, present, or future.

Figure 11: Participants' agreement to the influence of (a) trust in different entities and (b) different kinds of perceived usefulness on their wish to keep or delete a zombie account

for registration emails (n=82), followed by checking saved login credentials (n=69). The features provided by antivirus software (n=7) and closely related paid account deletion services (n=14) were the least prominent options among the participants.

6.6.5 Potential Triggers. To assess the impact of different types of information on the likelihood of deleting a zombie account, we asked participants whether certain types of information would make it more likely for them to delete a zombie account. As shown in Figure 10a, all types of information presented largely received agreement. While financial information is being agreed on by most participants (median = *strongly agree*) to increase the likelihood of deleting an account, health data received the least agreement (median = *agree*). Performing a Friedman test shows that the options are significantly different from each other (X^2 (4) = 18.408, p = .001). A Wilcoxon signed-rank test in combination with a Bonferroni correction further indicates that health data's impact as a trigger for the deletion of zombie accounts is significantly lower than that of personal identity information (z = 266.50, p = .010) or financial information (z = 83.0, p = .001).

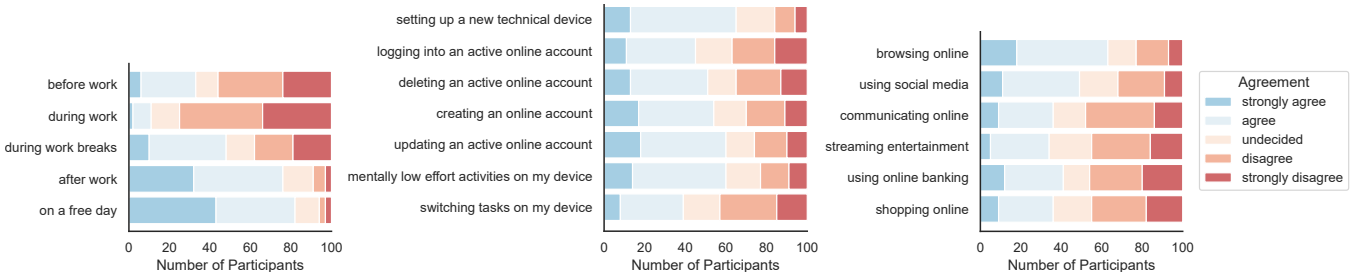
Participants stated that data breach notices might also trigger them to delete their zombie accounts. According to information from the news and their own experiences, both general notices were more likely to motivate users to delete their zombie accounts. As visualized in Figure 10b, only for the scenario where others tell the participants about a data leak on a zombie account, the corresponding notice is more likely to cause the deletion of a zombie account than a general one.

As shown in Figure 11a, also, lacking trust in the service provider (median = *agree*) as well as in a person the zombie account is shared with (median = *disagree*) increases the likelihood that the participants would delete that account. Sharing an account with a trusted person does not increase the likelihood that participants would delete a zombie account (median = *strongly agree*), highlighting the relevance of trust in this context.

6.6.6 Usefulness. Regarding the influence of perceived (potential) usefulness, the participants indicate that they would most likely want to keep an account they perceive as useful in the future (median = *strongly agree*). As shown in Figure 11b, past usefulness is a strong reason to keep a zombie account (median = *agree*), even though compared to the current (median = *agree*) and future usefulness, there is less agreement among the participants.

6.6.7 Suitable Moments. Moving forward from potential triggers toward suitable moments, participants preferred a free day (median = *agree*) over all offered options on working days. On a working day, as can be seen in Figure 12a, the time after work was preferred (median = *agree*) and deleting zombie accounts during work was rated mostly unsuitable (median = *disagree*). Regarding the temporal context, the participants slightly preferred setting up a new device (median = *agree*) and updating an online account (median = *agree*), as shown in Figure 12b. Logging into an account and switching between tasks were least preferred (medians = *undecided*).

Utilizing a Friedman test, the difference between the options is shown to be significant (X^2 (6) = 28.341, p < .001). A Wilcoxon signed-rank test in combination with a Bonferroni correction indicates the participants' agreement on switching tasks on a device is significantly lower than for setting up a new technical device (z = 182.00, p < .001), updating an active account (z = 453.50, p = .006), creating a new account (z = 328.00, p = .043), and performing mentally low effort activities on the device (z = 355.50, p = .002). The participants' agreement on the setup of a new technical device as a suitable moment to delete zombie accounts is significantly higher than logging into an active account (z = 339.00, p = .001), and deleting an active account (z = 399.00, p = .029).



(a) Parts of the day **(b) Concrete moments** **(c) Online tasks**

Figure 12: Participants' agreement to a) different parts of the day, b) different concrete moments, and c) different online tasks as suitable moments to delete a zombie account

For online tasks, most participants agreed that browsing online is preferable (median = *agree*) as a suitable moment to delete their zombie accounts. Figure 12c shows that during streaming entertainment (median = *undecided*) or shopping online (median = *undecided*), participants were less willing to deal with their zombie accounts. The differences between the tasks are significant (Friedman test: $X^2\,(5) = 33.257, p < .001$). Utilizing a Wilcoxon signed-rank test in combination with a Bonferroni correction shows that participants' agreement on browsing online as suitable moment is significantly higher than all other presented online activities (using social media ($z = 190.50, p = .033$), using online banking ($z = 358.50, p = 0.001$), shopping online ($z = 317.00, p < .001$), communicating online ($z = 429.00, p < .001$) or streaming entertainment ($z = 279.50, p < .001$)). It also indicates that participants' agreement on deleting zombie accounts during the use of social media is significantly higher than while communicating online ($z = 331.00, p = .034$), and streaming ($z = 273.00, p = .014$).

Answering RQ3 – Moments and Triggers to Encourage Deletion

According to the participants, setting up a new device, updating an active account, or browsing online are suitable moments for deleting zombie accounts. Furthermore, they preferred a free day over a working day for this task. Participants also stated that all queried information types would trigger them to delete the respective zombie account. Information on data breaches in the news, as well as personal experience, could also encourage the deletion of zombie accounts, while past, current, and especially future usefulness influenced the users' wish to keep them.

6.6.8 Feedback Preferences. To inform the design of a potential reminder, we asked participants to rate different options for such a message, including general and specific deletion instructions as well as information on the potential danger, a personalized list of zombie accounts to review, and one specific online account to consider deleting with concrete instructions. Figure 13 shows large agreement (median = *agree* for all options) with all proposed messages. Using a Friedman test, we found no significant difference between options ($X^2\,(4) = 7.353, p = .118$).

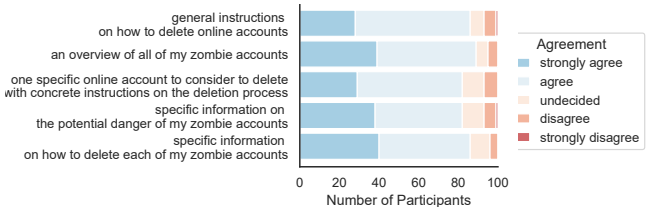


Figure 13: Participants' ratings regarding the potential contents of a reminder to delete zombie accounts

6.6.9 Notification Timing and Duration. The majority of participants would like to receive notifications to delete their zombie accounts monthly or every three months (see Figure 14a). More than a year or less than a week between reminders was unpopular.

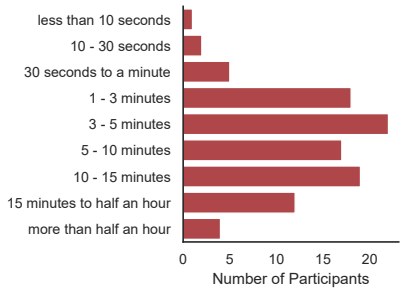
3 to 5 minutes was perceived as a reasonable duration for deleting a single account by most participants. Most selected time ranges were in the interval from 1 to 15 minutes (see Figure 14b).

Answering RQ4 – Resources and User Support

While all forms of support suggested to the participants got substantial support, most preferred a personalized list of their zombie accounts and specific information on how to delete each one. Participants would like to be reminded to delete their zombie accounts monthly or every 3 months, while for most of them, the acceptable duration for deleting a single zombie account was 1 to 15 minutes.

6.6.10 Open Feedback. 65 participants used the opportunity to comment on the questionnaire. Most feedback was positive. One participant reported technical issues, but did not specify the exact problem. Two participants commented that the questionnaire was confusing or complicated, while several others suggested further topics to investigate or described alternative strategies for dealing with zombie accounts, like manually changing the data saved within the account to nonsense instead of deleting it. Nine participants mentioned that the questionnaire triggered them to reconsider their zombie accounts and check their online security. Furthermore, participants described learning something from the questionnaire or shared experiences, like being hacked at a specific service.

(a) Time interval for reminders to delete zombie accounts



(b) Acceptable duration to delete one account

Figure 14: Participants' preferences regarding (a) the time interval of reminders as well as (b) the acceptable time commitment to delete zombie accounts.

7 Discussion

7.1 Key Findings and Design Recommendations

Liu et al. [30] found that, for mobile apps, users often have zombie accounts and wish to delete them, but are unable to do so. Our results align with those findings and support their conclusion that users' awareness should be improved and account deletion processes simplified. Our participants reported complicated procedures or hard-to-find entry points when wanting to delete an account, a phenomenon previously described by Schaffner et al. [52] and Kelly and Rubin [28]. Others have provided recommendations for service providers to improve their deletion processes [28, 30, 44, 52]. We focused on the user side of dealing with zombie accounts.

7.1.1 Participants had zombie accounts. Most users (more than 90% in each sample) reported having zombie accounts for shopping, accessing products or software, and communication. Aside from the current or future usefulness of an account, or the absence of reasons for deleting it, participants reported keeping accounts to stay connected, for memories, and to preserve the emotional value associated with the account. While these reasons may be relevant for accounts dedicated to communication, especially social media, they are arguably less relevant for accounts centered on shopping or granting access to a product or software. Further research could target those accounts with low emotional value specifically and investigate whether users are more likely or willing to delete zombie accounts in these categories compared to others.

Design Recommendation: Anticipate that users would like to keep certain zombie accounts.

To account for the diverse reasons users may have for keeping inactive accounts, provide users with an option to indicate whether they want to keep a zombie account. Also, avoid potential annoyance caused by repeated requests to delete such accounts.

7.1.2 Users underestimated the number of zombie accounts they have. Several participants believed they were using all their accounts actively and did not have any zombie accounts. Similarly, many participants estimated that they had significantly fewer zombie accounts than used ones. Even without considering forgotten zombie accounts, our lower-bound estimate shows that on average, each user has 53 zombie accounts, and around 40% of the accounts selected by the participants were also zombie accounts. Underestimating personal zombie accounts can impact the perceived danger arising from them, as an awareness of their number could also increase the perception of vulnerability and severity.

Design Recommendation: Consider that users are unaware of the number of zombie accounts they have.

Confronting users with a general estimate of zombie accounts per person or a personalized number is an opportunity to increase awareness and motivation to delete.

7.1.3 Not deleting zombie accounts is a problem of missing awareness, knowledge, and motivation. We found in the challenges study that the User Motivation Inventory (UMI) results were highest for external motivation with identified regulation. This means that the participants would delete zombie accounts because they accept the worth of this task for themselves. The scores of the integrated regulation subscale also indicate that the participants' values align with deleting zombie accounts. Nevertheless, the score for amotivation was also high, indicating that participants lacked motivation to delete their zombie accounts. This aligns with the various reasons participants mentioned for not deleting their zombie accounts. We found low perceived severity and vulnerability, which could benefit from more knowledge on potential threats, hopefully increasing the users' motivation to delete their zombie accounts. Additionally, participants' comments suggested a knowledge and awareness gap. This aligns with Liu et al. [30], who also indicated that more attention and consciousness for zombie accounts could increase the number of accounts users delete. In usable security research in general, these are common problems known for decades [1, 60]. However, we were able to characterize them in more detail for the deletion of zombie accounts.

Design Recommendation: Remind users about zombie accounts between monthly and up to every 3 months.

Some participants preferred a more frequent reminder, but most participants selected these intervals, indicating that users would at least initially accept such intervals. Future research could assess the long-term usefulness of these intervals and determine whether users would comply.

Design Recommendation: Provide users with a personalized overview of their zombie accounts and instructions on deleting each.

These two forms of assistance, which the participants favored most, can also help increase the users' awareness of their zombie accounts and provide knowledge on how to deal with them.

7.1.4 Participants were confident in their abilities to find and delete zombie accounts. We found that the average score on the Perceived Competence Scale was high (mean = 5.4), compared to the scale's range of 1 (not at all true) to 7 (very true). Participants also had high scores on the self-efficacy dimension of the PMT. Taken together, these findings show that participants felt relatively confident in their ability to find and delete zombie accounts. They reported deleting accounts in the past and facing challenges such as difficult procedures, thereby grounding the reported confidence in personal experience. Future research could determine the abilities users possess and whether they are overestimating their capabilities. Meanwhile, high self-efficacy and perceived competence are not common in usable security, where many measures and interventions fail due to a lack of users' awareness and confidence regarding the topic and the ability to perform measurements [51]. Studying the deletion of zombie accounts offers a rare opportunity to investigate the implications of existing self-efficacy and perceived competence on users' security behavior. Further insights into this topic might also help to inform other areas within usable security research on how to increase and maintain perceived competence and an adequate level of self-efficacy in the long term.

Design Recommendation: Design with users' perceived competence and self-efficacy in mind.

Based on the high confidence of users in dealing with their zombie accounts, assistance in the form of a tool could benefit substantially from maintaining and further promoting this. Both perceived competence and self-efficacy, as proposed by the Self-Determination Theory and the Protection Motivation Theory, are linked to motivation, which should be fostered accordingly to bring about a consequential change in behavior.

7.1.5 There were specific opportune moments for deleting zombie accounts. Most participants agreed on updating account information and setting up a new device as suitable moments. This insight supports the results of Parkin et al. [39] who found that the setup of a new device is a promising opportune moment for security interventions in general. Furthermore, participants preferred browsing online over other online-related tasks for deleting zombie accounts. Another time favored by the participants was during mentally low-effort tasks on their devices. This is consistent with the results reported by Iqbal and Bailey [27] and Fischer et al. [21]. Regarding potential triggers, both the sensitivity of the data and news on or experiences with data leaks were likely to increase the potential of deleting a zombie account for the participants. This could be utilized to provide effective and targeted user information.

Design Recommendation: Prompt users with reminders to delete zombie accounts while setting up a new technical device or updating an account.

Other alternatives for opportune moments would be during browsing online or mentally low-effort tasks on the user's device. If none of these moments are available or hard to identify, remind the users on a free day or after work, as these are their preferred time slots.

7.2 Implementation Opportunities

We see several opportunities for our findings and recommendations to be implemented into practical changes to benefit users. An opportunity to provide a personalized estimate of (potential) zombie accounts would be to leverage users' e-mail clients, as many service providers send links for verification purposes or provide a confirmation of the registration. When targeting accounts tied to device-specific apps (e.g., on a phone), providers like Apple and Google could leverage app usage for this purpose (similar to how Google removes permissions for unused apps[18]). An interface built on this data could provide an overview, send reminders for deletion, and offer the opportunity for whitelisting accounts that users want to keep. Reminders for deletion could also be directly sent by service providers, though this may need legal regulation, as account deletion will most likely not be in the service providers' interest. To avoid notifications and potential induced fatigue, it would also be possible to already indicate a preferred strategy for handling unused accounts during registration or sign-on. Users would further benefit from service providers avoiding, or lawmakers forbidding, deceptive designs in account deletion procedures [28, 30, 52]. For designing an easy way to delete accounts, Ramokapane and Rashid [44]'s framework for explainable deletion could be utilized.

7.3 Zombie Accounts at Discontinued Services

Within the top ten of our identified zombie accounts (Section 6.6.5) are two services that are no longer operational - the AOL/Instant Messenger, discontinued in December 2017[19], and Skype, discontinued on May 5th, 2025[20]. Although we did not query participants about their awareness of discontinued services, this raises the question of what happens with zombie accounts after a service is shut down. For example, Skype plans to delete all user accounts and associated data in January 2026 for accounts that have not been transferred by users to Microsoft Teams. However, service providers might not always be legally required to do this, especially due to

[18] Android auto-reset permissions:https://developer.android.com/about/versions/11/privacy/permissions?hl=en, last accessed February 17, 2026

[19] AOL Instant Messenger (AIM): https://aimemories.tumblr.com/post/166091776077/aimemories, last accessed February 17, 2026

[20] Skype is retiring in May 2025: https://support.microsoft.com/en-us/skype/skype-is-retiring-in-may-2025-what-you-need-to-know-2a7d2501-427f-485e-8be0-2068a9f90472, last accessed February 17, 2026

different legal regulations. Both the GDPR[21] and the CCPA[22] grant users the right to delete their data while specifying circumstances under which service providers are allowed to keep data. The CCPA in particular does not specify that user data needs to be automatically deleted after a service is shut down. If such data is kept but the related service is actually no longer accessible to users, users might be severely limited in options for deleting their accounts, while still being at risk of data leaks.

7.4 Outlook and Future Work

Building on the GDPR, the CCPA or similar data protection laws, further official regulations could improve the current state by obligating service providers to better protect users' security and privacy by automatically deleting inactive accounts after a certain period. However, currently, users themselves must take responsibility and action for deleting their zombie accounts. Research could explore the actual number of zombie accounts, including those users cannot remember, by searching for registration emails, and let users indicate the services they still use, to better assess the magnitude of this threat. Future work could correlate user characteristics, such as age, gender, technology, or security attitudes, with types of zombie accounts to gain further insights relevant to personalizing assistance. Future work could also improve the representativeness of our findings by incorporating less educated and technology-affine users, as well as investigating cultural differences. A topic of special interest, due to its potential to inform other security-related behaviors, is the high confidence and self-efficacy that participants reported in finding and deleting zombie accounts, and a comparison with actual user behavior. Building on our design recommendations, future work could also develop functional assistance, combine it with non-self-reported data, and assess its effectiveness, potentially in the long term, in the field.

8 Conclusion

Motivated by the threat posed by zombie accounts and their associated unused data, which is at risk in the event of data breaches, we investigated the deletion of zombie accounts and identified opportune moments to understand how to encourage users' deletion behavior. Within the accounts study, we prompted the participants with an account list based on JustDeleteMe and Tranco [29] to assess their zombie accounts. We found that users had zombie accounts. Prominent categories of such accounts were shopping, accessing products or software, and communication. In the challenges study, we built on these results and investigated users' experiences in deleting accounts, their attitude toward zombie accounts, self-reported motivation, and ability to find and delete zombie accounts, combined with suitable opportune moments and potential triggers. We found that users were confident in their abilities to find and delete zombie accounts, but could benefit from more awareness, knowledge, and motivation to succeed. Participants underestimated the number of zombie accounts they had, leaving them vulnerable to the threats arising from such accounts. Our findings could inform the design of a tool supporting users in deleting their zombie accounts. Our results regarding the identified opportune moments (such as setting up new devices or updating another account) and the desired frequency of reminders can provide valuable guidance for the design process.

[21] 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): https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679, last accessed February 17, 2026

[22] California Consumer Privacy Act (CCPA): https://oag.ca.gov/privacy/ccpa, last accessed February 17, 2026

Acknowledgments

We would like to thank the participants and pilot participants of both user studies. This project has been funded by the European Union – NextGeneration EU through the dtec.bw – Center for Digitization and Technology Research of the Bundeswehr as part of the projects MuQuaNet and Voice of Wisdom and by Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) as part of the Research and Training Group 2475 "Cybercrime and Forensic Computing" (grant number 393541319/GRK2475/2-2024).

References

[1] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (Dec. 1999), 40–46. doi:10.1145/322796.322806

[2] Florian Alt, Mariam Hassib, and Verena Distler. 2023. Human-centered Behavioral and Physiological Security. In *New Security Paradigms Workshop (NSPW '23)*. ACM, 48–61. doi:10.1145/3633500.3633504

[3] Steven Bellman, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse. 2004. International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society* 20, 5 (2004), 313–324. arXiv:https://doi.org/10.1080/01972240490507956 doi:10.1080/01972240490507956

[4] Sruti Bhagavatula, Lujo Bauer, and Apu Kapadia. 2020. (How) Do people change their passwords after a breach? doi:10.48550/ARXIV.2010.09853

[5] Nele Borgert, Luisa Jansen, Imke Böse, Jennifer Friedauer, M. Angela Sasse, and Malte Elson. 2024. Self-Efficacy and Security Behavior: Results from a Systematic Review of Research Methods. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24)*. ACM, 1–32. doi:10.1145/3613904.3642432

[6] Veronika Brandstätter, Julia Schüler, Rosa Maria Puca, and Ljubica Lozo. 2018. *Motivation und Emotion*. Springer Berlin Heidelberg. doi:10.1007/978-3-662-56685-5

[7] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101. arXiv:https://doi.org/10.1191/1478088706qp063oa doi:10.1191/1478088706qp063oa

[8] Florian Brühlmann, Beat Vollenwyder, Klaus Opwis, and Elisa D. Mekler. 2018. Measuring the "Why" of Interaction: Development and Validation of the User Motivation Inventory (UMI). In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–13. doi:10.1145/3173574.3173680

[9] Kelly Caine. 2016. Local Standards for Sample Size at CHI. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 981–992. doi:10.1145/2858036.2858498

[10] Claire C Chen, Dillon Shu, Hamsini Ravishankar, Xinran Li, Yuvraj Agarwal, and Lorrie Faith Cranor. 2024. Is a Trustmark and QR Code Enough? The Effect of IoT Security and Privacy Label Information Complexity on Consumer Comprehension and Behavior. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 832, 32 pages. doi:10.1145/3613904.3642011

[11] Xiaowei Chen, Lorin Schöni, Verena Distler, and Verena Zimmermann. 2025. Beyond Deterrence: A Systematic Review of the Role of Autonomous Motivation in Organizational Security Behavior Studies. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. ACM, 1–28. doi:10.1145/3706598.3713122

[12] Edward L. Deci and Richard M. Ryan. 1980. *The Empirical Exploration of Intrinsic Motivational Processes*. Elsevier, 39–80. doi:10.1016/s0065-2601(08)60130-6

[13] Edward L. Deci and Richard M. Ryan. 2002. Overview of Self-Determination Theory. *Handbook of self-determination research* (2002), 3 – 33.

[14] Sarah Delgado Rodriguez, Priyasha Chatterjee, Anh Dao Phuong, Florian Alt, and Karola Marky. 2024. Do You Need to Touch? Exploring Correlations between Personal Attributes and Preferences for Tangible Privacy Mechanisms. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*

(Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 981, 23 pages. doi:10.1145/3613904.3642863

[15] Jing Deng, Xiaoli Gao, and Chunyue Wang. 2016. Using Bi-level Penalized Logistic Classifier to Detect Zombie Accounts in Online Social Networks. In *Proceedings of the Fifth International Conference on Network, Communication and Computing* (Kyoto, Japan) *(ICNCC '16)*. Association for Computing Machinery, New York, NY, USA, 126–130. doi:10.1145/3033288.3033349

[16] Benjamin D. Douglas, Patrick J. Ewell, and Markus Brauer. 2023. Data quality in online human-subjects research: Comparisons between MTurk, Prolific, CloudResearch, Qualtrics, and SONA. *PLoS ONE* 18, 3 (March 2023), e0279720. doi:10.1371/journal.pone.0279720

[17] Janna Lynn Dupree, Richard Devries, Daniel M. Berry, and Edward Lank. 2016. Privacy Personas: Clustering Users via Attitudes and Behaviors toward Security Practices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5228–5239. doi:10.1145/2858036.2858214

[18] Nicola Döring and Jürgen Bortz. 2015. *Forschungsmethoden und Evaluation* (5 ed.). Springer-Verlag GmbH.

[19] Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 2873–2882. doi:10.1145/2702123.2702249

[20] Cori Faklaris, Laura Dabbish, and Jason Hong. 2019. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Berkeley, CA, Santa Clara, CA, USA. doi:10.13140/RG.2.2.29840.05125/3

[21] Joel E. Fischer, Chris Greenhalgh, and Steve Benford. 2011. Investigating episodes of mobile phone activity as indicators of opportune moments to deliver notifications. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services (MobileHCI '11)*. ACM. doi:10.1145/2037373.2037402

[22] Donna L. Floyd, Steven Prentice-Dunn, and Ronald W. Rogers. 2000. A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology* 30, 2 (Feb. 2000), 407–429. doi:10.1111/j.1559-1816.2000.tb02323.x

[23] Jon Fraenkel and Bernard Grofman. 2014. The Borda Count and its real-world alternatives: Comparing scoring rules in Nauru and Slovenia. *Australian Journal of Political Science* 49, 2 (2014), 186–205. doi:10.1080/10361146.2014.900530

[24] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A Personal Resource for Technology Interaction: Development and Validation of the Affinity for Technology Interaction (ATI) Scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467. doi:10.1080/10447318.2018.1456150

[25] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. "It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. ACM. doi:10.1145/3313831.3376511

[26] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2019. An Empirical Analysis of Data Deletion and {Opt-Out} Choices on 150 Websites. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS'19)*. USENIX Association, USA, 387–406.

[27] Shamsi T. Iqbal and Brian P. Bailey. 2005. Investigating the effectiveness of mental workload as a predictor of opportune moments for interruption. In *CHI'05 extended abstracts on Human factors in computing systems*. 1489–1492. doi:10.1145/1056808.1056948

[28] Dominique Kelly and Victoria L. Rubin. 2024. Identifying Dark Patterns in User Account Disabling Interfaces: Content Analysis Results. *Social Media + Society* 10, 1 (Jan. 2024). doi:10.1177/20563051231224269

[29] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczynski, and Wouter Joosen. 2019. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In *Proceedings 2019 Network and Distributed System Security Symposium (NDSS 2019)*. Internet Society. doi:10.14722/ndss.2019.23386

[30] Yijing Liu, Yan Jia, Qingyin Tan, Zheli Liu, and Luyi Xing. 2022. How Are Your Zombie Accounts? Understanding Users' Practices and Expectations on Mobile App Account Deletion. In *31st USENIX Security Symposium (USENIX Security 22)*. 863–880.

[31] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355. https://www.jstor.org/stable/23015787

[32] Davit Marikyan and Savvas Papagiannidis. 2023. *Protection Motivation Theory: A review*. 78–93.

[33] Peter Mayer, Yixin Zou, Byron M. Lowens, Hunter A. Dyer, Khue Le, Florian Schaub, and Adam J. Aviv. 2023. Awareness, Intention, (In)Action: Individuals' Reactions to Data Breaches. *ACM Transactions on Computer-Human Interaction* 30, 5 (Sept. 2023), 1–53. doi:10.1145/3589958

[34] Peter Mayer, Yixin Zou, Florian Schaub, and Adam J. Aviv. 2021. "Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 393–410. https://www.usenix.org/conference/usenixsecurity21/presentation/mayer

[35] Ambar Murillo, Andreas Kramm, Sebastian Schnorf, and Alexander De Luca. 2018. "If I press delete, it's gone"- User Understanding of Online Data Deletion and Expiration. In *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security* (Baltimore, MD, USA) *(SOUPS '18)*. USENIX Association, USA, 329–339.

[36] Doruntina Murtezaj, Viktorija Paneva, Verena Distler, and Florian Alt. 2024. Public Security User Interfaces: Supporting Spontaneous Engagement with IT Security. In *Proceedings of the New Security Paradigms Workshop (NSPW '24)*. ACM, 56–70. doi:10.1145/3703465.3703470

[37] Marek Muszyński. 2023. Attention checks and how to use them: Review and practical recommendations. *Ask: Research and Methods* 32, 1 (2023), 3–38. doi:10.18061/ask.v32i1.0001

[38] Stefan Palan and Christian Schitter. 2018. Prolific.ac—A subject pool for online experiments. *Journal of Behavioral and Experimental Finance* 17 (March 2018), 22–27. doi:10.1016/j.jbef.2017.12.004

[39] Simon Parkin, Elissa M. Redmiles, Lynne Coventry, and M. Angela Sasse. 2019. Security When it is Welcome: Exploring Device Purchase as an Opportune Moment for Security Behavior Change. In *Proceedings 2019 Workshop on Usable Security (USEC 2019)*. Internet Society. doi:10.14722/usec.2019.23024

[40] Eyal Peer, David Rothschild, Andrew Gordon, Zak Evernden, and Ekaterina Damer. 2021. Data quality of platforms and panels for online behavioral research. *Behavior Research Methods* 54, 4 (Sept. 2021), 1643–1662. doi:10.3758/s13428-021-01694-3

[41] Dulce G. Pereira, Anabela Afonso, and Fátima Melo Medeiros. 2014. Overview of Friedman's Test and Post-hoc Analysis. *Communications in Statistics - Simulation and Computation* 44, 10 (Aug. 2014), 2636–2653. doi:10.1080/03610918.2014.931971

[42] Susanne Poeller and Cody J. Phillips. 2022. Self-Determination Theory — I Choose You!: The Limitations of Viewing Motivation in HCI Research Through the Lens of a Single Theory. In *Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play (CHI PLAY '22)*. ACM, 261–262. doi:10.1145/3505270.3558361

[43] Sarah Prange, Niklas Thiem, Michael Fröhlich, and Florian Alt. 2022. "Secure settings are quick and easy!" – Motivating End-Users to Choose Secure Smart Home Configurations. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces (AVI 2022)*. ACM, 1–9. doi:10.1145/3531073.3531089

[44] Kopo Marvin Ramokapane and Awais Rashid. 2023. ExD: Explainable Deletion. In *New Security Paradigms Workshop (NSPW '23)*. ACM. doi:10.1145/3633500.3633503

[45] Kopo M. Ramokapane, Awais Rashid, and Jose M. Such. 2017. "I feel stupid i can't delete...": a study of users' cloud deletion practices and coping strategies. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS '17)*. USENIX Association, USA, 241–256.

[46] Felix Reichmann, Annalina Buckmann, Konstantin Fischer, M. Angela Sasse, and Alena Naiakshina. 2025. Bridging the Gap Between Usable Security Research and Open-Source Practice - Lessons From a Long-Term Engagement With VeraCrypt. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 911, 21 pages. doi:10.1145/3706598.3713983

[47] Ronald W. Rogers. 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology* 91, 1 (1975), 93–114. doi:10.1080/00223980.1975.9915803 PMID: 28136248.

[48] Ronald W. Rogers. 1983. Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social Psychophysiology: A Sourcebook* (1983), 153 – 177.

[49] R. M. Ryan, J. P. Connell, and E. L. Deci. 1985. A motivational analysis of self-determination and self-regulation in education. *Research on motivationin education: The classroom milieu* (1985), 13 – 51.

[50] Richard M. Ryan and Edward L. Deci. 2019. *Brick by Brick: The Origins, Development, and Future of Self-Determination Theory*. Elsevier, 111–156. doi:10.1016/bs.adms.2019.01.001

[51] M. Angela Sasse, Jonas Hielscher, Jennifer Friedauer, and Annalina Buckmann. 2023. *Rebooting IT Security Awareness – How Organisations Can Encourage and Sustain Secure Behaviours*. Springer International Publishing, 248–265. doi:10.1007/978-3-031-25460-4_14

[52] Brennan Schaffner, Neha A. Lingareddy, and Marshini Chetty. 2022. Understanding account deletion and relevant dark patterns on social media. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–43. doi:10.1145/3555142

[53] Lorin Schöni, Martin Strohmeier, Ivo Sluganovic, and Verena Zimmermann. 2025. Stop the Clock - Counteracting Bias Exploited by Attackers through an Interactive Augmented Reality Phishing Training. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 594, 23 pages. doi:10.1145/3706598.3714023

[54] Peter Sedlmeier and Frank Renkewitz. 2018. *Forschungsmethoden und Statistik für Psychologen und Sozialwissenschaftler* . Pearson Deutschland. 1.120 pages. https://elibrary.pearson.de/book/99.150005/9783863268084

[55] Gaurav Sood and Ken Cor. 2019. Pwned: The Risk of Exposure From Data Breaches. In *Proceedings of the 10th ACM Conference on Web Science (WebSci '19)*. ACM, 289–292. doi:10.1145/3292522.3326046

[56] Anne M. Turner, Thomas Engelsma, Jean O. Taylor, Rashmi K. Sharma, and George Demiris. 2021. Recruiting older adult participants through crowdsourcing platforms: Mechanical Turk versus Prolific Academic. In *AMIA annual symposium proceedings*, Vol. 2020. 1230.

[57] April Tyack and Elisa D. Mekler. 2020. Self-Determination Theory in HCI Games Research: Current Uses and Open Questions. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. ACM, 1–22. doi:10.1145/3313831.3376723

[58] April Tyack and Elisa D. Mekler. 2024. Self-Determination Theory and HCI Games Research: Unfulfilled Promises and Unquestioned Paradigms. *ACM Transactions on Computer-Human Interaction* 31, 3 (June 2024), 1–74. doi:10.1145/3673230

[59] Karen D. Wang, Zhongzhou Chen, and Carl Wieman. 2024. Can Crowdsourcing Platforms Be Useful for Educational Research?. In *Proceedings of the 14th Learning Analytics and Knowledge Conference* (Kyoto, Japan) *(LAK '24)*. Association for Computing Machinery, New York, NY, USA, 416–425. doi:10.1145/3636555.3636897

[60] Alma Whitten and J. D. Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *8th USENIX Security Symposium (USENIX Security 99)*. USENIX Association, Washington, D.C. https://www.usenix.org/conference/8th-usenix-security-symposium/why-johnny-cant-encrypt-usability-evaluation-pgp-50

[61] Geoffrey C. Williams and Edward L. Deci. 1996. Internalization of biopsychosocial values by medical students: a test of self-determination theory. *Journal of personality and social psychology* 70, 4 (1996), 767.

[62] Geoffrey C. Williams, Zachary R. Freedman, and Edward L. Deci. 1998. Supporting Autonomy to Motivate Patients With Diabetes for Glucose Control. *Diabetes Care* 21, 10 (Oct. 1998), 1644–1651. doi:10.2337/diacare.21.10.1644

[63] Maximiliane Windl, Philipp Thalhammer, David Müller, Albrecht Schmidt, and Sebastian S. Feger. 2025. PrivacyHub: A Functional Tangible and Digital Ecosystem for Interoperable Smart Home Privacy Awareness and Control. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 942, 15 pages. doi:10.1145/3706598.3713517

[64] Jerrold H. Zar. 2005. Spearman Rank Correlation. *Encyclopedia of Biostatistics* (Feb. 2005). doi:10.1002/0470011815.b2a15150

[65] Yixin Zou, Khue Le, Peter Mayer, Alessandro Acquisti, Adam J. Aviv, and Florian Schaub. 2024. Encouraging Users to Change Breached Passwords Using the Protection Motivation Theory. *ACM Transactions on Computer-Human Interaction* 31, 5 (Oct. 2024), 1–45. doi:10.1145/3689432

A Concerning Motivation Theories

Motivation impacts everyday life as the force that "drives all intentional behavior" [8]. Therefore, it is no surprise that interest in this research topic can be traced back to many classical psychological approaches at the beginning of the 20th century [6]. In the last century, motivational research has dealt with various types of motivation (e.g., achievement motivation and affiliation motivation) and has produced a variety of theories. To do justice to this diversity, enrich our perspective on the topic, and following the recommendation from Chen et al. [11], we utilize two motivation theories in this work. For insights into extrinsic and intrinsic motivation, we use the Organismic Integration Theory (Section A.1). Furthermore, we use the Protection Motivation Theory (Section A.2) to include threat perception in the context of motivation. Below, we provide explanations for these two theories.

A.1 Organismic Integration Theory

The Organismic Integration Theory (OIT) [49] is a sub-theory of the Self-Determination Theory (SDT) [12]. Highly influential in psychology and HCI [11, 42], the meta-theory SDT centers around the needs for autonomy, competence, and relatedness, that are considered as inherently human within this theory, and states that motivation and well-being originate from fulfilling those needs[23].

Building on this foundation, the OIT understands motivation as a continuum of different degrees of internalization between amotivation on the one end and intrinsic motivation on the other. In between, four subtypes of extrinsic motivation can be distinguished by the amount of internalization: external, introjected, identified, and integrated. The amount of internalization also describes how autonomous the person will behave [13]. In literature, the term autonomous behavior is used to sum up a broader type of motivation, capturing more than intrinsic motivation as it includes identified and integrated regulation [11, 50]. Furthermore, internalization is a process that can be enhanced by fulfilling the needs for autonomy, competence, and relatedness, while non-fulfillment of these needs can lead to stagnation of internalization and, in the absence of external motivators, to amotivation [50]. An overview of the theory is provided in Figure 15.

Regarding the meaning of the terms, Ryan and Deci [50] describe amotivation as the absence of motivation. According to them, intrinsic motivation is about finding a behavior interesting and enjoyable, and extrinsic motivation is defined "as instrumental motivation, and thus concerns all activities aimed at achieving outcomes separable from the behavior itself" [50]. This instrumental motivation can be:

- Externally regulated, which means "extrinsically motivated due to external pressures, reward contingencies, or coercion" [50].
- Regulated by introjection, meaning it "concerns behaviors driven by internally controlling pressures and regulations" [50].
- Regulated by identification, which implies the individual "consciously accepts the worth and value of the activity" [50].
- Integrated regulated, which indicates being in line "with the individuals' other values and identifications, allowing a full endorsement" [50].

To measure these different forms of motivation proposed by the OIT for technology use, Brühlmann et al. [8] present the User Motivation Inventory (UMI).

However, there is also criticism of the current use of SDT in HCI. Poeller and Phillips [42] point out that even though the SDT is a solid foundation for research, its frequent usage in HCI has limited the perspective on the topic of motivation. They, therefore, propose some alternative theories that could also be included in research to address this. Tyack and Mekler [57, 58] demonstrate the holistic use of the SDT so far in HCI literature, mostly concerning research on play and games. They highlight that many authors use SDT as an explanation, but do not provide a corresponding description of what they mean when using certain terms. Moreover, HCI researchers often do not use a corresponding mini-theory and remain vague in their statements.

A.2 Protection Motivation Theory

Rogers [47] presented the Protection Motivation Theory (PMT) in 1975 and revised it in 1983 to incorporate self-efficacy [48]. Initially developed for health research and widely used in several other research areas [32], it has also become very popular in usable security research for designing nudges or explaining behavior [43, 65].

The theory aims to explain pursuing maladaptive behavior or adopting adaptive behavior while facing a threat by stating two cognitive processes: threat appraisal and coping appraisal. These two components are common among all versions of the theory, even though some include or leave out different subparts [32]. We utilize the core parts of PMT similar to Zou et al. [65] in their work on motivating users to change breached passwords. Furthermore, we include intrinsic and extrinsic rewards [22] like Prange et al. [43], motivating users to choose secure smart home configurations.

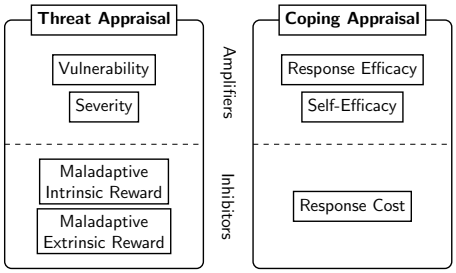


Figure 16: Overview of the constructs within the PMT

In the PMT, within the threat appeal a person evaluates the perceived severity of the threat for oneself, and perceived vulnerability, so how likely one will be affected by the threat. As shown in Figure 16, intrinsic and extrinsic rewards for the maladaptive behavior, like confirmation by a peer group, will inhibit the motivation arising from the threat appeal. The second process, the coping appeal, depends on the response efficacy and self-efficacy and is inhibited by the response cost. The response efficacy is the

[23] Center for Self-Determination Theory: https://selfdeterminationtheory.org/the-theory/, last accessed February 17, 2026

Type of Motivation	Amotivation	Extrinsic Motivation				Intrinsic Motivation
Type of Regulation	Non-regulation	External Regulation	Introjected Regulation	Identified Regulation	Integrated Regulation	Intrinsic Regulation

Figure 15: The continuum of internalization as proposed in the OIT (adapted from Deci and Ryan [13] and Brühlmann et al. [8])

assessment of whether a certain strategy will be an effective measure against the threat. The response costs are the resources (e.g., time, effort) needed to carry out that behavior. Finally, self-efficacy is described as the users' confidence in their ability to perform the adaptive behavior [32]. Notable here is the huge interest of the usable security research community in the concept of self-efficacy [5], demonstrating its impact aside from the PMT.

B Resulting List of Zombie Accounts of the Accounts Study

Overview of services selected at least by 20% of the respective participants as zombie accounts with the assigned categories, absolute and relative to group size click rates for the categories surveyed.

Service	Category	known		account		zombie	
		abs	rel	abs	rel	abs	rel
Instagram	Social Media	9	0.9	8	0.8	2	0.2
MySpace	Social Media	6	0.6	2	0.2	2	0.2
Shopify	(Software) Product	9	0.9	2	0.2	2	0.2
Upwork	Service/ Product Offer	9	0.9	3	0.3	2	0.2
1xBet	Entertainment	5	0.5	3	0.3	2	0.2
Disney+	Streaming	7	0.7	6	0.6	2	0.2
ESPN	Streaming	7	0.7	3	0.3	2	0.2
Lyft	Service/ Product Offer	5	0.5	3	0.3	2	0.2
Pandora	Shopping	4	0.4	2	0.2	2	0.2
Photomath	Education	3	0.3	2	0.2	2	0.2
Quizlet	Education	3	0.3	2	0.2	2	0.2
AOL/ Instant Messenger	Communication	5	0.5	2	0.2	2	0.2
Avast!	Security	5	0.5	5	0.5	2	0.2
Indeed	Search Engine	9	0.9	6	0.6	2	0.2
Nextdoor	Social Media	5	0.5	3	0.3	2	0.2
Temu	Shopping	5	0.5	3	0.3	2	0.2
TextNow	Communication	3	0.3	3	0.3	2	0.2
Apple ID/ iTunes	(Software) Product	8	0.8	7	0.7	2	0.2
AT&T	Communication	4	0.4	2	0.2	2	0.2
Blue Apron	Shopping	6	0.6	2	0.2	2	0.2
Facebook Messenger	Communication	8	0.8	8	0.8	2	0.2
Marriott	Shopping	3	0.3	2	0.2	2	0.2
McAfee	Security	7	0.7	4	0.4	2	0.2
PlayStation Network	(Software) Product	7	0.7	4	0.4	2	0.2
Tinder	Dating	6	0.6	3	0.3	2	0.2
Western Union	Finance	6	0.6	4	0.4	2	0.2
Xfinity	Communication	6	0.6	4	0.4	2	0.2
Zappos	Shopping	5	0.5	3	0.3	2	0.2
About.me	(Software) Product	5	0.5	2	0.2	2	0.2
AVG	Security	2	0.2	2	0.2	2	0.2
Bank Of America	Finance	8	0.8	4	0.4	2	0.2
GasBuddy	Recommendation/ Discount	5	0.5	4	0.4	2	0.2
GoDaddy	(Software) Product	8	0.8	4	0.4	2	0.2
hCaptcha	(Software) Product	6	0.6	2	0.2	2	0.2

Continuation:

Service	Category	known		account		zombie	
		abs	rel	abs	rel	abs	rel
TED	Streaming	6	0.6	5	0.5	2	0.2
Uber	Service/ Product Offer	9	0.9	6	0.6	2	0.2
Yelp	Recommendation/ Discount	7	0.7	5	0.5	2	0.2
Chewy	Shopping	5	0.5	3	0.3	2	0.2
Dashlane	Security	2	0.2	2	0.2	2	0.2
discovery+	Streaming	6	0.6	3	0.3	2	0.2
Netgear	Shopping	4	0.4	2	0.2	2	0.2
Square	Finance	4	0.4	2	0.2	2	0.2
T-Mobile	Communication	9	0.9	4	0.4	2	0.2
GameStop	Shopping	5	0.56	3	0.33	2	0.22
Quora	Recommendation/ Discount	5	0.56	3	0.33	2	0.22
Shazam	(Software) Product	6	0.67	4	0.44	2	0.22
Dropbox	(Software) Product	5	0.56	3	0.33	2	0.22
Groupon (Worldwide)	Recommendation/ Discount	5	0.56	4	0.44	2	0.22
Classmates	Social Media	3	0.33	2	0.22	2	0.22
Comcast	Communication	6	0.67	2	0.22	2	0.22
Logo Maker	(Software) Product	2	0.22	2	0.22	2	0.22
Walmart Canada	Shopping	6	0.67	2	0.22	2	0.22
Zoom	Communication	9	1.0	8	0.89	2	0.22
McDonald's	Shopping	10	0.91	5	0.45	3	0.27
Opera	(Software) Product	9	0.82	6	0.55	3	0.27
Plenty of Fish	Dating	4	0.36	3	0.27	3	0.27
Activision	Gaming	4	0.36	3	0.27	3	0.27
Barnes & Noble	Shopping	8	0.73	3	0.27	3	0.27
Bing	Search Engine	9	0.82	3	0.27	3	0.27
Pokemon GO	Gaming	5	0.45	3	0.27	3	0.27
Ticketmaster	Shopping	9	0.82	5	0.45	3	0.27
TripAdvisor	Recommendation/ Discount	9	0.82	3	0.27	3	0.27
Tubi	Streaming	5	0.45	5	0.45	3	0.27
Wish	Shopping	5	0.45	3	0.27	3	0.27
WordPress.com	(Software) Product	6	0.55	3	0.27	3	0.27
Experian	(Software) Product	7	0.64	4	0.36	3	0.27
iHeart	Entertainment	9	0.82	3	0.27	3	0.27
Rakuten	Recommendation/ Discount	6	0.55	5	0.45	3	0.27
Adobe	(Software) Product	8	0.8	5	0.5	3	0.3
PornHub	Adult Content	7	0.7	3	0.3	3	0.3
Acer	(Software) Product	5	0.5	3	0.3	3	0.3
Acorns	Finance	5	0.5	4	0.4	3	0.3
HBO Max	Streaming	7	0.7	6	0.6	3	0.3
OnlyFans	Adult Content	9	0.9	3	0.3	3	0.3
Peacock	Streaming	8	0.8	7	0.7	3	0.3
Skype	Communication	8	0.8	6	0.6	3	0.3
Best Buy	Shopping	6	0.67	4	0.44	3	0.33
Craigslist	Service/ Product Offer	6	0.67	4	0.44	3	0.33
AliExpress	Shopping	6	0.67	3	0.33	3	0.33
Roku	Shopping	7	0.64	4	0.36	4	0.36
LinkedIn	Social Media	7	0.7	6	0.6	4	0.4
Hotmail	Communication	8	0.8	5	0.5	4	0.4
Yahoo!	Search Engine	7	0.78	6	0.67	4	0.44
Robinhood	Finance	7	0.78	5	0.56	4	0.44
eBay	Service/ Product Offer	10	0.91	6	0.55	5	0.45
Google Pay	Finance	11	1.0	9	0.82	5	0.45
Starbucks	Shopping	10	0.91	7	0.64	5	0.45
Coinbase	Finance	8	0.89	7	0.78	5	0.56
Pinterest	Social Media	9	0.9	9	0.9	6	0.6