Used, Avoided, Restricted? Perceptions, Behavior, and Changes in Video Conferencing of German-speaking Users During and After the Pandemic

Lydia Weinberger
lydia.weinberger@fau.de
Friedrich-Alexander-Universität
Erlangen-Nürnberg (FAU)
Erlangen, Germany

Christian Eichenmüller
christian.eichenmueller@fau.de
Friedrich-Alexander-Universität
Erlangen-Nürnberg (FAU)
Erlangen, Germany

Freya Gassmann
freya.gassmann@rptu.de
Rheinland-Pfälzische Technische
Universität Kaiserslautern
Landau (RPTU)
Kaiserslautern, Germany

Gaston Pugliese
gaston.pugliese@cs.fau.de
Friedrich-Alexander-Universität
Erlangen-Nürnberg (FAU)
Erlangen, Germany

Zinaida Benenson
zinaida.benenson@fau.de
Friedrich-Alexander-Universität
Erlangen-Nürnberg (FAU)
Erlangen, Germany

ABSTRACT

The COVID-19 pandemic required a sudden deployment of video conferencing (VC) in work and social environments. A few months after contact restrictions were lifted, we conducted an exploratory online survey with 251 German-speaking participants and investigated perceptions, behavior, and changes in the use of VC apps. Particularly, we considered security, privacy, usability, and familiarity of ten popular VC apps and how these factors influenced behavior during and after the lockdown. We showed significant dependencies between the usability and security perception of ten well-known VC apps. While perceived usability was significantly correlated with familiarity in most cases, we were only able to show a connection between familiarity and security perception for some of these applications. Usability played the greatest role in deciding to use an app. Yet, depending on the app, security had a significant influence as well. A lack of usability and security also played an important role in the avoidance of apps, but the influence of third-party decisions to restrict the use was the most significant. A lack of autonomy in app usage sometimes led to the use of apps that were associated with security concerns. In some cases, uncomfortable experiences and incidents triggered by the incorrect use of functions, e.g., activating audio by mistake, led to more extensive protective measures. Participants generally perceived threats from other attendees as more realistic than from external attackers.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; **Privacy protections**.

KEYWORDS

video conferencing, UCC, UC, online meeting, privacy, security, usability, user study, survey

ACM Reference Format:
Lydia Weinberger, Christian Eichenmüller, Freya Gassmann, Gaston Pugliese, and Zinaida Benenson. 2024. Used, Avoided, Restricted? Perceptions, Behavior, and Changes in Video Conferencing of German-speaking Users During and After the Pandemic. In *The 2024 European Symposium on Usable Security (EuroUSEC 2024), September 30-October 1, 2024, Karlstad, Sweden.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3688459.3688478

EuroUSEC 2024, September 30-October 1, 2024, Karlstad, Sweden

ACM ISBN 979-8-4007-1796-3/24/09
https://doi.org/10.1145/3688459.3688478

1 INTRODUCTION

In spring 2020, the global lockdown was brought about by the COVID-19 pandemic. Contact restrictions [45] led to a sudden deployment of online meetings in work and social environments. The use of video conferencing (VC) apps, also called Unified Communications and Collaboration (UCC[1]) apps, massively increased. Globally, the market for corresponding apps grew by 24, 9% [50]. Zoom, for example, had 10 million daily meeting participants at the end of 2019. The following year, this number had increased to 300 million [47]. During this period, security incidents and intrusions into users' privacy also increased.

Especially Zoom, as the most popular VC app, was often attacked. With Zoom bombing, unauthorized persons were able to break into ongoing conferences by guessing the meeting IDs [30], and videos of embarrassing Zoom incidents surfaced on the Internet [2]. When using the iOS version of the software, users' personal data was forwarded to Facebook [53]. Kagan et al. [23] showed how to extract personal information from images of Zoom meetings shared on the web and linked it with other available information, e.g., from social networks. A vulnerability allowed a customized version of Zoom's invitation links to be faked [21]. Zoom also falsely claimed to use end-to-end (E2E) encryption, although at that time only transport encryption was guaranteed [15]. In 2021-2022, a security gap in

[1]UCC integrates communication and collaboration methods (instant messaging, video conferencing, screen sharing, virtual whiteboards, etc.) into a single interface [22].

the auto-update process allowed to seize root privileges via Zoom Client for macOS [34].

Other VC apps also had serious security and privacy incidents. Activating the mute button on Webex did not prevent the transmission of audio data to the provider's telemetry server [51]. Microsoft employed human analysts who used voice recordings from Skype calls to improve their voice services [29]. MS Teams was also not immune to critical vulnerabilities, such as allowing malicious code to be injected via the platform's chat messages, thereby jeopardizing the security of the entire system [48]. Even the use of open-source software is no guarantee of seamless security and privacy. For example, when installing Jitsi with docker containers, the standard password "passw0rd" was used for internal XMPP accounts, enabling unauthorized access from outside [33].

New threats related to AI are also emerging. In summer of 2022, e.g., at least three high-ranking European politicians, incl. the mayors of Berlin, Madrid, and Vienna, were deceived by a deepfake pretending to be the mayor of Kyiv [4, 6].

Motivation. The discovery of security-related vulnerabilities in VC apps partially led to apps being improved, with some now offering security and privacy features [52]. Yet, it remains unclear to what extent these measures are used and whether usability restrictions are accepted in favor of increased protection. In most cases, the secure use of VC seems to represent a trade-off between security, privacy and usability [17]. This led us to the following research questions:

RQ1: To what extent do perceptions of security, privacy, and usability influence each other when using VC apps?

RQ2: Which factors influence behavioral changes in usage of VC apps *during* and *after* the COVID-19 pandemic?

RQ3: How does the perception of security and privacy threats to VC apps affect usage behavior?

Contributions. Using an online survey with 251 participants conducted from August to October 2022, we took an exploratory approach and were the first to consider not only the exceptional situation with online meetings during the pandemic, but also the transition to normality afterwards. While VC apps are now part of everyday life, our study period is characterized by the fact that the participants – shortly after the end of the lockdown – still vividly remembered their (often first-time) participation in video conferences and the associated challenges during the pandemic. At the same time, we were able to capture the experience of a new everyday life with these VC apps and identify factors influencing behavior in the usage *during* and *after* the pandemic. Our contributions are as follows:

(1) We show that usage of Skype, which is closer to Unified Communications (UC [2]) due to a lack of collaboration options, was overtaken by VC apps such as Zoom and MS Teams with a larger variety of features (see Figure 2, Section 4.1).
(2) By correlating ratings of ten popular VC apps, we assess the interplay between security, privacy, and usability (Figure 3), and find strong significant correlations between these factors for almost all apps.
(3) Familiarity also had a strong significant influence on the usability perception of these apps, but contrary to expectations from related work [13], we found that familiarity played only a minor role in influencing perceptions of security and privacy of a VC app (see Table 2).
(4) For some apps (e.g., Zoom, MS Teams, Discord, Skype for Business, Jitsi, BigBlueButton), we were able to show a significant correlation between actively choosing to use them and their security perceptions, but for most participants, usability was most important when deciding for an app (see Table 3).
(5) Using linear regression, we show behavioral changes in usage during and after the pandemic. We found that a lack of usability and also security concerns weighed heavily in the avoidance of apps, though we registered the greatest influence from the decisions of third parties (e.g., employers) to restrict usage (see Table 4, Section 4.4.1).
(6) A lack of decision-making autonomy sometimes led to the use of VC apps that were associated with security concerns (see Section 4.5.1). We found that participants felt particularly threatened by malicious intent within a conference (e.g., recordings by other conference attendees) rather than threats from outside (e.g., privilege escalation, see Section 4.7.1). This was also reflected in the protective measures they took (e.g., (de)activating audio/video on demand, see Section 4.6).
(7) The extent of protective measures taken by participants (see Table 5) was significantly determined by the knowledge of issues about the security and privacy of apps, as well as by incidents that the participants had experienced through the incorrect use of functions (e.g., accidentally activate audio).

Outline. First, we review related work in Section 2. In Section 3, we explain our methodology regarding survey procedure, demographics, recruitment of our participants, ethics, and data analysis. In Section 4, we present our results, including the different periods of usage, threats to VCs, the interplay between security, privacy, and usability factors, as well as usage patterns. Finally, we discuss our results in Section 5 and conclude the paper in Section 6.

2 RELATED WORK

Emami-Naeini et al. [13] conducted a global online survey in 2020 focusing on a deep understanding of users' behaviors, attitudes, and concerns while using VC. For this purpose, the 220 participants were surveyed about three different modes of remote communication: learning, working, and socializing from home. They described their work as "the first paper to study remote communications at the transition of the pandemic".

During the pandemic, there was a particular research focus on the use of VC systems in health-related [3, 26] and educational environments [31, 49]. In user stories by Prange et al. [35], 140 participants presented incidents that involved information disclosure from private living spaces. Sandhu et al. [40] evaluated a structural equation model with 484 professionals and provided insights into compromises users are willing to make towards privacy concerns while using VC apps in a work-related context. Based on semi-structured interviews after the pandemic, Reisinger et al. [38] addressed the question which solutions from the field of UC are

[2]UC combine different media channels, but do not have collaboration capabilities. Examples include well-known instant messengers such as WhatsApp and Signal. [37]

suitable for digital activists. With regard to a user-centered perspective, we mainly refer to Emami-Naeini et al. [13], as the focus of other studies was less broad, focusing on unpleasant incidents [35], or concentrating only on one context or specific user group [38, 40].

From a technical perspective, Maleckas et al. [27] provided an in-depth analysis of Jitsi's cryptography and design of the platform, and pointed out that there is "surprisingly little technical security analysis of VC systems". Hasan and Hasan [19] created a generalized threat model for VC apps using STRIDE [20, 42]. Reisinger et al. [37] also used STRIDE in their systematic security analysis of ten popular UC systems and supplemented their security threat model with LINDDUN [11], which addresses privacy threats. The versatility of UCC technologies (different protocols, communication modes, hosting, and integration of multiple media channels) requires a systematized view of these apps. For this reason, we also base our threat modeling on STRIDE and LINDDUN (see Section 3.2). By combining both frameworks, we were able to explicitly consider specific security and privacy threats (see Appendix E).

3 METHODS

We conducted an exploratory online survey between August and October 2022 on the use of VC apps with 251 German-speaking participants. Figure 1 shows the structure of the questionnaire, which consisted of 53 subject matter questions and 8 demographic questions (Appendix A). After filling in the questionnaire, the participants could take part in a raffle for 15 Amazon vouchers (10 EUR each) that was conducted using a separate independent survey (see Section 3.3). The median participation duration in the survey was 15.37 minutes and 18.9 on average. Subsequently, we present our study design and highlight differences to related studies, especially Emami-Naeini et al. [13].

3.1 Survey Procedure

Firstly, participants were informed that our survey's focus is on UCC apps such as Zoom, MS Teams, Jitsi, or Skype, and not on instant messaging (IM). In contrast, Emami-Naeini et al. [13] also included IMs such as WhatsApp. Like Reisinger et al. [38], they therefore considered UC (UCC + IM) and thus a broader field. However, since UCC is facing other challenges in terms of security and privacy (e.g., implementation of E2E encryption), we refrained from looking at IMs. After the participants gave their informed consent (IC1, see Figure 1), they were asked about their use of VC apps. To limit extensive recall bias, the prerequisite for further participation was that usage of VC had taken place at least within the last two years prior to the study (SQ1). We then provided participants with an extensive list of VC software and asked about their use, while also offering to add further apps (SQ2). Participants were asked about choice, avoidance, and restrictions related to specific apps (SQ3-7).

Unlike other studies, we did not only focus on the pre-pandemic phase [41], the pandemic phase [35], or both [13], but we were able to also incorporate the time after the pandemic. Thereby, our survey covered three different periods in total: *before* the pandemic (imposed by the lockdown in spring 2020), *during* the pandemic, and the period starting in May 2022 when contact restrictions had largely been lifted in Germany (*after*). In addition to the phase of use (SQ8-9, SQ11), the frequency of use (*"not at all"* to *"daily"*) and the purpose of use (*"professional"*, *"private"*, *"both"*) during these periods were surveyed as well (SQ10).

All apps in use were evaluated with respect to usability (*SQ12*), as well as to security and privacy (SQ30). For evaluating both, usability and security, we opted for a 5-point Likert scale (1=*very bad*, 5=*very good*), as the participants had to rate up to ten VC apps, such that the rating should be as simple as possible. Furthermore, established usability ratings (e.g., SUS [8], UMUX [14]) are suitable for the time directly after the use of an app, which was not the case in our retrospective survey. The reason for using *security* and *privacy* together in the survey is that users often conflate them [1, 24, 39, 46]. To address security and privacy concerns equally (e.g, with regard to the avoidance of certain functions; SQ16) or usage of security measures (SQ24), we made sure to use the terminology *"to protect your communication and privacy"*. From here on, we write "security" for brevity, but mean "security and privacy".

Additionally to apps used, the survey also inquired about use or avoidance of certain functions as a protection measure (SQ13-16). In terms of VC locations, we not only included VC from home [13], but also from the workplace and on the move (e.g., in public places) and also the respective devices of participation (SQ17-20). Furthermore, participants indicated whether they had experienced or were exposed to unintentional disclosure of content in connection with certain functions, and whether these situations were associated with a feeling of embarrassment (SQ21-23). In addition to audio and video, as already considered by others [13, 35], we also included functions such as chat, reactions, or screen sharing, which can also lead to threats such as information disclosure. As training can help to avoid such situations, we also asked which apps our participants had received training for (SQ25-27). Subsequently, participants were asked whether they heard of security and privacy issues in VC (SQ28-29), and whether they had taken measures of protection (SQ24). Lastly, 10 exemplary threat scenarios (based on our threat model, see Section 3.2) were rated on a 5-point Likert scale in terms of their realism (SQ52).

Through existing work [13, 35], we were able to offer a variety of closed answer options for the majority of our questions, in addition to free text fields (only SQ23 and SQ53 are exclusively open-ended, see Section 3.5.5). Furthermore, working on the basis of a threat model allowed us to view concerns, protective measures, and also threats from a holistic perspective and to take this into account in our response options. In addition to general usage, each participant also described a usage scenario of their choice. As this paper, unlike others [13, 35, 38, 40], focuses on general usage of VC apps, these context-specific scenarios are not included in the analysis and are left to future work.

3.2 Threat Model

The perceived risk of threats is decisive for the perception and attitude towards security and privacy of VC apps [13, 38]. For this reason, participants rated 10 exemplary threats regarding their closeness to reality on a 5-point Likert scale (1=*very realistic*; 5 = *not realistic at all*; see Section 4.7; SQ52). We asked for the perceived closeness to reality because users are more inclined to protect themselves against threats that seem real to them [38]. We presented threats that had already received media attention (see Section 1),

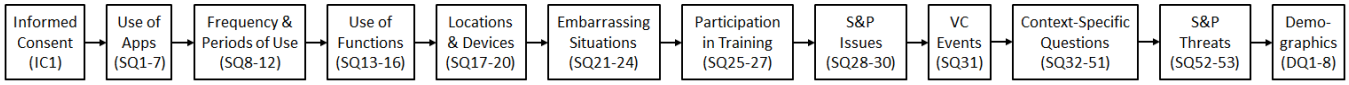


Figure 1: Questionnaire structure (see Appendix A for complete questionnaire).

rather than hypothetical possible dangers, as hearing about issues can influence the participants' risk awareness.

Like Reisinger et al. [37], we used STRIDE [42] and LINDDUN [11] to systematically identify threats to VC apps. While STRIDE looks at six types of security threats from an attacker's perspective (**S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of Service, **E**levation of Privilege), LINDDUN focuses on seven strategies to undermine the privacy of a system: **L**inkability, **I**dentifiability, **N**on-repudiation, **D**etectability, Information **D**isclosure, Content **U**nawareness, Policy/consent **N**on-compliance. On this basis, we first created a set of 30 possible threats that covered all security and privacy threat types mentioned by STRIDE and LINDDUN, and then broke them down to 10 (see Table 7) in a joint discussion with all authors. Explanatory descriptions of all types of these threats and the classification of our specific examples can be found in Appendix E, and the wording of the questionnaire in Appendix A.4.

3.3 Ethics

Participation in the survey was voluntary, and data collection was completely anonymous. The purpose of the study was described in advance, and the questionnaire had been approved by our institution's data protection office prior to distribution. The survey tool LimeSurvey was hosted locally at our lab. All 251 participants gave informed consent and were at least 18 years old. For the Amazon voucher raffle, participants could voluntarily provide their email addresses in a separate survey to avoid inferences to the survey data. All email addresses were deleted after the raffle.

3.4 Participants

340 people clicked on the survey link. 63 of them left the page without participating, five did not give their consent, 13 had not used VC apps within the last two years and thus did not belong to the target group. Two persons invested only five minutes in participating, which was considered too short for conscientious answers. Timing statistics of four participants who had taken over an hour revealed that three of them had paused the survey at only one point, while one interrupted it at several points and was excluded, since sufficient concentration on the questionnaire was in doubt. Three other persons overlooked relevant apps in our list and added them manually. Since this meant they missed questions regarding listed apps, these participants could not be included in the overall evaluation and analysis. Finally, two participants gave contradictory responses within specific usage scenarios and were therefore also excluded. As a result, survey data of 251 participants were included in the analysis.

3.4.1 Participant Recruitment. We deliberately recruited our participants using snowballing to ensure diversity. Different from others [13, 35], we decided against online platforms (e.g., Prolific), which primarily appeal to people for whom remote or online settings are part of their everyday life. Otherwise, user groups who were confronted with an online context for the first time during the pandemic would have been neglected. Participants were instead recruited by asking personal contacts to participate in our survey and forwarding the survey to their contacts. When reaching out to contacts, we ensured that people with different professional backgrounds and from different regions in Germany and Austria were addressed. Since different time periods are decisive for our study, we deliberately limited ourselves to the German-speaking countries, as the contact restrictions and their lifting provided the same temporal conditions. In addition, we recruited participants via mailing lists of different departments at our institution and asked to distribute at other institutions. As participation was anonymous, we are unable to make statements about regional distributions.

3.4.2 Participant Demographics. 93.6% of the $N = 251$ respondents were aged 18-29 ($n = 158$) or 30-49 ($n = 77$). Less than 4% ($n = 10$) were 50 years or older. Slightly more men ($n = 130$) than women ($n = 115$) participated in the survey. Most participants reported a Bachelor's ($n = 70$) or Master's ($n = 65$) degree as their highest level of education. 40 respondents completed vocational training and 39 had previously earned only a high school diploma. At just under 53% ($n = 133$), the majority of participants were employed, while almost 40% ($n = 100$) were students. About a third ($n = 81$) reported working in computer science or a similar field. Seventeen participants abstained from providing one or more demographic items (voluntarily collected), indicated by "*na*" in Table 1. These persons were excluded in linear regression analysis to ensure the comparability of the models when demographic control variables are added (see Section 3.5.1). In total, over 35% ($n = 88$) of our participants had only used VC apps for the first time after the introduction of contact restrictions (during the pandemic).

3.5 Data Analysis

3.5.1 Behavioral Changes. To investigate factors for behavioral changes in usage of VC apps over two time periods, *during* and *after* the pandemic, we created five linear regression models (see Table 4). We opted for a regression analysis to explain observations by exploratory approach and the effects of various factors on them. This method benefits from the possibility of testing various hypothetical influencing factors and creating models that contribute to the explanatory value of the dependent variable by iteratively adding further independent or control variables.

Our dependent variable DV_{bc} (behavioral changes) is metric and counts differences between usage frequencies (*"not at all"* – *"daily"*, SQ11) of both time periods per app for each participant. DV_{bc} increases by one for a participant who changed the frequency of use of a specific app, for each app used. For example, if a participant used Zoom during the pandemic monthly and after the pandemic weekly, then DV_{bc} increases by one (Freq_{during} = monthly; Freq_{after} = weekly; $\mathrm{Freq}_{during} \neq \mathrm{Freq}_{after}$ means *behavioral change*; $\Rightarrow \mathrm{DV}_{bc} := \mathrm{DV}_{bc} + 1$). Similarly, the counter increases

Table 1: Participants' demographic information (N = 251).

GENDER		IT BKGD.		AGE		HIGHEST DEGREE				EMPLOYMENT			
Female	45.8%	Yes	32.3 %	18-29	62.9%	Still at school	<1%	Bachelor	27.9%	Employed	52.9%	Home-maker	<1%
Male	51.8%	No	65.3%	30-49	30.7%	<High school	<1%	Master	25.9%	Student	39.8%	Retired	<1%
Other	0.0%	*na*[1]	2.4%	50-64	3.2%	High school	15.5%	Phd	3.6%	Self-employed	2.4%	Unemployed	<1%
na[1]	2.4%			>64	<1%	Vocational training	15.9%	*na*[1]	1.6%	Pupil/Apprentice	1.6%	*na*[1]	1.2%
				na[1]	2.4%	Specialized degree	8.8%						

na = missing value; BKGD. = BACKGROUND.

by one if this participant used MS Teams daily during the pandemic and not at all after the pandemic. The total DV_{bc} for this participant, if they exclusively changed their behavior on Zoom and MS Teams, is 2.

For each participant, only apps which were used at least monthly in one of the two periods are included in DV_{bc}. For example, if a participant used Jitsi *less than monthly* during the pandemic and *not at all* afterwards ($Freq_{during} \wedge Freq_{after} < monthly$), this app is not included in DV_{bc}. We only measured changes in frequency and did not include the frequency of use *per se*. One advantage of this procedure is that it minimizes possible measurement errors due to memory gaps caused by overly accurate frequency detection.

We include two independent variables (IV_1, IV_2) in **Model 1** and a further one (IV_3) in **Model 2**. IV_1 counts the number of apps avoided due to lack of usability, IV_2 counts apps avoided due to security concerns, and IV_3 counts apps prohibited or restricted by third parties per participant. For example, if a participant avoided Zoom due to a lack of usability and was also prohibited from using it by the employer, both IV_1 and IV_3 increase by one. Each of our models contributes to the explanatory value of DV_{bc}: If we consider **Model 1** alone, IV_1 and IV_2 are significant factors. If we then consider **Model 2**, the security concerns (IV_2) become insignificant, which suggests that these security concerns result mostly from restriction by third parties (IV_3). Furthermore, demographic factors must be considerate to a change in behavior. **Model 3** contains IT background. This control variable (categorical) is supplemented by gender and highest education degree in **Model 4** and finally by age in **Model 5**. We also tested other possible influencing factors (e.g., purpose of use, participation in training) but were unable to measure any significant influence on DV_{bc}.

3.5.2 Security Measures Usage. Factors for the use of security measures in VC were evaluated in three further models (see Table 5). DV_{mu} is calculated by the number of all types of measures ever used per participant (see Section 4.6). We consider the effects of the independent variables IV_1 (counts of all types of sources from which a participant heard about security issues of VC apps) and IV_2 (counts of all types of functions with which a participant experienced incidents). In the case of IV_1, we did not count if a participant gave their own experience as the source from which he had heard about issues, as the own experience of an incident is already mapped in IV_2.

Model A only includes the IVs. In **Model B**, we added control variables (CV; same demographic data as in Section 3.5.2). In **Model C**, we also include the general extent of the participant's usage of VC apps (CV_f). For each participant, this is calculated from the sum of the maximum frequency for each app ever used over three time periods. Due to different distances in the scale level for frequency, the values must be re-coded to establish comparability of the intervals.

Taking our shortest time period (three months after pandemic) into account, all participants who have used an app *"once"* are assigned the value 1 for this app, while other frequency values are coded as follows: *"less than monthly"* = 2; *"monthly"* = 3; *"weekly"* = 12 (3*4 weeks per month); *"daily"* = 60 (12*5 days per week). For example, if a participant used Zoom in the most active usage phase *daily* (=60) and MS Teams *monthly* (=3), then CV_f sums up to 63.

3.5.3 Correlations. For correlations based on two ordinal-scaled variables, we used Spearman rank correlation (ρ_{spearman}): e.g., correlation between frequency of use (1-5: 1 = *once*; 5 = *daily*) and usability ratings (5-point Likert scale; 1 = *very bad*; 5 = *very good*). To express a general measure of familiarity, we used the maximal frequency of use over all three time periods. We used Pearson correlation coefficient (r_{pearson}) to examine correlations between variables measured with uniform scale and identical scale distances, which therefore can be considered numerical. For example, usability and security ratings were both measured on the 5-point Likert scale from *very bad* (=1) to *very good* (=5).

3.5.4 Independent Samples. When comparing independent samples, we used a Welch two-sample t-test to express differences between both groups (see Table 3). For example, we compared usability ratings of specific apps and differentiated between participants who self-initiated using this app (n_1) and those who used the app as well, but never initiated using it by themselves (n_0). As proposed by Rasch et al. [36], we used a two-sided Welch t-test designed for larger between-sample variances, as samples have unequal variances in some cases (e.g., BigBlueButton: n_1=8; n_0=33; sd_{n1}=0.46; sd_{n0}=1.09). Effect sizes were expressed by the size of mean value differences between both groups. Taking BigBlueButton as example, we compared the mean of usability ratings for the app in group n_1 ($\varnothing U_{n1}$ = 4.25) and the mean of usability ratings in group n_0 ($\varnothing U_{n0}$ = 3.24), which resulted in an effect size of 1.01 ($\triangle_{\varnothing U_{n1}, \varnothing U_{n0}}$).

3.5.5 Open-Ended Responses. We asked participants whether they had ever been confronted with an embarrassing situation involving the incorrect use of certain functions, providing them with a list of possible mishaps (*SQ21-22*). In free-text, they were able to add their own experiences (*SQ24*). If answers did not align with options from the list, a new code word was added in a joint discussion between two coders. 27 participants responded to question *"What makes you feel personally threatened or harmed when using video conferencing applications?"* (*SQ53*). Code words were deductively assigned using

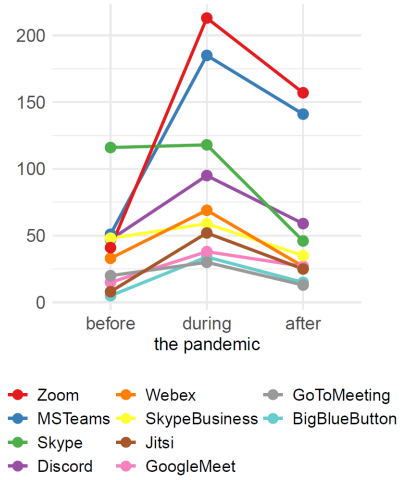


Figure 2: Usage figures of top-10 VC apps in use by participants before (N = 163), during (N = 251), and after the pandemic (N = 224)

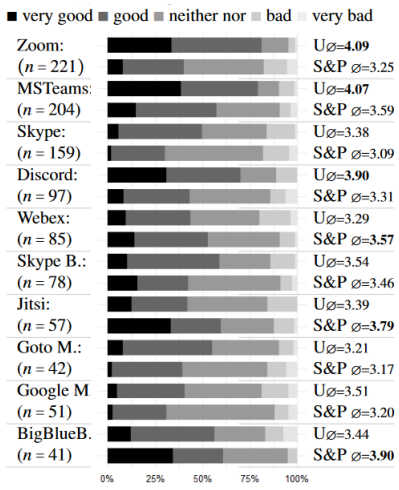


Figure 3: Participants' ratings on usability and security of (at least once) used apps on 5-point Likert scales (*very bad:* 1; *very good:* 5; avg.: ∅; >3.5 in bold).

the categories of the STRIDE and LINDDUN frameworks (see Section 3.2). Only 3 participants gave a free text answer on how they dealt with hearing about security issues in a specific app (*SQ29*).

4 RESULTS

The survey referred to three time periods: before the lockdown in spring 2020 (*before the pandemic*), within the two years before the end of the lockdown (*during the pandemic*), and within the three months before study participation (*after the pandemic*). While 163 out of 251 participants (64.9%) had already used VC apps before the pandemic, 88 participants (35.1%) indicated that their first use of VC apps happened during the pandemic. Of those 88 participants, who never used VC apps before the pandemic, 78% continued to use it after the pandemic. Of those who had experience with VCs prior to the pandemic, only 8 reported to have not used it during the three months before our study.

4.1 Course of Application Usage

Based on participants' top-10 VC apps in use, an overall peak in usage numbers is observed for all apps during the pandemic. Yet, in most cases, this only had limited sustainability (see Figure 2). Before the pandemic, Skype was the most used app among participants (n = 116), followed by MS Teams (n = 51), Skype for Business (n = 48), and Discord (n = 47). During the pandemic, Zoom and MS Teams became by far the most used apps with n = 213 and n = 185 participants, respectively. While the usage numbers increased for all VC apps during the pandemic, only Skype (n = 118) did not experience a notable increase, despite being by far the most used app before the pandemic. While usage numbers decreased across all apps after the pandemic, those of Skype (72/188; −61%), Jitsi (35/52; −51, 9%), and BigBlueButton (15/34; −55, 9%) dropped by more than half. Although usage numbers for Zoom (157/213; −26.2%) and MS Teams (141/185; −23.8%) also decreased by around a quarter, they remained the two most used VC apps.

4.1.1 Usability and Security Ratings. Figure 3 summarizes participants' ratings of VC apps wrt. usability and security on a 5-point Likert scale (5=very good, 1= very bad), including the respective average values per app (∅). Zoom (221/251) and MS Teams (204/251) were not only most frequently used, but also best-rated in terms of usability (∅ > 4.0). Almost 81% of Zoom users and 79% of MS Teams users rated the apps as good or very good in usability (see Figure 3).

Only 57% gave such a good rating for MS Teams security. For Zoom, the figure is even lower at 40%. We observed similar values for Discord ($\varnothing_U$=3.9; $\varnothing_{S\&P}$=3.31). Accordingly, these apps seemed to represent a trade-off between usability and security for our participants ($\triangle_{\varnothing_U,\varnothing_{S\&P}}$ >0.48). However, this picture is reversed for Jitsi and BigBlueButton (BBB) ($\triangle_{\varnothing_U,\varnothing_{S\&P}} \leq -0.4$). Fewer people gave good to very good ratings for usability (Jitsi: 42%, BBB: 56%) than for security (Jitsi: 60%, BBB: 61%). These apps were also, alongside Webex, rated best in terms of security (∅ < 3.57).

4.2 Usability, Security and Familiarity

As noted in Section 4.1.1, participants rated apps they used at least once on a 5-point Likert scale with respect to their *usability* and *security*. As an additional influencing factor, we measured their *familiarity* with the apps based on the maximum frequency of use over all three time periods (see Table 8 in Appendix B).

4.2.1 Interplay of Usability and Security. The first column of Table 2 (r_{pearson} for U&S) shows the correlations between usability and security ratings for each app individually. There was a moderate ($r_{\text{pearson}} \geq 0.3$) to strong ($\geq 0.5$) significant correlation between participants' ratings regarding usability and security for almost all examined apps. According to this, participants tended to rate usability better if they were satisfied with the security of an app. This even applied to those that, on average, showed the largest discrepancies between the two ratings (e.g., Zoom, MS Teams, Discord;

Table 2: Correlations between usability (U) and security (S) ratings (Pearson), and between U/S ratings and familiarity (F, Spearman) for used apps (see Section 3.5.3; $N = 251$; multiple apps per participant possible).

		U [1] & S [1]	U [1] & F [2]	S [1] & F [2]
App.	n	r_{pearson}	ρ_{spearman}	ρ_{spearman}
Zoom	221	0.487^{***}	0.283^{***}	0.058
MSTeams	204	0.372^{***}	0.369^{***}	0.130^{+}
Skype	159	0.284^{***}	0.238^{*}	0.063
Discord	97	0.391^{***}	0.389^{***}	0.174^{+}
Webex	85	0.444^{***}	0.331^{**}	0.071
Skype B.	78	0.215^{+}	0.095	0.304^{**}
Jitsi	57	0.433^{***}	0.494^{***}	0.391^{**}
Google M.	51	0.300^{*}	0.509^{***}	0.103
GoTo M.	42	0.581^{***}	0.465^{**}	0.295^{+}
BigBlueB.	41	0.266^{+}	0.210	0.168

r /ρ correlation coefficient: low = .10; medium = .30; strong = .50; Significance level: $^{+}$p<0.1; *p<0.05; **p<0.01; ***p<0.001;
[1] Score 1-5: 1 indicates *very bad*, 5 indicates *very good*; [2] Scale 1-5: 1 indicates *once*, 5 indicates *daily*; max. value over 3 periods.

Table 3: Dependence between self-initiated use (n_1) of app and usability (2nd column) and security ratings (3rd column) measured by Welch two sample t-test per app. ($N = 204$; effect size = difference in the mean values of ratings by both groups (n_1, n_0)).

	Samples [1]		Usability rating [2]		Security rating [2]	
App.	n_1	n_0	$\triangle_{\varnothing U_{n1},\varnothing U_{n0}}$	df	$\triangle_{\varnothing S\&P_{n1},\varnothing S\&P_{n0}}$	df
Zoom	118	103	0.63^{***}	209.2	0.38^{**}	210.2
MSTeams	105	99	0.57^{***}	186.9	0.31^{*}	201.2
Skype	62	97	0.55^{***}	151.1	0.24^{+}	150
Discord	38	59	0.69^{***}	89.2	0.66^{**}	71.3
Webex	14	71	1.02^{***}	24.6	0.35	20.5
SkypeB.	19	59	0.54^{**}	46.0	0.50^{*}	30.6
Jitsi	29	28	0.55^{*}	52.1	0.64^{*}	53.3
GoogleM.	11	40	0.74^{***}	46.0	-0.02	13.4
GoTo M.	4	38	0.87^{***}	37.0	0.09	4.9
BigBlueB.	8	33	1.01^{***}	27.6	1.21^{***}	29.7

[1] Sample n_1: use was self-initiated (at least once); Sample n_0: use was never self-initiated; [2] t-test: $\triangle_{\varnothing_{n1},\varnothing_{n0}}$ = difference between average ratings of both samples with significance level: $^{+}$p<0.1; *p<0.05; **p<0.01; ***p<0.001; df = degrees of freedom.

see Figure 3). The only exceptions were Skype (0.28^{***}), BigBlueButton (0.27^{+}), and Skype for Business (0.22^{+}), where only small correlations between usability and security ratings occurred.

4.2.2 Interplay of Usability and Familiarity. Not only did we find significant correlations between the usability ratings and security perceptions, but participants generally rated apps also better in usability when they were more familiar with using them (see 2nd column in Table 2; ρ_{spearman} for U&F). Here, again, the three apps mentioned above, namely Skype, BigBlueButton, and Skype for Business, stand out due to lower correlations ($\rho_{\text{spearman}} < 0.3$). Zoom also narrowly missed a moderate correlation (0.28^{***}). Jitsi's and Google Meet's usability ratings seemed to benefit the most from a higher familiarity (> 0.49). Conversely, usability ratings here suffered the most from less familiarity with the apps.

4.2.3 Interplay of Security and Familiarity. While we measured a moderate to high significant correlation between usability rating and familiarity in most cases, the situation was different with dependencies between security rating and familiarity (see 3rd column in Table 2; ρ_{spearman} for S&F). For Zoom, Skype, and Webex, more frequent use was not related to a more secure perception of the app ($\rho_{\text{spearman}} < 0.1$). BigBlueButton and Google Meet showed low effect sizes about such a relationship (≤ 0.17) and GoTo Meeting even medium (0.3^{+}), but no significance was detected here either. A significant moderate correlation was only measured in two cases, namely Jitsi (0.39^{**}) and Skype for Business (0.31^{**}). Participants who were more familiar with using these two apps were more likely to give good security ratings.

4.3 Choice of Applications

We looked at differences between two user groups: Participants who stated that they themselves had ever chosen or suggested a specific app for use in online meetings (n_1) versus the reference group (n_0) whose use was never self-initiated. Table 3 shows the size of both groups per app (n_1; n_0), differences between the mean values of ratings of both groups ($\triangle_{\varnothing_{n1},\varnothing_{n0}}$), and the significance of the two-sample t-test. The first t-test included the own decisions and differences in usability ratings per group (2dn column), and the second test did the same for security ratings (3rd column).

4.3.1 Interplay of Choice and Usability. Zoom was not only used by most participants (see $n_1 + n_0$ in Table 3), but its usage was also most often based on participants' initiative: More than half of Zoom users ($n_1 = 118$). The situation is similar with MS Teams ($n_1 = 105$), and both Zoom and MS Teams were rated better than the other apps in overall usability ratings (see Figure 3). Comparing the average usability ratings of those who have decided to use these apps themselves with those who have never made this decision themselves (Zoom: $\triangle_{\varnothing U_{n1},\varnothing U_{n0}}=0.63^{***}$; MS Teams: $\triangle_{\varnothing U_{n1},\varnothing U_{n0}}=0.57^{***}$, see Table 3), we find large significant differences between ratings of both groups per app. We made similar observations in relation to the remaining VC apps ($\triangle_{\varnothing U_{n1},\varnothing U_{n0}}>0.5$).

Without exception, the self-made choice for the ten apps examined is significantly related to a more positive usability rating. Nevertheless, the influence of a positive usability evaluation on one's own decision should be viewed with caution for apps with very small samples, such as BigBlueButton, GoTo Meeting, Google Meet and Webex. Here, we identified the largest mean discrepancy between the groups ($\triangle_{\varnothing U_{n1},\varnothing U_{n0}}>0.75$), while having only 4–14 participants who initiated the use of these apps.

4.3.2 Interplay of Choice and Security. Jitsi and Skype for Business, which had some of the least significant values in the usability t-tests ($\triangle_{\varnothing U_{n1},\varnothing U_{n0}}= 0.55^{*}$ and 0.54^{**}, respectively; see Table 3), were among the six apps that showed significant dependencies between good security ratings and the own choice of app ($\triangle_{\varnothing S\&P_{n1},\varnothing S\&P_{n0}}= 0.64^{*}$ and 0.50^{*}, respectively). The discrepancy between the two sample groups (n_1, n_0) was also comparatively high for both apps (>0.5). BigBlueButton stood out the most in the t-test results: Eight people who chose BigBlueButton all gave good

to very good ratings in both evaluations. Discord was also chosen significantly often in connection with a positive perception of security. Here, too, comparable values were observed between security ($\triangle_{\varnothing S\&P_{n1},\varnothing S\&P_{n0}}$= 0.66***) and the usability t-tests ($\triangle_{\varnothing U_{n1},\varnothing U_{n0}}$= 0.69***). Even though Zoom was rated worst in terms of security on average ($\varnothing_{S\&P}$=3.25; see Figure 3), the group that already chose it themselves gave more positive ratings on average than the other group ($\triangle_{\varnothing S\&P_{n1},\varnothing S\&P_{n0}}$=0.38). The perception of security and participants' self-made choices are only significantly related for some specific apps (i.e., BigBlueButton, Discord, Zoom, Skype for Business, Jitsi).

4.4 Avoidance and Restriction of Usage

Participants stated whether they avoided apps (i) due to a lack of usability (used at least once), (ii) due to security concerns, or whether they had ever been (iii) restricted or prohibited by third parties (e.g., employers, customers, others attendees). For the latter two reasons, participants reported apps that they have never used for these reasons (see Appendix C). Avoidance due to lack of usability is especially prominent for Skype (30%), Webex (28%), and BigBlueButton (27%). Overall, like the self-initiated choice (see Section 4.3), the rejection of certain apps seemed to occur more often due to usability rather than for security. Thus, 80% of participants (201/251) never avoided an app due to security concerns, whereas only 52% (130/251) never avoided an app due to usability issues. Again, Zoom was avoided the least because of usability (8% of Zoom users), but was the most avoided due to security concerns (11% of all users) and the most restricted by third parties (24% of all users). Skype, apart from being avoided the most due to lack of usability, was also avoided by 6% of users due to security concerns and restricted by third parties in 12% of cases.

4.4.1 Impact of Avoidance on Behavioral Changes. The overall usage figures (224/251) remained high even after the pandemic. But usage frequency for certain apps changed (see Table 8). Using linear regression (see Section 3.5.1), we determined to what extent usability, security and restrictions could have influenced these changes in usage behavior.

Anyone who used an app at least monthly during or after the pandemic showed a pattern of behavior. If this pattern changed in frequency between both time phases, we speak of behavioral change *(DV_{bc}; dependent variable)*. Our first regression model (**Model 1**; see Table 4) includes two potential factors: one variable that counts the number of apps avoided due to lack of usability (IV_1), and one that counts the number of apps avoided due to security concerns (IV_2).

Both variables have a significant impact on changes in user behavior. The effect of avoidance due to lack of usability on changing behavior is stronger than that of security concerns. The R^2 is 0.067, so only 7% of the variance in the dependent variable can be explained by the two variables.

4.4.2 Impact of Restrictions on Behavioral Changes. For **Model 2**, which includes the number of apps restricted by third parties (IV_3), the R^2 is almost double compared to Model 1. This implies a lack of autonomy in decision-making regarding the use and avoidance of VC apps. The effects of avoidance due to a lack of usability (IV_1) and due to security concerns (IV_2), decreases and becomes insignificant for the latter one. Thus, restrictions by third parties are primarily due to concerns about security. In **Model 3**, we took into account whether a person has an IT background and measured a strong significant effect, i.e., participants who come from IT or a similar field changed their behavior more than others. For both IV_1 and IV_2, the effect size decreases. Avoidance due to lack of usability also becomes insignificant, but the effect of IV_3 (restrictions by third parties) is almost as high as in Model 2. Thus, avoidance due to usability and security concerns occurs mainly among participants with an IT background. Model 3 can explain 21% of the variance of behavioral changes (DV_{bc}). **Model 4** also includes gender and the highest degree, and has an R^2 of 0.288. Males changed their behavior more than females, and participants with an academic degree (i.e., Bachelor, Master, PhD) changed their behavior more than those without an academic degree. Finally, **Model 5** (incl. age) explains 30.1% of the variance of DV_{bc}. Older participants changed their behavior more than younger ones. However, we cannot detect a significant effect here. This might be due to the significant influence of educational attainment (≥ Bachelor: 0.606**) and the fact that younger people are more likely not (yet) to have a degree.

4.5 Security and Privacy Issues

A factor that influences the perception and comfort when using VC apps is the personal experience or confrontation with vulnerabilities and threats [13].

4.5.1 Issues and Obligations for Usage.

73.7% of all participants (185/251, Table 10 in Appendix D) already heard about security issues of VC apps. 48.1% of those participants (89/185) stated that these issues had no effect on their further usage. 32% of those who affirmed an effect (31/96) reported that they would have liked to avoid affected apps, but were not able to do so. P220 described this circumstance: *"You can either join in or look for a new job."* P64 limited the use of *"perturbing"* apps to *"operational purposes/reasons"*. Here, too, we saw the influence of third parties and a lack of individual decisions in the choice of software (see Section 4.4.1). The decision to use (or not use) certain apps, however, does not come from employers alone. P57 stated: *"I myself have no concerns. However, I am considerate of people who find certain apps problematic and do not use them."* That a waiver or continued use does not need to be absolute was also reflected in the response options chosen. Thus, 15 of those who would have preferred to avoid an app, but could not, still avoided it in certain situations.

4.5.2 Incidents Due to Incorrect Usage. Some open-ended responses from participants emphasized that threats in online meetings do not necessarily arise from malicious intent or from software vulnerabilities. *P*199 wrote: *"I'm afraid of inadvertently providing more insight into data and privacy than I actually want."* Concerning possible information disclosure or triggers for unpleasant situations, we particularly noticed the functions of audio, video, chat, screen sharing, filter, and reactions. 58.6% of the participants (147/251 see Table 6) experienced an incident due to incorrect use of these functions. Accidental audio activation (78.8%; 78/99) was more often associated with a feeling of embarrassment than video (72.6%; 37/51).

Some participants described such situations in open-ended responses: P2 was embarrassed when a *"colleague at work made*

Table 4: Results from regression models to clarify factors influencing changes in usage behavior ($N = 234$): Dependent variable behavioral changes DV_{bc} is metric and counts differences between usage frequencies *during* and *after* the pandemic per app.

	Model 1		Model 2		Model 3		Model 4		Model 5	
Factors	Estimate	Std. Error	Estimate	Std. Error	Estimate	Std. Error	Estimate	Std. Error	Estimate	Std. Error
Usability lack *(IV_1)*	0.305^{***}	(0.089)	0.195^{*}	(0.089)	0.095	(0.089)	0.096	(0.086)	0.123	(0.087)
S&P concerns *(IV_2)*	0.163^{*}	(0.080)	0.077	(0.079)	0.005	(0.078)	−0.048	(0.076)	−0.054	(0.076)
Third parties *(IV_3)*			0.254^{***}	(0.056)	0.210^{***}	(0.055)	0.206^{***}	(0.053)	0.205^{***}	(0.053)
IT background					0.869^{***}	(0.199)	0.802^{***}	(0.193)	0.738^{***}	(0.195)
gender: female	reference category									
male							0.538^{**}	(0.167)	0.454^{**}	(0.173)
degree: vocational	reference category									
≥ bachelor							0.708^{**}	(0.226)	0.606^{**}	(0.232)
≤ high school							0.235	(0.223)	0.144	(0.273)
age: 18-29	reference category									
30-49									0.331^{+}	(0.192)
50-64									0.512	(0.482)
>64									−0.583	(0.885)
Constant	1.131^{***}	(0.118)	1.048^{***}	(0.115)	0.915^{***}	(0.115)	0.198	(0.216)	0.211	(0.215)
Observations	234		234		234		234		234	
R^2	0.067		0.144		0.210		0.288		0.301	
Adjusted R^2	0.059		0.132		0.196		0.267		0.270	
Residual Std. Error	1.383		1.328		1.279		1.222		1.218	
F Statistic	8.346^{***}		12.861^{***}		15.176^{***}		13.03^{***}		9.599^{***}	
	(df = 2; 231)		(df = 3; 230)		(df = 4; 229)		(df = 7; 226)		(df = 10; 223)	

Note: $^{+}$p<0.1; *p<0.05; **p<0.01; ***p<0.001 DV = dependent variable; IV = independent variable

his opinion known and his micro was not muted". P242 told about *"[i]nappropriate behavior during video transmission (nose picking)"*. P244, who wrote the *"password in the chat"*, reported how critical information disclosure via the chat can be.

4.6 Security and Privacy Measures

Most prominently, 96.3% of those participants who used audio (234/243) and 90.8% of those who used video (226/249) deactivated (at least once) the microphone or camera to protect themselves against unwanted listeners or viewers, respectively. In general (N=251), special measures were taken by participants to protect their physical environment from unwanted views: 146 participants (58%) paid attention to the orientation of their cameras or arranged the set-up of their location. Almost as many people ($n = 144$; 57%) used a background filter to protect their physical environment, and 54% ($n = 135$) used a physical camera cover. The precaution of closing all other apps in the event of screen sharing was used by 142 participants (57%). However, technical measures or those that require more extensive interaction were used less frequently: only 57 participants (23%) adapted the security settings, 21% ($n = 53$) ever used pseudonyms instead of their real names, and end-to-end encryption was activated the least frequently by 16% ($n = 41$).

Impact of Issues and Incidents on Measures Usage. The participants indicated from which sources they heard about security issues of VC apps (see Section 4.5.1). They also experienced unwanted insights into their privacy by accidentally activating functions (see Section 4.5.2).

Linear regression (**Model A**; Table 5) illustrates, that the number of sources from which participants learned about security issues (IV_1) has a significant influence (0.684^{***}) on the extent of security measures these participants used (DV_{mu}). The number of functions associated with an incident due to incorrect use (IV_2) has a smaller but still significant influence (0.272^{***}). Overall, both factors explain 22% (R^2=0.22) of the variance of DV_{mu}: The more extensive the knowledge about security problems with VC apps and the more frequently the participants experienced problems by using functions incorrectly, the more extensive the number of measures they took to protect themselves.

In **Model B**, we added demographic data as control variables and obtained a total R^2 of 0.289. Participants with IT background tended to use more measures. Likewise, participants with a higher level of education also used protective measures more extensively. Participants without an academic degree used significantly fewer protective measures in comparison (rc: academic degree). The younger the participants were, the greater was the effect on DV_{mu}. Since the extent of measures taken might be influenced by extensive usage of apps *per se*, we introduced a further control variable in **Model C** (see Section 3.5.2). The extent of usage (CV_f) is a significant factor for the extensive usage of measures (0.063^{***}). However, incidents due to incorrect use of functions also increase with increasing usage, and these participants also heard more about security issues. The influence of IT background becomes insignificant, as they probably

use apps more extensively. R^2 rises to 0.346 in the model and thus offers an explanatory value of almost 35%.

4.7 Security and Privacy Threats

Participants rated 10 exemplary threats regarding their closeness to reality on a 5-point Likert scale (see Section 3.2).

4.7.1 Perceptions of Security Threats.

In general, participants perceived threats from within a meeting as more realistic than threats from outsiders (see Table 7). For example, the danger of being recorded by other conference attendees was rated as realistic or very realistic in over 82% of cases. *P*171 felt particularly threatened by *"[u]nauthorized recording"* of a video call. The misuse of legitimate recordings (54.4%) and fake invitations to VCs (77.4%) were also rated as particularly realistic. Recording by the provider was rated as realistic to very realistic by 68%.

That the occurrence of such situations does not always have to be perceived as threatening to one's own person was shown by the response of P140: *"I have no discomfort with the use of my data [...] to improve the app, and for advertising, and I have no reason to believe that the data will be used for malicious purposes"*. In comparison, P71 felt threatened by *"surveillance by the video service provider and permanent potential to be recorded"*. Privilege escalation threats are such as the loss of control over a conference and third-party access to one's own device are less likely to be classified as realistic. Nevertheless, two participants expressed explicit concern about this. For example, P76 feared the "*[t]akeover of the computer by third parties due to programming errors (see Zoom)"*. Five people felt threatened by *"nothing at all"* when using VC apps.

4.7.2 Reactions to Security and Privacy Threats. Activating E2E encryption may prevent recording by the provider as well as by authorities. Those 41 participants who used E2E encryption rated both threats as significantly more realistic with a large effect size than those 210 who never used it (0.70*** and 0.69***, respectively; see Appendix F).

In some cases, VC apps also grant permissions for accessing camera or microphone to other apps. As P8 put it: *"Video camera continues to run after the meeting has ended (recognizable by illuminated LED)"*. Users cannot simply counteract this by pressing the mute button or deactivating the video. Instead, changes can be made to the app's security settings by revoking permissions, a measure that has ever been used by around 23% of the participants (see Section 4.6).

Participants who used pseudonyms ($n = 52$) felt significantly more threatened by other attendees recording (0.44**), than those ($n = 199$) who participated with real names. The same applied to those (142/251) who closed other apps before screen sharing (0. 28*) and those (146/252) who tried to prevent sharing physical location details by changing the camera focus or the room setting (0.40**).

5 DISCUSSION

5.1 The Interplay of Security, Privacy and Usability (RQ1)

Although we see discrepancies between security and usability ratings of some apps, they should not be considered isolated: Even if the actual decision in favor of an app is significantly related to a good usability perception, this perception is also significantly driven by the perception of security (see Table 2). A strong security promise can therefore also improve the user comfort and thus encourage the decision for an app [13]. VC apps providers are taking advantage of this by advertising with strong security promises [27], and many providers indeed made extensive improvements since 2020 in terms of security features [5]. For example, the threat of improper content sharing (e.g., Zoom bombing [30]), which was rated as rather or very realistic by the majority of our participants (see Table 7), have been fought with per default password-protected meetings and explicit permission for screen sharing [27]. Despite appropriate security features, popular VC apps still lack technical measures to protect privacy [37, 40].

According to Emami-Naeini et al. [13], familiarity is the second most frequently named reason for satisfaction with an app and appears to influence privacy and security concerns. In our case, familiarity influences perceptions of usability strongly, but correlations with security occurred only for a few apps (see Table 2). Nevertheless, familiarity with an app and thus better usability perception (e.g., because one gets used to avoiding pitfalls) can have a strong influence on security if it avoids situations that embarrass users or reveal insights into their privacy (see Section 4.5.2) The fact that measures such as audio and video (de)activation were used by more than 90% of participants underlines the need for users to protect themselves from such threats (see Section 4.6). So if they are forbidden to work with the apps they are most familiar with or that are easier for them to use, this leads to incidents triggered by incorrect use (see Section 4.4.2). This is where users become active and look for a remedy, as we showed a significant correlation between the extent of measures used and the occurrence of such incidents (see Section 4.6).

5.2 The Factors of Behavioral Changes in Usage (RQ2)

Not all threats have mitigations that users can control, e.g., when a device is taken over by escalation of privileges [48], or another attendee seizes administrator rights during a meeting due to a vulnerability [34]. The only solution would be to avoid affected apps (see Section 4.4, Section 4.5.1). Same as Emami-Naeini et al. [13], we saw a lack of decision-making autonomy here (see Section 4.5). However, when not influenced by third parties, some participants preferred to avoid apps. We were able to demonstrate an actual change in usage behavior, which was reflected in a decreased usage frequency with a significant effect of avoidance due to security concerns (see Table 4). However, avoidance due to a lack of usability and the decision of third parties to restrict or ban apps weighed more heavily.

Third parties (e.g., employers) should be encouraged to take a differentiated view and provide recommendations for security-compliant handling instead of prohibiting apps. Attention should be drawn to the existence or lack of security functions. Provided security features and marketing promises should not be blindly trusted. By only relying on publicly available policies [7, 12, 25], many recommendations by data protection and supervisory authorities lack a basic technical analysis or a user-centered view. Still,

Table 5: Results from regression models to clarify factors influencing the usage of security measures (DV_{mu}). Dependent variable is metric and counts the number of different security measures ever used per participant ($N = 234$). The control variable DV_f shows the general extent of the participant's usage of apps (see Section 3.5.2).

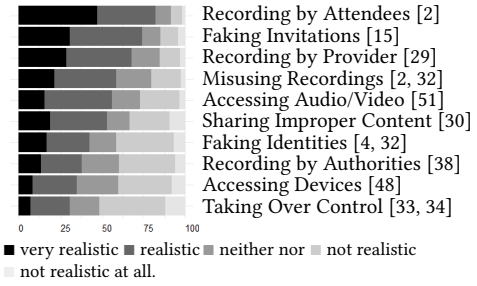
	Model A		Model B		Model C	
Factors	Est.	Std. E	Est.	Std. E	Est.	Std. E
S&P Issues (IV_1)	0.684^{***}	(0.116)	0.571^{***}	(0.123)	0.488^{***}	(0.120)
Incidents (IV_2)	0.272^{***}	(0.079)	0.223^{**}	(0.079)	0.165^{*}	(0.077)
IT background			0.649^{*}	(0.264)	0.289	(0.266)
age: 18-29 (rc)						
30-49			−0.388	(0.260)	−0.267	(0.251)
50-64			−0.531	(0.657)	−0.418	(0.632)
>64			-3.226^{**}	(1.207)	-2.586^{*}	(1.169)
gender: female (rc)						
male			−0.264	(0.233)	−0.409	(0.227)
degree: ≥ bachelor (rc)						
vocational			−0.232	(0.273)	−0.054	(0.265)
≤ high school			-0.734^{*}	(0.317)	−0.566	(0.307)
Usage extent (CV_f)					0.063^{***}	(0.014)
Constant	3.533^{***}	(0.188)	4.019^{***}	(0.249)	3.136^{***}	(0.312)
Observations	234		234		234	
R^2	0.220		0.289		0.346	
Adjusted R^2	0.213		0.260		0.317	
Residual Std. Error	1.716		1.664		1.599	
F Statistic	32.501^{***} (df=2; 231)		10.104^{***} (df=9; 224)		11.795^{***} (df=10; 223)	

Est. = Estimate; Std. E. = Standard Error; rc = reference category;
$^{+}p<0.1$; $^{*}p<0.05$; $^{**}p<0.01$; $^{***}p<0.001$

Table 6: Participants n_1 who used functions (at least once) and n_2 experienced accidentally (de)activating functions, those n_3 who were embarrassed by this incident & n_4 avoided the function (N=251).

	used by	incident n_2 & embarrassed n_3			avoided n_4 & embarrassed	
Function	n_1	n_2	n_3	n_3/n_2	n_4	n_4/n_3
Audio	249	51	37	72.6	19	51.4
Video	243	99	78	78.8	22	28.2
Chat	238	40	32	80.0	0	0.0
Sharing	221	62	30	48.4	7	23.3
Reaction	218	36	19	34.5	*na*	*na*
Filter	*na*	18	7	38.9	*na*	*na*

Table 7: Participants' ratings of exemplary threats on a 5-point Likert scale ($N = 251$). Threats are based on LINDDUN [11] and STRIDE [42]. Exemplary descriptions of the respective threats can be found in Appendix A.4.



companies are encouraged to adhere to such guidelines. The LINDDUN threat "Policy/consent Non-compliance" by providers, which has already proven to be problematic with various apps [15, 27, 29], is disregarded thereby. In some cases, the assurances given are only half-true or true under certain conditions. For example, instant messaging in Zoom [54] indicates encrypted messages. Despite the lock symbol and additional activation effort, this is not E2E encryption. Concurrently, the feature becomes an availability issue because messages can no longer be decrypted if the chat is accessed from a device that is too old. Jitsi claims to use E2E in meetings by default, which does not apply to chat messages, and also promises of E2E encryption for non-text-based communication cannot be kept [27].

5.3 The Effects of Security and Privacy Perceptions on Usage Behavior (RQ3)

The subjective perception of increased security is sometimes sufficient for an app to be perceived as more pleasant, as users often cannot differentiate between perceived and actual security [13]. Webex, Jitsi, and BigBlueButton were considered particularly secure (see Figure 3). Although Webex is not open-source, security may be associated with Cisco as a provider known for security software and hardware [10]. However, there might also be a great interest in user data on the part of the provider [51]. Jitsi and BigBlueButton are considered to be particularly privacy-friendly [16] and, unlike other apps, they offer the opportunity to confirm this through public source code. However, this seems to represent a trade-off with usability, where they scored much lower (see Section 4.1.1).

Participants' self-driven decision to use these two apps was slightly more dependent on their perception of security than on their usability perception (see Table 3). Nevertheless, transparency should not be equated with security, as it does not imply immunity against vulnerabilities [27, 33]. Enhanced security settings such as those provided by Zoom and MS Teams (e.g., removing/muting participants, or conferences restricted to authenticated users) are challenging for untrained users. Overall, technical and non-default security measures are used by participants to a negligible extent (see Section 4.6). A smaller number of measures were taken by older participants and those with lower education, even if they were confronted with incidents (see Section 4.6). Usage of security measures currently requires effort, time, understanding, and can be a hindrance to effectiveness. Activation of E2E, e.g., often means a compromise in terms of platform performance [17], number of participants [28], or the use of features [18]. Only 16% of participants had ever used E2E encryption, which may be due to a lack of understanding of security implications, relevance to protecting data from the provider (see Section 4.7.1), or E2E is assumed as default setting, as was observed for instant messengers [1].

5.4 Limitations

This work focused on usage of VC apps during the COVID-19 contact restrictions and three months after they were lifted. We did not conduct a longitudinal study with representative user samples across various countries, but focused on German-speaking users in a retrospective study. As noted by Emami-Naeini et al. [13], privacy concerns and attitudes may differ in different countries and cultures. Since participants' country of residence was not a statistically significant factor in their study, we referred directly to a specific population, as suggested. We identified a further factor for our recruitment decision through global differences in handling of the pandemic, as the consideration of different usage phases and corresponding behavioral changes was decisive for our study. In this way, were we able to capture a unique period in which the participants were already able to come to terms with the new reality of VC in everyday life, but were still able to remember the recent transition.

Likely due to snowballing recruitment, our sample is biased, since about a third of our participants have an IT background, 63% of them were aged between 18-29 (see Table 1, [43]), and their education is above the German average [9]. However, similar side effects cannot be ruled out when using crowdsourcing platforms. Participants recruited via Prolific, e.g., tend to be younger and more highly educated [13, 44]. Through snowballing, we tried to reach users who are less familiar with online settings and used VC for the first time during the pandemic (88/251).

Methodologically, we cannot rule out that external influences (e.g., semester breaks for students, or return to office due to end of contact restriction) may be more significant than the influences we measured. Also, we directly addressed security and privacy in some questions of the survey, so participants may have been primed accordingly. From a time perspective, the period *after* the pandemic (three months) is relatively small. As we conducted a retrospective study, it was important to reduce the influence of possible inaccurate memories about the time during the restrictions, at the same time ensuring that the participants could have experienced the changes after the restrictions. In order to reduce this recall bias, we restricted participation in the survey to people who had used VC at least within the two years prior to study participation (see Section 3.1). We also adjusted our regression model for changes in behavior accordingly (see Section 3.5.1). Furthermore, related work [13, 40] that took place during the pandemic used a similar timeframe to capture impressions of the most recent period of use, ensuring some comparability with their results.

6 CONCLUSION

We showed that usability factors outweighed security for most participants when using VC apps.

Usability also weighed heavily in the avoidance of apps, though the greatest influence came from the decisions of third parties to restrict usage. A lack of autonomy in deciding on a tool sometimes led to the use of VC apps that were associated with security concerns. This is of particular interest to decision-makers, which should be encouraged to make differentiated choices balancing usability, security, and privacy. From a user-centered perspective, it would be interesting to learn what perceptions and practices exist regarding E2E encryption in VC systems, as this feature underlines the specific challenge of balancing security and usability.

ACKNOWLEDGMENTS

We thank Lisa Marier Dreier and Julian Geus for helpful discussions. This work has been supported by the Bavarian Ministry of Science and Arts as part of the project "Security in Everyday Digitization" (ForDaySec).

REFERENCES

[1] Ruba Abu-Salma, M Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the adoption of secure communication tools. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Jose, CA, 137–153.

[2] CGTN America. 2022. 2020's Most Embarrassing Zoom Moments. https://www.youtube.com/watch?v=yZpEpNPaxsw, [Online; accessed on February 15, 2024].

[3] Sharon Bassan. 2020. Data privacy considerations for telehealth consumers amid COVID-19. *Journal of Law and the Biosciences* 7, 1 (2020), lsaa075.

[4] Patrick Beuth. 2022. Deepfake oder cheap fake? Falscher Klitschko narrt auch Warschaus Bürgermeister. https://www.spiegel.de/netzwelt/web/franziska-giffey-und-vitali-klitschko-falscher-klitschko-narrt-auch-warschaus-buergermeister-a-611b49b7-cd53-4266-ad82-e7d0600829ba, [Online; accessed on February 15, 2024].

[5] Josh Blum, Simon Booth, Oded Gal, Maxwell Krohn, Julia Len, Karan Lyons, Antonio Marcedone, Mike Maxim, Merry Ember Mou, Jack O'Connor, et al. 2020. E2e encryption for zoom meetings. *Zoom Video Commun., Inc., San Jose, CA, Tech. Rep. Version* 2, 1 (2020), 57.

[6] Matyáš Boháček and Hany Farid. 2022. Protecting world leaders against deep fakes using facial, gestural, and vocal mannerisms. *Proceedings of the National Academy of Sciences* 119, 48 (2022), e2216035119.

[7] Stefan Brink. 2021. Videokonferenzsysteme Hinweise des LfDI zur praktischen Nutzung von Videokonferenzsystemen (VKS). https://www.baden-wuerttemberg.datenschutz.de/videokonferenzsysteme/; [Online; accessed February 15, 2024].

[8] John Brooke et al. 1996. SUS-A quick and dirty usability scale. *Usability evaluation in industry* 189, 194 (1996), 4–7.

[9] Statistisches Bundesamt. 2019. Bildungsstand. https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bildung-Forschung-Kultur/Bildungsstand/_inhalt.html [Online; accessed on February 15, 2024].

[10] Cisco. 2022. Webex Meetings Security White Paper. https://www.cisco.com/c/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.html, [Online; accessed on February 15, 2024].

[11] Mina Deng, Kim Wuyts, Riccardo Scandariato, Bart Preneel, and Wouter Joosen. 2011. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering* 16, 1 (2011), 3–32.

[12] Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg. 2020. Datenschutzfreundliche technische Möglichkeiten der Kommunikation. https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/ [Online; accessed February 15, 2024].

[13] Pardis Emami-Naeini, Tiona Francisco, Tadayoshi Kohno, and Franziska Roesner. 2021. Understanding Privacy Attitudes and Concerns Towards Remote Communications During the COVID-19 Pandemic. In *Seventeenth Symposium on Usable Privacy and Security, SOUPS 2021, August 8-10, 2021*, Sonia Chiasson (Ed.). USENIX Association, California, CA, 695–714.

[14] Kraig Finstad. 2010. The usability metric for user experience. *Interacting with computers* 22, 5 (2010), 323–327.

[15] FTC. 2020. FTC Requires Zoom to Enhance its Security Practices as Part of Settlement. https://www.ftc.gov/news-events/news/press-releases/2020/11/ftc-requires-zoom-enhance-its-security-practices-part-settlement [Online; accessed on February 15, 2024].

[16] Berliner Beauftragte für Datenschutz und Informationsfreiheit. 2020. Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten. *Version 1.0 vom 3. Juli 2020* 15 (2020), 1–15. https://www.datarea.de/berliner-datenschutzbeauftragte-aktualisiert-hinweise-zu-anbietern-von-videokonferenzdiensten/ [Online; accessed on February 15, 2024].

[17] Rainer W Gerling, Sebastian Gerling, Stefan Hessel, and Ronald Petrlic. 2020. Stand der Technik bei Videokonferenzen – und die Interpretation der Aufsichtsbehörden: "Naming and shaming" beim Datenschutz. *Datenschutz und Datensicherheit-DuD* 44 (2020), 740–747.

[18] GoTo. 2024. How do I create an end-to-end encrypted session? https://support.goto.com/meeting/help/how-do-i-create-an-end-to-end-encrypted-session, [Online; accessed on February 15, 2024].
[19] Raiful Hasan and Ragib Hasan. 2021. Towards a threat model and security analysis of video conferencing systems. In *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, Las Vegas, NV, USA, 1–4.
[20] Michael Howard and Steve Lipner. 2006. The Security Development Lifecycle.
[21] Adi Ikan, Liri Porat, and Ori Hamama. 2020. Fixing the Zoom 'Vanity Clause' – Check Point and Zoom collaborate to fix Vanity URL issue. https://blog.checkpoint.com/security/fixing-the-zoom-vanity-clause-check-point-and-zoom-collaborate-to-fix-vanity-url-issue/ [Online; accessed February 15, 2024].
[22] Balu N. Ilag. 2021. Tools and technology for effective remote work. *International Journal of Computer Applications* 174, 21 (2021), 13–16.
[23] Dima Kagan, Galit Fuhrmann Alpert, and Michael Fire. 2023. Zooming into video conferencing privacy. *IEEE Transactions on Computational Social Systems* 11, 1 (2023), 933–944.
[24] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My Data Just Goes Everywhere: User Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*. USENIX, Ottawa, Canada, 39–52.
[25] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK). 2020. Orientierungshilfe Videokonferenzsysteme. https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf [Online; accessed on February 15, 2024].
[26] Tiffany C Li. 2020. Privacy in pandemic: law, technology, and public health in the COVID-19 crisis. *Loy. U. Chi. LJ* 52 (2020), 767.
[27] Robertas Maleckas, Kenneth G Paterson, and Martin R Albrecht. 2023. Practically-exploitable Vulnerabilities in the Jitsi Video Conferencing System.
[28] Microsoft. 2024. Use end-to-end encryption for Microsoft Teams calls. https://support.microsoft.com/en-us/office/use-end-to-end-encryption-for-microsoft-teams-calls-1274b4d2-b5c5-4b24-a376-606fa6728a90, [Online; accessed on February 15, 2024].
[29] Carrie Mihalcik. 2020. Microsoft listened to Skype calls with 'no security' to protect recordings. https://www.cnet.com/news/privacy/microsoft-listened-to-skype-calls-with-no-security-to-protect-recordings-report-says/, [Online; accessed on January 10, 2022].
[30] R. Mir and G. Gebhart. 2020. Harden Your Zoom Settings to Protect Your Privacy and Avoid Trolls. https://www.eff.org/deeplinks/2020/04/harden-your-zoom-settings-protect-your-privacy-and-avoid-trolls [Online; accessed on February 15, 2024].
[31] Sara Morrison and Rebecca Heilweil. 2020. How teachers are sacrificing student privacy to stop cheating. https://www.vox.com/recode/22175021/school-cheating-student-privacy-remote-learning [Online; accessed on February 15, 2024].
[32] Deeraj Nagothu, Ronghua Xu, Yu Chen, Erik Blasch, and Alexander Aved. 2021. Defake: Decentralized enf-consensus based deepfake detection in video conferencing. In *2021 IEEE 23rd International Workshop on Multimedia Signal Processing (MMSP)*. IEEE, Tampere, Finland, 1–6.
[33] NIST. 2020. CVE-2020-11878 Detail. https://www.cve.org/CVERecord?id=CVE-2020-11878 [Online; accessed on February 15, 2024].
[34] NIST. 2022. CVE-2022-28756 Detail. https://nvd.nist.gov/vuln/detail/CVE-2022-28756 [Online; accessed on February 15, 2024].
[35] Sarah Prange, Sarah Delgado Rodriguez, Lukas Mecke, and Florian Alt. 2022. "I Saw Your Partner Naked": Exploring Privacy Challenges During Video-Based Online Meetings. In *Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia* (Lisbon, Portugal) *(MUM '22)*. Association for Computing Machinery, New York, NY, USA, 71–82. https://doi.org/10.1145/3568444.3568468
[36] Dieter Rasch, Klaus D Kubinger, and Karl Moder. 2011. The two-sample t test: pre-testing its assumptions does not pay off. *Statistical papers* 52 (2011), 219–231.
[37] Thomas Reisinger, Isabel Wagner, and Eerke Albert Boiten. 2022. Security and privacy in unified communication. *ACM Computing Surveys (CSUR)* 55, 3 (2022), 1–36.
[38] Thomas Reisinger, Isabel Wagner, and Eerke Albert Boiten. 2023. Unified Communication: What do Digital Activists need?. In *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE Computer Society, Los Alamitos, CA, USA, 141–149.
[39] Karen Renaud, Melanie Volkamer, Arne Renkema-Padmos, Emiliano De Cristofaro, and Steven J Murdoch. 2014. Why doesn't Jane protect her privacy?. In *14th International Symposium on Privacy Enhancing Technologies-PETS 2014*. Springer, Amsterdam, The Netherlands, 244–262.
[40] Ramandeep Kaur Sandhu, João Vasconcelos-Gomes, Manoj A Thomas, and Tiago Oliveira. 2023. Unfolding the popularity of video conferencing apps–A privacy calculus perspective. *International Journal of Information Management* 68 (2023), 102569.
[41] Marwin Schmitt, Judith Redi, Dick Bulterman, and Pablo S Cesar. 2017. Towards individual QoE for multiparty videoconferencing. *IEEE Transactions on Multimedia* 20, 7 (2017), 1781–1795.
[42] Adam Shostack. 2014. Threat Modeling: Designing for Security.
[43] Statista. 2022. Bevölkerung nach relevanten Altersgruppen 2021. https://de.statista.com/statistik/daten/studie/1365/ [Online; accessed on February 14, 2024].
[44] Prolific Team. 2023. What are the advantages and limitations of an online sample? https://researcher-help.prolific.com/hc/en-gb/articles/360009501473-What-are-the-advantages-and-limitations-of-an-online-sample [Online; accessed on May 15, 2024].
[45] Los Angeles Times. 2020. Coronavirus social distancing around the world. https://www.latimes.com/world-nation/story/2020-04-06/coronavi-social-distancing-around-the-world, [Online; accessed on February 15, 2024].
[46] Jan Tolsdorf, Florian Dehling, Delphine Reinhardt, and Luigi Lo Iacono. 2021. Exploring mental models of the right to informational self-determination of office workers in Germany. *Proceedings on Privacy Enhancing Technologies* 2021, 3 (2021), 5–27.
[47] Victoria Turk. 2020. Zoom took over the world. This is what will happen next. https://www.wired.co.uk/article/future-of-zoom, [Online; accessed on February 15, 2024].
[48] O. Vegeris. 2020. "Important, Spoofing"- zero-click, wormable, cross-platform remote code execution in Microsoft Teams. https://github.com/oskarsve/ms-teams-rce https://github.com/oskarsve/ms-teams-rce [Online; accessed on February 15, 2024].
[49] Cody Venzke. 2020. For remote learning, privacy challenges go beyond zoom-bombing. https://nvd.nist.gov/vuln/detail/CVE-2022-28756 [Online; accessed on February 15, 2024].
[50] Business Wire. 2021. Worldwide Unified Communications & Collaboration (UC & C) market soars in 2020, according to IDC. https://www.businesswire.com/news/home/20210329005600/en, [Online; accessed on February 15, 2024].
[51] Yucheng Yang, Jack West, George K. Thiruvathukal, Neil Klingensmith, and Kassem Fawaz. 2022. Are You Really Muted?: A Privacy Analysis of Mute Buttons in Video Conferencing Apps. *Proc. Priv. Enhancing Technol.* 2022, 3 (2022), 373–393.
[52] Eric S. Yuan. 2020. Zoom Blog: A Message to Our Users. https://blog.zoom.us/a-message-to-our-users/, [Online; accessed on February 15, 2024].
[53] Eric S. Yuan. 2020. Zoom's Use of Facebook's SDK in iOS Client. https://blog.zoom.us/zoom-use-of-facebook-sdk-in-ios-client/ [Online; accessed on February 15, 2024].
[54] Zoom. 2024. Setting up advanced chat encryption. https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0065662, [Online; accessed on February 15, 2024].

A SURVEY QUESTIONS

A.1 Informed Consent

The purpose of this survey is to learn about my use and perception of video conferencing apps. I consent to the collection, processing, and use of my responses for research purposes by *anonymous.instution*. I can cancel this survey or withdraw my consent at any time without any disadvantage to me. The data will be completely deleted. For further analysis of the collected data, any information about my person will be anonymized. My participation in this survey is completely voluntary.
I can withdraw my consent at any time by sending an email to *anonymous.authors.email*.

- By selecting "I agree", you indicate that you have read the consent form and given your consent.
  ○ I agree ○ I do not agree

A.2 General Questions - Part 1

A.2.1 Use of Applications.

- **SQ1:** Have you used video conferencing applications within the last 2 years? [*The rest of the questionnaire will only be presented if the answer is "Yes".*]
  ○ Yes ○ No
- **SQ2:** Please select all applications that you have used at least once.
  □ Amazon Chime □ BigBlueButton □ Cisco Webex Meetings □ Discord □ Google Meet □ GoToMeeting □ Logitech □ Microsoft Teams □ Skype □ Skype for Business □ Slack □ TeamViewer Meeting (Blizz) □ Jitsi Meet □ Viber □ Zoom □ Own applications of the company □ Other apps: [ ]
- **SQ3:** For which of the applications used did you suggest using on your own initiative?
  ○ none/never suggested an application myself □ …<list of **selected** options from **SQ2**> □ Other apps: [ ]
- **SQ4:** Which of the applications you use have you ever avoided due to lack of usability?
  ○ none/never avoided an application due to lack of usability □ …□ Amazon Chime □ BigBlueButton □ Cisco Webex Meetings □ Discord □ Google Meet □ GoToMeeting □ Logitech □ Microsoft Teams □ Skype □ Skype for

Business □ Slack □ TeamViewer Meeting (Blizz) □ Jitsi Meet □ Viber □ Zoom □ Own applications of the company □ Other apps: [ ]

- **SQ5:** For which applications have the use already been prohibited or restricted by others (e.g. employers, customers, other participants, etc.)?
  ○ none/use has never been restricted or prohibited □ …<list of **all** options from **SQ2**>
- **SQ6:** Have you ever avoided an application because of your own security or privacy concerns?
  ○ Yes ○ No
- **SQ7:** Which applications have you avoided due to these concerns?
  □ …<list of **all** options from **SQ2**>

A.2.2 Frequency and Period of Use.

- **SQ8:** Were you already using video conferencing apps before the lockdown in spring 2020?
  ○ Yes ○ No
- **SQ9:** Are you currently still using video conferencing applications?
  ○ Yes ○ No
- **SQ10:** Did you use the applications used for professional or private purposes?
  <list of **selected** options from **SQ2**>: ○ professionally ○ privately ○ both
- **SQ11:** How frequently did you use the applications during the following time periods?
  - **Before lockdown 2020:** *[Will only be presented if **SQ8** was answered with "Yes".]*
    <list of selected options from **SQ2**>: ○ not at all ○ once ○ less often than monthly ○ monthly ○ weekly ○ daily
  - **During lockdown 2020:**
    <list of selected options from **SQ2**>: ○ not at all ○ once ○ less often than monthly ○ monthly ○ weekly ○ daily
  - **Within the last 3 months:** *[Will only be presented if **SQ9** was answered with "Yes".]*
    <list of selected options from **SQ2**>: ○ not at all ○ once ○ less often than monthly ○ monthly ○ weekly ○ daily
- **SQ12:** How do you rate the usability of the applications used?
  <list of selected options from **SQ2**>: ○ very good ○ good ○ neither good nor bad ○ bad ○ very bad

A.2.3 Use of Functions.

- **SQ13:** Please select all functions that you have already used in videoconferences.
  ○ none of these functions □ Audio □ Video □ Chat □ Reactions (e.g., raise hand) □ Screen Sharing □ Background Filter □ Other Functions: [ ]
- **SQ14:** Have you ever hosted or co-hosted a videoconference?
  ○ Yes ○ No
- **SQ15:** Please select all functions that you have already used as host or co-host in videoconferences. *[Will only be presented if **SQ14** was answered with "Yes".]*
  ○ none of these functions □ Live Translation □ Recording □ Cloud Storage □ Waitingroom □ Allow Microphone (enable/disable) □ Allow Video (enable/disable) □ Allow Screen Sharing (enable/disable) □ Lock Meeting □ Suspend Participant Activities □ Remove Participants □ Other Functions: [ ]
- **SQ16:** Have you ever avoided functions to protect your privacy or communication?
  ○ No, never for this reason. □ Audio □ Video □ Chat □ Recording □ Cloud Storage □ Screen Sharing □ Other Functions: [ ]

A.2.4 Locations and Devices.

- **SQ17:** Please select all locations from which you have already participated in video conferences.
  □ From home:
  - □ bedroom □ kitchen □ living room □ study room □ nursery □ bathroom □ garden □ balcony

  □ From workspace:
  - □ individual office □ multi-party office (2-5 people) □ open-plan office (over 5 people) □ conference room

  □ From other locations:
  - □ public transport (e.g., train, bus, train) □ gastronomy (e.g., cafe, restaurant) □ public facilities (e.g., library, co-working spaces, cultural facilities, train stations, airport) □ open-air public spaces (e.g., green spaces, street furniture, cultural assets) □ at friends, acquaintances, relatives or partners house

  □ From other places: [ ]
- **SQ18:** Have you already participated in professional videoconferences from the home-office?
  ○ Yes ○ No
- **SQ19:** Please select all devices that you have already used to participate in video conferences.
  □ desktop computer □ notebook or laptop □ tablet □ mobile phone □ landline phone □ conference system □ other devices: [ ]
- **SQ20:** Have you ever used external devices (e.g. headset, microphone, headphones, camera) to participate in video conferences for certain reasons?
  ○ No, I have never used external devices. □ to improve the quality of audio/video □ to protect my privacy □ to avoid disturbing others □ other reasons: [ ]

A.2.5 Embarrassing/Unpleasant Situations.

- **SQ21:** Please select all situations that have already happened to you or other participants in videoconferences.
  □ accidentally shared audio content □ accidentally shared video content □ accidentally shared screen content □ accidentally activated inappropriate reaction (e.g. clapping). □ accidentally activated unsuitable video filters □ accidentally shared inappropriate content in the chat ○ none of these situations
- **SQ22:** Have you ever experienced these situations as uncomfortable or embarrassing for yourself or others?
  <list of selected options from **SQ21**>: ○ Yes, it was embarrassing/uncomfortable at least once ○ No, never
- **SQ23:** If you have experienced other embarrassing or unpleasant situations in a videoconference, you can add them here. [ ]
- **SQ24:** Which of these measures have you already taken to protect your privacy or communications?
  □ enable/disable microphone only when needed □ enable/disable the camera in certain situations □ change camera orientation or room setup □ using background filters or virtual backgrounds □ using pseudonyms instead of real names □ close other applications before activating screen sharing □ enable end-to-end encryption □ masking the camera or using the camera cover □ customize an application's security settings ○ none of these measures □ other measures: [ ]

A.2.6 Participation in Training.

- **SQ25:** Have you ever attended training courses on how to use video conferencing applications?
  ○ No ○ Yes, initiated by the employer ○ Yes, initiated by myself
- **SQ26:** Please select all applications for which you have already attended training. *[Will only be presented if **SQ25** was answered with "Yes".]*
  ○ none of these applications □ <list of **selected** options from **SQ2**>
- **SQ27:** What content was part of the training courses attended? *[Will only be presented if in **SQ26** at least one tool has been selected.]*
  <list of **selected** options from **SQ26**>: □ handling/usage □ security/privacy □ other content

A.2.7 Security and Privacy Issues.

- **SQ28:** Have you ever heard of security and privacy issues related to video conferencing applications?
  ○ No, never □ from the media □ from my work environment □ from my private environment □ from personal experience □ from other sources
- **SQ29:** Have these issues influenced your use of video conferencing applications? *[Will only be presented if in **SQ28** was not answered with "No".]*
  ○ No, it had no effect. □ I continue to use the affected applications, but would like to avoid them. □ I continue to use the affected applications and have adjusted the security settings. □ I use applications that I consider less critical. □ I have become more cautious when using video conferencing applications.
  □ other reactions: [ ]
- **SQ30:** You have stated that you have used the following applications at least once. How do you rate the security and privacy of the applications?
  <list of selected options from **SQ2**>: ○ very good ○ good ○ neither good nor bad ○ bad ○ very bad

A.2.8 Videoconference Events.

- **SQ31:** What type of videoconference have you already conducted yourself or attended as a participant? Do not choose either option if you have never attended the event mentioned.
  □ conducted □ attended as a participant
  - private communication with friends, acquaintances, or relatives
  - leisure, sports, music, and cultural events
  - distance learning or lectures
  - professional collaboration
  - customer contact
  - job interviews

- professional celebrations
- advice on IT and technology
- advice on legal issues
- advice on finances and contracts
- doctor consultations and health care
- political involvement
- church services
- other events

A.3 Context-Specific Questions

Since the focus of this paper is on a general consideration of the use of video conferencing applications and in order to be able to look at the results from the *General Questions* part of the survey in depth, we excluded the context-specific questions from this paper.

A.3.1 Description of Usage Scenario. <Context-Specific Questions: **SQ32** – **SQ47**> :

A.3.2 Perception of Usage Scenario. <Context-Specific Questions: **SQ48** – **SQ51**> :

A.4 General Questions - Part 2

Security and Privacy Threats.

- **SQ52:** How realistic do you generally assess the following threats when using video conferencing applications?
  ○ very realistic ○ rather realistic ○ neither nor ○ not really realistic ○ not realistic at all
  - Fake identities in a conference (e.g., people pretending to be someone else in a conference).
  - Loss of control over a conference (e.g., guest participants illegally taking over admin rights)
  - Third-party access to own devices via a conference (e.g., chat messages that automatically run malware)
  - Access to camera/microphone by other applications (e.g., apps/websites that automatically gain access during a conference)
  - Sharing fake invitation links (e.g., emails requesting conference attendance and login credentials)
  - Sharing inappropriate or disturbing content (e.g., by people entering a conference without authorization)
  - Recording of content by other participants (e.g., using external programs to record)
  - Recording of content by providers (e.g., for analysis purposes)
  - Recording of content by authorities (e.g., by police, law enforcement, or intelligence agencies)
  - Misuse of recordings (e.g., legitimate recordings that are misappropriated)
- **SQ53:** What makes you feel personally threatened or harmed when using video conferencing applications?
  [ ]

A.5 Demographics

[All demographic information is optional.]

- Please indicate your year of birth:
  [*2004-1922*] ○ no response
- Please indicate your gender:
  ○ female ○ male ○ various ○ no response
- What describes your marital status best?
  ○ single ○ living together in partnership ○ married/in registered partnership ○ divorced/ living separately ○ widowed ○ no response
- Do you have children?
  ○ Yes ○ No ○ no response
- Please indicate your current professional (main) activity:
  ○ employee, civil servant ○ self-employed ○ student ○ trainee ○ student ○ unemployed ○ housewife, househusband, or on parental leave ○ pensioner ○ no response
- Please indicate your highest school education degree:
  ○ no general school leaving certificate ○ still in school education ○ secondary school leaving certificate ○ middle school leaving certificate ○ high school diploma ○ no response
- Please indicate your highest professional education degree:
  ○ no professional qualification ○ apprenticeship/vocational training ○ technical school qualification (master, technician, etc.) ○ bachelor ○ master, diploma, state examination, magister ○ PhD ○ no response
- Are you employed in computer science or a similar field (work or study)?
  ○ Yes ○ No ○ no response

B OVERVIEW OF USAGE FREQUENCY

Table 8: Usage frequencies for top-ten apps *before*, *during*, and *after* the pandemic (N=251).

	before the pandemic					*during* the pandemic					*after* the pandemic				
	once	>monthly	monthly	weekly	daily	once	>monthly	monthly	weekly	daily	once	>monthly	monthly	weekly	daily
Zoom	7	16	11	5	2	14	37	33	84	45	13	36	44	58	6
MSTeams	7	13	8	13	10	8	28	36	54	59	5	20	25	38	53
Skype	7	80	24	2	3	21	45	30	18	4	9	22	9	5	1
Discord	1	9	16	10	11	14	21	14	29	17	7	14	15	11	12
Webex	4	14	4	8	3	13	23	12	17	4	7	3	8	7	2
SkypeB.	2	20	5	8	13	2	21	5	16	15	4	2	6	11	12
Jitsi	1	4	2	0	1	8	19	13	10	2	5	8	4	6	2
GoogleM.	6	5	2	2	0	11	13	6	7	1	7	7	5	7	1
GoToM.	2	11	3	4	0	6	14	3	7	0	3	4	3	3	0
BBB	1	2	0	2	0	9	11	3	9	2	3	5	1	5	1

C OVERVIEW OF APPLICATIONS USED

Table 9: Top-ten: The most used apps in the study; best median and best average usability and security rating scores per column in bold (N = 251).

			Only apps that have been used at least once [2]										*Incl. "never used"* [3]	
	used by		Usability rating [1]		Security rating [1]		self-chosen		avoided due to usability		avoided due to security		restricted by third parties	
Apps.	*n*	%	med	avg	med	avg	*n*	%	*n*	%	*n*	%	*n*	%
Zoom	221	88	**4**	**4.086**	3	3.249	118	53	18	8	27	11	59	24
MS Teams	204	81	**4**	**4.069**	4	3.593	105	51	32	16	10	4	23	9
Skype	159	63	3	3.377	3	3.094	62	39	48	30	14	6	30	12
Discord	97	39	**4**	**3.897**	3	3.309	38	39	16	16	6	2	12	5
Webex	85	34	3	3.294	4	3.565	14	16	24	28	4	2	9	4
Skype Business	78	31	4	3.539	3	3.462	19	24	14	18	5	2	12	5
Jitsi	57	23	3	3.386	**4**	**3.790**	29	51	11	19	1	0	6	2
Google Meet	51	20	4	3.510	3	3.196	11	22	2	4	11	4	7	3
GoTo Meeting	42	17	3	3.214	3	3.167	4	10	10	24	2	1	4	2
BigBlueButton	41	16	4	3.439	**4**	**3.902**	8	20	11	27	0	0	6	2

[1] Score between 1 and 5 where 1 indicates *very bad*, and 5 indicates *very good*; [2] Percentages refer to the number of users per app;
[3] Percentages refer to the number of all users (N = 251).

D EXPERIENCE WITH SECURITY AND PRIVACY ISSUES

Table 10: Participants' sources for learning about security and privacy issues, and participants' reaction

Sources from which participants learned about security and privacy issues (N = 251)				*Reaction to knowledge of security and privacy issues in relation to affected apps* (N = 185)[1]		
n	learned from *x* source types	*n*	learned about issues from …	*n*	n^3	responded to affected app by
66	0	66	never [2]	89	89	showing no reaction
91	1	138	media	31	16	would like, but could not avoid
5	2	92	work life	40	15	becoming more cautious when video conf.
28	3	55	social life	36	21	adjusting their security settings
10	4	19	own experience	41	41	switching to less precarious apps
1	5	26	other sources	3	–	other reactions

[1] all participants who learned about issues; [2] never learned about issues; [3] number of participants for whom this was the most severe response.

E EXAMPLE THREATS BASED ON STRIDE AND LINDDUN

Table 11: Example threats based on STRIDE and LINDDUN with descriptions of threats. Descriptions are based on Reisinger et al. [37]. Exemplary threats are only assigned as examples and may correspond to more than one category.

STRIDE	**Description of Security Threats**	**Exemplary threat**
Spoofing	attacker pretend to be another attendee	Faking Identities [4, 32]
Tampering	attacker modifies VC data	Sharing Improper Content [30]
Repudiation	attacker claims to be not responsible	Misusing Recordings [32]
Information Disclosure	attacker is unauthorized provided with data	Accessing Devices [48]
Denial of Service	attacker harms availability of the VC	Faking Invitations [15]
Elevation of Privilege	attacker gains unauthorized further permissions	Taking Over Control [33, 34]
LINDDUN	**Description of Privacy Threats**	**Exemplary threat**
Linkability	attacker can infer a relation between data	Misusing Recordings [23]
Identifiability	attacker violates pseudonymity/anonymity	Misusing Recordings [53]
Non-repudiation	attack prevents the user to deny sth.	Recording by Attendees [2]
Detectability	attacker can discover whether an item exists	Recording by Authorities [38]
Information **D**isclosure	attacker is unauthorized provided with data	Accessing Audio/Video [51]
Content **U**nawareness	user is unaware that a system collects data	Recording by Provider [51, 53]
Policy/consent **N**on-compliance	VC app does not comply with its privacy policy	Recording by Provider [15, 29]

F T-TEST FOR USED MEASURES AND REALISM OF THREATS

Table 12: Dependence between use of security measures and perceptions of threats; Welch tow-sample t-test results for mean differences in perception of threats ($\varnothing T$) between sample n_1 (used specific measure) sample n_0 (did not use specific measure), $N = 251$**.**

Measure	Samples [1]		Threat	Realism of Threat [2]		T-Test	
	n_1	n_0		$\varnothing T_{n_1}$	$\varnothing T_{n_0}$	$\triangle_{\varnothing T_{n_1},\varnothing T_{n_0}}$	df
activate E2E	41	210	recording by providers	4.37	3.67	0.70^{***}	65.8
activate E2E	41	210	recording by authorities	3.63	2.94	0.69^{***}	56.2
adapt settings	57	194	accessing audio/video	3.56	3.36	0.20	88.5
cover camera	135	116	by third parties	3.44	3.37	0.07	240.4
disable audio	234	17		4.23	3.59	0.64	17.3
disable video	226	25		4.24	3.68	0.56^{*}	27.9
filter background	144	107	recording	4.26	4.08	0.19	222.3
pseudonyms	52	189	by attendees	4.53	4.09	0.44^{**}	95.5
close other apps	142	109		4.30	4.03	0.28^{*}	225.9
focus camera	146	105		4.35	3.95	0.4^{**}	192.4
disable audio	234	17		3.59	3.35	0.23	17.5
disable video	226	25		3.60	3.32	0.28	27.8
filter background	144	107	misusing legitimate	3.57	3.57	0.0	224.4
pseudonyms	52	189	recordings	3.79	3.51	0.28^{+}	87.3
close other apps	142	109		3.61	3.52	0.08	226.4
focus camera	146	105		3.71	3.38	0.33^{*}	212.3

t-test: $^{+}$p<0.1; *p<0.05; **p<0.01; ***p<0.001. [1] Sample 1: used measure (at least once); Sample 0: used measure not at all;

[2] Score 1-5: 1 indicates *not realistic at all*, 5 indicates *very realistic*; df = degrees of freedom.