

USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

From Thrift Stores to Digital Storefronts: Users' Perspectives on Privacy and Security of Online Second-Hand Shopping in Germany

Darya Zarkalam and Anna Lena Rotthaler, *Paderborn University;*
Lucy Simko, *Barnard College;* Yasemin Acar, *Paderborn University*

https://www.usenix.org/conference/soups2026/presentation/zarkalam

This paper is included in the Proceedings of the Twenty-Second Symposium on Usable Privacy and Security.

August 24–26, 2026 • Hannover, Germany

ISBN 978-1-939133-59-5

Open access to the Proceedings of the Twenty-Second Symposium on Usable Privacy and Security is sponsored by USENIX.

From Thrift Stores to Digital Storefronts: Users' Perspectives on Privacy and Security of Online Second-Hand Shopping in Germany

Darya Zarkalam
Paderborn University

Anna Lena Rotthaler
Paderborn University

Lucy Simko
Barnard College

Yasemin Acar
Paderborn University

Abstract

The emergence of online second-hand shopping platforms such as eBay, Craigslist, and Facebook Marketplace has added new ways for consumers to shop second-hand. Although these platforms offer some features for security and safety, users still encounter fraud, scams, and personal safety risks when (trying to) purchase second-hand goods online. Here, we seek to understand users' privacy, safety, and security practices when using online second-hand shopping platforms, both technical and interpersonal. We conducted semi-structured interviews with 20 users of online second-hand shopping platforms in Germany, to learn their security and privacy perceptions and concerns, experiences, and protective strategies. Our study identifies key security and privacy concerns, including scams, personal safety, and the misuse of personal information. We find that platform-integrated features, such as user reviews and payment systems, are perceived as effective for mitigation. Furthermore, we find that trust in platforms is shaped by social factors. Based on these insights, we make recommendations for platforms to increase user safety.

1 Introduction

Second-hand online shopping markets such as eBay, Facebook Marketplace, Vinted, and Kleinanzeigen[1] are a thriving and growing practice around the world [103], and particularly in Germany, where our study was conducted. Consumers shop online for second-hand goods for a variety of reasons, including recreation, environmental and sustainability concerns, financial constraints, and a sense of community [102, 105]. While second-hand online shopping markets share characteristics with both conventional online shopping and offline second-hand shopping, they occupy a unique space in between—a digitization of offline secondhand shopping practices (e.g., flea markets and newspaper ads). This digitization allows users to shop at any time from home, rather than going to a physical market that may operate, say, for a few hours once a week. Platforms enrich user-to-user interactions with features like ratings, reviews, messaging, and integrated payment—features that mimic some offline interactions for trust-building and safety. It is the nature of these user-to-user interactions, and the role of the platform in supporting but not controlling them, that makes second-hand online shopping markets unique from a perspective of interpersonal, online, and offline privacy and security.

Despite their popularity, online second-hand shopping platforms have been associated with a range of privacy and security risks. For example, malicious actors have phished would-be buyers with an external phishing site for payment [11], and have abused PayPal's buyer protection by posing as both buyer and seller [65]. These issues may disproportionately affect vulnerable populations—e.g., people experiencing poverty [55]—due to the nature of the platforms.

Due to the role of the platform as *moderator* but not *seller*, online second-hand shopping both carries inherent risk, and presents an opportunity for platforms (as moderators) to protect both buyers and sellers. To better support the safety of users (and help the platforms do so), the security and privacy community needs to understand how users perceive and experience security and privacy threats on online second-hand shopping platforms.

Existing literature about second-hand online shopping primarily focuses either narrowly on left-behind data on electronic devices, or broadly on consumers' interactions (without a focus on privacy and security); there is little research on how the collection of privacy threats interact. This paper, therefore, aims to explore users' experiences, perceptions, and privacy

[1] Vinted and Kleinanzeigen are popular in Germany.

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Hannover, Germany.

and security practices on online second-hand platforms in Germany. We ask the following research questions:

RQ1: *What are users' security and privacy concerns on online second-hand shopping platforms?*

RQ2: *How do users perceive the effectiveness of security and privacy measures implemented by the platforms?*

RQ3: *What strategies do users employ to mitigate security and privacy risks when engaging with these platforms?*

RQ4: *How do users perceive trust on online second-hand shopping platforms?*

Through interviews with 20 users of online second-hand platforms in Germany, we find that users face a variety of security and privacy concerns, from scams and misuse of personal information to physical safety risks. We identify security and privacy features that users consider effective, including user reviews and ratings and date of joining, as well as platform-integrated payment systems. We find that users mitigate security and privacy risks by communicating with other platform users, limiting the personal information they share, opting for safe payment strategies and taking precautionary steps to ensure personal safety when meeting other sellers or buyers. Our study also reveals that users' trust in online second-hand shopping platforms is shaped by a combination of social and systemic security and privacy elements.

While our case study takes place in Germany, our findings may produce insights and recommendations transferable to other parts of the world, as the key insight is the necessity of the platform to support both privacy and flexibility through user-to-user negotiation and transaction. We make recommendations for policy-makers and platforms to increase trust and safety in the online second-hand shopping ecosystem, through additional safety features and UX/UI design.

2 Background and Related Work

Here we provide background information about the platforms in our study and explore prior work in security and privacy in second-hand shopping, including security and privacy of used electronic devices, and security and privacy risks and challenges in online marketplaces.

Platforms in Our Study. To contextualize participants' experiences and our results, we first describe the platforms used by our participants here: Vinted, Kleinanzeigen, and eBay (key features summarized in Appendix Table 2).

All three platforms let users create platform-specific profiles, post or browse listings, and communicate through built-in messaging, in order to sell or buy second-hand goods online. At the same time, they differ in how they organize payment, buyer protection, reputation, verification, and, in some cases, shipping or handover. Vinted and Kleinanzeigen both offer platform-supported payment flows in which buyer protection is tied to the integrated transaction process, usually for a fee paid by the buyer [46, 49, 81, 82]. eBay similarly offers buyer protection for eligible purchases completed through its own payment flow [20, 24]. In our work, participants distinguished between transactions completed within a platform-supported flow and those negotiated externally.

The three platforms also differ in how they help users evaluate the trustworthiness of others. eBay has a long-standing feedback system tied to transactions [22], Vinted allows users to leave star ratings and written reviews after completed orders [87], and Kleinanzeigen provides ratings and badges that also reflect interaction behavior outside completed purchases [44, 52]. Public-facing user verification is also uneven. Vinted is the only platform that offers optional visible account verification [79], while Kleinanzeigen emphasizes profile activity and badges [51]. Similarly, eBay does not appear to rely on a general visible user-verification feature, but instead on a combination of transaction-based reviews and other trust signals for some qualifying commercial sellers, such as the *"eBay Top Service"* label [21, 22, 26, 27]. These differences help explain why participants sometimes spoke about "ratings" or "verification" as if they were comparable across platforms, while in practice the underlying mechanisms differed.

Additionally, platforms also make some transaction paths more prominent than others. For example, Vinted encourages users to trade through its integrated system, linking it to benefits such as support, reviews, and listing visibility [88]. Some integrated flows have privacy implications, such as limiting when address information is disclosed during shipping [85, 93]. Kleinanzeigen and eBay likewise emphasize protected or platform-supported payment methods and warn users about risky arrangements outside those flows [30, 41, 47].

Left-Behind Data on Second-Hand Devices. In our research community, much of the work about security and privacy in the second-hand market has focused on data left behind on used electronics. Though we summarize this work here, we direct readers to [62] for a more in-depth survey.

Prior work has shown that second-hand storage devices available from secondary markets often retain residual data [34]; for example, one study found that 71% of 311 analyzed devices contained residual data, including personally identifiable, personal, or business information [76]. Second-hand hard drives and USB storage devices can contain substantial recoverable private information, including medical records, financial details, and authentication tokens [33, 39, 66, 71]. Sensitive information on mobile and IoT devices—even after factory resets— includes call logs, contacts, app tokens, and browsing histories [4, 6, 70]. Sensitive information persists on gaming consoles too despite factory resets, including recoverable credentials, browsing histories, and linked payment information on Sony PlayStations [13, 14] and residual eShop credentials, Wi-Fi details, and saved game data remain forensically accessible on other gaming devices even after console resets, with cloud synchronization introducing fur-

ther security challenges [32, 68, 108]. Additionally, users also do not always understand how to securely erase data [56]. Roberts et al. found, in a study of stolen devices resold by U.S. police, that the phones were not securely wiped, exposing victims' emails, videos, and financial data to secondary users [70]. As this body of work shows, inadequate data sanitization practices and tools result in privacy and security risks that present harm to users (such as identity theft and financial fraud), highlighting a systemic need for improving safeguards in the second-hand electronics ecosystem [4, 70]. We build off this foundational body of work by considering the security and privacy in the *entire* second-hand shopping ecosystem.

Security and Privacy Risks and Challenges in Online Marketplaces. Prior work has explored security and privacy risks in online marketplaces in general (not just second-hand). Users care deeply about security and privacy when online shopping and using other user-to-user platforms (like ride-sharing and home-sharing), with concerns including fraud [57], platform data misuse [62, 109], identity theft [72], scams [62], and physical safety [2, 9, 58, 62]. Platform affordances do not always support user security and privacy, leaking data [60], enabling manipulation of ratings and reviews [36, 69], and failing to entirely catch scam posts [3].

Most relevant to our work are Mokhberi's studies of Facebook Marketplace examining how trust, privacy, and safety shape users' decision-making process [62], and the practical steps users take to manage these concerns, including how users establish trust with others, protect their privacy, and avoid safety risks during transactions [61]. Our study builds on this line of research by examining second-hand platforms commonly used in Germany—Kleinanzeigen, Vinted, and eBay—rather than a single North American, social-media-based marketplace. This difference matters not only at the level of setting, but also in terms of the privacy, trust, and safety dynamics. Unlike Facebook Marketplace, where activity is tied to users' Facebook identities and users have limited ability for pseudonymity, the platforms in our study allow platform-specific profiles. As a result, our findings suggest how different platform designs shape privacy, safety, and trust in practice. We find substantial overlap with Mokhberi et al. in that users in our study also relied on selective information sharing, payment-related caution, trustworthiness assessments, and precautions for in-person meetings [61]. Additionally, some of the issues users face, and many of the trust, privacy, and safety strategies identified for Facebook Marketplace, also appear across platforms in Germany. This suggests that these are not tied to a single marketplace, but exist across different platform designs and contexts, and across countries and continents. In addition, our results place greater emphasis on platform affordances themselves—especially integrated payment systems, buyer protection, ratings and reviews, and built-in communication features—as mechanisms that shape users' sense of safety and trust, while at times also creating new privacy concerns.

3 Methodology

Given the exploratory nature of our research, we used qualitative interviews to capture the detailed narratives of users of online second-hand shopping platforms. This is commonly done when researching users' security and privacy perceptions [53, 55]. We conducted semi-structured interviews with 20 users of online second-hand shopping platforms between September and November 2024.

In this section, we describe our methodology, including protocol, recruitment, demographics, interview procedure, and data analysis, as well as our ethical considerations.

3.1 Interview Protocol Development

Interview questions were developed based on our research questions and using and reviewing the platforms to understand their workflows and features. After creating an initial draft, we conducted two pilot interviews and then made minor adjustments to the interview flow and question wording. The second pilot interview was included in the final dataset, as the participant matched our recruitment criteria and the interview guide remained unchanged. The interview guide is organized as follows: We first asked participants about their motivations for using online second-hand platforms in order to set context. We then discussed security and privacy concerns (RQ1), perceptions of security measures on the platforms (RQ2), and protective strategies (RQ3). Finally, we discussed trust on online second-hand shopping platforms (RQ4). The full interview protocol can be found in the replication package [64].

3.2 Recruitment

To recruit participants, we used our personal network and posted a recruitment message on social media platforms such as Instagram and X. The recruitment message included general information about our study's objectives, a brief overview of our ethical considerations and confidentiality, and the link to our screening and demographics survey (which was preceded by our consent form). After consent, the survey served to determine whether those interested fit our inclusion criteria: at least 18 years old, and having used online second-hand shopping platforms at least once to buy or sell. We collected general demographic details, such as age, gender, country of residence, level of education, field of study, employment status, and income level. We used our university's instance of the online open-source tool LimeSurvey[2]. The complete survey can be found in the replication package [64]. At the end of the recruitment phase, we were able to make appointments with 24 volunteer participants. Out of these, 11 participants were recruited through our personal network, and the remaining 13 participants from social media. We initially wanted to recruit an international sample, but had trouble recruiting

[2] https://limesurvey.org/

outside Germany, so we later discarded interview data from four international participants to focus on our final group of 20 participants located in Germany.

3.3 Demographics

Our 20 participants all resided in Germany; their ages ranged from 18 to 44 years, many being 25–34. There were 13 men, 6 women, and 1 participant who preferred not to disclose their gender. They came from diverse fields of study, including Computer Science/IT (9), Engineering (6), Business/Economics (2), Social Sciences (1), Education (1), and Humanities/Arts (1). Income ranged from no income to €50,000–€69,999 annually, with the largest group (8) earning between €10,000 and €29,999. Detailed participant demographics are in Appendix A.1.

3.4 Interview Procedure

We conducted all interviews remotely via Zoom. All interviews were conducted in English by the first author; all participants were also fluent in English. Interviews lasted between 23 and 46 minutes with an average of 33 minutes.

Each interview started with introducing ourselves, outlining the general purpose of our research and describing the interview process. We reminded participants of their rights as outlined in the consent form, emphasizing that their participation was voluntary and that they could withdraw at any time or decline to answer questions. Although consent had already been obtained during the survey, we emphasized that it could be withdrawn at any point without consequences. We then explained that there were no right or wrong answers and reassured them that the interview would be conducted in a non-judgmental manner, emphasizing that our sole interest was learning about their experiences and thoughts. Before starting the interview, we addressed their questions. We then obtained consent to record and transcribe the interview.

For each topic, we started with open-ended general questions to encourage participants to share freely, asking follow-up questions as necessary. We followed the sequence of blocks in our interview guide from RQ1 to RQ4, starting with security and privacy concerns in online second-hand platforms and progressing through perception of platform measures, mitigation strategies, and trust dynamics. However, due to the semi-structured nature of the interviews, we remained flexible, allowing participants to deviate from this flow.

3.5 Data Analysis

We recorded all interviews using the GDPR-compliant transcription tool provided by Zoom, manually correcting transcripts afterward. We made efforts to de-identify all transcripts to preserve participants' privacy, described further in Section 3.6. We conducted thematic analysis, as outlined by Braun and Clarke [10], and followed their six-phase framework to systematically identify, analyze, and report patterns. To code, we adopted a joint inductive-deductive approach. We first created an initial codebook based on our research questions, and then expanded it with additional codes that emerged inductively through open-coding [104]. The first author coded all transcripts, while preliminary coding decisions and potential themes were regularly discussed with co-authors. The first author performed multiple iterative passes over the transcripts to refine the codes and ensure that they represented the data. Codes were added, merged, or removed until thematic saturation, i.e., no new codes were added [35, 73]. Using this codebook, the second author then independently coded four transcripts. We compared and discussed code applications and discrepancies, iterating structure but not definitions of the codebook. This process was repeated until all transcripts were coded by both and all disagreements were resolved; we therefore omit reporting IRR, in line with best practices [59].

The final codebook is included in the replication package [64]. Examples of codes include *Fraud and Scam*, *Transparency*, and *In-Person Meeting Precautions*. Finally, we used affinity diagramming in Miro to organize our codes, and clustered them into high-level themes. Examples of themes include *Reviews and Ratings as Effective Security Features*, *Strategies for Secure Payments*, and *The impact of social dynamics on trust*.

3.6 Ethics Statement

We did not formally require nor obtain ethics approval. We adhered to the ethical principles outlined in the Menlo report, including consent, withdrawal/skipping questions without loss of benefits along with data protection guidelines [5]. Participants were not compensated. Prior to consent, we thoroughly informed participants about our study procedure and the measures taken to protect their privacy, including data handling and de-identification of data.

To de-identify the data, if participants mentioned any potentially identifying information, such as their names or the cities they live in, we removed these details in the transcripts.

3.7 Limitations

Our study is subject to the limitations inherent to qualitative research, including self-reporting and recall bias, limited generalizability, and researcher bias. Our sample exhibits a gender imbalance, as it was predominantly composed of male participants. Additionally, all participants resided in Germany, with the majority being students in computer science. Our recruitment strategies, too, began with our social circles, which limited the diversity of our sample (both demographically and in terms of *types* of buyers and sellers). Therefore, this sample may not be representative of the larger population of online second-hand shopping platform users and may not



Figure 1: Qualifiers used throughout our results.

fully capture the breadth of user experiences, perceptions, and behaviors of other demographic groups. This may restrict the generalizability of our findings. However, generalizability was not our objective. While we acknowledge our study's limitations, our findings provide novel insights into users' perceptions and behaviors within the complex online second-hand ecosystem.

4 Results

We present results from 20 interviews with users of online second-hand platforms, including findings on privacy and security concerns (Section 4.1), perceived effectiveness of security features (Section 4.2), strategies to mitigate security and privacy risks (Section 4.3), and discussions about trust (Section 4.4). To avoid a quantitative interpretation of our work, we rely on qualifiers (see Figure 1).

Participants reported using three online second-hand platforms: Kleinanzeigen, eBay, and Vinted. Our findings, therefore, are specific to these platforms, but may also reflect trends across other platforms as well.

4.1 Privacy and Security Concerns

Participants reported multiple concerns stemming from privacy violations on online second-hand shopping platforms, including fraud, scams, financial loss, personal safety issues, and concerns related to information sharing. Despite reporting concerns, some believed they had adequate technical knowledge to protect themselves against risks. Notably, *offline* safety risks and concerns about sharing personal information with others in order to make purchases are specific to second-hand online shopping rather than conventional online shopping.

4.1.1 Financial Concerns

Most participants reported concerns about financial loss due to scammers.

Participants are concerned about scams. P13 referred to scams as "*a big concern*" and mentioned that such concerns influenced their behavior: "*that adds to me being a little bit more critical about security in these applications*" (P13). Participants shared personal experiences of being scammed, such as not receiving items they paid for. Participants also reported that hearing experiences of scam victims influenced their decision to use certain platforms, even if they had never personally encountered such issues. As P1 explained, "*there's a platform called Viagogo for reselling tickets, and I've heard that a lot of people get scammed on it. I will definitely not use it*". P5 explained they were discouraged from using online second-hand platforms after learning about scammers' techniques:

> "*Since I've looked this topic up and heard about all the new ways to scam people where it doesn't look like a scam, and it actually is so easy to do that [. . .] I have been a bit discouraged from second-hand shopping.*" — P5

Participants said they were suspicious of advertisements as scams. P7 avoided Facebook Marketplace because they perceived a lot of advertisements on the platform as possible scams: "*For example, on Facebook, I just check the prices, but I will never buy something, because I would say 90%, there's no statistics that I've heard about it, [...] I would say 90% of the ads on Facebook are fake. You can always see that*" (P7).

Participants' concerns about scams reflect reality, as scams do occur in second-hand online markets. Additionally, we observe that participants drew much of their threat modeling not only from personal experience but from stories they had heard from others, showcasing the influence of social networks in shaping threat models and privacy expectations [106].

Participants are concerned about certain payment models. Participants associated financial concerns with different payment paradigms, particularly pre-payment.

P20 shared their experience of identifying a potential scammer by the idiosyncratic way the other party instructed them to pay: "*And [the seller said] 'I only accept PayPal and I can't accept anything else. Don't put some information in the reference of the PayPal, in the note or something like that'* " (P20).

Financial loss is a real risk on second-hand platforms, as many transfer mechanisms widely used on these platforms are similar to cash in the sense that money, once sent, cannot be retrieved. As we report in Section 4.2, platform-integrated tools for financial protection were at the top of users' minds.

4.1.2 Offline Safety Risks

Users' concerns are not limited to security and privacy risks when navigating the platform or during online interactions, but also extend to physical, offline security and privacy.

The location for physically exchanging goods substantially impacts security concerns. Most participants highlighted concerns about meeting the other party in person, mostly related to the other person's behavior and the location and time of the meeting.

Risks ranged from fear of financial loss or theft to physical safety. Some described feeling physically at risk when they met the other person in their own residence. P17 described a hypothetical scenario to illustrate their concern about how an in-person exchange might go wrong: "*Then he comes to my place and it's like really unfriendly and threatens me if this*

thing isn't working". P9 shared a story about being physically intimidated into a lower price for their kitchen equipment[3]:

> "*[We] agreed on a price and everything, then suddenly, 5 guys came... they wanted to pay a quarter of the price we negotiated, and it was like those 5 guys were just standing there, and they didn't do anything. But it was obvious that they wanted to somehow force us to just give them the kitchen.*" — P9

Similarly, P18 felt at risk when meeting a seller:

> "*One time when I went to pick up the [stuff], it was a remote place and about outside of the city, and, you know, it was like a garden and I should go to this private garden to pick the property and that made me a bit unsecure.*" — P18

Physical security is an unavoidable component of exchanging goods in person, and there is by nature a limited role that the platform can play in mediating the actual interaction. However, online second-hand platforms could follow the lead of some ride-share apps in supporting physical safety with features allowing users to send their location to a friend or report an immediate issue. Additionally, it may be possible for community organizations to support physical safety by maintaining trusted and safe physical locations designated for the exchange of second-hand goods [15].

Gender considerations in perceptions of security threats. A few participants discussed the influence of gender on physical security. P12 highlighted the need for additional precautions for women: "*It doesn't necessarily have anything to do with the seller. It's just that when you're a woman, I feel like you have to be more careful*" (P12).

P8, a man, acknowledged feeling less vulnerable as a man, and emphasized that safety concerns mostly affect women:

> "*And I think it's sad, it's a topic that's more relevant or more affecting women. I think more often that people are approaching them on these platforms as well. So, it's one of the privileges of being a man, I'm afraid. I'm not affected that much.*" — P8

These participants highlight how identity affects safety risks arising from privacy and security violations, in line with prior work about rideshare safety [58].

4.1.3 Sharing Personal Information

Participants expressed substantial concerns about sharing personal information on online second-hand platforms, particularly information in their profiles (e.g., picture, location, etc) and financial information. In addition to concerns about misuse or theft of information by other users (as in Section 4.1.1), some also considered the platform itself an adversary, reflecting a realistic understanding of how companies may sell data or experience data breaches.

[3] In Germany, some flats do not come with "a kitchen"(Küche), which usually means a fitted kitchen unit (cabinets, countertops, sink, stove, etc.). It is common to sell/buy the kitchen unit when moving.

Participants are concerned about how platforms handle their data. About half of the participants expressed concerns about platforms' management of their information, fearing "*data breach*" (P1) and "*hacking*" (P18). P13 discussed discomfort with data sharing:

> "*I also am not comfortable just sharing data with the application. But sometimes you just don't have a choice. If you want to use the app, you have to share data, which I am concerned about...*" — P13

Participants are concerned about how information on their profile could be misused by other users. Information sharing concerns were not limited to the platform's data handling. Participants reported concerns about misuse of data by other users. They considered addresses, full names, profile pictures, and banking information the most sensitive types of information, and were cautious about sharing these with other users. P15 expressed concerns about sharing their full name: "*Privacy, for security, because if they know my name, my family name and obviously, if I buy something, you're going to know my address, and it doesn't feel so good*" (P15). P12 also explained their decision to not share their profile picture for safety: "*Because you never know the people who look at your profile. And there's weird people out there. So that's just a way to keep myself safe*" (P12).

4.1.4 Non-concerns

While some participants expressed concerns about privacy violations leading to financial loss or information loss, others felt these risks were minimal, acceptable, or unavoidable. About half of them expressed little or no concerns about sharing personal information on online second-hand shopping platforms. Some said they do not think about such issues (P7), while others said they do not "*put much information there*" anyways (P20). P12 expressed a feeling of "*security... based on the fact that I genuinely believe that people can be good*".

Technological confidence helps navigating on second hand platforms. Some participants considered technological confidence an advantage in navigating security and privacy risks. P4 described themselves as a "*tech-savvy person*" and said this competence contributed to their own awareness of security and privacy risks and ability to protect themselves: "*I think that it is important for other people to look at the website address, if there's HTTPS, or not*" (P4). While phishing was not part of participants' threat models for second-hand online shopping, it is always important to consider website legitimacy. We note, too, that prior work has found that security *confidence* affects secure practices more than *knowledge* [74], and that this may introduce opportunities to support users with any background.

Privacy fatigue and nihilism. While some acknowledged the risks, they also believed they did not have a choice but to accept the risks associated with online shopping. A few participants expressed privacy fatigue, as their data is already

shared with other platforms on the internet: "*I should [be concerned], but I think I just grew up with the internet and everything*" (P14). P2's privacy fatigue was somewhat mitigated by their trust in privacy regulations:

> "*I gotta admit I'm mostly too lazy to read the entire agreement and all that, but it seems that with this entire deal or these data privacy regulations we have nowadays, I guess that should be fine.* " — P2

4.2 Platform affordances as safety features

Despite concerns about financial loss, physical harm, and information loss, participants *do* use online second-hand markets, expressing that certain platform features—either real or desired—do (or could) support their privacy, security, and safety. These affordances, including transparency in data handling, verification of other users, and content moderation/scam detection, represent opportunities for online shopping platforms to better foster safe second-hand shopping experiences.

4.2.1 Crowd-sourced user reviews and ratings

Participants identified user-generated reviews and ratings as critical tools for evaluating safety, security, and privacy risks.

Participants assess users' reviews before interacting. Most participants reported reviews of potential buyers and sellers as determining factors in their interactions with others. P9 referred to themselves as "*one of those people who's always checking the ratings and experiences*", and P20 said that if a user does not have "*good*" reviews, they would not "*even send a message*". Participants reported the *number* of ratings as more important than the score itself: P18 would not "*trust*" a user based on "*a few good reviews*", but would rather they have "*a lot of good reviews*".

P17 explained that their decision was platform-dependent: On eBay, they would use ratings to determine risk, whereas they did not use the ranking system on Kleinanzeigen because they did not trust it:

> "*I think there are most risks for Kleinanzeigen. I think in eBay, I look at the ratings and if it's like below 98%, I don't communicate with them, so it's kind of strict also because there are a lot of buyers and the people are kind of ready to give five stars if everything is okay. And on Kleinanzeigen, they have a different ranking, and I actually don't trust the ranking so much, so I don't look at the ranking*" — P17

Here, we amplify two key points from participants: that not all user rating systems are created equal, so design is important; and that well-designed rating systems are crowd-sourced sociotechnical privacy, safety, and security.

4.2.2 Platform-Integrated Payment Features

Most participants mentioned platform-integrated payment mechanisms as one of the most effective features to address their concerns about fraud and scam.

Platform-integrated payment features protect users from scams. P12 said built-in payment contributes to security because they do not have to share financial information: "*I think giving out your bank information, for example, is a really bad idea. So I like when platforms have a built-in function for that*" (P12). Participants explained that the built-in payment feature provided protection for *both* sides. As P19 pointed out, it creates a "*bridge between you and the seller*". P20 explained the escrow feature on Vinted:

> "*I've heard in Vinted, for instance, there is a safe payment in between, so you transfer the money until the objects that you've ordered arrived to your place, have been delivered, they won't receive you the money from the payment in between.*" — P20

Participants also highlighted the safe payment feature on Kleinanzeigen, in which the buyer sends a purchase request to a seller directly. As P5 emphasized, this tool is particularly useful when "*you don't want to negotiate*" with other users. They remarked that this method satisfies both buyer and seller, guaranteeing the seller receives their money if and only if the buyer acquires the item: "*everybody's happy*" (P5). Similarly, P6 showed appreciation for the "*Käuferschutz (Buyer's protection)*" feature on Kleinanzeigen, referring to it as a "*big change*" in the online second-hand ecosystem. As P6 pointed out: "*this gives me security for my money*".

Participants prefer platform-integrated payment features over external payment methods. Participants emphasized that safe payment tools on online second-hand platforms addressed their payment concerns, when they did not wish to use external payment methods. P5 commented:

> "*With the direct payment option, it's also quite handy that they are the ones taking care of the payment, and you don't have to go through PayPal, and then go through the whole dispute thing, in case something doesn't work out.*" — P5

In Section 4.3.2, we report how participants used platform-integrated payment to address payment-related concerns. The preference for platform-integrated payment highlights a tension between privacy and security: keeping payment within the platform supports *security* by protecting users' financial details from each other, but violates the *privacy* of third-party or cash transactions. Indeed, some participants were uncomfortable sharing financial information with the platform, e.g., P11, who does "*not trust second-hand online platforms*" was not comfortable sharing "*anything with the bank data, like credit or debit card.*"

4.2.3 Platform-supported user verification

Participants suggested opportunities for platforms to more comprehensively support their privacy and security through transparency, user verification, and automated scam detection in addition to existing measures.

Verification of users' identities by platforms. A few participants believed platforms could verify user legitimacy, perhaps upon registration, towards minimizing scam and fraud. P7 suggested that platforms verify new users through government IDs: "*Somebody comes first, they see me and my documents, and after that I will be just a person there*" (P7).

A few participants reported using platform-generated information—a publicly displayed sign-up date—to evaluate other users' trustworthiness based on when they joined the platform. Participants reported less concern about users who had been active for a long time: "*On Kleinanzeigen if somebody has an account for years, and is pretty active, and you can kind of conclude if you can trust this person*" (P2).

However, requiring more information would cause concern for some. Some participants reported distrusting online second-hand platforms that required too much personal data, such as phone numbers, addresses, or banking information. P15 described increasing distrust based on information requested: "*If they ask something more than expected, like...they asked me about my job, something like this or the office address or something, that's a red flag* " (P15).

4.2.4 Scam detection and resolution

Monitoring user activity to detect scams. A few participants suggested artificial intelligence (AI) to proactively detect scams and flag suspicious behaviors.

P13 expressed concerns about certain advertisements and hate speech, proposing AI for analyzing advertisements and monitoring messages:

> "*I know that the messages are being tracked by the platforms. A scenario that I could think of would be harassment or some kind of hate speech being transferred across in these messages, so maybe more moderation in this regard. And another thing would be identifying scams, having maybe artificial intelligence systems to look at the advertisements, and kind of give a percentage to it. So how much you can trust this particular advertisement or not. And also having a clear distinction between an advertisement and a proper offering.*" — P13

P11 also said they would feel safer with AI monitoring conversations to address personal safety risks:

> "*I would feel more safe if a third person is watching over the conversation; in this case it could be AI. So if he's telling you to come to this address, when you don't have a friend, when you're new to the country, or you want to do it alone, if there's somebody else watching over your shoulder and checking the situation, that's good.*" — P11

The use of AI to monitor for hate, harassment, and scams has been explored and implemented for years; here we note the participants' *comfort* with AI as a privacy and safety tool.

Participants want platforms to have a role in resolving buyer-seller issues. Participants highlighted platform-integrated support systems as an important part of safety. They trusted platforms more when they could actively resolve issues, e.g., related to payment. As P16 explained, "*I think it's good when the platform helps you with problems.*" P19 also emphasized that platforms would be more trustworthy if they managed problematic transactions:

> "*For example, they keep the trace of the transactions. If something serious happened, they can manage this situation. For example, give the information of the seller or buyer to the police.*" — P19

4.2.5 Built-in chat feature

Participants use platform-integrated communication for more security. About half of the participants reported only using platform-integrated messaging to communicate because this made them feel safe and it was recommended by the platforms: "*I would always follow the advice of the platform, and I always try to keep the conversation where it can be monitored. ...[but] people are like 'Oh, but it's more convenient to text on Whatsapp. Can you give me your number?'*" (P5)

4.3 Interpersonal Strategies to Mitigate Risks

Given the privacy and security risks and concerns presented in Section 4.1, and the use of (or desire for) platform-supported privacy affordances (Section 4.2), we now turn to how participants protect their privacy, security, and safety with interpersonal strategies. Methods ranged from precautions when communicating with other users (e.g., minimal information sharing), to safe payment methods, to physical safety strategies. As we discuss in Section 5, these strategies showcase the physicality of privacy, and present both opportunities and limitations of technical solutions.

4.3.1 Communication Strategies

Almost all participants reported personal privacy-focused communication rules, ranging from not engaging with users who seemed "*rude*" (P14), or ending the conversation if anything seemed "*suspicious*" (P10), to only using built-in messaging, to limiting information shared.

Participants avoid sharing personal information. Most participants reported that they limited the personal information shared with other users, believing that other users did not need to have more information than what was on the

platform. P5 avoided "*oversharing personal information*" because "*we're just two strangers on the internet*". P12 would not risk their security for a purchase:

> "*I try to share as little information about myself as necessary or as I can. And I think sometimes you can tell by the way somebody texts, if they're being kind of weird. And at the end of the day, any kind of product is not really worth risking my security for, so I will just end those conversations.*" — P12

Participants prefer progressive disclosure of personal information. Participants reported sharing information gradually, avoiding sensitive information "*at the first step*" (P4). P14 noted that when "*random people*" messaged them and "*directly ask for the address*", they preferred to share information only after exchanging "*a few messages*" (P14). P13 also preferred a "*back and forth*" (P13) to determine whether the other party was genuinely interested in buying or selling the item. P9 strongly preferred keeping the conversation "*neutral*" to "*get to know more*" if the person "*really has an interest in*" their listed item. They further explained that they only disclosed the information in the "*last step.*"

Participants use secondary email addresses for more security. Some participants reported using alternative email addresses, either using email relay services or simply a second account. P4 mentioned that "*with Apple, I have the opportunity to also hide my exact email address and use temporary email addresses to log in*" (P4).

P9 used an email address separate from the one they use for "*important stuff*", while P12 reported having "*a few email addresses*" for "*sketchy stuff*" (P12). P3 emphasized that such alternatives made them less concerned about information sharing: "*I used to give them the mail ids which I mostly never use. So for me, it's okay even if it gets misused by them*" (P3).

We observe that these strategies are specifically *external* to the platform and rely on users' understanding and practice of local social norms. One of the tensions in this sociotechnical ecosystem is, in fact, these social rules and norms that are ungovernable by technology, though as we discuss in Section 5, there may be opportunities for platforms to support users in setting written community guidelines.

4.3.2 Payment outside platform-integrated systems

Participants reported several approaches to safe financial transactions. While PayPal, cash, and platform-integrated payment systems were most common in our dataset, perceptions of *safe* payment methods varied. Some participants used platform-integrated payment systems, described in more detail in Section 4.2.2, preferred for protection against financial loss. However, for those who completed transactions outside the platform payment services, security concerns arose; we focus on safety and mitigation strategies here. We note, too, that there are *also* privacy properties associated with payment outside the platform. Some preferred cash due to its immediate and simple nature, while others preferred PayPal or platform-integrated payments for buyer protection. Direct wire transfers and prepayments were distrusted.

Some participants prefer PayPal for safety. P19 favored PayPal in order to have some "*proof about the buying or selling something*". P13 considered PayPal "*the safest*" payment option "*because I do have two-factor authentication on Paypal*" (P13). Participants also considered PayPal safe because it provides customer support and helped resolve disputes: "*Because I had some issues sometimes with payment, and they are really helpful when you contact Paypal over chatting or via phone*" (P16).

Some participants do not use PayPal (as sellers). Some participants avoided using PayPal. For P8, it was mainly related to personal "*grievances*" with PayPal, while P10 avoided PayPal due to warnings that buyers could reclaim funds by canceling their transactions:

> "*I heard from someone that if someone pays you by Paypal, he can cancel the transaction immediately. The money you think you got is removed, and gets back to his account. Because of that, I am afraid.*" — P10

Some participants prefer cash for simplicity and privacy. About half of participants considered cash a safe payment alternative for simplicity or safety of banking information. For some, it was the simplicity and immediate nature of this payment option. P2 elaborated on the ease of cash transactions: "*Cash is pretty safe. Isn't it? I mean, you can go to the person picking whatever you intend to buy, and give them the money if you are okay with it, and just leave if you're not*" (P2). Others avoid disclosing their banking information to other users so that it would not "*get misused*" (P3).

The value of the item impacts the payment method. For instance, P19 was not "*comfortable to use ATM to get 1,000 cash to give to the seller*". P15 discussed the importance of digital records of payment: "*In Kleinanzeigen, because if I want to purchase something expensive, I'd rather pay it online, via PayPal. I don't want to pay with cash because then later, if something happens, I have some documents*" (P15).

4.3.3 Face-to-Face Transactions

Almost all participants reported physical safety strategies when meeting in person. As we discuss in Section 5, the physical nature of these transactions limits the ability of the platform to support safety; however, online platforms may still be able to adopt digital support for physical safety.

Participants do not go alone to face-to-face transactions. About half of the participants mentioned taking a companion to in-person meetings. P11 expressed concerns about physical harm or theft emphasizing the importance of not being alone:

> "*I think the most important factor is just not to be alone or have somebody, always have a phone in*

your hand, ready to call the police or something, when things are going south." — P11

Participants do face-to-face transactions in public places and during daylight. Some participants highlighted that meeting in public (e.g., parking lots, shopping centers, or outdoor areas) felt safer. Participants said they would generally avoid meeting inside their homes, and would rather meet "*outside*" (P5, P6, P11, P17). P9 said meeting other users "*downstairs*" helped ensure personal safety, emphasizing that they would understand if the situation were reversed:

> "*For me it's totally fine and I don't have any problems when a person is saying, "Please wait. I will come down". And then they come out, close the door and give me the stuff, because I would do exactly the same.*" — P9

For some, the meeting time also played an important role in their sense of security. P5 avoided meeting during "*super late hours,*" preferring "*good daylight and working hours.*"

4.4 Sociotechnically bootstrapping trust

We find that trust in the platform itself—a key factor in comfort, safety, and privacy and safety decisions—is circularly and sociotechnically built, through both social factors (including shared experiences and trust in users), and platform-specific characteristics (e.g., security and privacy mechanisms).

Participants' trust in online second-hand platforms is shaped by trust in their users. About half of the participants reported that their trust in the *platforms* depended on their trust in *other users*. Participants noted that knowing that other users are "*real*" (P7) enhanced their trust. Conversely, they were less inclined to trust the platform if "*it doesn't look like it came from honest people*" (P17). P11 referred to other users as the "*biggest issue with trust*", reasoning that "*the platform is just a platform, you cannot trust a platform.*" However, they believed that platforms should take responsibility for ensuring users' trustworthiness: "*The thing is still, you don't trust the platform. Platforms play a big role in representing the trust of the user, or putting the trust of the user to show, or somehow being able to show the reviews, or the trustworthiness of the user*" (P11).

P5 highlighted issues caused by "*people who try to earn your trust, and then scam you*" (P5). They elaborated that "*it's not the fault of the platform. It's the fault of human factors*" (P5). Similarly, P2 believed it would be unrealistic to hold the platform fully responsible for safety because "*that's a platform where people interact with each other, and you can't expect a platform to make 100% sure that there's no black sheep*" (P2).

External opinions and public reviews influence trust in platforms. All participants reported that their trust in the platforms was influenced by reviews on external websites, such as Reddit, Google Reviews, and Trust Pilot, as well as friends, relatives, experiences. P13 said that

> "*if somebody has already used a particular platform that I haven't used, and I'm thinking about using it, I would go and talk to them about it. And if they say that the experience is not good, I've come across many scams here, and then, if they know people who have faced scams, then that impacts my decision making in this regard.*" — P13

Participants emphasized that learning about others' experiences was *part* of their strategy for security and privacy, but they often still took other safety measures.

5 Discussion

We now discuss the implications of our study. We provide recommendations for future researchers and platform providers.

5.1 Lessons

Fraud and scams remain persistent challenges on online shopping platforms. We find that scams and financial loss are some of users' major concerns on online second-hand platforms. Participants frequently reported encountering (or hearing about) potential or actual scammers, in line with prior work [3, 72]. Some risk is inherent due to the need for user interaction unlike other forms of e-commerce, where goods are sold by the platform or its verified sellers. This relationship introduces uncertainty and vulnerability when users have to evaluate trustworthiness without institutional safeguards.

***Online* privacy and security mechanisms can impact *offline* safety.** Users' concerns are not limited to *online* transactions: as reported in Section 4.1.2, most participants expressed concerns about in-person meetings, including theft and harassment, among other personal safety risks. Additionally, two participants reflected on gendered vulnerability in relation to perceived personal safety, consistent with prior work on physical safety risks for women using online shopping platforms [62]. Participants reported handling offline risks by refusing to meet unknown buyers or sellers when alone or at a private residence. In line with our findings, Mokhberi et al. highlighted that users relied on areas that are either public or semi-public for safety [62].

Users choose modes of payment based on security and privacy but are not always able to use their preferred method. Participants reported various strategies to mitigate financial loss, including preferring certain payment methods: some preferred online payment methods for buyer protection features and proof of transaction; others preferred cash payments for immediacy and privacy, particularly for lower-value items. Users' different preferences for different types of payment are supported by the literature [67, 78, 107], and support our recommendations to platforms in Section 5.2.

Reviews and ratings are a critical part of users' trust-building. Participants relied on reviews and ratings to assess the trustworthiness of others. As we reported in Section 4.2.1, participants said these feedback mechanisms facilitated their decision to interact with unknown users. Prior studies on rating and review systems on similar platforms acknowledge their utility but also raise concerns about reliability [36,60,69], driving our recommendations to platforms in Section 5.2.

Trust in users influences trust in platforms. Participants tied trust in the platform to trust in users, and said it could be facilitated by platform mechanisms such as identity verification. Communication and interaction with other users mattered: how the other person wrote messages, whether the conversation seemed *suspicious*, if the other party insisted on moving the conversation off-platform, or whether trust was built and developed gradually over the course of conversation and exchange. This resembles prior work on online second-hand markets, which finds feelings of uncertainty for these transactions, requiring users to partly depend on communication and other interactional cues when assessing users on the other side of the transaction and negotiating the terms of the exchange [54]. Participants viewed the implementation of mechanisms that support these assessments as the responsibility of the platforms in creating a safe environment, i.e., an environment that minimizes threats to users' safety and personal privacy and security, while providing enough information to assess whether an interaction with another user should continue. Consistent with prior work [8, 63, 77], our findings indicate that trust within online second-hand platforms functions as a dual-layered dynamic in which trust in the platform and trust in individual users are interconnected and mutually reinforcing. From a broader perspective, this necessitates that platforms take responsibility for providing a safe environment with mechanisms that facilitate trust.

Security-, privacy-, and transparency-related platform features drive users' trust in platforms. We find that trust in platforms is also shaped by platform affordances: trust in users through reviews, ratings, and identity verification; platform transparency in data handling and security mechanisms (Section 4.4). We identify opportunities for platforms to make the second-hand shopping ecosystem safer (Section 5.2).

Future research should consider an in-depth cross-platform comparison. Our work, an interview study in Germany, shows a need for additional research about privacy, security, and safety in online second-hand shopping, to quantify and broaden beyond Germany and the platforms in our study. For example, we find that some of the safety features already implemented *are* effective in addressing some users' safety concerns—but that the same features evoke privacy concerns for others. Future research should consider a larger-scale study of demographics to understand whether certain safety features disproportionately benefit users with certain identities. Such work could ask whether users with different levels of technical confidence, selling experience, gendered safety concerns, marginalized identities, or needs for pseudonymity benefit differently from existing platform safety features. Comparisons between platforms, too, are key, in order to understand how different implementations of features support trust, safety, and privacy more than others—as, for example, we found that ratings may be trusted on some platforms but not others. Building on these findings, future work could conduct a systematic cross-platform study to compare how people use and trust different online second-hand shopping platforms. Such a study could investigate features that differ across platforms, such as rating systems, integrated payment flows, verification signals, and handover options, and investigate how users interpret and rely on them. This could identify where these platform designs support or weaken privacy, security, safety, and trust in practice. Future work should seek to understand the space of second-hand online shopping platforms more broadly, systematizing the privacy and security features, the user bases, and social norms on the platforms.

5.2 Recommendations for Platforms

We identify platforms as an obvious and powerful stakeholder in the second-hand shopping ecosystem, with the potential to increase safety, security, privacy, and trust. We observe that doing so is difficult because of their role as a mediator of interactions that may be interpersonal, physical, or both, depending on the platform, transaction mode, and whether users decide to remain within platform-supported transaction flows. Users may negotiate communication method, payment mechanism, price, and information disclosure before deciding whether to meet in person—potentially at one of their homes—or have items shipped. While platforms such as Vinted support shipped transactions, users may still decide to negotiate alternative arrangements or move some parts of the interaction outside platform-supported systems, which may require sharing the buyer's address for shipping, although some platform-supported shipping options, including parcel shops or package lockers, can reduce direct address disclosure. This intensely personal and ultimately brief series of negotiations is unique to online second-hand shopping, and while we can and should borrow ideas and tools from other domains to support users, they must be evaluated for suitability and adapted for second-hand shopping.

Here, we discuss how platforms might do so, including how they are already succeeding in supporting safety for some users. Critically, one of the biggest sociotechnical hurdles is that different users place different values on certain safety, security, and privacy interventions—some users may prefer a feature because it supports their security, while others may prefer *not* using the feature for their own privacy. These mismatched preferences are especially salient for online second hand shopping and point to this key stage of *negotiation* between users regarding communication, payment, and meeting; platforms must understand and support this negotiation stage.

Integrated payment systems as an option. Our findings reveal that users appreciate having an integrated and secure payment system with buyer protection *as an option*, but that some may prefer to exchange money *outside* the platform for privacy from the platform itself. For some users, an integrated payment system with buyer protection alleviates concerns about being scammed and losing money, or being robbed or intimidated to a new price in person. For other users, an integrated payment system is a violation of privacy, or less trustworthy than an external payment system they already use. They may also choose not to use an internal payment system if the cost is high—as saving money is one of the main reasons to use these platforms. Users may choose different payment systems for different circumstances too, e.g., based on the cost of the item or whether they need a record. All of the platforms in our study supported integrated payment [20, 24, 46, 82], but not *all* other second-hand online shopping platforms do (e.g., Craigslist in the US does not, and in fact discourages users from any electronic payment [12]). While platforms should not *require* users to use an integrated payment system, users may find it a safe and secure option. Platforms could support users in negotiating the choice of payment system itself by both letting users state on their profiles which payment system(s) they use, and by explaining options available to users (e.g., built-in payment systems, an external system, cash, etc).

Platform as data escrow for identity verification. Participants expressed a desire for identity verification for others, but shared concerns about revealing their own personal data *both* to other users and to the platform itself. We observe that sharing data with other users is synonymous with sharing data with the platform—unless done off-platform or through a built-in encrypted messenger—so if data can be shared *only* with the platform (and users can trust the platform to verify the information properly), that supports user security and privacy more than the alternative (asking users to share data either openly or piecemeal with other users). We recommend, then, that platforms act as a data escrow, allowing users to verify their identity in some way, and revealing only *whether* they are verified rather than the information itself—perhaps revealing how the verification happened, e.g., that a user's government-issued ID was determined to be valid, or that they connected a phone number, etc. Prior work on sharing-economy platforms discussed identity verification as a trust-building signal among several [75]. Similar verification models are used in other sharing-economy contexts: Airbnb verifies users through trusted third-party sources or government ID and displays an identity-verified badge on users' profiles noting that identity information is not shared with hosts or guests [1]. In practice, this tradeoff requires users' deep trust in the platform to process sensitive identity documents rather than posting identifying information more publicly but without proof (e.g., a profile picture of their face rather than uploading their ID). Additionally, this tradeoff recalls any number of data breaches of sensitive documents collected for user verification [101], and must be implemented with extreme caution and care.

Making collusion for reviews as hard as possible. Participants said they use ratings and reviews to help decide whether to interact with another person on the platform (Section 4.2.1). Prior research has tried to improve the usability of reviews, e.g., through AI-assisted summaries of text-based reviews to make them more useful [7] or detecting fraudulent reviews [37]. While our participants reported more trust in text-based reviews (e.g., eBay), pre-defined ratings such as "on time", "honest", "reliable" (e.g., used by Kleinanzeigen) can be useful as an overview instead of AI summaries. Some platforms already provide measures against fraudulent reviews (e.g., on Vinted one can only write a review once a transaction is completed, so the barrier is high). We recommend that other platforms learn from this and also make collusion harder by only allowing users to write reviews when there has been a realistic interaction.

Setting community norms—or at least norms around negotiation and discord—regarding disclosing information, going off-platform, and meeting in person. Finally, we return to the criticality of negotiation between buyers and sellers. Participants said that not only do they negotiate price, but also communication medium, payment mechanism, and disclosure of personal information. Different communities or cultures may have different norms around these negotiations—the sociotechnical options available to users, and the language around negotiation itself. Prior work on rideshare drivers also found that users rely not only on the platform's safety mechanisms but also develop their own safety strategies, such as exchanging safety information and learning from other users' experiences [2]. Some differences in negotiation or information disclosure styles may be indicative of safety issues, and others may be due to community or cultural differences. We recommend—taking inspiration from moderated sub-Reddits—that platforms more actively support communities in developing written guidelines and norms around in-person meetings, communication, payment, and information disclosure. Platforms could also consider adopting safety features from ride-sharing services, like location sharing with a friend, and emergency help [38].

6 Conclusion

We report on our in-depth, semi-structured interview study with 20 users of online second-hand shopping platforms in Germany. We identified key security and privacy concerns, protective strategies, perceptions of platforms' security and privacy measures, and trust dynamics.

We find that users' security and privacy concerns are related to scams, financial loss, and personal safety risks. Our findings have implications and opportunities primarily for platform developers, and further for future researchers and users.

References

[1] Airbnb. Verifying your identity on Airbnb. https://www.airbnb.co.uk/help/article/1237, 2026. Accessed: June 16, 2026.

[2] Mashael Yousef Almoqbel and Donghee Yvette Wohn. Individual and collaborative behaviors of rideshare drivers in protecting their safety. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), November 2019.

[3] Hamad Alsaleh and Lina Zhou. A Heuristic Method for Identifying Scam Ads on Craigslist. In *2018 European Intelligence and Security Informatics Conference (EISIC)*, pages 69–72, 2018.

[4] Olga Angelopoulou, Andy Jones, Graeme Horsman, and Seyedali Pourmoafi. A Study of the Data Remaining on Second-Hand Mobile Devices in the UK. *Journal of Digital Forensics, Security and Law*, 17(2):5, 2022.

[5] Michael Bailey, David Dittrich, Erin Kenneally, and Doug Maughan. The Menlo Report. *IEEE Security & Privacy*, 10(2):71–75, 2012.

[6] Oussama BenRhouma, Ali AlZahrani, Ahmad AlKhodre, Abdallah Namoun, and Wasim Ahmad Bhat. To sell, or not to sell: social media data-breach in second-hand Android devices. *Information and Computer Security*, 30(1):117–136, 2022.

[7] Zihan Bian and Cheng Che. How AI Overview of Customer Reviews Influences Consumer Perceptions in E-Commerce? *Journal of Theoretical and Applied Electronic Commerce Research*, 20(4), 2025.

[8] Fabienne Chameroy, Stéphane Salgado, Virginie de Barnier, and Damien Chaney. In platform we trust: How interchangeability affects trust decisions in collaborative consumption. *Technological Forecasting and Social Change*, 198:122997, 2024.

[9] Xue Chi, Zhi-Ping Fan, and Zhongpeng Dong. Dealing with safety risks from peer-to-peer service sharing: optimal pricing and safety investment for a sharing platform. *International Transactions in Operational Research*, 32(4):2278–2310, 2025.

[10] Victoria Clarke and Virginia Braun. Thematic analysis. *The Journal of Positive Psychology*, 12(3):297–298, 2017.

[11] Luis Corrons. Scammers are targeting online second-hand shopping platforms. https://blog.avast.com/online-secondhand-shopping-scams, January 2023. Accessed on June 21, 2024.

[12] Craigslist. Avoiding scams. https://www.craigslist.org/about/help/safety/scams/avoiding, n.d. Accessed June 3, 2026.

[13] Gunnar Daugs, Knut Kröger, and Reiner Creutzburg. Remarks on forensically interesting Sony Playstation 3 console features. In Cees G. M. Snoek, Nicu Sebe, Lyndon Kennedy, Reiner Creutzburg, and David Akopian, editors, *Multimedia on Mobile Devices 2012; and Multimedia Content Access: Algorithms and Systems VI*, volume 8304, page 83040R. International Society for Optics and Photonics, SPIE, 2012.

[14] Matthew Davies, Huw Read, Konstantinos Xynos, and Iain Sutherland. Forensic analysis of a Sony PlayStation 4: A first look. *Digital Investigation*, 12:S81–S89, 2015. DFRWS 2015 Europe.

[15] Fremont Police Department. Safe exchange zone. https://www.fremontpolice.gov/crime-prevention/exchange-zone, n.d. Accessed: April 14, 2025.

[16] eBay. Abholung anbieten. https://www.ebay.de/help/default/default/abholung-anbieten, n.d. Accessed: April 29, 2026.

[17] eBay. Buying with confidence. https://pages.ebay.de/safetycenter/buyingwithconfidence.html, n.d. Accessed: April 29, 2026.

[18] eBay. Creating an eBay Account. https://www.ebay.com/help/account/signing-ebay-account/signing-ebay-account?id=4191, n.d. Accessed: April 29, 2026.

[19] eBay. eBay Authenticity Guarantee. https://www.ebay.com/help/selling/selling-tools/ebay-authenticity-guarantee?id=4644, n.d. Accessed: April 29, 2026.

[20] eBay. eBay-Käuferschutz. https://pages.ebay.de/einkaufen/ebay-kaeuferschutz.html, n.d. Accessed: April 29, 2026.

[21] eBay. eBay Top Service. https://www.ebay.de/verkaeuferportal/programme-gewerbliche-verkaeufer/ebay-top-service, n.d. Accessed: June 4, 2026.

[22] eBay. Feedback and seller ratings. https://www.ebay.com.au/sellercentre/feedback-seller-ratings, n.d. Accessed: April 29, 2026.

[23] eBay. Feedback manipulation policy. https://www.ebay.de/help/policies/feedback-policies/grundsatz-zur-manipulation-von-bewertungen?id=4231&srsltid=AfmBOorTzHOQzZyXl-klzYLDHdwbgjiU5XPuCrDEtC7x0_yzQZf4L4eU, n.d. Accessed: April 29, 2026.

[24] eBay. Grundsatz zum eBay-Käuferschutz. https://www.ebay.de/help/policies/ebay-money-back-guarantee-policy/grundsatz-zum-ebaykuferschutz?id=4210, n.d. Accessed: April 29, 2026.

[25] eBay. How to recognize fake calls and emails. https://www.ebay.de/help/account/protecting-account/geflschte-anrufe-und-emails-erkennen?id=4195, n.d. Accessed: April 29, 2026.

[26] eBay. Leave ratings for buyers. https://www.ebay.de/help/selling/leaving-feedback-buyers/leaving-feedback-buyers?id=4078, n.d. Accessed: April 29, 2026.

[27] eBay. Leave ratings for sellers. https://www.ebay.de/help/buying/leaving-feedback-sellers/bewertungen-fr-verkufer-abgeben?id=4007&srsltid=AfmBOoo7t7T8YG8OIZ_uH82HimodjsNyHw8SOSIoiXSleFrvGlJ0c4JD, n.d. Accessed: April 29, 2026.

[28] eBay. Principle regarding abusive buyer behavior. https://www.ebay.de/help/policies/rules-policies-buyers/buying-practices-policy?id=4374, n.d. Accessed: April 29, 2026.

[29] eBay. Profile policy. https://www.ebay.com/help/policies/identity-policies/profile-policy?id=4234&ra=true#section2, n.d. Accessed: April 29, 2026.

[30] eBay. Sicher bezahlen auf eBay. https://pages.ebay.de/safetycenter/payingsafely.html, n.d. Accessed: April 29, 2026.

[31] eBay. Your eBay Profile Page. https://www.ebay.com/help/selling/selling/ebay-profile-page?id=5184, n.d. Accessed: April 29, 2026.

[32] Maximilian Eichhorn, Janine Schneider, and Gaston Pugliese. Well Played, Suspect!–Forensic examination of the handheld gaming console "Steam Deck". *Forensic Science International: Digital Investigation*, 48:301688, 2024.

[33] Simson L Garfinkel and Abhi Shelat. Remembrance of data passed: A study of disk sanitization practices. *IEEE Security & Privacy*, 1(1):17–27, 2003.

[34] William Bradley Glisson, Tim Storer, Andrew Blyth, George Grispos, and Matt Campbell. In the wild residual data research and privacy. *Journal of Digital Forensics, Security and Law*, 11(1):77–98, 2016.

[35] Judith Green and Nicki Thorogood. *Qualitative Methods for Health Research*. SAGE Publications Ltd, 4 edition, 2018.

[36] Eugenia Y Huang, Shu-Chiung Lin, and I-Ting Hsieh. Online marketplace sellers' influence on rating scores and comment orientation. *Electronic Commerce Research*, 23(2):1241–1270, 2023.

[37] Sami Ben Jabeur, Hossein Ballouk, Wissal Ben Arfi, and Jean-Michel Sahut. Artificial intelligence applications in fake review detection: Bibliometric analysis and future avenues for research. *Journal of Business Research*, 158:113631, 2023.

[38] Saeed Jaydarifard, Tan Yigitcanlar, and Alexander Paz. Risk factors and safety strategies for mitigating violations, harassment and assault in taxi and ride-hailing services. *Transport Reviews*, 45(5):776–800, 2025.

[39] Andy Jones, Thomas Martin, and Mohammed Alzaabi. The 2012 Analysis of Information Remaining on Computer Hard Disks Offered for Sale on the Second Hand Market in the UAE. In *Proceedings of the 10th Australian Digital Forensics Conference*, Perth, Western Australia, 2012.

[40] Kleinanzeigen. Freundlichkeits-abzeichen. https://hilfe.kleinanzeigen.de/hc/de/articles/17111986199708-Freundlichkeits-Abzeichen, n.d. Accessed: April 29, 2026.

[41] Kleinanzeigen. Hinweis zu PayPal und Sicher bezahlen. https://hilfe.kleinanzeigen.de/hc/de/articles/17211553583388, n.d. Accessed: April 29, 2026.

[42] Kleinanzeigen. Lasst uns sicher handeln. https://themen.kleinanzeigen.de/lasst-uns-sicher-handeln/?utm_source=google&utm_medium=organic&utm_campaign=themen, n.d. Accessed: April 29, 2026.

[43] Kleinanzeigen. Nachhaltigkeits-abzeichen. https://hilfe.kleinanzeigen.de/hc/de/articles/17112134185756-Nachhaltigkeits-Abzeichen, n.d. Accessed: April 29, 2026.

[44] Kleinanzeigen. Nutzer bewerten. https://hilfe.kleinanzeigen.de/hc/de/articles/17106550059164-Nutzer-bewerten, n.d. Accessed: April 29, 2026.

[45] Kleinanzeigen. Phishing mit QR-Codes erkennen und vermeiden. https://hilfe.kleinanzeigen.de/hc/de/articles/21576844233116-Phishing-mit-QR-Codes-erkennen-und-vermeiden, n.d. Accessed: April 29, 2026.

[46] Kleinanzeigen. Sicher bezahlen. https://hilfe.kleinanzeigen.de/hc/de/articles/17229475427612, n.d. Accessed: April 29, 2026.

[47] Kleinanzeigen. Sicherheitshinweise. https://themen.kleinanzeigen.de/sicherheitshinweise/, n.d. Accessed: April 29, 2026.

[48] Kleinanzeigen. Sicherheitshinweise zu Fake-Chats und sicherer Abholung. https://hilfe.kleinanzeigen.de/hc/de/articles/17134550447132, n.d. Accessed: April 29, 2026.

[49] Kleinanzeigen. Wie funktioniert der Käuferschutz. https://hilfe.kleinanzeigen.de/hc/de/articles/17211553583388-Was-ist-Sicher-bezahlen-wie-funktioniert-der-K%C3%A4uferschutz, n.d. Accessed: April 29, 2026.

[50] Kleinanzeigen. Wie kann ich bezahlen. https://hilfe.kleinanzeigen.de/hc/de/articles/17212587276956-Wie-kann-ich-bezahlen, n.d. Accessed: April 29, 2026.

[51] Kleinanzeigen. Woraus besteht mein Nutzerprofil. https://hilfe.kleinanzeigen.de/hc/de/articles/17113513090460-Woraus-besteht-mein-Nutzerprofil, n.d. Accessed: April 29, 2026.

[52] Kleinanzeigen. Zuverlässigkeits-abzeichen. https://hilfe.kleinanzeigen.de/hc/de/articles/17112184040732-Zuverl%C3%A4ssigkeits-Abzeichen, n.d. Accessed: April 29, 2026.

[53] Jan H Klemmer, Stefan Albert Horstmann, Nikhil Patnaik, Cordelia Ludden, Cordell Burton Jr, Carson Powers, Fabio Massacci, Akond Rahman, Daniel Votipka, Heather Richter Lipford, et al. Using AI Assistants in Software Development: A Qualitative Study on Security Practices and Concerns. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, pages 2726–2740, 2024.

[54] Maksym Kolomoiets. The impact of transaction framing: exploring barriers to participation in the online second-hand economy for casual e-commerce consumers. *Qualitative Market Research: An International Journal*, 28(3):528–544, 04 2025.

[55] Anastassija Kostan, Sara Olschar, Lucy Simko, and Yasemin Acar. Exploring digital security and privacy in relative poverty in Germany through qualitative interviews. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 2029–2046, Philadelphia, PA, August 2024. USENIX Association.

[56] Barbara Krumay. The E-Waste-Privacy Challenge. In *Privacy Technologies and Policy*, volume 9857 of *Lecture Notes in Computer Science*, pages 48–68, Cham, 2016. Springer International Publishing.

[57] Yuru Liu and Yan Wan. Consumer Satisfaction with the Online Dispute Resolution on a Second-Hand Goods-Trading Platform. *Sustainability*, 15(4), 2023.

[58] Ning F. Ma, Veronica A. Rivera, Zheng Yao, and Dongwook Yoon. "Brush it Off": How Women Workers Manage and Cope with Bias and Harassment in Gender-agnostic Gig Platforms. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[59] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. ACM Hum.-Comput. Interact.*, 3(CSCW), November 2019.

[60] Tehila Minkus and Keith W. Ross. I Know What You're Buying: Privacy Breaches on eBay. In Emiliano De Cristofaro and Steven J. Murdoch, editors, *Privacy Enhancing Technologies*, pages 164–183, Cham, 2014. Springer International Publishing.

[61] Azadeh Mokhberi, Yue Huang, and Konstantin Beznosov. Users' Strategies for Ensuring Trust, Privacy, and Safety on Facebook Marketplace: Challenges and Recommendations. *Proc. ACM Hum.-Comput. Interact.*, 9(7), October 2025.

[62] Azadeh Mokhberi, Yue Huang, Guillaume Humbert, Borke Obada-Obieh, Masoud Mehrabi Koushki, and Konstantin Beznosov. Trust, Privacy, and Safety Factors Associated with Decision Making in P2P Markets Based on Social Networks: A Case Study of Facebook Marketplace in USA and Canada. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. Association for Computing Machinery.

[63] Emi Moriuchi and Ikuo Takahashi. The role of perceived value, trust and engagement in the C2C online secondary marketplace. *Journal of Business Research*, 148:76–88, 2022.

[64] Netlify. Replication Package. https://second-hand-replication-package.netlify.app/, n.d. Accessed: June 17, 2026.

[65] LKA Niedersachsen. Betrug über eBay Kleinanzeigen. https://www.lka.polizei-nds.de/praevention/aktuellewarnmeldungen/betrug-ueber-ebaykleinzeigen-115310.html, n.d. Accessed: June 21, 2024.

[66] Kavous Salehzadeh Niksirat, Diana Korka, Quentin Jacquemin, Céline Vanini, Mathias Humbert, Mauro

Cherubini, Sylvain Métille, and Kévin Huguenin. Security and Privacy with Second-Hand Storage Devices: A User-Centric Perspective from Switzerland. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2024(2):22, 2024.

[67] Betty Purwandari, Syahrul Alam Suriazdin, Achmad Nizar Hidayanto, Suryana Setiawan, Kongkiti Phusavat, and Mutia Maulida. Factors Affecting Switching Intention from Cash on Delivery to E-Payment Services in C2C E-Commerce Transactions: COVID-19, Transaction, and Technology Perspectives. *Emerging Science Journal*, 6(Special Issue):136–150, 2022.

[68] Huw O.L. Read, Konstantinos Xynos, Iain Sutherland, Matthew Bovee, and Clyde Tamburro. Nintendo 3DS forensics: A secondhand case study. *Forensic Science International: Digital Investigation*, 50:301815, 2024. DFRWS APAC 2024 - Selected Papers from the 4th Annual Digital Forensics Research Conference APAC.

[69] Bob Rietjens. Trust and reputation on eBay: Towards a legal framework for feedback intermediaries. *Information & Communications Technology Law*, 15(01):55–78, 2006.

[70] Richard Roberts, Julio Poveda, Raley Roberts, and Dave Levin. Blue Is the New Black (Market): Privacy Leaks and Re-Victimization from Police-Auctioned Cellphones. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 3332–3336, 2023.

[71] Nikki Robins, Patricia A. H. Williams, and Krishnun Sansurooah. An investigation into remnant data on USB storage devices sold in Australia creating alarming concerns. *International Journal of Computers and Applications*, 39(2):79–90, 2017.

[72] Knowledge Rusere, Stanford Musarurwa, Fungai Bhunu Shava, and Munyaradzi Maravanyika. Security Concerns on Social Media Customer-to-Customer Online Transactions. A Case of Namibia Facebook Users. In *2022 IST-Africa Conference (IST-Africa)*, pages 1–9, 2022.

[73] Benjamin Saunders, Julius Sim, Tom Kingstone, Shula Baker, Jackie Waterfield, Bernadette Bartlam, Heather Burroughs, and Clare Jinks. Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & quantity*, 52:1893–1907, 2018.

[74] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 2202–2214, 2017.

[75] Nils Siegfried, Julian Löbbers, and Alexander Benlian. The Trust-Building Nature of Identity Verification in the Sharing Economy: An Online Experiment. In *Proceedings of the 15th International Conference on Wirtschaftsinformatik*, pages 1506–1521, 2020.

[76] Stellar Data Recovery. Residual Data Study on Second-Hand Devices. https://www.stellarinfo.com/pdf/Stellar-Residual-Data-Study-on-Second-Hand-Devices-Report-April-2019.pdf, 2019. Accessed: 2025-08-28.

[77] Timm Teubner and David Dann. How platforms build trust. *Available at SSRN 3266472*, 2018.

[78] Rito Septi Tombe, N. F. Ayuning Budi, A. Nizar Hidayanto, Rika K. Ekawati, and P. Anussornnitisarn. Why does people use e-payment systems in C2C e-marketplace? a trust transfer perspective. In *2017 Second International Conference on Informatics and Computing (ICIC)*, pages 1–6, 2017.

[79] Vinted. Account verification. https://www.vinted.co.uk/help/406, n.d. Accessed: April 29, 2026.

[80] Vinted. Automated listing check. https://www.vinted.co.uk/help/375, n.d. Accessed: April 29, 2026.

[81] Vinted. Buyer Protection. https://www.vinted.co.uk/help/550, n.d. Accessed: April 29, 2026.

[82] Vinted. Buyer Protection Fee. https://www.vinted.de/help/342, n.d. Accessed: April 29, 2026.

[83] Vinted. Buyer Protection Pro. https://www.vinted.de/help/909, n.d. Accessed: April 29, 2026.

[84] Vinted. Buying basics. https://www.vinted.co.uk/help/25, n.d. Accessed: April 29, 2026.

[85] Vinted. Confidentiality. https://www.vinted.co.uk/help/392/81, n.d. Accessed: April 29, 2026.

[86] Vinted. Electronics verification. https://www.vinted.de/help/1360-electronics-verification-service-for-buyers, n.d. Accessed: April 29, 2026.

[87] Vinted. Feedback and reviews. https://www.vinted.co.uk/help/14, n.d. Accessed: April 29, 2026.

[88] Vinted. Guidelines for safe and smooth trading on vinted. https://www.vinted.de/help/1417, n.d. Accessed: April 29, 2026.

[89] Vinted. Information on phishing and how to recognize and avoid phishing messages and scams. https://www.vinted.ie/help/628, n.d. Accessed: April 29, 2026.

[90] Vinted. Item bump. https://www.vinted.co.uk/help/340, n.d. Accessed: April 29, 2026.

[91] Vinted. Item verification. https://www.vinted.de/item_verification, n.d. Accessed: April 29, 2026.

[92] Vinted. Privacy policy. https://www.vinted.de/privacy-policy#role, n.d. Accessed: April 29, 2026.

[93] Vinted. Profile data and visibility. https://www.vinted.ie/help/392/405, n.d. Accessed: April 29, 2026.

[94] Vinted. Seller basics. https://www.vinted.co.uk/help/26, n.d. Accessed: April 29, 2026.

[95] Vinted. Showcase. https://www.vinted.co.uk/help/452, n.d. Accessed: April 29, 2026.

[96] Vinted. Signing up on Vinted. https://www.vinted.co.uk/help/105-signing-up-on-vinted, n.d. Accessed: April 29, 2026.

[97] Vinted. Supported payment methods. https://www.vinted.de/help/94, n.d. Accessed: April 29, 2026.

[98] Vinted. Vinted balance. https://www.vinted.co.uk/help/437, n.d. Accessed: April 29, 2026.

[99] Vinted. Vinted safety. https://www.vinted.ie/safety, n.d. Accessed: April 29, 2026.

[100] Vinted. Withdrawing money and identity verification. https://www.vinted.co.uk/help/111, n.d. Accessed: April 29, 2026.

[101] Jacqui Wakefield. My ex stalked me, so I joined a 'dating safety' app. Then my address was leaked. https://www.bbc.com/news/articles/ce87rer52k3o, August 2025. Accessed: June 1, 2026.

[102] Bairong Wang, Yuxuan Fu, and Yong Li. Young consumers' motivations and barriers to the purchase of second-hand clothes: An empirical study of China. *Waste Management*, 143:157–167, 2022.

[103] Kangning Wei, Yuzhu Li, Yong Zha, and Jing Ma. Trust, risk and transaction intention in consumer-to-consumer e-marketplaces: An empirical comparison between buyers' and sellers' perspectives. *Industrial Management & Data Systems*, 119(2):331–350, 2019.

[104] Michael Williams and Tami Moser. The art of coding and thematic exploration in qualitative research. *International management review*, 15(1):45–55, 2019.

[105] Mengling Wu, Abdullah Al Mamun, Qing Yang, and Muhammad Mehedi Masud. Modeling the reuse intention and practices of secondhand clothing: Evidence from a developing nation. *Humanities and Social Sciences Communications*, 10(1):1–12, 2023.

[106] Yuxi Wu, W. Keith Edwards, and Sauvik Das. Sok: Social cybersecurity. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1863–1879, 2022.

[107] Liu Xinyan, Wan Jingjing, and Chen Lu. An Empirical Study on the Types of C2C Sellers' Perceived Risk in the Entire Transaction Process. In *2010 International Conference on E-Business and E-Government*, pages 2209–2212, 2010.

[108] Konstantinos Xynos, Huw O. L. Read, Iain Sutherland, and Matthew Bovee. Back in the game: Privacy concerns of second-hand game consoles. *IEEE Security & Privacy*, 24(1):16–25, 2026.

[109] Marzieh Zendehdel and Laily Hj Paim. Perceived risk of security and privacy in online shopping: A study of Malaysia context. *Life Science Journal*, 9(4):983–987, 2012.

A Appendix

A.1 Demographics

Table 1: Participant Demographics.

Participant	Age	Gender	Field of Study	Income Level
P1	25–34	Woman	Computer Science / IT	No income
P2	35–44	Man	Computer Science / IT	€10,000–€29,999
P3	18–24	Woman	Computer Science / IT	€10,000–€29,999
P4	25–34	Man	Engineering	€10,000–€29,999
P5	25–34	Woman	Business / Economics	€30,000–€49,999
P6	25–34	Man	Engineering	€50,000–€69,999
P7	25–34	Man	Engineering	€30,000–€49,999
P8	25–34	Man	Computer Science / IT	€30,000–€49,999
P9	25–34	Man	Social Sciences	€50,000–€69,999
P10	25–34	Man	Engineering	€10,000–€29,999
P11	25–34	Man	Humanities / Arts	€10,000–€29,999
P12	18–24	Woman	Business / Economics	No income
P13	25–34	Man	Computer Science / IT	€10,000–€29,999
P14	18–24	Prefer not to disclose	Computer Science / IT	< €10,000
P15	25–34	Man	Engineering	€30,000–€49,999
P16	25–34	Woman	Education	< €10,000
P17	25–34	Man	Computer Science / IT	€50,000–€69,999
P18	25–34	Man	Engineering	€10,000–€29,999
P19	25–34	Man	Computer Science / IT	€10,000–€29,999
P20	25–34	Woman	Computer Science / IT	€50,000–€69,999

A.2 Platform Features

Table 2: Comparison of Platform Features.

Platform	Integrated chat	Integrated Payment Service?	Buyer Protection (Paid/Unpaid)	Ratings/Reviews	User/Profile Verification
Definition	Users can communicate without leaving the platform	Whether buyers can pay within the platform's checkout or payment flow	The platform acts as escrow and offers refund/protection if something goes wrong	Public reputation information shown on user profiles	Whether the platform provides the option for users to verify their identity and display it on their profile
Vinted	Yes, app and website	Yes, integrated ("Buy Now") function	Yes, if the "Buy Now" function is used, buyer protection is applied for payment methods offered/supported by Vinted. Fees apply: fixed fee of €0.70, usually 5% of the article price.	Star ratings and written feedback for both sides of the transaction after the transaction is completed.	Optional profile verification through Facebook and Google, visible to other members; advertised as improving selling chances.
Kleinanzeigen	Yes, app and website	Yes, "Sicher bezahlen" function	Yes, if the "Sicher bezahlen" function is used, buyer protection is applied for payment methods offered/supported by Kleinanzeigen. Fees apply: flat service fee of €0.50 plus 4.5% of the article price.	User ratings and activity/reputation badges exist, but not detailed transaction-based written reviews; ratings can reflect interaction behavior. Users can rate each other after exchanging messages. Transaction completion is not required for rating users.	No general visible profile ID verification, but activity/reputation badges instead.
eBay	Yes, app and website	Yes, eBay checkout with supported payment methods	Yes, for eligible purchases completed through eBay checkout with supported payment methods. Free.	Detailed feedback and star ratings for both sides of the transaction.	No general visible ID-verification badge

A.3 Detailed Platform Background

This appendix provides additional detail on the three platforms used and discussed by participants: Kleinanzeigen, Vinted, and eBay. It supplements the brief overview in Section 2 and Table A.2 by describing platform features most relevant to the study's findings, including communication flows, payment and buyer-protection mechanisms, review and rating systems, verification signals, fraud-prevention measures, and practices related to information visibility and disclosure.

Kleinanzeigen

Kleinanzeigen functions as a classifieds platform centered on direct negotiation between users. Sellers create listings, and interested buyers initiate contact through the platform's integrated chat. Transactions may proceed via in-person handover or shipment. Kleinanzeigen's rating system differs from the more transaction-focused systems employed by eBay and Vinted [22, 87]. Users may rate each other after exchanging at least two messages, regardless of whether a sale is completed [44]. Therefore, ratings serve as assessments of interaction behavior, such as reliability or friendliness, rather than post-purchase evaluations [40, 52]. These ratings are displayed on user profiles alongside badges and other indicators of account activity. Kleinanzeigen awards badges for reliability, friendliness, and sustainability, each linked to prior activity and evaluations [40, 43, 52]. Public profile information may include the selected profile name, account age, listing counts, overall evaluation, badges, and typical response time [51]. Kleinanzeigen also states that personal information, such as name, address, location, or phone number will not be displayed in users' public profiles [51].

Kleinanzeigen also offers an integrated escrow and payment feature called *"Sicher bezahlen"* ("Secure Payment"), which is embedded in the messaging flow and is mainly intended for shipped transactions [46]. The platform presents this feature as a way to protect transaction data and to provide safeguards in cases such as non-delivery or receipt of incorrect goods [47]. Buyer protection is tied to use of this flow, and the buyer pays a service fee composed of a fixed amount and a percentage of the item price [49]. The platform also explicitly distinguishes this protected flow from external payment arrangements, including PayPal payments arranged in chat, which it says fall outside its protected process [49]. Supported payment methods for Secure Payment include credit card, Apple Pay, Google Pay, and SEPA transfer for eligible offers [50].

In addition to these built-in mechanisms, Kleinanzeigen provides user guidance and advises buyers and sellers to use the protected payment feature when available, exercise caution with pickup and shipping arrangements, and avoid high-risk payment methods such as Western Union, PaySafe, or MoneyGram [42]. Users are further encouraged to keep copies of listings, message histories, and necessary address information, use insured shipping, and confirm receipt of funds rather than relying solely on email confirmations [42]. The platform also issues warnings regarding forged identity documents, fraudulent payment confirmations, fake chats, and phishing attempts, including those involving QR codes [45, 48]. For in-person exchanges, public meeting places are recommended, and users are urged to exercise additional caution if pickup details change unexpectedly [48]. Kleinanzeigen states that it employs automated technologies to detect fraudulent advertisements and suspicious activity [47].

Vinted

Vinted is structured around an integrated in-platform transaction flow. Sellers create listings with photos and item descriptions, while buyers can browse items through the app or website, contact sellers directly, make offers, or use the platform's *Buy Now* flow to complete the purchase [84, 94].

At signup, Vinted allows users to register via Facebook, email, Google, or Apple ID [96]. Users choose a username during account creation, and depending on the signup method, may later be required to verify their email address. Vinted users are not allowed to maintain multiple accounts. Apple signup additionally allows users to hide their real email address behind Apple's relay feature.

The *"Buy Now"* flow is central to Vinted's design. When used, payment and shipping are both handled within the platform, and buyer protection applies to the purchase [81]. The fee is usually calculated as a fixed amount plus a percentage of the item or bundle price [82]. The supported payment methods include debit and credit cards, Vinted Balance, Apple Pay, Google Pay, PayPal, Tink direct bank payments, and Klarna for some items [97]. Once a transaction is completed, sellers receive the money in their Vinted Balance and may either spend it on the platform or withdraw it to a bank account, in some cases after identity verification [98, 100]. Vinted also offers a separate buyer-protection model for purchases from some professional sellers [83]. Vinted's documentation explicitly encourages users to stay within the Vinted system and to use Buy Now for safety [88, 99]. The platform also links this in-platform flow to practical benefits such as customer support, shipping options, and verified post-transaction reviews [88]. Sellers who push buyers towards off-platform transactions may receive lower listing visibility, even if they are not directly banned from selling outright [88]. Profile verification is also presented as a visible trust signal that can improve perceived credibility and may support sales [79]. In addition, Vinted offers paid visibility features such as Item Bump and Showcase [90, 95].

Vinted profiles display structured information where other users may see the username, profile picture, profile text, location, listed items, reviews, login recency, followers, followed members, and visible verification information [79, 87, 93]. The real name, address, email address, phone number, birth date, and payment information of users are generally not visible to others [93]. However, some information only becomes visible later in the transaction. The other party may see the full name and delivery address once a purchase has been made and shipping is arranged, and this information may also appear on the shipping label [85, 92, 93].

Vinted also documents several fraud- and safety-related measures. The safety materials on their website explain that the platform offers mechanisms such as *"risk scoring"* (*"use predictive analysis to try to detect suspicious activities"*), anti-spam tools to identify inappropriate content and suspicious messages, and automated checks for newly uploaded listings [80, 99]. It also offers paid *"Item Verification"* and *"Electronics Verification"* for selected higher-value items, where the item is first routed through a verification hub before being sent on to the buyer [86, 91]. In addition to these mechanisms, Vinted gives direct behavioral and safety guidance to their users. They encourage users not to move communication or payment off-platform, to be cautious of urgent messages, not to click suspicious links, to check message details carefully, not to share unnecessary personal information, to use Buy Now, and to learn how to distinguish genuine Vinted messages from scams [89, 99].

eBay

Users on eBay can list items, browse listings, message one another, and complete eligible purchases through eBay's own checkout flow that offers buyer-protection [20, 24]. The buyer protection applies to eligible purchases completed through supported payment methods within eBay's checkout flow, including PayPal, credit card, Apple Pay, Google Pay, Klarna variants, direct debit, and related methods [20, 24]. Payments completed wholly or partly outside this checkout process are excluded [20, 24]. eBay presents this protection as covering issues such as non-delivery, damaged goods, and substantial mismatch between the item and the listing description [17, 24]. Its payment guidance also strongly recommends PayPal and warns against unsafe or prohibited methods such as Western Union or MoneyGram [30].

eBay additionally supports local pickup through a structured process (this support system does not exist in Kleinanzeigen and Vinted): buyers receive pickup information during checkout and then use a code that the seller confirms in the app at handover [16].

At account creation, eBay requires an email address and also supports signup through Facebook, Google, or Apple. Before buying or selling, users must verify the account by email [18]. Apple signup also allows users to choose whether to share their email address or to hide it through Apple's relay system. eBay further allows multiple accounts, provided that each uses a different email address and username.

eBay profiles combine a limited amount of automatically displayed information with optional self-presentation. Profiles include basic information

such as username and recent feedback, and users may optionally add a profile picture and a description [31]. If they do not add a description, eBay may instead display a few basic facts, such as when the user started selling and the current feedback rating. eBay's profile policy also prohibits contact information, links to outside pages, and promotion of off-platform sales in profiles [29]. eBay's feedback mechanism allows buyers and sellers to leave transaction feedback tied to completed transactions, and feedback scores (star ratings) that appear next to usernames [22]. In addition to short textual comments, eBay offers detailed seller ratings across dimensions such as item description, communication, shipping time, and shipping and handling charges [22]. eBay also gives explicit advises to buyers to read seller feedback carefully and to pay particular attention to recent negative reviews [17]. Moreover, the platform has outlined a "Principle regarding the manipulation of ratings" that encourages users to write genuine and unbiased reviews. Furthermore, the policy states that any coordinated feedback exchanges, or bribing other users in any form (e.g., free items, discounts or benefits) to write positive reviews are prohibited [23].

The platform also documents authenticity-related programs, reporting tools, dispute resolution, and broader safety guidance [19, 30]. The account-security materials of eBay advise users to be cautious about requests for personal or financial information, to treat urgent or threatening messages with suspicion, not to click links from unknown senders, not to open unsolicited attachments, and to verify whether messages are legitimate through eBay's own message system [25]. eBay provides buyer-protection materials describing several forms of abusive buyer behavior that can invalidate a protection claim, such as false claims of non-delivery, false mismatch claims, or returning a different item than the one received [28].