Groups vs. Booking Websites: Investigating Collaborative Strategies Against Deceptive Patterns

Paul Miles Preuschoff
RWTH Aachen University
Aachen, Germany
preuschoff@cs.rwth-aachen.de

Sarah Sahabi
RWTH Aachen University
Aachen, Germany
sahabi@cs.rwth-aachen.de

René Schäfer
RWTH Aachen University
Aachen, Germany
rschaefer@cs.rwth-aachen.de

Lea Emilia Schirp
RWTH Aachen University
Aachen, Germany
lea.schirp@rwth-aachen.de

Marcel Lahaye
RWTH Aachen University
Aachen, Germany
lahaye@cs.rwth-aachen.de

Jan Borchers
RWTH Aachen University
Aachen, Germany
borchers@cs.rwth-aachen.de

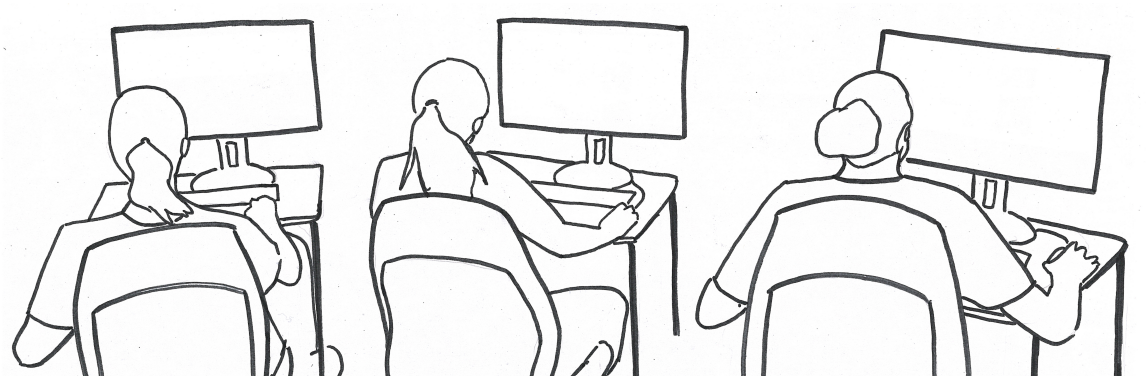

Figure 1: The setup of our user study. To book a fictitious trip together, groups of three participants were using the same booking websites that contained numerous deceptive patterns. We were interested in collaborative strategies to deal with those patterns.

Abstract

Deceptive (or dark) patterns are interface design strategies widely used in apps and online services that manipulate users into making decisions against their best interests. Prior work has explored their effects on individuals and potential countermeasures. We aimed to investigate how collocated groups of users handle deceptive patterns when they encounter them collectively. To this end, we observed seven groups of three users booking flights and rental cars together by browsing the same real websites on separate devices in the same room. We found users collaborating to address deceptive patterns by synchronizing, helping others, and through mutual comparisons. We provide first observations and insights into the strategies that emerge in groups dealing with deceptive patterns in social scenarios.

CHI EA '25, Yokohama, Japan

ACM ISBN 979-8-4007-1395-8/25/04
https://doi.org/10.1145/3706599.3720225

CCS Concepts

• **Security and privacy** → *Usability in security and privacy*; • **Human-centered computing** → *Empirical studies in HCI*; Empirical studies in collaborative and social computing.

Keywords

dark patterns, deceptive patterns, collaboration, group study

ACM Reference Format:
Paul Miles Preuschoff, Sarah Sahabi, René Schäfer, Lea Emilia Schirp, Marcel Lahaye, and Jan Borchers. 2025. Groups vs. Booking Websites: Investigating Collaborative Strategies Against Deceptive Patterns. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3706599.3720225

1 Introduction

Deceptive (or dark[1]) patterns are manipulative design strategies used on websites and in apps to nudge users towards choices that might be against their own best interests [15, 19]. The adverse effects of these patterns on users are widely documented [8, 18], and the research community has begun to structure these patterns

[1]Following the recommendations by ACM's Diversity, Equity, and Inclusion Council, we use *deceptive pattern* instead of *dark pattern*. For this work, the terms are synonymous.

into taxonomies [20] and ontologies [12] and has called for ways to mitigate them [11].

So far, research has focused on how individual users react to deceptive patterns. In contrast, we are investigating how collocated groups of users deal with such patterns. Two reasons drove our decision to look into this scenario: First, it is not uncommon for several collocated users to access a website together in parallel [23], e.g., when planning a trip together. This makes understanding how deceptive patterns affect such interactions relevant in practice. Second, we anticipated that groups might naturally exhibit behaviors to counteract some deceptive patterns. We thus formulated the following research question:

> **RQ:** What behaviors occur in collocated collaborating groups when exposed to deceptive patterns on websites?

To answer it, we conducted an observational study with seven groups of three participants using two real-world booking websites. Participants showed strong signs of annoyance when they encountered deceptive patterns. Our observations revealed several strategies that might make groups more resilient against certain deceptive patterns by comparing, helping each other, and potentially reducing stress. We believe that our insights into group behaviors can support the development of deceptive pattern countermeasures for groups.

2 Related Work

We review related work in the areas of deceptive patterns, their countermeasures, and collocated collaboration.

2.1 Deceptive Patterns

Deceptive patterns are prevalent [8] and commonly used on websites and in apps [7, 8, 15]. To better understand which patterns exist, researchers have structured them into taxonomies [e.g., 2, 20, 22], the most recent one being the ontology by Gray et al. [12]. Here, the authors combined existing taxonomies and unified names for commonly used deceptive patterns, splitting them into 65 high-, meso-, and low-level patterns.

To reduce their negative impact, countermeasures are considered a viable option. Several researchers have presented approaches to designing such countermeasures. Bösch et al. [2] propose ideas for countermeasures for privacy-related deceptive patterns. Further ideas include helping designers [5, 33], developing a rating system for authorities to assess how malicious websites are [21], nudging users towards user-friendly options with "bright patterns"[2] [13, 28], and leaving full autonomy to users by abstaining from using manipulations in either direction with "fair patterns" [25], or automatically detecting deceptive patterns [6, 19] and then visually altering or removing them on the user's device [17, 30, 31].

Another potential field for countermeasures is user awareness. While Gray et al. [10] reported 79.3% of their participants to be able to detect manipulative user interfaces, other studies propose users have difficulties in recognizing deceptive patterns [7, 16]. Luguri and Strahilevitz [18] observed that aggressive deceptive patterns, while receiving a considerable backlash from users, were still very effective [18]. Bongard-Blanchy et al. found that awareness of deceptive patterns does not necessarily increase resilience against embedded manipulations [1].

[2]These patterns use similar strategies as deceptive patterns, but to nudge users towards options that are indeed in the users' interests.

2.2 Collocated Collaboration

In general, group interaction in an organizational setting can be categorized into high-level roles [24] that simplify collaboration and make it more fruitful [34] by showing typical behaviors. Effective teamwork frequently exhibits five different high-level behaviors: *Team Leadership*, *Mutual Performance Monitoring*, *Backup Behavior* (assisting each other when needed), *Adaptability*, and *Team Orientation* [27]. We will relate our findings to these categories. The advantages of collaboration are also the focus of *Computer-Supported Cooperative Work (CSCW)*, which aims at supporting collaboration with software, often in an organizational context [14]. In contrast, our primary goal was to understand a collaborative setting by observing it. Ideally, this would lead to discovering strategies that the research community can leverage to support this type of collaboration effectively moving forward.

3 Methods

Our study investigated how collocated users collaborate when encountering deceptive websites together on separate devices. Before the study, participants read and signed an informed consent form. Next, they performed two similar online booking tasks on *recordrentacar.com* and *opodo.com*. Afterward, we collected demographic data and general information, such as deceptive pattern experience, on a seven-point Likert scale. Later, those results were binned into Low, Medium, and High. To avoid self-reporting bias impacting group behavior, we asked deceptive pattern-specific questions only after the tasks were completed. The study took approximately one hour. We captured audio and video of the whole group and screen recordings of each participant.

3.1 Setup and Task

Each group consisted of three participants seated at adjacent identical computer setups (Fig. 1). Participants could see all screens, point at neighboring screens, and move to other group members if desired. This arrangement was designed to support social interactions and feel natural.

We provided "organizing a group trip" as a general context and asked each group to complete two tasks, CAR and FLIGHT. Aside from the goals we set for the groups, they were free to approach the tasks however they felt fit. In the CAR task, participants booked a rental car. We specified time, location, and type of car. Participants had to book only one car as a group. In the FLIGHT task, participants booked a flight. We specified time and destination to keep the task compact and predictable. We asked participants to book their flights in parallel while making sure to end up on the same plane. This encouraged collaboration and required participants to discuss choices while using the website in parallel on their individual devices. To account for potential order effects, we alternated the task order.

Two of the authors evaluated popular websites for car rentals and flight reservations in search for real, deceptive websites to expose the groups to. From each category, we selected a website that we considered to be particularly manipulative because it exhibited a large number of strongly deceptive patterns. Below, we briefly

describe the two websites used and their embedded deceptive patterns according to Gray et al.'s ontology [12]. For this, an author went through each site's processes and documented any deceptive patterns encountered (Fig. 2 shows examples).

3.1.1 CAR Website. Going through the rental process on *recordrentacar.com* revealed around 10 instances of the deceptive patterns *Visual Prominence*, *False Hierarchy*, *Wrong Language*, *Decontextualizing*, and *High Demand*. Of these, *Visual Prominence* was most common, (e.g., Fig. 2, Example 1).

3.1.2 FLIGHT Website. The process of booking a flight on *opodo.com* revealed over 20 instances of deceptive patterns, mainly from the categories *Sneaking*, *Interface Interference*, and *Social Engineering*. For example, the website regularly created *Urgency* through a pop-up repeatedly reminding users that prices would go up soon (Fig. 2, Example 2 and Appendix A). Particularly noticeable was the *Hidden Costs* pattern, as the price displayed throughout the process includes a discount that only applies to users with a Prime subscription, which is revealed only when finalizing the order (Fig. 2, Example 3 and Appendix A). At that point, users must decide to either pay for the Prime subscription or increase the price of their flight. The site also uses multiple versions of *False Hierarchy*.

3.2 Analysis

Reflexive thematic analysis by Braun and Clarke [4] is a typical approach in group behavior research [9] and has become an established HCI research approach [3]. Following their workflow, one of the authors performed reflexive thematic analysis of the video recordings. In line with recommendations [26], we do not report frequency counts for qualitative results. We started by taking notes during the study to get a general sense of the content. Afterward, we generated initial codes and refined them iteratively using the recordings. In accordance with Braun and Clarke [4], we included descriptive and interpretative aspects. Descriptive parts captured participants' statements, while interpretative parts relied on the coders' subjectivity to capture patterns like body language or sarcasm. We then grouped our resulting codes using visual mapping and physical representations of the codes through sticky notes and constant data engagement. Finally, we reviewed the resulting themes using the recordings to verify that they fit the data.

3.3 Participants

Participants were selected by means of convenience sampling. They were not compensated for participation. Informed consent was given at the beginning of the study. We aimed for groups of people who already knew each other to be able to observe more natural behavior. The study was conducted with seven groups of three users each, for a total of 21 participants aged 21–31 years (M=26 years, SD 3.2). 11 participants identified as male, 10 as female. Most participants self-reported their awareness regarding deceptive patterns as high (19 High, 1 Medium, 1 Low). One group self-reported their familiarity with each other as low, two groups as high, and the remaining four as medium.

4 Results and Discussion

This section reports on the results and interpretation of our reflexive thematic analysis. Participant quotes have been translated where necessary. In the following, the notation *G7,P3*, for example, refers to the third participant of the seventh group.

4.1 Behaviors

In this subsection, we present our observations and interpretations of group behaviors related to deceptive patterns, such as when a participant actively interacted with or referred to an element we reviewed as deceptive. We grouped our observations into two categories that we labeled *Syncing* and *Helping*.

Syncing describes behavior aimed at keeping the group's selections or their position in the process synchronized. The behaviors we collected in this category are related to *Mutual Performance Monitoring*, which Salas et al. [27] describe as monitoring each other's performance and providing feedback to ensure that the team meets its objective. We observed several behaviors that we interpreted as *Syncing*:

Looking: When encountering a deceptive element (in many cases an instance of *Pressured Selling*), we observed participants turning their heads and glancing at their neighbor's screen. We observed two different types of situations in which participants did this: either when they were slower than their peers or when they were faster. For example, one participant encountered a deceptive Prime subscription element, paused, and looked at their neighbor, who was just making a selection for that pattern, afterward acting in the same way (*G3,P2*). In another case, a participant looked at a peer's screen and noticed a difference between their corresponding websites, followed by a discussion about whether a mistake had occurred for one of them.

> *G1,P3: "Did you choose something else? Did you agree (to) something?"*

It turned out that an optional plane seat reservation had been selected by accident. We think there might be two reasons for users to look at other screens when encountering a deceptive pattern: for self-assurance or to check in on others actively. This could, for example, depend on their own confidence and the perceived competence of their peers. This behavior might be helpful for users when encountering deceptive patterns that confuse them, like the instances of *Pressured Selling* seemingly did.

Gathering: At the beginning of each task, we asked participants to sit at their desks. On the FLIGHT page, they were asked to buy individual tickets, while on the CAR page, they were asked to book a single car together. We observed that for the FLIGHT task, participants generally stayed in that seating arrangement, with one participant briefly joining another one occasionally. In those cases, they helped or discussed an aspect of the page. For the CAR page, most groups gathered around one device at some point. They often discussed deceptive elements together.

> *- G6,P2: (Annoyed) "Now what is that? (...) Isn't that (offer) again exactly what we rejected just now?"*
> *- G6,P3: "Yeah, they want you to click this (points at the more expensive option) all the time."*

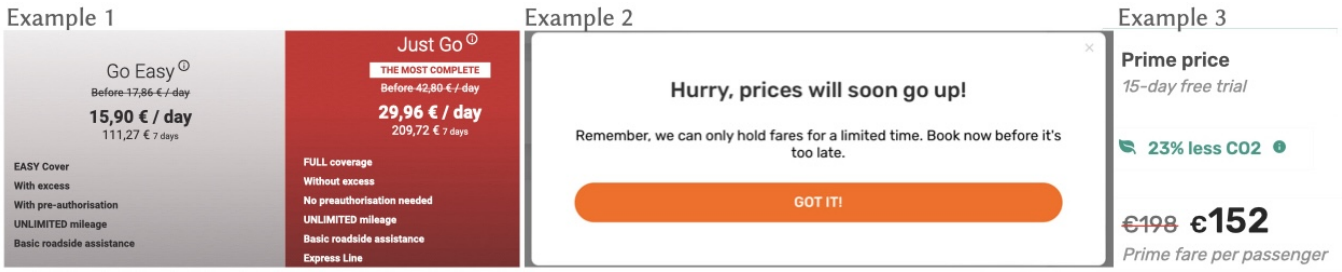

Figure 2: Some deceptive patterns on the websites used. Example 1: *Visual Prominence* on the CAR website. Example 2: *Urgency* pop-up on the FLIGHT website. Example 3: *Hidden Cost* on the FLIGHT website. The FLIGHT website was particularly deceptive. Additional examples can be found in Appendix A.

The difference in behavior between the websites is likely influenced by the task difference. It seems like after getting to know the website, users prefer to work on a single shared device if just a single booking has to be made. When individual bookings have to be made, they seem to prefer working in parallel. A question is whether working on a shared device or parallel devices is more beneficial against deceptive elements. Multiple users paying attention to the same interface might make users more likely to spot sneaky, deceptive patterns like *Trick Questions* or *Sneak Into Basket*. However, in some cases, participants also showed signals of low attention (looking away, low communication) after the group gathered.

Prices: Comparing prices between participants was a prominent behavior. Price differences often caused the group to start syncing to compare their decisions:

> *- G4,P1: (shouts) "What? 177? Oh, I must have screwed up something."*
> *- G4,P2: "Yeah, it has selected standard by default. You have to pick basic."*

During the study, we noticed that the FLIGHT website used targeted pricing, sometimes resulting in different prices for our participants. Those differences between the exact same options led to irritation:

> *G2,P1: (shouts) "What? Why does the flight cost 146 for me, 147 for her, and 145 for you?"*

Also, when a price increased in the process without the group expecting it, participants were alarmed:

> *G4,P3: "Why is this (price) more than a moment ago? Like, I definitely did not book anything in addition."*

The current overall price seems to be used to indicate the current position in the process and the decisions made. Since price differences were often treated as an error that had to be resolved, participants seemed to assume that if two users had the same price, this would indicate that their selections were aligned. This might make some deceptive patterns, like *Bad Defaults* or *Sneak Into Basket*, which aim to obfuscate price increases, easier to spot since all group members need to be fooled to keep the price synchronized. By using targeted prices between individuals, websites introduce a potential obstacle for group synchronization since users might be misled to try to identify the cause of the different prices and get the cheaper one, even if that is not possible.

Checkpointing: We observed groups discussing the status of their process at varying intervals, often when completing major process steps, typically when pressing continue in a process. For example, after selecting a flight from a list of candidates:

> *G1,P2: "We still have the same flight, let's confirm it. (reads flight number, other participants nod) Okay, great, so let's continue."*

This was often coupled with comparing prices. When no differences were found (or different decisions had been made on purpose), the group would continue to the next step. Otherwise, they would assume that a mistake had occurred, and the group would try to find and resolve it.

> *- G3,P3: "Okay, should we continue?" - G3,P1: "I need a second!" - G3,P2: "I have a different price."*
> *- G3,P3: "Oh you have the Prime subscription for some reason, I don't have that one."*
> *(The group starts to investigate what went wrong and resolves it)*

Groups seem to treat major process steps like a checkpoint. *Checkpointing* might increase the chance of users noticing that they fell for patterns that are easy to miss, like *Bad Defaults*. We believe that this may increase the confidence of users, because they can compare whether they are on the right track so far, potentially making the process less stressful. This feeling of security could also be deceptive in situations where all team members excessively depend on the group to remain vigilant; however, we did not notice such situations.

The following observations are about participants **Helping** each other actively. Behaviors from this category fit into the *Backup Behavior* identified by Salas et al. [27], as they are aimed to assist each other to improve overall team performance.

Asking for Advice: Participants sometimes asked the group for clarification when they encountered deceptive elements:

> *G6,P1: (encounters a pressured-selling instance) "Is it mandatory to book seats, or will they be randomly assigned when we book none?"*

They also wondered how to deal with deceptive elements that appeared suddenly:

> *- G3,P2: (Hurry, prices will soon go up) "Do you guys also have this pop-up? (points at screen)"*
> *- G3,P1: "Oh, I had that too. I simply X-ed it immediately."*

In most of these cases, the group provided help and actually was able to provide helpful advice. Being able to ask a peer seems to be helpful for users when encountering deceptive elements that confuse or pressure users, like *Pressured Selling*. This might reduce stress, which would weaken the negative impact of such patterns, rendering the user more resilient.

Warning: In rare cases, participants warned others about a deceptive element.

> *G2,P3: (referring to the deceptive Prime subscription with costs) "That is the Prime fare, you have to get Prime for that price. It actually costs 195 €, but if you have Prime it costs less."*

This preventive helping behavior was less common than reactive helping.

Scouting: Group members sometimes engaged in behaviors in which they diverged from the group and went ahead in the process, gathering additional information about the subsequent steps.

> *G5,P2: "I just wanted to know how much the extra luggage costs: We would have to pay 73.50 € extra with the Eurowings flight."*

At times, they also 'dug deeper' into confusing elements of the current step, like the terms of service or "More Information" boxes. Those were often instances of *Hiding Information* designed to make relevant information harder to access.

> *G5,P1: (after reading through a long informational text about Opodo Prime) "Look, here it says that the subscription will change to a paid membership after 15 days."*

Scouting behavior might be effective against deceptive patterns like *Hidden Costs* or *Hiding Information*, as it allows groups to compare different options in parallel and decide based on information that is disclosed later in the process. It might make users more resilient against these deceptive patterns as the mental load can be shared, but it might also slow them down.

4.2 Group Dynamics

We observed that individual group members tended to display different behaviors. Some participants were quick. They tended to perform scouting and helping behaviors, as well as initiate and coordinate syncing behaviors. Those participants might have been more confident or competent in the task domain and seemed willing to support the group. Slower participants asked for advice and often followed the decisions of others. Those participants may have profited the most from being in a group.

During large portions of the study, participants showed strong signs of **Frustration** that were connected to deceptive patterns. We observed sighing, cursing, groaning, shouting, screaming, sounds of disgust, gestures implying violence against the monitor, leaning back from the device, and more. One user started filing a complaint using the website's feedback function. When talking to each other, users referred to elements that we identified as deceptive, calling them "horrible" (*G4,P1*), "nasty" (*G7,P1*), "antisocial" (*G6,P3*), "stress-inducing" (*G6,P2*), "annoying" (*G5,P2*), "impudent" (*G4,P3*), and more. Especially the FLIGHT website caused strong signs of frustration. The causes seemed to be:

- Interruptions of the task flow, to a large extent demonstrated by a high amount of pop-ups on the FLIGHT website.
  - G5,P1: "How often does this side still want to say hurry up, prices go up soon?"
  - G5,P2: "Yeah, this is the moment where I would just quit the page!"
- Being forced to reject the same offer multiple times during the process.
  G4,P1: "No, I really, REALLY do not want to book a hotel!"
- Features that were designed to induce pressure and overwhelm users.
  G2,P1: "I feel like a 50-year-old who would actually need the help of their son or nephew for this."
- Desynchronization of prices between participants without apparent reason.
- Relevant information being vague, incomplete, or obstructed.
  G5,P1: "And what I find really crappy on this website, for example, is that you can't say exactly what the deductible is, how the car is insured, and so on."

This appeared to foster a lack of trust in the service provider.

> *G6,P3: "Wow, that is mean, I wouldn't book there!"*

Deceptive patterns are known to reduce the trust of individual users in the brand [32], and this effect appears to translate to groups.

Numerous groups began to express incredulous laughter when encountering especially impudent deceptive elements like repeated pop-ups (Appendix 5). Participants also often agreed on certain deceptive patterns, such as the pop-ups, to be ridiculous. It seemed for all groups like the website became a *common foe*, and frustration sometimes turned into an annoyed bemusement. Maybe it was comforting for participants to see that they were not the only person struggling with deceptive elements. This might reduce the manipulative effect that stress-inducing deceptive patterns have on group members, since participants realize that it is not their fault that the website feels overwhelming.

5 Conclusion and Future Work

We investigated and interpreted the collaboration strategies that small collocated groups adopt when encountering deceptive patterns on booking websites together on multiple devices. Our findings indicate that groups use *Synchronization* and *Helping* behaviors, which may increase their resilience against some kinds of online deception. Group members did not warn each other much but compared their actions often. Mistakes triggered by deceptive patterns were often detected by *checkpointing* (syncing after a major process step), often using *prices* as an indicator and, if a difference was detected comparing choices, resulting in identifying the mistake and correcting it. Relying on synchronization and comparison behaviors may alleviate stress for individual users, as they are able to depend on their group in addition to themselves. Shared frustration and annoyance about deceptive patterns led to a surprisingly lighthearted atmosphere, with the group tackling the website together while making fun of it.

One limitation of our study is that our participants were rather young and self-reported relatively high expertise in deceptive patterns. Also, while participants self-reported how well they knew

each other, we did not collect the nature of the relationship between them, which could also have influenced group behavior. Furthermore, we focused on two travel-related booking pages, while deceptive patterns are also present in many other contexts.

5.1 Future Work

Special deceptive pattern countermeasures that support group behaviors seem to be a promising next step. Such countermeasures could help by making choices and resulting prices easier to compare, for example, by visualizing them. They could also show choices that other members of the group have made, either to verify them or to use them for orientation. In addition, groups seem to profit from users who are willing to scout or provide advice. With the current advancements in LLMs and their potential to deal with deceptive patterns [29], it may be feasible to use this technology to simulate an additional team member. Such an assistant could either be proactive and scout to warn users of hidden costs, or it could take the form of a chat assistant who can provide advice when asked. When combining this with crowd intelligence, similar to the concept of ad blockers, this could even be used to simulate a competent peer for individual users.

A fascinating open question is whether the group behaviors that are aimed to increase resilience against deceptive patterns actually achieve that compared to individual scenarios. Therefore, the next step following this work is an experimental study to quantify our observations. Our findings would also be strengthened by verifying them with other populations, such as less experienced users, and in a broader context. Ultimately, our goal is to improve the understanding of groups that encounter deceptive patterns, to support the research community in developing deceptive pattern countermeasures for groups, and maybe transfer promising behaviors to the domain of individual users.

Acknowledgments

We would like to thank our reviewers for their constructive feedback, and our participants for engaging in our study. In addition, we want to thank Sofie van Anrooij for illustrating Figure 1 and Anke Brocker for proofreading. This work was funded in part by the German B-IT Foundation.

References

[1] Kerstin Bongard-Blanchy, Arianna Rossi, Salvador Rivas, Sophie Doublet, Vincent Koenig, and Gabriele Lenzini. 2021. "I Am Definitely Manipulated, Even When I Am Aware of It. It's Ridiculous!" - Dark Patterns from the End-User Perspective. In *Proceedings of the 2021 ACM Designing Interactive Systems Conference* (Virtual Event, USA) *(DIS '21)*. Association for Computing Machinery, New York, NY, USA, 763–776. doi:10.1145/3461778.3462086

[2] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales From the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proceedings on Privacy Enhancing Technologies* 4 (2016), 237–254. doi:10.1515/popets-2016-0038

[3] Robert Bowman, Camille Nadal, Kellie Morrissey, Anja Thieme, and Gavin Doherty. 2023. Using Thematic Analysis in Healthcare HCI at CHI: A Scoping Review. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 491, 18 pages. doi:10.1145/3544548.3581203

[4] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[5] Evan Caragay, Katherine Xiong, Jonathan Zong, and Daniel Jackson. 2024. Beyond Dark Patterns: A Concept-Based Framework for Ethical Software Design. In *CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. ACM, New York, Article 291, 16 pages. doi:10.1145/3613904.3642781

[6] Jieshan Chen, Jiamou Sun, Sidong Feng, Zhenchang Xing, Qinghua Lu, Xiwei Xu, and Chunyang Chen. 2023. Unveiling the Tricks: Automated Detection of Dark Patterns in Mobile Applications. In *Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology* (San Francisco, CA, USA) *(UIST '23)*. Association for Computing Machinery, New York, NY, USA, Article 114, 20 pages. doi:10.1145/3586183.3606783

[7] Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto Bacchelli. 2020. UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. doi:10.1145/3313831.3376600

[8] European Commission and Directorate-General for Justice and Consumers, F Lupiáñez-Villanueva, A Boluda, F Bogliacino, G Liva, L Lechardoy, and T Rodríguez de las Heras Ballell. 2022. *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation (final report)*. Publications Office of the European Union, Brussels. doi:10.2838/859030

[9] Casey Fiesler, Jed R. Brubaker, Andrea Forte, Shion Guha, Nora McDonald, and Michael Muller. 2019. Qualitative Methods for CSCW: Challenges and Opportunities. In *Companion Publication of the 2019 Conference on Computer Supported Cooperative Work and Social Computing* (Austin, TX, USA) *(CSCW '19 Companion)*. Association for Computing Machinery, New York, NY, USA, 455–460. doi:10.1145/3311957.3359428

[10] Colin M. Gray, Jingle Chen, Shruthi Sai Chivukula, and Liyang Qu. 2021. End User Accounts of Dark Patterns as Felt Manipulation. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 372 (Oct 2021), 25 pages. doi:10.1145/3479516

[11] Colin M. Gray, Johanna T. Gunawan, René Schäfer, Nataliia Bielova, Lorena Sanchez Chamorro, Katie Seaborn, Thomas Mildner, and Hauke Sandhaus. 2024. Mobilizing Research and Regulatory Action on Dark Patterns and Deceptive Design Practices. In *Extended Abstracts of the 2024 CHI Conference on Human Factors in Computing Systems (CHI EA '24)*. Association for Computing Machinery, New York, NY, USA, Article 482, 6 pages. doi:10.1145/3613905.3636310

[12] Colin M. Gray, Cristiana Teixeira Santos, Nataliia Bielova, and Thomas Mildner. 2024. An Ontology of Dark Patterns Knowledge: Foundations, Definitions, and a Pathway for Shared Knowledge-Building. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 289, 22 pages. doi:10.1145/3613904.3642436

[13] Paul Graßl, Hanna Schraffenberger, Frederik Zuiderveen Borgesius, and Moniek Buijzen. 2021. Dark and Bright Patterns in Cookie Consent Requests. *Journal of Digital Social Research* 3, 1 (2021), 1–38. doi:10.33621/jdsr.v3i1.54

[14] J. Grudin. 1994. Computer-supported cooperative work: history and focus. *Computer* 27, 5 (1994), 19–26. doi:10.1109/2.291294

[15] Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog, and Christo Wilson. 2021. A Comparative Study of Dark Patterns Across Web and Mobile Modalities. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2, Article 377 (Oct 2021), 29 pages. doi:10.1145/3479521

[16] Maxwell Keleher, Fiona Westin, Preethi Nagabandi, and Sonia Chiasson. 2022. How Well Do Experts Understand End-Users' Perceptions of Manipulative Patterns?. In *Nordic Human-Computer Interaction Conference* (Aarhus, Denmark) *(NordiCHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 52, 21 pages. doi:10.1145/3546155.3546656

[17] Konrad Kollnig, Siddhartha Datta, and Max Van Kleek. 2021. I Want My App That Way: Reclaiming Sovereignty Over Personal Devices. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI EA '21)*. ACM, New York, Article 393, 8 pages. doi:10.1145/3411763.3451632

[18] Jamie Luguri and Lior Jacob Strahilevitz. 2021. Shining a Light on Dark Patterns. *Journal of Legal Analysis* 13, 1 (Mar 2021), 43–109. doi:10.1093/jla/laaa006

[19] Arunesh Mathur, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW, Article 81 (nov 2019), 32 pages. doi:10.1145/3359183

[20] Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer. 2021. What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 360, 18 pages. doi:10.1145/3411764.3445610

[21] Thomas Mildner, Merle Freye, Gian-Luca Savino, Philip R. Doyle, Benjamin R. Cowan, and Rainer Malaka. 2023. Defending Against the Dark Arts: Recognising Dark Patterns in Social Media. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference* (Pittsburgh, PA, USA) *(DIS '23)*. Association for Computing Machinery, New York, NY, USA, 2362–2374. doi:10.1145/3563657.3595964

[22] Alberto Monge Roffarello, Kai Lukoff, and Luigi De Russis. 2023. Defining and Identifying Attention Capture Deceptive Designs in Digital Interfaces. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 194, 19 pages. doi:10.1145/3544548.3580729

[23] Meredith Ringel Morris. 2008. A survey of collaborative web search practices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Florence, Italy) *(CHI '08)*. Association for Computing Machinery, New York, NY, USA, 1657–1660. doi:10.1145/1357054.1357312

[24] Troy V. Mumford, Michael A. Campion, and Frederick P. Morgeson. 2006. Situational judgment in work teams: A team role typology. In *Situational judgement tests: Theory, measurement, and application*, Jeffrey A. Weekley and Robert E. Ployhart (Eds.). Lawrence Erlbaum Associates, Mahwah, NJ, 319–343.

[25] Marie Potel-Saville and Mathilde Da Rocha. 2024. From Dark Patterns to Fair Patterns? Usable Taxonomy to Contribute Solving the Issue with Countermeasures. In *Privacy Technologies and Policy*, Kai Rannenberg, Prokopios Drogkaris, and Cédric Lauradoux (Eds.). Springer Nature Switzerland, Cham, 145–165.

[26] Priscilla M. Pyett. 2003. Validation of Qualitative Research in the "Real World". *Qualitative Health Research* 13, 8 (2003), 1170–1179. doi:10.1177/1049732303255686 arXiv:https://doi.org/10.1177/1049732303255686

[27] Eduardo Salas, Dana E. Sims, and C. Shawn Burke. 2005. Is there a "Big Five" in Teamwork? *Small Group Research* 36, 5 (2005), 555–599. doi:10.1177/1046496405277134 arXiv:https://doi.org/10.1177/1046496405277134

[28] Hauke Sandhaus. 2023. Promoting Bright Patterns. Position Paper at the Workshop "Designing Technology and Policy Simultaneously: Towards A Research Agenda and New Practice" at CHI '23, 9 pages. doi:10.48550/arXiv.2304.01157

[29] René Schäfer, Paul Preuschoff, Rene Niewianda, Sophie Hahn, Kevin Fiedler, and Jan Borchers. 2025. Don't Detect, Just Correct: Can LLMs Defuse Deceptive Patterns Directly?. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI EA '25)*. Association for Computing Machinery, New York, NY, USA, 11 pages. doi:10.1145/3706599.3719683

[30] René Schäfer, Paul Miles Preuschoff, and Jan Borchers. 2023. Investigating Visual Countermeasures Against Dark Patterns in User Interfaces. In *Proceedings of Mensch Und Computer 2023* (Rapperswil, Switzerland) *(MuC '23)*. Association for Computing Machinery, New York, NY, USA, 161–172. doi:10.1145/3603555.3603563

[31] René Schäfer, Paul Miles Preuschoff, René Röpke, Sarah Sahabi, and Jan Borchers. 2024. Fighting Malicious Designs: Towards Visual Countermeasures Against Dark Patterns. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 296, 13 pages. doi:10.1145/3613904.3642661

[32] Christian Voigt, Stephan Schlögl, and Aleksander Groth. 2021. Dark Patterns in Online Shopping: of Sneaky Tricks, Perceived Annoyance and Respective Brand Trust. In *HCI in Business, Government and Organizations*, Fiona Fui-Hoon Nah and Keng Siau (Eds.). Springer International Publishing, Cham, 143–155.

[33] Leah Zhang-Kennedy, Maxwell Keleher, and Michaela Valiquette. 2024. Navigating the Gray: Design Practitioners' Perceptions Toward the Implementation of Privacy Dark Patterns. *Proc. ACM Hum.-Comput. Interact.* 8, CSCW1, Article 97 (2024), 26 pages. doi:10.1145/3637374

[34] Haibin Zhu, Mengchu Zhou, and Ming Hou. 2015. *Support Collaboration with Roles*. Wiley-IEEE Press, unknown. 575 – 598 pages. doi:10.1002/9781119036821.ch15 Cited by: 4.

A Additional Screenshots of Deceptive Patterns

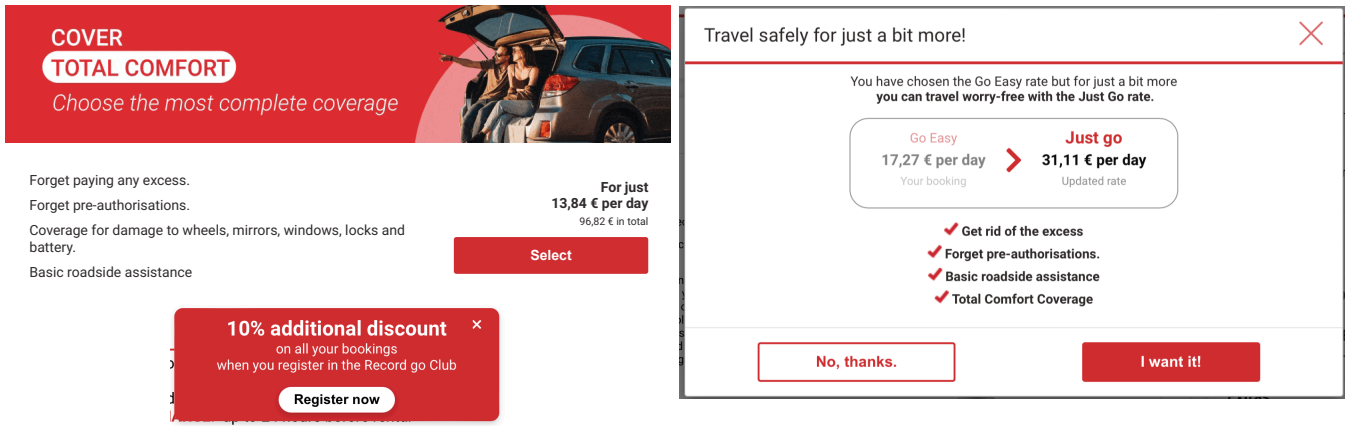

Figure 3: Additional examples of deceptive patterns on the CAR website. Users were nudged to create an account and to choose more expensive options.

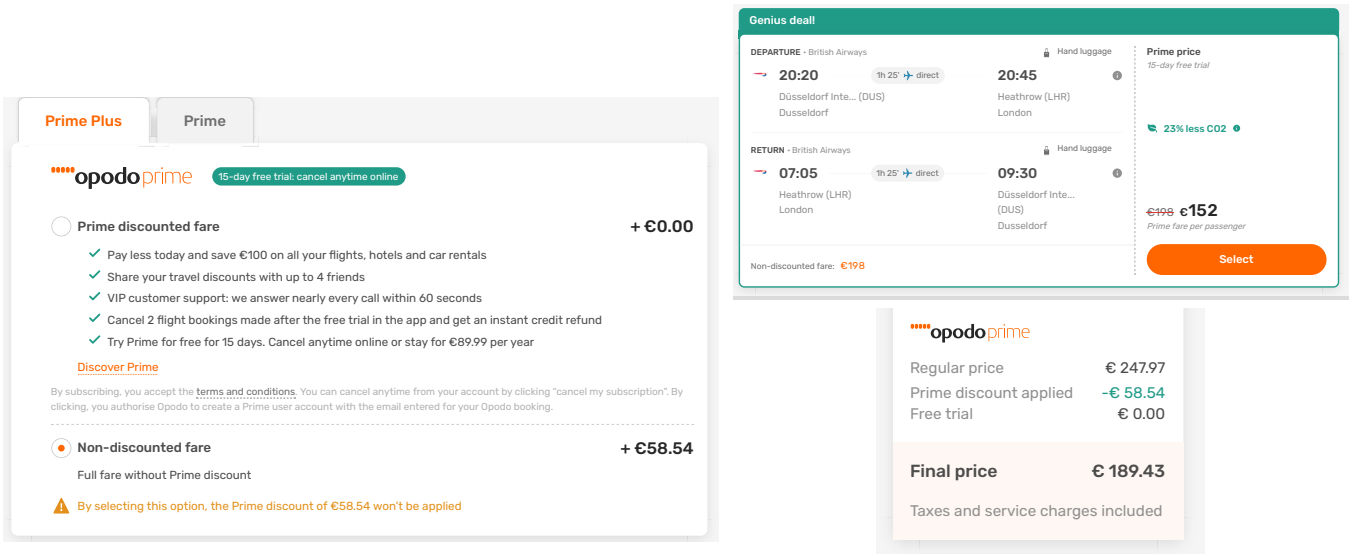

Figure 4: Additional examples of deceptive patterns related to Prime on the FLIGHT website. Users were at the end nudged to subscribe to a paid service that was required to get the shown discounts.

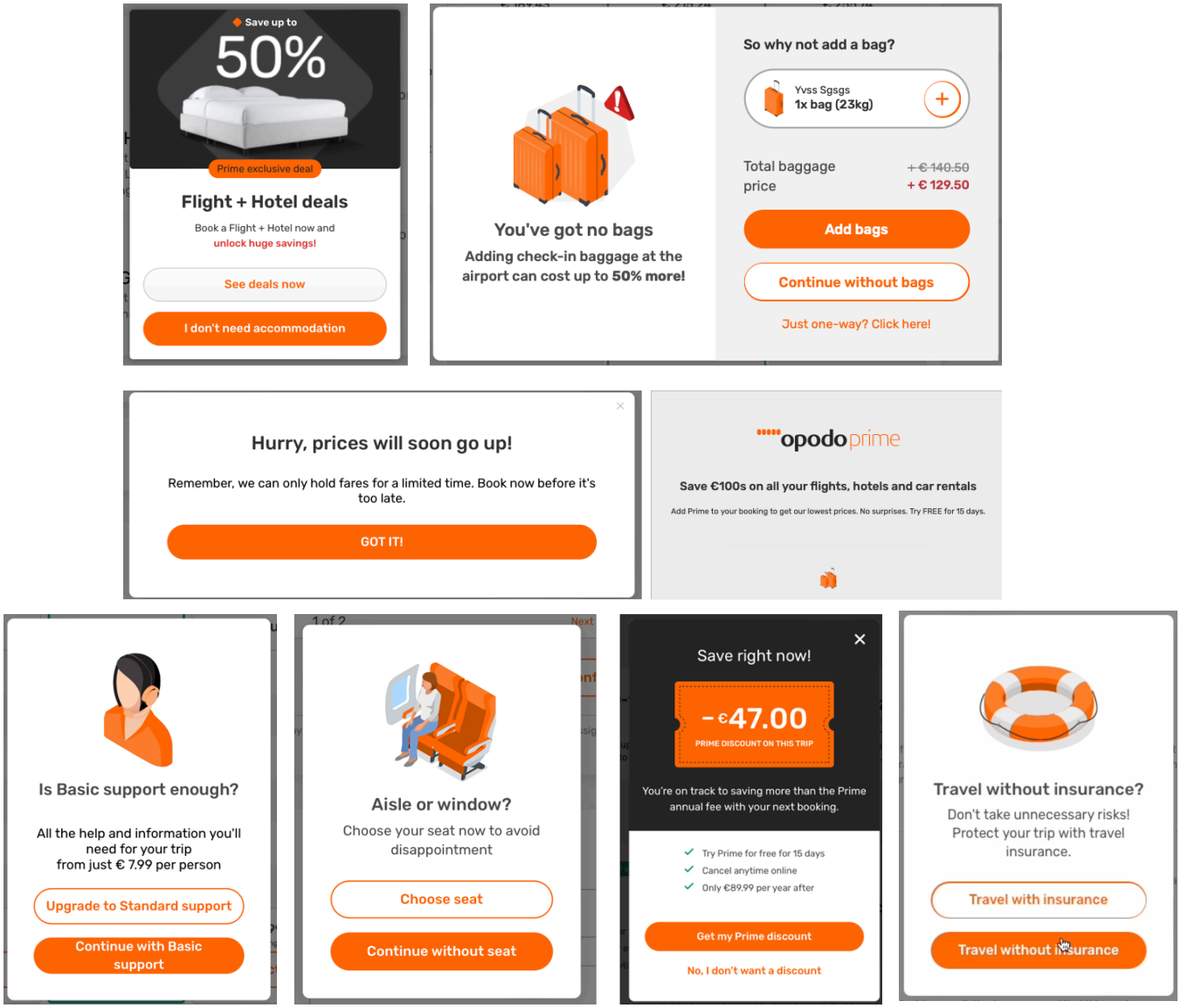

Figure 5: Additional examples of pop-ups on the FLIGHT website. Users encountered a high number of pop-ups during the booking process, that tried to sell additional services or induced time pressure.