"If They Have No Choice, They'll Accept!": How Children and Adolescents Assess Deceptive Designs

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

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

Lucia Karl
RWTH Aachen University
Aachen, Germany
lucia.karl@rwth-aachen.de

Sophie Hahn
RWTH Aachen University
Aachen, Germany
sophie.hahn@rwth-aachen.de

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

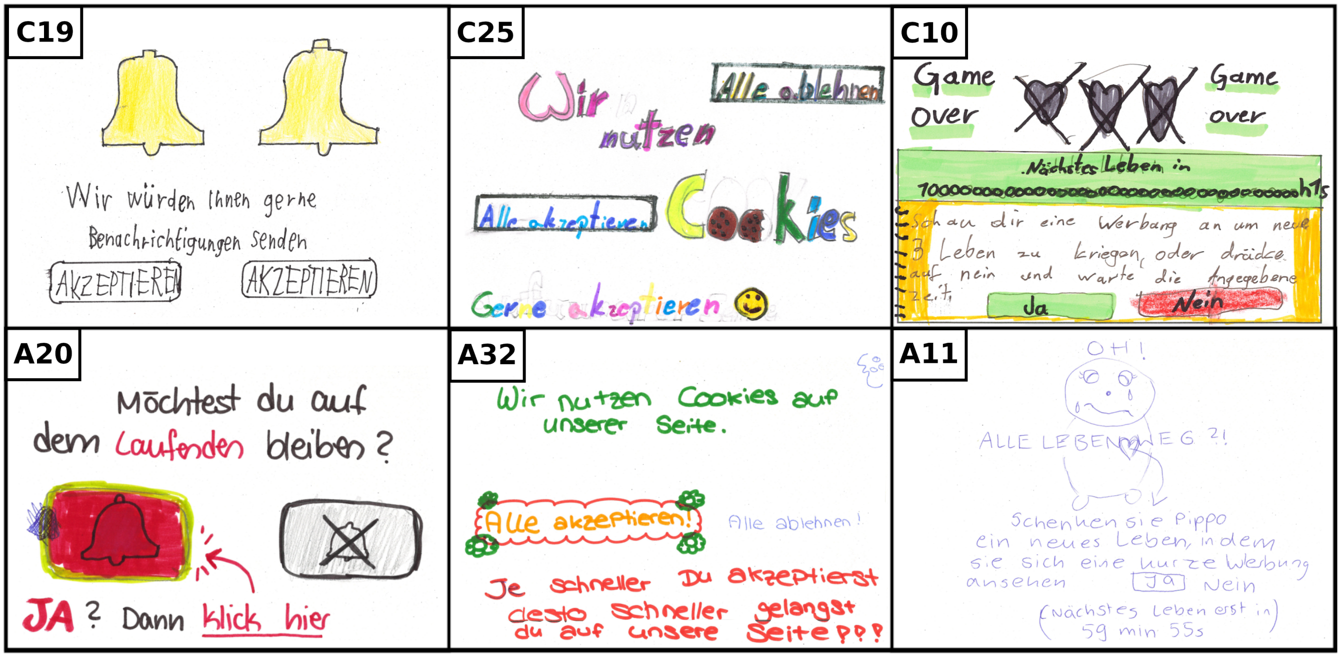

C19
Wir würden Ihnen gerne Benachrichtigungen senden
AKZEPTIEREN
AKZEPTIEREN
C25
Wir nutzen Cookies
Alle ablehnen
Alle akzeptieren
Gerne akzeptieren
C10
Game over
Game over
Nächstes Leben in
1000000000000000000000000000000000000000000h1s
Schau dir eine Werbung an um neue 3 Leben zu kriegen, oder drücke auf nein und warte die Angegebene zeit
Ja
Nein
A20
Möchtest du auf dem Laufenden bleiben?
JA? Dann klick hier
A32
Wir nutzen Cookies auf unserer Seite.
Alle akzeptieren!
Alle ablehnen!
Je schneller Du akzeptierst desto schneller gelangst du auf unsere Seite???
A11
OH!
ALLE LEBEN WEG?!
Schenken sie Pippo ein neues Leben, indem sie sich eine kurze Werbung ansehen
Ja
Nein
(Nächstes Leben erst in 59 min 55s)

Figure 1: In our study, children (top) and adolescents (bottom) redesigned fair versions of three different dialogs that originally asked users to accept notifications (left), to accept cookies (center), or to watch an ad to continue playing (right). We asked participants to nudge users toward acceptance. Redesigns contained no option to decline (C19), visual nudging (A20), colorful designs (C25, A32), increased wait times (C10), and emotional manipulation (A11). English translations are provided in Figure 5.

Abstract

Deceptive (or dark) patterns are UI design strategies that manipulate users into decisions against their best interests. Unlike with adults, their effects on children and adolescents, who are especially vulnerable groups and experience such designs from a young age, have received little attention. Therefore, we explored how these two age groups assess deceptive patterns. In our study, 45 children (10–12 years) and 37 adolescents (16–18 years) redrew fair designs to make them deceptive and ranked deceptive interfaces by how effectively they might influence users. Both age groups used most of the high-level deceptive patterns from an existing ontology, but also less common manipulative strategies. While children opted for more extreme designs, including threats and rewards, adolescents chose subtler manipulations closer to tactics employed in reality, like False Hierarchy. We contribute these and other insights into how these groups perceive deceptive patterns, and how those findings map to existing pattern literature.

*Both authors contributed equally to this research.

IDC '25, Reykjavik, Iceland
© 2025 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1473-3/25/06
https://doi.org/10.1145/3713043.3731497

CCS Concepts

• **Human-centered computing** → **User studies**; • **Social and professional topics** → *Children*; *Adolescents.*

Keywords

deceptive patterns, dark patterns, children, adolescents, drawings

ACM Reference Format:

René Schäfer, Sarah Sahabi, Lucia Karl, Sophie Hahn, and Jan Borchers. 2025. "If They Have No Choice, They'll Accept!": How Children and Adolescents Assess Deceptive Designs. In *Interaction Design and Children (IDC '25), June 23–26, 2025, Reykjavik, Iceland.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3713043.3731497

1 Introduction

Deceptive (or dark) patterns are manipulative UI design strategies that nudge users toward decisions favoring the service owner [19]. Their prevalence in apps and online [7, 19] makes it essential to study how vulnerable groups understand and assess such manipulations. One such important group is children and adolescents [8], because they tend to engage in riskier online behavior than adults [30] and are heavily exposed to mobile applications, especially games, where deceptive patterns are prevalent [7, 13]. So far, however, deceptive pattern research has primarily focused on adult users [e.g., 1, 7, 14] and only recently begun to consider children and adolescents [22, 24, 26]. This led us to two research questions: (RQ1) What strategies do children and adolescents consider the most manipulative for decision-making? (RQ2) How does this assessment differ between children and adolescents?

To answer these, we conducted a study with 45 children (10–12 years) and 37 adolescents (16–18 years) in a German school. Participants were tasked to alter fair designs to nudge users towards a specific decision and to rank interfaces containing deceptive patterns by perceived effectiveness.

We observed an overlap between strategies used in the drawings and known deceptive patterns. Moreover, children used more extreme and exaggerated nudging than adolescents. For their ranking, children and adolescents both found designs containing a Countdown Timer or Hidden Information to be very effective. Additionally, adolescents perceived a fair design as relatively ineffective compared to designs containing deceptive patterns.

Thus, our key contributions are (1) insights into how children and adolescents each assess deceptive patterns, and (2) how these findings align with the literature on deceptive patterns.

2 Related Work

Deceptive patterns manipulate by exploiting users' general human constitution [2] and overruling their usual preferences [9, 17]. Consequently, users may exhibit negative reactions [10], from annoyance and frustration [6, 29] to anxiety and alertness [17]. To create a shared language, Gray et al.'s ontology [12] categorizes 60 deceptive patterns from the literature into five high-level deceptive strategies: Obstruction, Sneaking, Interface Interference, Forced Action, and Social Engineering. We list the definitions of those patterns relevant to our work in Appendix A. To mitigate the effects of deceptive patterns, researchers call for countermeasures [11] such as automatic detection [5, 19], visually altering found patterns [25], and educating users [1]. Making users aware of the existence of deceptive patterns and educating them can help them recognize [7], although not necessarily resist [1] these patterns.

Minors, who are easier to manipulate than adults [28], are particularly vulnerable to such patterns [17]. Although children have demonstrated an awareness of manipulative designs, their vigilance often extends to non-dangerous elements like genuine warnings, indicating a lack of understanding or ability to protect themselves effectively [22]. Children often turn to their parents for guidance when facing online risk [16, 24]. However, this approach is not consistently reliable due to parents' misconceptions about online security [16] and their decreasing influence over their children's online behavior as they grow older [16, 23, 27]. This makes it essential to educate minors about deceptive patterns. One effective strategy for this is helping them understand the intent behind such manipulations [22]. This, however, requires first studying how different underage groups perceive and assess deceptive patterns.

Previously, we examined 10–11-year-olds' understanding of deceptive designs [26] and found that they understood the intent behind such manipulative strategies to a degree. This included a drawing task because *creating* is a measure of high-level understanding according to Bloom's revised taxonomy [15]. However, the drawing task in that study took place after children had been introduced to the concept of deceptive designs. Therefore, we conducted another study with an unbiased drawing task. This is the study we report on in this paper. To enhance generalizability and explore the differences between age groups, we expanded this study to include not only 10–12-year-olds but also 16–18-year-old adolescents. While such an unbiased drawing task has not been investigated previously for deceptive patterns, findings from other areas suggest that children aged 12–13 display higher materialism and lower self-esteem than adolescents aged 16–18 [4], making them potentially more prone to Social Engineering or reward-and-punishment-based tactics.

3 Study

To address our research questions, we conducted a study with two classes of 6th-graders and two of 11th-graders in four separate sessions at a local German school. After filling in a demographics questionnaire, each participant individually completed two tasks on paper. To prevent priming, we only revealed the study topic and referred to *deceptive patterns* and *manipulation* after all tasks had been completed.

In the first task, we adapted the drawing task from our previous study [26] to deepen our understanding of how children and adolescents perceive and interpret deceptive interfaces. Participants received one of three manipulation-free dialogs (Figure 3), which ask users to accept cookies, allow notifications, or watch an ad for an extra life in a game. We then asked them to draw a redesign of their dialog so that more users would accept cookies or notifications or watch an ad, and to explain their redesign in writing. In task 2, our participants received nine designs (Figure 4) and ranked them based on which designs would make users more likely to invite their friends to a mobile game, adapting the *arranging cards* method used in research with children [18]. Afterward, they justified their ranking. One design was fair, while all others contained at least one deceptive pattern, such as *Countdown Timer*, *Activity Message*, *Confirmshaming*, or *Trick Question*, covering textual and visual manipulations.

We followed the *ACM Code of Ethics*[1] and the standards of the *Ethical Research Involving Children*[2] project; our department did not have an ethics committee at the time of the study. Before the study, we collected written consent from a parent or legal guardian and explicit consent from participants. Upon request from the teacher, children and adolescents without a signed consent form stayed in the classroom and completed the tasks but were not considered in the data analysis. Following Mertala [20] and Punch [21], our interfaces use a playful design. All answers were anonymized to protect participants' identities. To minimize potential stress, a teacher the students were familiar with was present during the study. We included a 10-minute break to give participants time to recuperate.

Overall, we had 82 participants: 37 adolescents (16–18 years, M=17, SD=0.58; 29 female, 8 male) and 45 children (10–12 years, M=11, SD=0.37; 19 female, 25 male, 1 undisclosed). All adolescents stated using their smartphones several times a day, while 30 children use them several times a day, 14 multiple times per week, and 1 once a week. Below, we refer to participants with letter–number codes (C: children, A: adolescents, e.g., A12 = adolescent participant no. 12).

3.1 Drawings

To investigate participants' understanding of manipulative designs and their own strategies, we analyzed the drawings using reflexive thematic analysis [3]. Based on the manipulations used, one author inductively created codes and developed themes for similar strategies in each age group. This resulted in 28 codes for the children's data, 27 for adolescents, and five themes per age group. Below, we present the most prominent themes describing the deceptive strategies participants used. We then highlight overlaps between our themes and Gray et al.'s pattern ontology [12].

Theme 1: Emotional Cues Both children and adolescents used cues to trigger emotions, such as guilt or compassion, in favor of one option over another. Participants would use colors, symbols, or linguistic tricks to make the "Accept" option look better or more ethical or the "Reject" option look worse. These tricks combine the Social Engineering and Emotional or Sensory Manipulation patterns from the ontology [12]. For example, many drawings contained green and red buttons to mark "good" and "bad" options (e.g., C10, Figure 1)—an instance of the Positive or Negative Framing pattern. Others used writing or symbols to trivialize the harm of accepting cookies, ads, or notifications (e.g., "The smiling face represents a 'friendly' cookie that you would willingly accept" (A01) or C25 in Figure 1) or trigger guilt or compassion to make users accept them (e.g., "We ask you to please help us. You will not take any harm from this. Thank you very much" (C07 in the cookie banner scenario) or A11 in Figure 1), instantiating Confirmshaming.

Theme 2: Visual Dominance Participants frequently made "Accept" buttons clearly *stand out visually* over alternatives, matching the high-level Interface Interference pattern. Some highlighted buttons using colors, bigger button sizes, or fonts, or by framing them with symbols or other eye-catching motifs (e.g., A20, A32, Figure 1). Others did the opposite by making the "Reject" button less obtrusive, e.g., by replacing it with a small × in the upper right corner. While Interface Interference is one of the most common deceptive patterns in practice [7], this strategy was particularly dominant among adolescents. This may be because they have been exposed to deceptive patterns longer than children, suggesting a persistent influence of such manipulations on users. Unlike in our previous study [26], only few children adopted this strategy. This supports our assumption that children in our previous study were primed towards Interface Interference designs through prior tasks, explaining its dominance in their drawings there.

Theme 3: Rational Persuasion Both participant groups used tricks to convince users that choosing the "Accept" option was the *logically smartest* decision. Some stressed the advantages of accepting or the disadvantages of rejecting, e.g., "If you click on accept, you will receive important notifications from us, without which you would probably be at a disadvantage to others" (C05), or C10 in Figure 1. Moreover, some adolescents tried to evoke a (false) sense of control, e.g., by informing the user that they could "end [the notification subscription] at any time" (A12). Both children and adolescents introduced additional, *attractive enticements* to lure users into selecting "Accept": "I've added an extra 100 coins to encourage players to watch the ads, as they get another reward in addition to a life" (A33). What we only observed for children, however, was threatening or punishing users for selecting the "Reject" option. For example, users would need to accept unless they wanted to lose in-game coins (C09). As a more extreme example, C04 wrote: "If you click on 'No', your cell phone and address will be hacked. Wait until a kidnapper rings your doorbell". While prominent among children's drawings, there were no threats or punishments in the drawings of our previous study with participants of a similar age group [26]. Children's use of more extreme tactics suggests that they connect such extreme and unrealistic practices to harm that could befall them online. Therefore, children might fail to properly estimate the harm done by more latent strategies, exposing them to higher risks. Corresponding regulations must be formulated to limit the use of subtle but effective deceptive designs. Educators should also consider this a possible starting point for an appropriate and child-focused education plan. While many drawings matched existing deceptive patterns, the manipulative strategies used within this theme are not listed in the ontology. In fact, *Rational Persuasion* stands in direct contrast with the definition of deceptive patterns: While such patterns may influence users towards decisions that go against their own interest [19], *Rational Persuasion* allows for an informed decision based on given advantages and disadvantages. Nevertheless, its manipulative nature is incontestable, raising the question about the line between manipulation and persuasion.

Other tactics we identified in the drawings included designs impeding users from choosing the "Reject" option, e.g., by hiding or removing the button (C19, Figure 1), evoking trust, or pressuring users. Similar to how deceptive patterns appear in combinations in real mobile apps [7], we also found combinations of several strategies in the drawings.

[1] https://www.acm.org/code-of-ethics, *last accessed March 27, 2025*
[2] https://childethics.com/ethical-guidance/, *last accessed March 27, 2025*

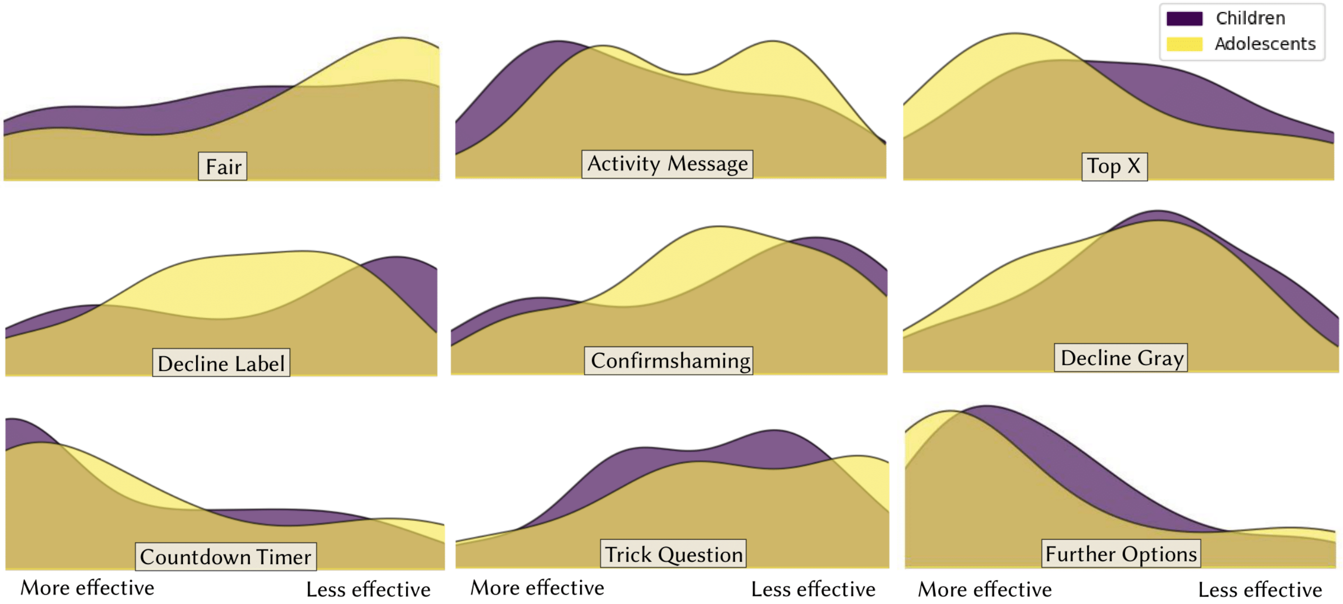


Figure 2: The rankings of all nine interfaces from task 2 (in the same order as in Figure 4) for both children (purple) and adolescents (yellow). Participants ranked interfaces based on whether they would make it more (left) or less (right) likely that users would invite their friends to the app. For example, adolescents considered a fair design as 'ineffective' more clearly than children. Both groups considered, e.g., *Countdown Timer* to be very effective at nudging users.

3.2 Ranking Deceptive Designs

To further strengthen our understanding of how children and adolescents assess deceptive patterns, we analyzed how they ranked our nine dialog designs based on how likely they would make users invite their friends to the app. Figure 2 shows the distribution of these ranks per design (Figure 4). For **children**, a Friedman test showed significant effects of the dialog on the ranking ($\chi^2(8)$=51.055, p<0.001). Wilcoxon signed-rank tests with Holm correction revealed significant effects between *Countdown Timer* and *Further Options* compared to most other dialogs. Both were perceived as significantly more effective than *Decline Gray* (p<0.05), *Confirmshaming* (p<0.01), *Decline Label* (p<0.01), and *Trick Question* (p<0.01). *Countdown Timer* was also ranked as significantly more effective than *Fair* (p<0.05). For **adolescents**, a Friedman test also showed significant effects ($\chi^2(8)$=45.638, p<0.001). Wilcoxon signed-rank tests with Holm correction revealed significant differences between the following dialogs: Adolescents ranked *Further Options* as significantly more effective than *Confirmshaming* (p<0.05) and *Trick Question* (p<0.01). *TopX* was ranked as significantly more effective than *Trick Question* (p<0.05), and *Decline Gray* was ranked as significantly more effective than *Fair* (p<0.05). Other differences were not significant (p>0.05). Overall, children and adolescents ranked *Countdown Timer* as most effective (24× and 12×). Both put *Further Options* on the second rank (12× and 11×), with adolescents also ranking it first 10 times. Children found *Fair* (12×) and *Decline Label* (11×) to be least effective, while adolescents opted for *Trick Question* (13×) and *Fair* (11×).

One interesting insight from this was how children and adolescents assessed manipulative formulations like *Confirmshaming*. While adolescents considered them funny, ineffective, provocative, and simplistic, children mainly viewed them as impolite. This may be because adolescents' higher self-esteem [4] meant that the attempted shaming affected them less than children. Another important difference between the age groups appears to be the perception of *Urgency*. Nearly all written justifications for *Countdown Timer* from children only addressed the potential reward one gains when inviting friends to the app. Only a single child addressed the time pressure of the timer. While several adolescents also mentioned the reward for *Countdown Timer*, many addressed the *Urgency* that it created, indicating they were more aware of this manipulation. This could also mean that children are particularly easy to influence with simple rewards, which matches the higher materialism found in their age group compared to older adolescents [4].

3.3 Limitations

One limiting factor of our study was the design of *Trick Question* and *Countdown Timer*: For *Trick Question*, many children and adolescents stated that they did not fully understand it. With this, the ranking of this particular dialog is likely more random than the others. Regarding *Countdown Timer*, participants addressed the reward that the dialog mentioned. Hence, *Countdown Timer* probably did not entirely fulfill its intended purpose of creating URGENCY. We did not expect children to overlook the timer and solely focus on the reward, which is an intriguing finding in itself. Lastly, all of our participants were from the same German school. Cultural differences for young people from other schools, countries, and social backgrounds could influence how they assess deceptive patterns and manipulation in general. Therefore, the generalizability of these findings to children and adolescents from different backgrounds needs further investigation. For example, it might be interesting whether they assess the *Countdown Timer* in combination with its reward in the same way as the participants in our study.

4 Conclusion and Future Work

As underage users frequently access the online world from an early age today [23], we wanted to better understand how they perceive, assess, and understand commonly used deceptive patterns and how this differs between children and adolescents. In our study at a German school, 45 children and 37 adolescents drew redesigns of fair interfaces to nudge users toward a specific decision. Then, they ranked nine different interfaces based on how likely they considered them to be able to influence users. Our results clearly show differences between the two groups: While children tended to be more drastic in their approaches to influence users, even including threats and punishments, adolescents applied more subtle and realistic strategies that closely resemble common deceptive patterns from the ontology by Gray et al. [12]. Both children and adolescents considered a *Countdown Timer* (Figure 4g) to be the most effective technique, but for different reasons. While children mainly explained their choice with the potential reward, adolescents frequently addressed the time pressure that the timer added, which was rarely mentioned by any of the children. Additionally, children disliked manipulative formulations (e.g., using CONFIRMSHAMING) for being impolite, while adolescents referred to them as being ineffective, provocative, or funny.

Future work should explore how the exposure to deceptive patterns from an early age impacts users, in order to inform new educational strategies and help designers and policymakers adapt design guidelines for more ethical interfaces. We hope that our work helps pave the way towards safeguarding children and adolescents from the adverse effects of deceptive designs in our increasingly digital world.

Acknowledgments

This work was funded in part by the German B-IT Foundation. We also want to thank the school, the teachers, and all participants for making this research possible.

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. https://doi.org/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. https://doi.org/10.1515/popets-2016-0038

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

[4] Lan Nguyen Chaplin and Deborah Roedder John. 2007. Growing up in a material world: Age differences in materialism in children and adolescents. *Journal of Consumer Research* 34, 4 (2007), 480–493. https://doi.org/10.1086/518546

[5] 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. https://doi.org/10.1145/3586183.3606783

[6] Gregory Conti and Edward Sobiesk. 2010. Malicious Interface Design: Exploiting the User. In *Proceedings of the 19th International Conference on World Wide Web* (Raleigh, North Carolina, USA) *(WWW '10)*. Association for Computing Machinery, New York, NY, USA, 271–280. https://doi.org/10.1145/1772690.1772719

[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. https://doi.org/10.1145/3313831.3376600

[8] Dan Fitton, Beth T Bell, and Janet C Read. 2021. Integrating Dark Patterns into the 4Cs of Online Risk in the Context of Young People and Mobile Gaming Apps. In *IFIP Conference on Human-Computer Interaction - INTERACT 2021*. Springer Nature Switzerland, Cham, Switzerland, 701–711. https://doi.org/10.1007/978-3-030-85610-6_40

[9] 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. https://doi.org/10.33621/jdsr.v3i1.54

[10] Colin M. Gray, Jingle Chen, Shruthi Sai Chivukula, and Liyang Qu. 2021. End User Accounts of Dark Patterns as Felt Manipulation. In *Proceedings of the ACM on Human-Computer Interaction*, Vol. 5. Association for Computing Machinery, New York, NY, USA, Article 372, 25 pages. https://doi.org/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. https://doi.org/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. https://doi.org/10.1145/3613904.3642436

[13] Shun Hidaka, Sota Kobuki, Mizuki Watanabe, and Katie Seaborn. 2023. Linguistic Dead-Ends and Alphabet Soup: Finding Dark Patterns in Japanese Apps. 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 3, 13 pages. https://doi.org/10.1145/3544548.3580942

[14] 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. https://doi.org/10.1145/3546155.3546656

[15] David R. Krathwohl. 2002. A Revision of Bloom's Taxonomy: An Overview. *Theory into Practice* 41, 4 (2002), 212–218. https://doi.org/10.1207/s15430421tip4104_2

[16] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2017. No Telling Passcodes Out Because They're Private: Understanding Children's Mental Models of Privacy and Security Online. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 64 (Dec 2017), 21 pages. https://doi.org/10.1145/3134699

[17] Francisco Lupiáñez-Villanueva, Alba Boluda, Francesco Bogliacino, Giovanni Liva, Lucie Lechardoy, and Teresa Rodríguez de las Heras Ballell. 2022. *Behavioural Study on Unfair Commercial Practices in the Digital Environment: Dark Patterns and Manipulative Personalisation.* Publications Office of the European Union, Luxembourg, Luxembourg. https://doi.org/10.2838/859030

[18] Ana Maria Marhan, Mihai Ioan Micle, Camelia Popa, and Georgeta Preda. 2012. A Review of Mental Models Research in Child-Computer Interaction. *Procedia-Social and Behavioral Sciences* 33 (2012), 368–372. https://doi.org/10.1016/j.sbspro.2012.01.145

[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. https://doi.org/10.1145/3359183

[20] Pekka Mertala. 2021. *Using Playful Methods To Understand Children's Digital Literacies.* Sage Publications Ltd, London, UK, 179–191.

[21] Samantha Punch. 2002. Research With Children: The Same or Different From Research With Adults? *Childhood* 9, 3 (2002), 321–341. https://doi.org/10.1177/0907568202009003005

[22] Karen Renaud, Cigdem Sengul, Kovila Coopamootoo, Bryan Clift, Jacqui Taylor, Mark Springett, and Ben Morrison. 2024. "We're Not That Gullible!" Revealing Dark Pattern Mental Models of 11-12-Year-Old Scottish Children. *ACM Transactions on Computer-Human Interaction* 31, 3, Article 33 (Aug 2024), 41 pages. https://doi.org/10.1145/3660342

[23] Bernhard Rohleder. 2022. Bitkom Kinder- und Jugendstudie 2022. Bitkom e.V., Berlin, Germany. https://www.bitkom.org/sites/main/files/2022-06/Bitkom-Charts_Kinder_Jugendliche_09.06.2022_0.pdf

[24] Lorena Sanchez Chamorro, Carine Lallemand, and Colin M. Gray. 2024. "My Mother Told Me These Things are Always Fake" - Understanding Teenagers' Experiences with Manipulative Designs. In *Proceedings of the 2024 ACM Designing Interactive Systems Conference* (Copenhagen, Denmark) *(DIS '24)*. Association for Computing Machinery, New York, NY, USA, 1469–1482. https://doi.org/10.1145/3643834.3660704

[25] 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. https://doi.org/10.1145/3603555.3603563

[26] René Schäfer, Sarah Sahabi, Annabell Brocker, and Jan Borchers. 2024. Growing Up With Dark Patterns: How Children Perceive Malicious User Interface Designs. In *Proceedings of the 13th Nordic Conference on Human-Computer Interaction* (Uppsala, Sweden) *(NordiCHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 25, 17 pages. https://doi.org/10.1145/3679318.3685358

[27] Carla Sousa and Ana Oliveira. 2023. The Dark Side of Fun: Understanding Dark Patterns and Literacy Needs in Early Childhood Mobile Gaming. *European Conference on Games Based Learning* 17, 1 (2023), 599–610. https://doi.org/10.34190/ecgbl.17.1.1656

[28] Patti M. Valkenburg and Jessica T. Piotrowski. 2017. *Plugged In: How Media Attract and Affect Youth.* Yale University Press, New Haven, Connecticut, USA. https://doi.org/10.12987/yale/9780300218879.001.0001

[29] 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 (HCII 2021)*, Fiona Fui-Hoon Nah and Keng Siau (Eds.). Springer International Publishing, Cham, 143–155. https://doi.org/10.1007/978-3-030-77750-0_10

[30] Claire M. White, Michaela Gummerum, and Yaniv Hanoch. 2015. Adolescents' and Young Adults' Online Risk Taking: The Role of Gist and Verbatim Representations. *Risk Analysis* 35, 8 (2015), 1407–1422. https://doi.org/10.1111/risa.12369

A Deceptive Patterns

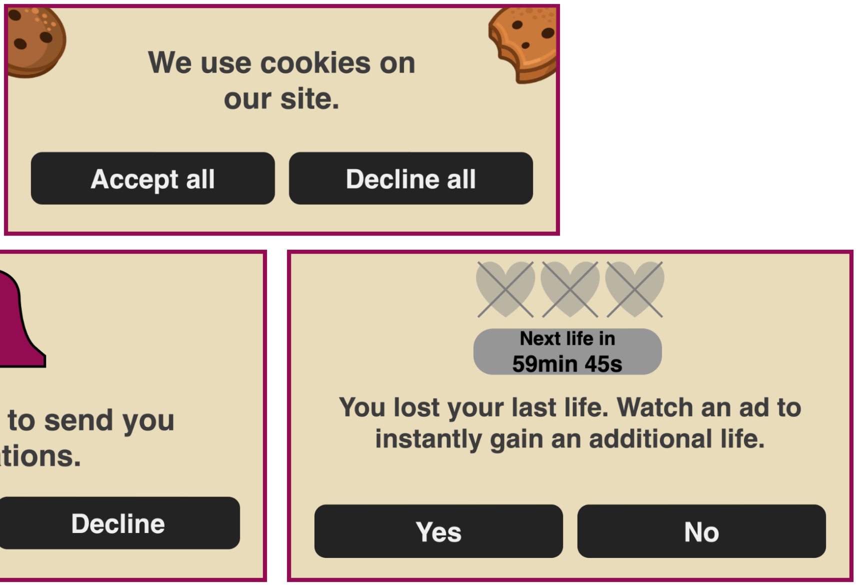
Table 1 contains relevant deceptive patterns for this paper with their definition from the ontology by Gray et al. [12].

Deceptive Pattern	Definition from Gray et al. [12]
Forced Action	"Forced Action is a strategy that requires users to knowingly or unknowingly perform an additional and/or tangential action or information to access (or continue to access) specific functionality, preventing them from continuing their interaction with a system without performing that action."
Interface Interference	"Interface Interference is a strategy which privileges specific actions over others through manipulation of the user interface, thereby confusing the user or limiting discoverability of relevant action possibilities."
Obstruction	"Obstruction is a strategy which impedes a user's task flow, making an interaction more difficult than it inherently needs to be, dissuading a user from taking an action."
Sneaking	"Sneaking is a strategy which hides, disguises, or delays the disclosure of important information that, if made available to users, would cause a user to unintentionally take an action they would likely object to."
Social Engineering	"Social Engineering is a strategy which presents options or information that causes a user to be more likely to perform a specific action based on their individual and/or social cognitive biases, thereby leveraging a user's desire to follow expected or imposed social norms."
Activity Message	"Activity Messages use Urgency as a type of Social Engineering to describe other user activity on the site or service, even though the data presented about other users' purchases, views, visits, or contributions are misleading or false. As a result, the user may falsely feel a sense of urgency, assuming that others users are purchasing or otherwise interested product or service, leading to their uninformed purchase of a product or service."
Confirmshaming	"Confirmshaming uses Personalization as a type of Social Engineering to frame a choice to opt-in or opt-out of a decision through emotional language or imagery that relies upon shame or guilt. As a result, the user may be convinced to change their goal due to the emotionally manipulative tactics, resulting in being steered away from making a choice that matched their initial goal."
Emotional or Sensory Manipulation	"Emotional or Sensory Manipulation subverts the user's expectation that the design of the site will allow them to achieve their goal without manipulation, instead altering the language, style, color, or other design elements to evoke an emotion or manipulate the senses in order to persuade the user into a particular action."
False Hierarchy	"False Hierarchy Manipulates the Choice Architecture, using Interface Interference to give one or more options visual or interactive prominence over others, particularly where items should be in parallel rather than hierarchical. As a result, the user may misunderstand or be unable to accurately compare their options, making a selection based on a false or incomplete choice architecture."
Hidden Information	"Hidden Information subverts the user's expectation that relevant information will be made accessible and visible, instead disguising relevant information or framing it as irrelevant."
Trick Question	"Trick Questions subvert the user's expectation that prompts will be written in a straightforward and intelligible manner, instead using confusing wording, double negatives, or otherwise leading language or interface cues to manipulate a user's choice."
Visual Prominence	"Visual Prominence Manipulates the Choice Architecture, using Interface Interference to place an element relevant to user goals in visual competition with a more distracting and prominent element. As a result, the user may forget about or be distracted from their original goal, even if that goal was their primary intent."

Table 1: Definitions for several deceptive patterns by Gray et al. [12]. The upper block contains the five high-level deceptive patterns, while the lower block contains meso- and low-level patterns.

B Study Materials

Figure 3 contains our fair designs for task 1 (Section 3.1) and Figure 4 shows our designs for task 2 (Section 3.2).

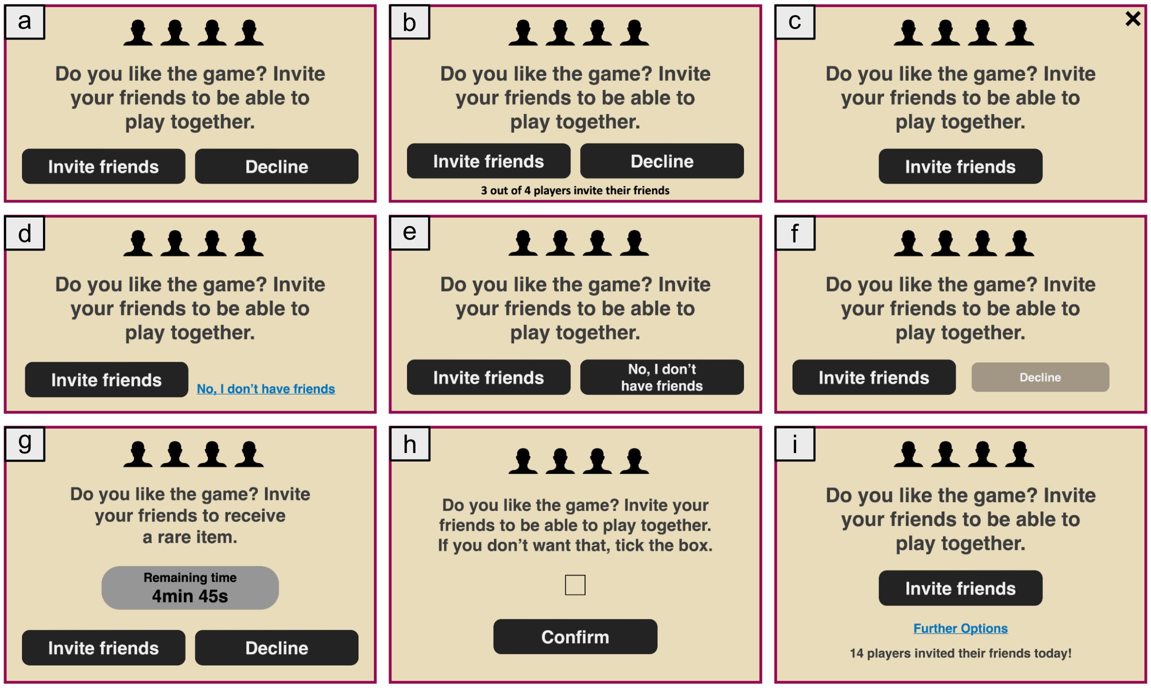


We use cookies on our site.

We would like to send you notifications.

You lost your last life. Watch an ad to instantly gain an additional life.

Figure 3: The three different fair designs that participants saw and redesigned in task 1 (Section 3.1) to make users accept cookies, notifications, or watching an ad.



Do you like the game? Invite your friends to be able to play together.

Do you like the game? Invite your friends to be able to play together.

3 out of 4 players invite their friends

Do you like the game? Invite your friends to be able to play together.

Do you like the game? Invite your friends to be able to play together.

Do you like the game? Invite your friends to be able to play together.

Do you like the game? Invite your friends to be able to play together.

Do you like the game? Invite your friends to receive a rare item.

Do you like the game? Invite your friends to be able to play together. If you don't want that, tick the box.

Do you like the game? Invite your friends to be able to play together.

14 players invited their friends today!

Figure 4: The nine dialogs participants ranked in task 2 (Section 3.2) based on how nudging they are: a) *Fair*, b) *Activity Message*, c) *TopX* (False Hierarchy), d) *Decline Label* (Confirmshaming + False Hierarchy), e) *Confirmshaming*, f) *Decline Gray* (False Hierarchy), g) *Countdown Timer*, h) *Trick Question*, i) *Further Options* (Hidden Information + False Hierarchy + Activity Message). Pattern definitions are listed in Table 1.

C Translated Drawings

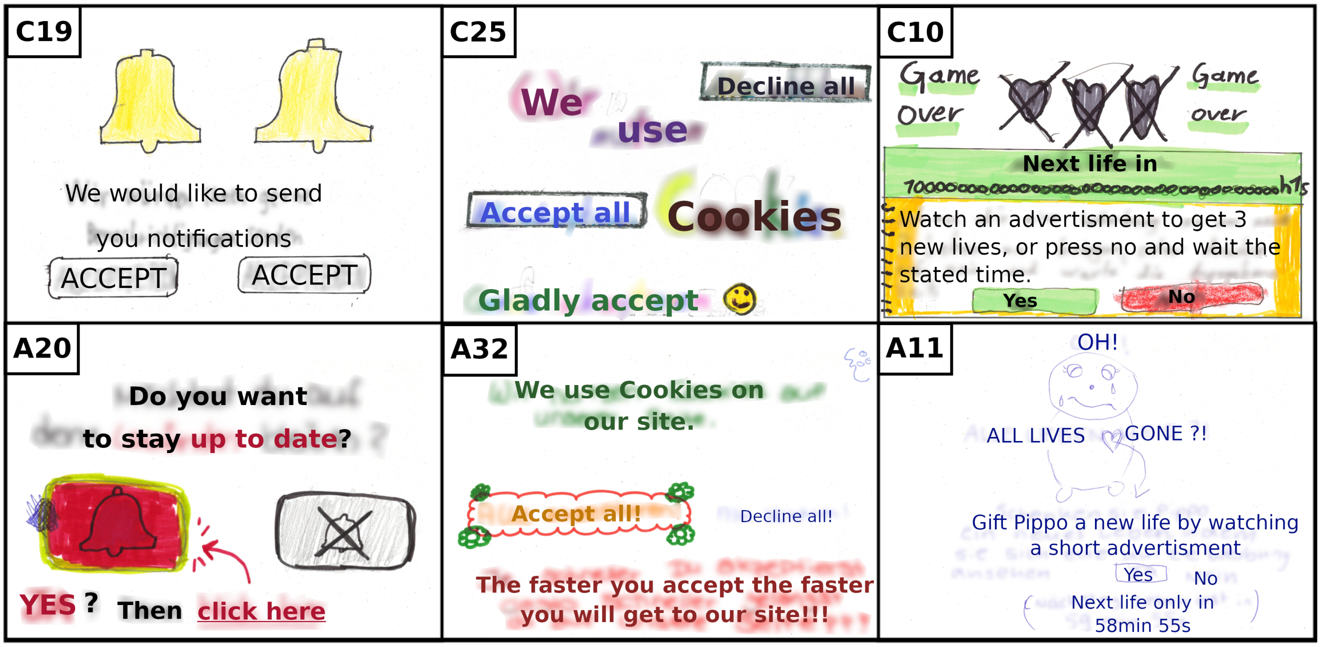


Figure 5: The translated drawings from Figure 1. The upper row contains images from children, while the lower row contains drawings from adolescents.