From Awareness to Action: The Effects of Experiential Learning on Educating Users about Dark Patterns

Jingzhou Ye
Computer and Information Science
The University of Central Florida
Orlando, Florida, USA
jingzhou.ye@ucf.edu

Yao Li
University of Central Florida
Orlando, Florida, USA
yao.li@ucf.edu

Wenting Zou
Education Psychology
The Pennsylvania State University
State college, Pennsylvania, USA
wpz5135@psu.edu

Xueqiang Wang
University of Central Florida
Orlando, Florida, USA
xueqiang.wang@ucf.edu

Abstract

Dark patterns (DPs) refer to unethical user interface designs that deceive users into making unintended decisions, compromising their privacy, safety, financial security, and more. Prior research has mainly focused on defining and classifying DPs, as well as assessing their impact on users, while legislative and technical efforts to mitigate them remain limited. Consequently, users are still exposed to DP risks, making it urgent to educate them on avoiding these harms. However, there has been little focus on developing educational interventions for DP awareness. This study addresses this gap by introducing DPTrek, an experiential learning (EL) platform that educates users through simulated real-world DP cases. Both qualitative and quantitative evaluations show the effectiveness of DPTrek in helping users identify and manage DPs. The study also offers insights for future DP education and research, highlighting challenges such as user-unfriendly taxonomies and the lack of practical mitigation solutions.

CCS Concepts

• **Security and privacy** → *Social aspects of security and privacy*; • **Social and professional topics** → **Computing education**.

Keywords

dark pattern, experiential learning, security, privacy

ACM Reference Format:
Jingzhou Ye, Yao Li, Wenting Zou, and Xueqiang Wang. 2025. From Awareness to Action: The Effects of Experiential Learning on Educating Users about Dark Patterns. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26–May 01, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 22 pages. https://doi.org/10.1145/3706598.3713493

1 Introduction

In 2010, Harry Brignull coined the term "dark pattern" (DP) [18] to describe a wide range of unethical user interface (UI) designs that deceive users into making unintended and potentially harmful decisions, ultimately benefiting online businesses. Typical DPs include online shopping websites that stealthily add unwanted items to a user's shopping cart, leading to unintentional purchases and financial losses [20], and websites that aggressively track users by making the cookie opt-out process deliberately complex and frustrating [22]. Recent years, DPs have drawn significant attention within the Human-Computer Interaction (HCI) research [26, 47, 59, 60, 85, 86, 92], with a focus on developing comprehensive taxonomies to classify various categories of DPs and empirically studying their manipulation on users. Current efforts to regulate DPs in real-world software and websites focus only on specific aspects, such as DPs that clearly involves deception (e.g., those regulated by the FTC Act [14]) and DPs in children-related advertisements (e.g., reviewed by CARU [109]). While a few studies have attempted to mitigate DPs by rewriting UIs [42, 43, 73], the proposed solutions have not been widely adopted in real-world settings due to deployment challenges [42, 43].

Therefore, the widespread prevalence of DPs is likely to continue exposing online users to harms. Even worse, knowledge about DPs remains largely confined to research communities, and online users struggle to identify their exposure to DPs, let alone confidently avoid its potential harms. So far, there has been limited attention to developing and evaluating educational interventions that effectively teach users about DPs, such as its characteristics, harms, and ways to identify and cope with them. To address this gap, our study investigates the design and effectiveness of user education on DPs through a new learning platform called DPTrek. The key feature of DPTrek is its use of experiential learning (EL) [72] to provide users with concrete experiences related to DPs – the first attempt of its kind. Specifically, we built simulated DP cases by replicating DP instances reported in the real-world [4, 18, 60], which cover all five DP categories as described in widely used DP taxonomies [60], such as *Nagging*, *Obstruction*, and *Sneaking*. Based on the simulated DP cases, DPTrek educates users about each DP category through a four-phase module, *Experience-Reflection-Learning-Experiment*, corresponding to the major phases of the EL learning model.

CHI '25, Yokohama, Japan

ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3713493

To evaluate DPTrek, we recruited 38 participants and performed a controlled experiment, dividing participants into the treatment group, which learns about DPs through DPTrek, and the control group, which learns through *Web-based Static Content Learning*. We perform a series of post-intervention evaluations on participants' capabilities to identify and avoid DPs, their knowledge about DPs, and their subjective learning experiences (quantitatively and qualitatively). The evaluation results are encouraging. DPTrek enhances users' abilities to identify and cope with DPs, as well as their understanding of the associated consequences. Participants found DPTrek enjoyable and aesthetically appealing. Additionally, participants appreciated the use of real DP cases in DPTrek in the interviews. However, our evaluation also reveals several issues in DP education, such as practical challenges in coping with DPs and difficulties in identifying the categories of DPs. We discuss these issues and explore the implications of our research for both DP education and broader cybersecurity education. We released a website with detailed information about the DPTrek design at https://dptrek.github.io/dptrek/.

Our study contributes by making the first attempt to educate users about DPs with concrete experiences through EL, which informs the design of EL-based educational approaches in the field of HCI and cybersecurity. It also provides valuable insights and advances understanding of issues and gaps in current DP research. Particularly, it highlights the limitations of the existing DP taxonomies that prevent broad end-user awareness and identifies the lack of effective tools for mitigating DPs, which are important for guiding future research in this domain.

2 Related Work

2.1 Dark Patterns

Recent studies have investigated DPs from multiple research perspectives. For instance, a number of studies analyzed DP instances reported by practitioners, developed definitions, types, and taxonomies of these patterns, and evaluated their consequences in both general settings [60, 82, 83, 86] and specific contexts such as online games [124] and privacy features offered by software or IT systems [15]. These studies contributed to a better understanding of DPs within the research community, yet the resulting taxonomies are often not designed with end users in mind.

From a regulatory perspective, policymakers and regulators, such as the FTC [1], enforce consumer- and privacy-focused laws and regulations[14, 29, 45, 46, 80, 119] to combat DPs, particularly those that lead to deception or privacy violations [30–32, 51, 95]. Also, self-regulatory organizations, such as the Children's Advertising Review Unit (CARU), have established guidelines for online businesses to self-regulate dark patterns involved in advertising targeting children [109]. These regulatory efforts are designed to address DP instances that clearly involve deception or privacy violations. At the same time, as reported by the FTC workshop on "*Bringing Dark Patterns to Light*" [52], even such efforts are constrained by the limited resources available to regulators for investigation. Consequently, a significant portion of DPs that involves manipulative practices remains uncovered.

Further, to measure the prevalence of DPs in the wild, prior research developed methods for automatically detecting DPs through UI analysis using techniques such as computer vision and natural language processing [25, 26, 49, 81, 84, 85], empirical content analysis [47, 59, 89, 92], and user-based studies [47, 88, 105]. For example, Mathur et al. [85] crawled 11,000 shopping websites and detected those using DPs by clustering and inspecting textual UI elements. Similarly, Moser et al. [92] analyzed 200 shopping websites by examining the content hosted on the websites. Radesky et al. [105] reported the prevalence of DPs in child-directed apps by analyzing children's usage data from mobile applications. However, many of these studies face technical or scalability challenges, such as being unable to detect DPs spanning multiple UIs (as reported in [84]), or requiring an unaffordable amount of manual effort to review the UIs. In addition to detection, several studies went further into mitigating DPs by rewriting (or modifying) UIs [42, 43, 73], or highlighting suspicious patterns to end users [25]. These solutions have not been widely adopted in real-world settings due to deployment challenges, such as high implementation workload, scalability concerns, robustness issues, and the risk of voiding software warranties [42, 43].

In fact, the communities have recognized the importance of educating end users for minimizing the harms of DPs [52]. However, aside from online websites [18] and social media accounts [17] that expose websites or software involved in DPs to the public, and a few studies that highlight potential DPs to users [25], there has been a lack of research on developing effective DP education for end users.

2.2 Cybersecurity Education

In this section, we review cybersecurity education literature to examine whether existing cybersecurity education approaches can inspire DP education, as DPs are closely related to cybersecurity.

Cybersecurity education plays a crucial role in safeguarding users from cyber threats, encompassing a broad range of topics including cryptography, authentication, secure programming, privacy, misinformation, and phishing [37, 116]. One major effort is the formal cybersecurity education, such as coursework, seminars and certification programs, which are mostly instructor-led in structured settings, providing foundational cybersecurity knowledge to nurture future cybersecurity workforce [34, 58, 103, 104, 118]. Existing research on formal cybersecurity education has focused on pedagogical approaches, curriculum design, and the evaluation of student learning outcomes [116]. For instance, Jones et al. interviewed cyber professionals to rate the importance of cybersecurity knowledge, skills, and abilities based on the National Initiative for Cybersecurity Education (NICE) Framework [94], and recommended cybersecurity curricula [69]. Organizational research has proposed various workplace cybersecurity trainings to increase employees' awareness and compliance with information security policies [5, 9, 56, 64, 71]. Though formal cybersecurity education are vital, their influence often remains within the boundaries of their home institutions [110], hindering broader impact beyond formal settings.

Informal cybersecurity learning, which happens outside formal settings, offers users a flexible, accessible way to cybersecurity education [40, 103]. Users can learn in everyday lives [40, 122], making it a valuable alternative channel for promoting cybersecurity knowledge. For instance, Fact-and-Advice delivers cybersecurity knowledge in text [120], graphic [74], or video format [8, 41] through webpages, news, and social media [93, 103, 107]. Storytelling uses plots and narratives to share stories of cybersecurity incidents and to resonate with listeners, promoting social influence among people [39, 54, 66, 99, 104]. Cybersecurity games gamify cybersecurity education via role-playing simulation [10, 33, 121], tabletop card games [13, 44, 57, 63, 114], capture-the-flag [27, 79, 98], and adventure games [48]. Research has shown that these informal methods significantly improve users' ability to combat cybersecurity threats, while providing more accessible and flexible cybersecurity education to the public [11, 63, 74, 98, 120, 121].

While both formal and informal methods have achieved considerable success in cybersecurity education, neither have specifically addressed the education of users about DPs. DPs affect a diverse range of users during their everyday interactions with websites, suggesting that informal methods might better enhance the accessibility and flexibility of education. However, existing informal cybersecurity education methods often fall short in providing first-hand experience. For instance, "Fact-and-Advice" methods lack relevance to learners' personal experiences [120]. Storytelling, which shares others' experiences, does not involve direct participation or emotional engagement from learners. While gamified cybersecurity education allows learners to experience cyber threats and gain knowledge first-hand, it structures real-world experiences into game-like activities with defined rules, objectives, and outcomes [10, 33, 121]. This structured approach differs from the unstructured nature of real-world experiences. Additionally, gamified education often lacks support for reflection, a crucial component for internalizing lessons, understanding personal growth, and making improvements [72]. As DPs are deceptive, complex and not transparent, sometimes resulting in immediate benefits to users in exchange for long-term privacy and security risks, learning through experience, namely Experiential Learning [72], will allow learners to accelerate the whole process of DPs to experience the harmful consequences. Additionally, EL enables learning through a cycle of experience, reflection, and experiment [72], which supports first-hand engagement to reinforce cybersecurity practices.

2.3 Experiential Learning

Experiential learning (EL) is a learning model in which learners gain knowledge through concrete experiences combined with critical reflection on those experiences [72]. This model encompasses four essential components: *concrete experience*, *reflective observation*, *abstract conceptualization*, and *active experimentation* [72]. These components form a cyclical process, with each stage feeding into the next, and the cycle can be entered from any stage. Typically, most applications begin with concrete experience. In contrast to traditional learning methods that rely on lectures and repetition, EL integrates both conceptual and practical knowledge, applying it to real-world situations [72]. A common example of EL is an internship, where students apply theoretical knowledge gained in the classroom to practical work settings within a company [70, 111, 115]. During internships, students engage in specific job tasks to gain concrete, hands-on experience and reflect on their experiences through documentation and mentoring meetings. They learn from mentors, who are professionals in the field, helping them bridge the gap between academic concepts and practical application. Through reflection and conceptual learning, students gain new insights and experiment with these insights in subsequent tasks. As they encounter new challenges, this iterative EL process deepens their understanding of the knowledge acquired and enhances their ability to apply it effectively in real-world scenarios. EL is most effective when learners need to acquire practical skills and actively apply them to solve complex real-world problems [87, 91]. As real-world problems are often context-specific and ill-structured, EL provides learners with direct, personal encounters that help them understand the context and develop problem-solving skills [12, 91]. EL has been widely applied in domains that emphasize real-world problem-solving, such as entrepreneurship [87], public administration [12], and HCI [50, 67], and demonstrated its effectiveness [91]. For example, Ibrahim et al. [67] utilized EL to investigate how pregnant individuals with Gestational Diabetes Mellitus learn lifestyle management strategies. They found that EL was beneficial in helping these individuals gain a sense of control over their condition. El-Glaly et al. [50] applied EL to teach computer science students about creating accessible software and found it effective in raising awareness about the importance of accessibility and educating students on foundational accessibility topics.

While EL has seen extensive application in various domains, its use in cybersecurity education remains limited. To our best knowledge, only a few studies have explored EL within digital literacy training. For example, Pretorius et al. [100] effectively employed EL to teach college students how to assess the reliability of information sources. Similarly, Zou et al. [126] applied EL to enhance social media literacy. Their study demonstrated that EL led to higher engagement and improved learning outcomes among youth learners [100, 126]. Despite these promising results in applying EL to digital literacy education, the understanding of its application in cybersecurity education – particularly in the context of DP education – is still limited. DP education emphasizes real-world problem solving for addressing DPs, which aligns with the core focus of EL. Second, DPs are highly context-specific, with their design, layout, and functionality varying across different environments. EL enables learners to recognize and address various DPs in realistic, contextually rich scenarios. Third, the consequences of DPs are often dangerous, ambiguous, and ill-structured. EL offers a safe environment for learners to explore and understand these consequences while developing the critical thinking and problem-solving skills required to navigate them effectively. These factors motivate us to design an EL-based platform specifically for DP education.

3 Methods

3.1 DP Experiential Learning Platform: DPTrek

Recognizing the potential of EL to engage learners and enhance understanding by connecting abstract concepts to hands-on practice, we developed DPTrek, an EL platform that simulates real-world DP cases to teach online users about the concepts and consequences of DPs, and ways to cope with it.

Five modules of DPTrek. DPTrek contains five modules corresponding to five DP categories as classified in Gray et al. [60]. Specifically, (1) *Nagging*: persistently reminding users to take an action, often in an annoying and coercive manner. (2) *Obstruction*: deliberately making a process more difficult than necessary to discourage or prevent specific actions. (3) *Sneaking*: hiding, disguising, or postponing the revelation of information important to the users. (4) *Interface Interference*: manipulating UIs to prioritize specific actions over others. (5) *Forced Action*: requiring the user to complete a specific action to gain or maintain access to certain functionality.

Four simulated DP cases for each module. We gathered four real-world DP cases reported in prior efforts, including Gray et al. [60], the companion website [4], and Brignull's website [18]. These cases are used in different phases of the study: two are used in DPTrek for users to experience and experiment with DPs, and two are used in the test. Each case is accompanied by options for successfully avoiding harms of the case, such as rejecting, leaving the website, or reporting it. In Table 7, we present the descriptions of the DP cases, their sources, the phases of the study in which they are used, their consequence and strategies. Based on the collected real-world DP cases from prior efforts, we created the web-based simulations of the DP cases through a semi-automated process using large language models. Specifically, we used the descriptions of the reported real-world DP cases (as shown in Table 7 in Appendix A) as input and requested ChatGPT [97] to generate web code that mimics the interfaces described. We adjusted the code to ensure it was both functional and visually appealing to end users.

Four phases in each module. To guide learners through EL, each module of DPTrek is structured into four phases: 1) *Experience* phase, which corresponds to the *concrete experience* in Kolb's Experiential Learning (EL) cycle that learners engage with new information through tangible, immersive experiences [72]. In this phase, learners are presented with a simulated DP case and navigate it freely, while simultaneously protecting their interests. If they fall into the DP case, they experience simulated consequences that illustrate the harms of such cases, such as targeted advertisements and financial loss, based on prior studies [4, 45, 60]. 2) *Reflection* phase, which aligns with *reflective observation* in Kolb's EL cycle. Here, learners reflect on their experiences in the DP case, including their observations, feelings, and the frequency of similar encounters in everyday life [72]. 3) *Learning* phase, which pertains to *abstract conceptualization* in Kolb's EL cycle. In this phase, learners are introduced to concepts of DPs, descriptions of previously reported DP cases through text and graphics, and suggestions for navigating them – similar to the Web-based Static Content Learning education used in Zielinska et al. [72, 125]. 4) *Experiment* phase, which involves *active experimentation* in Kolb's EL cycle. Learners are presented with a different simulated DP case, along with feedback on their actions (e.g., whether their strategies effectively mitigate the adverse impacts of the DP case). If they fail to manage the DP case effectively, they will see the simulated consequences. Figure 1 shows the screenshot of DPTrek in the experience phase of *Forced Action.* We have also released a website with detailed information about the DPTrek design at https://dptrek.github.io/dptrek/.

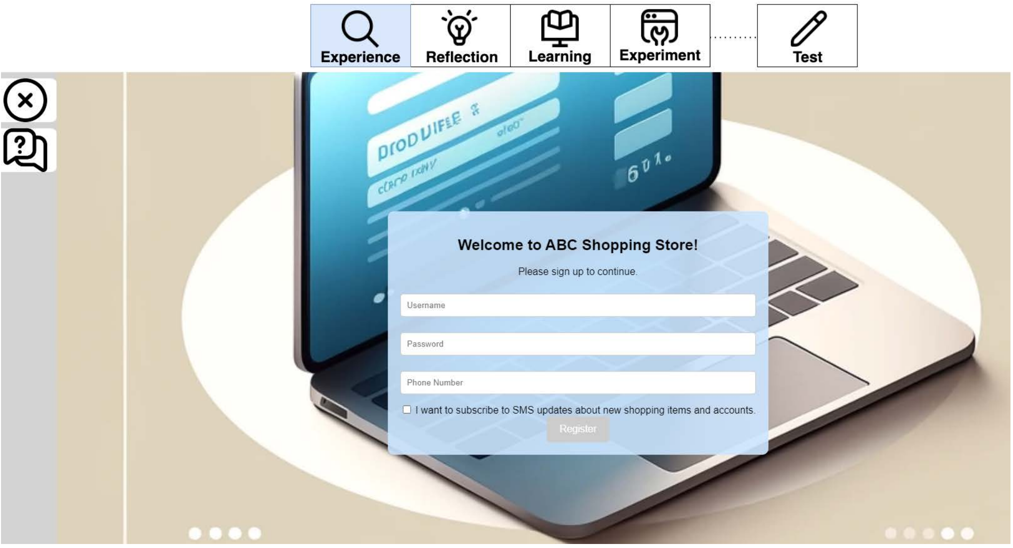
Four phases in each module. We implemented DPTrek on webpages. Before the full-scale evaluation, we conducted 6 one-on-one pilot sessions with education experts and learners to gather feedback and improve DPTrek. These 6 pilot sessions involved two education experts (one education researcher and one educator) and four learners (students from our institution), whom were recruited through our personal networks. The pilot sessions were conducted via Zoom. In the pilot sessions, the experts and learners were asked to navigate through our DPTrek prototype and provide feedback. After we improved DPTrek based on the feedback from the pilot sessions, we hosted follow-up meetings with the experts and learners to reassess the improvements made to DPTrek. In total, 6 pilot sessions and 8 follow-up meetings were conducted, with two participants attending follow-up meetings twice. The implementation and iterative improvement process took approximately 3.5 months. The participants in the pilot sessions were not invited to the official study. The data collected in the pilot sessions were not included the data analysis.

3.2 Study Procedure

We conducted a controlled experiment to examine the causal effect of DPTrek on educating users about DPs. Figure 2 shows the design overview.

3.2.1 Recruitment and Screening. We recruited participants in the U.S., targeting Internet users aged 18 years or older. Recruitment information was disseminated through social media platforms (Facebook, Twitter, and Reddit), institutional mailing lists, flyers posted on campus, and participant referrals. In total, 38 participants were recruited, with 36 from our institution and 2 from social media. Interested participants first completed a screening survey, which was administered via Qualtrics [2]. This survey began with a consent form and eligibility questions. The survey also included demographic questions, such as gender, level of education, and major. Additionally, we inquired whether participants had heard of DPs and the frequency of cybersecurity training they had received in the past year. These questions were included to ensure a diverse participant sample. Finally, we collected potential participants' email addresses for the purpose of contacting them and scheduling the study. After participants completed the screening survey, we sent email invitations to those who met the eligibility criteria and scheduled the study based on their availability. In total, we recruited 38 participants and conducted 38 individual sessions. Table 8 in Appendix A provides a detailed overview of the demographics of the participants. Each participant was compensated with a $20 Amazon gift card for completing the study.

3.2.2 Learning through DPTrek versus Web-based Static Content Learning. The 38 participants were randomly assigned to either the treatment or control group. 19 participants were assigned to the treatment group, where they used the DPTrek. The remaining 19 participants were assigned to the control group, where they received web-based static content learning on DPs, which provides information through text and images in a manner similar to the "Fact-and-Advice" approach used in prior cybersecurity education [120]. Both DPTrek and web-based static content are implemented



Welcome to ABC Shopping Store!

Please sign up to continue.

Username

Password

Phone Number

□ I want to subscribe to SMS updates about new shopping items and accounts.

Figure 1: A screenshot of the EL-based DPTrek. DPTrek features a four-phase learning experience – *Experience, Reflection, Learning,* and *Experiment* – corresponding to the *concrete experience, reflective observation, abstract conceptualization,* and *active experimentation* components of the EL model.

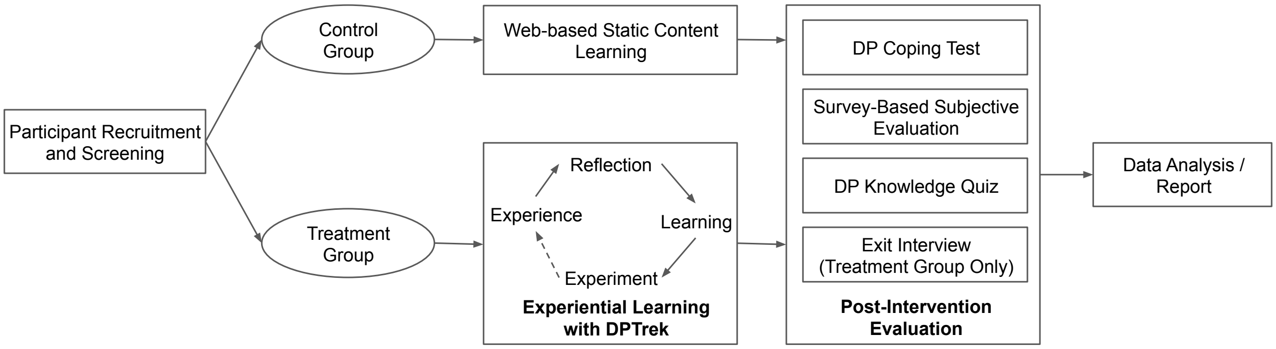

Participant Recruitment and Screening
Control Group
Treatment Group
Web-based Static Content Learning
Reflection
Experience
Learning
Experiment
Experiential Learning with DPTrek
DP Coping Test
Survey-Based Subjective Evaluation
DP Knowledge Quiz
Exit Interview (Treatment Group Only)
Post-Intervention Evaluation
Data Analysis / Report

Figure 2: Overview of the study design

on web pages. Web-based static content was identical to the materials used in the "Learning" phase of DPTrek, ensuring that both groups received the same educational content. The key difference was the absence of "experience, reflection, experiment" phases that embody the core principles of experiential learning.

The study was conducted via Zoom. Upon joining the session, we welcomed the participants, introduced ourselves, and explained the procedure, emphasizing that they should behave as they would in their normal life and focus on protecting their private information. We then provided the participants with the link to their assigned DP education. Participants opened the link in their browsers and began screen-sharing. We recorded the entire session using Zoom's recording feature.

In the learning phase, we collected participants' actions on all web pages through web logging, including button clicks, timestamps of actions, and page entry and exit events. These logs were temporarily stored in the local storage of the web pages. Upon completion of the study, participants submitted their data by pressing the "Submit" button, which triggered the conversion of log data into JSON format and its upload to the authors' cloud storage on AWS S3 [112]. To prevent accidental data contamination, we restricted the AWS S3 web page capabilities to write-only and generated pseudo-random file names for the uploaded JSON files. Using these logs, we evaluated participants' success or failure in handling each DP case in the treatment group. Success was defined as participants taking actions to protect their interests, such as avoiding manipulation, leaving the page, or reporting simulated DP cases. For instance, a participant successfully avoided the consequences of a DP by unchecking the default "Enable personalized ads" checkbox, which exemplifies *Interface Interference.* Additionally, we collected participants' responses during the reflection phase, including their observations, feelings, and the frequency of similar encounters in everyday life. No DP success or failure data was collected for the control group, as they did not experience DPs during the learning phase.

3.2.3 Post-Intervention Evaluation. After the participants completed their assigned DP education, we conducted a series of post-intervention evaluations, including a DP coping test, a DP knowledge quiz, a survey-based subjective evaluation, and an exit interview. The DP coping test, DP knowledge quiz, and survey-based subjective evaluation were implemented on web pages following the DP learning website, with instructions directing participants to each. The exit interviews were conducted orally via Zoom.

DP coping test. After participants completed each DPTREK module (corresponding to a specific category of DPs), they were presented with two new simulated DP cases to assess their learning outcomes in coping with DPs. A detailed description of these cases is provided in Table 7 in the Appendix. Participants navigated through the two cases without any guidance. Similar with the learning phase, we logged participants' actions on the DP testing cases. Based on the web logged actions, we recorded whether they successfully coped with each DP (i.e., success or failure) and summed the total number of successes per DP type per participant.

DP knowledge quiz. To evaluate participants' mastery of DP concepts, we developed an online quiz. This assessment aims to measure participants' understanding of DP categories and their consequences through a series of multiple-choice questions. Each question presents a scenario or concept, with only one correct answer among the options provided. The quiz (in Appendix B) challenges participants to classify various DP categories and identify appropriate consequences for given DP cases, reflecting the key learning objectives of our educational intervention. Participants' answers to the quiz were logged. We compared their answers with the correct answers, and recorded correct and incorrect answers per participant.

Survey-based subjective evaluation. In addition to objective evaluation using the DP knowledge quiz, we asked participants to report their subjective learning experience with the assigned DP education intervention. Most cybersecurity education studies have measured constructs such as enjoyment [66, 113, 121], confidence [66, 113], perceived usability [8, 55, 65], aesthetic appeal [65, 96, 106], and perceived reward [55, 65, 106] to evaluate learners' subjective experiences with educational interventions. Based on these precedents, we included these measurements in our survey. Additionally, inspired by the Theory of Planned Behavior [7], we aimed to assess whether DPTREK influences learners' attitudes toward DPs and DP coping, as well as their future behavioral intentions. To this end, we also included attitudes toward coping with DPs, perceived risks of DPs, and future behavioral intention to engage in DP training. The specific constructs are: 1) *Enjoyment*: the extent to which taking the assigned DP education is perceived to bring pleasure and fulfillment, which was measured by 4 items from [6, 66]. 2) *Confidence*: the learners' belief that they can effectively deal with DPs in the future, measured by 3 items from [66]. 3) *Perceived usability*: the frustration or difficulties encountered during the interaction with the assigned DP education, which was adapted from [6, 65]. 4) *Aesthetic appeal*: the attractiveness and appeal of the user interface of the assigned DP education, which was adapted from [65]. 5) *Reward*: the interaction being perceived as worthwhile and interesting [65]. 6) *Attitude of coping with DPs*: the overall evaluation of attitudes towards coping with DPs, which was adapted from [7]. 7) *Risks of DPs*: the perceived uncertainty resulting from the DPs, measured by 4 items from [123] 8) *Future behavioral intention*: the intent to engage with the assigned DP education again in the future, which adapted 3 items from [6]. All items were measured using 5-point Likert scales, ranging from *strongly disagree* to *strongly agree*. A detailed list of the questions can be found in Table 9 in Appendix A.

Exit interview. We interviewed participants in the treatment group to gather their qualitative evaluations and feedback on DPTREK. We sought participants' evaluations and suggestions regarding DPTREK. This included their overall impressions of DPTREK, perceived benefits, the knowledge and strategies they gained, any difficulties or dissatisfaction they experienced, suggestions for improvement, and feedback on the DP categories and definitions. The full list of interview questions is listed in Table 10 in Appendix A.

3.2.4 Ethical Consideration. Certain DPs in our study required participants to enter sensitive information, such as passwords and phone numbers. To address potential privacy and ethical concerns, we took several measures. First, participants were informed prior to the study that providing such information was entirely optional and would not affect their participation or compensation. During the study, password inputs were masked during entry, ensuring they were not visible to researchers or included in the recordings. Additionally, the passwords and phone numbers entered during interactions with DPs were neither logged nor stored. To further protect participant privacy, raw data, such as Zoom recordings and web logs, were deleted after data anonymization.

3.3 Data Analysis

Since both quantitative and qualitative data were collected in the study, we performed both quantitative and qualitative data analyses. The specific data used for each analysis and their corresponding collection phases and analysis methods are summarized in Table 1.

3.3.1 Quantitative Data Analysis. To compare the effectiveness of the assigned DP education between treatment and control groups, we performed Mann-Whitney U Test [35], as our samples are not normally distributed, the sample sizes are small, the outcome variables are ordinal or continuous and the two groups are independent. To compare the learning outcomes before and after EL within the treatment group, we performed Wilcoxon signed-rank tests [35], as the before and after responses are repeated measures and our samples are not normally distributed. All the tests were conducted in R [102]. Since the constructs in the survey-based subjective evaluation were measured using multiple items, we computed Cronbach's Alpha [38] for each construct to verify its reliability. Once reliability was confirmed, we calculated the mean score for each construct for each participant to represent the overall level of that construct.

3.3.2 Qualitative Data Analysis. We first transcribed the interview recordings into text and anonymized any identifiable information about the interviewees. We then conducted a thematic analysis [16] to analyze the interview data. To begin, we read through all

Table 1: Data collected during the study

Data Type	Data Collected	Data Collection Phase	Group	Data Analysis
Quantitative	Success/Failure on DPs	Experience	Treatment	Wilcoxon signed-rank test for before-after comparison
	Success/Failure on DPs	Experiment	Treatment	
	# success on DPs	DP Coping Test	Both	Mann-Whitney U for between-group comparison
	Correct/Incorrect answers	DP Knowledge Quiz	Both	
	5-point Likert ratings	Survey-based Subjective Evaluation	Both	
Qualitative	Interview Recordings	Exit Interview	Treatment	Thematic Analysis for qualitative feedback

the transcripts to familiarize ourselves with the data and independently noted initial codes related to the interviewees' perceptions, attitudes, and opinions regarding DPTrek. These codes serve as meaningful labels attached to specific segments of the interview data. Next, we compared our initial codes, moving back and forth between the codes and the original data. Through multiple meetings, we discussed our interpretations of each code and refined and revised them, until we each had agreement on all codes. Afterward, we collated similar codes into larger, meaningful patterns by examining the codes, the associated data, and the relationships between the codes. We further grouped these patterns into overarching themes by identifying the relationships between them. This process resulted in a thematic map consisting of themes, sub-themes, and codes. With the initial thematic map developed, we reviewed and refined it by checking whether the themes and sub-themes accurately captured the meanings in the coded data segments and formed a coherent pattern. Four authors were involved in the analysis.

4 Quantitative Results

4.1 Comparison Between Treatment and Control

To evaluate the effectiveness of DPTrek, we conducted Mann-Whitney U Test [3] to compare the results of the DP coping test, DP knowledge quiz, and survey-based subjective evaluations between the treatment and control groups. In the following subsections, we will present the comparison results accordingly.

4.1.1 DP Coping Test. The accuracy of the DP coping test is significantly higher in the treatment group compared to the control group. This trend is observed not only in the overall accuracy comparison between the two groups, but also across each DP category. As shown in Figure 3, the treatment group that completed DPTrek achieved better accuracy in both the overall DP coping test and for each DP category than the control group, which did not use DPTrek. These between-group differences were further tested using Mann-Whitney U Test, as outlined in Table 2, with all p-values less than 0.05, indicating statistical significance. This demonstrates that DPTrek is effective in improving participants' ability to identify and cope with DPs.

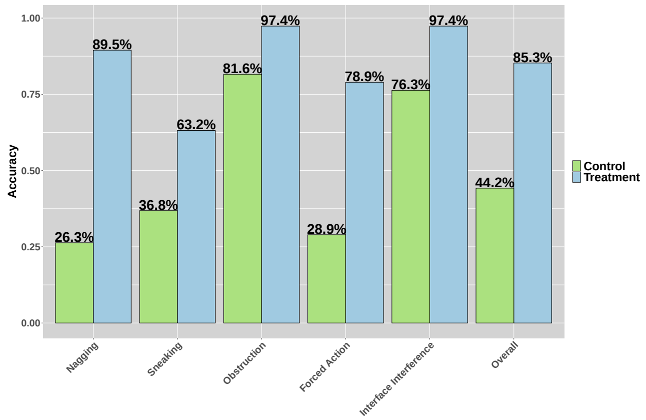


Figure 3: DP coping test accuracy

Table 2: Mann-Whitney U Test results: Comparison of DP coping test scores by treatment and control groups

	Test Statistic	P-value	Significance
Nagging	311.0	0.000	Significant
Sneaking	245.5	0.046	Significant
Obstruction	228.5	0.039	Significant
Interface Interference	247.5	0.009	Significant
Forced Action	287.0	0.001	Significant
Overall	324.5	0.000	Significant

4.1.2 DP Knowledge Quiz. While the overall accuracy in the DP knowledge quiz does not significantly differ between the treatment and control groups, we found that the treatment group performed better in the quiz questions related to identifying DP consequences. Figures 4, 5, and Table 3 present the comparison of results between the two groups. In Figure 4, the accuracy for DP consequence questions is higher in the treatment group (87.4%) compared to the control group (73.7%), a difference that is statistically significant (Test Statistic = 250.0, P-value = 0.031 < 0.05), as confirmed by the Mann-Whitney U Test (Table 3).

However, the overall accuracy in the DP knowledge quiz, which increases from 60.5% to 65.8% between the control and treatment groups, is not statistically significant. The accuracy for DP category questions is higher in the control group, but this difference is also not statistically significant according to the Mann-Whitney U Test (Table 3).

When broken down by each DP category, the accuracy of the DP knowledge quiz is generally higher in the treatment group, as shown in Figure 5. Nonetheless, these differences are not statistically significant based on the results from the Mann-Whitney U Test (Table 3). These findings suggest that while DPTrek does not significantly impact the overall or category-based accuracy of the DP knowledge quiz, it does enhance participants' understanding of the consequences of DPs.

4.1.3 Survey-Based Subjective Evaluation. Before comparing the survey-based subjective evaluation between the two groups, we

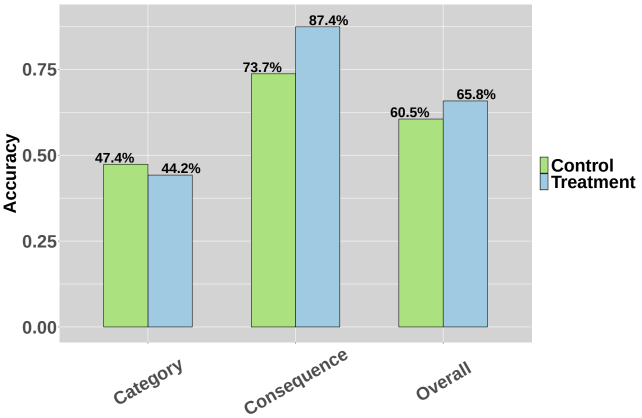


Figure 4: DP knowledge quiz accuracy comparison by question type

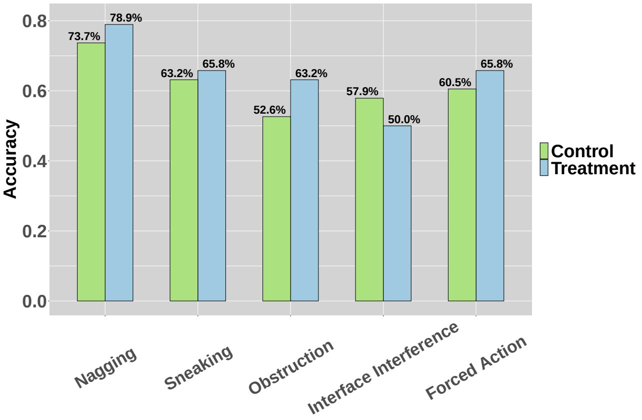


Figure 5: DP knowledge quiz accuracy comparison by DP category

Table 3: Mann-Whitney U Test results of DP knowledge quiz

		Test Statistic	P-value	Significance
Overall		185.5	0.894	Not Significant
By Question Type	Consequence	250.0	0.031	Significant
	Category	167.0	0.695	Not Significant
By DP Category	Nagging	186.0	0.861	Not Significant
	Sneaking	174.5	0.859	Not Significant
	Obstruction	215.5	0.261	Not Significant
	Interface Interference	148.5	0.311	Not Significant
	Forced Action	210.5	0.322	Not Significant

first assessed the validity of the constructs used in the evaluation. As shown in the "Cronbach's Alpha" column of Table 4, most constructs exhibited Cronbach's alpha values greater than 0.7, indicating acceptable reliability. However, two constructs, *Attitude Toward Coping with DPs* and *Future Behavioral Intention*, had slightly lower values of 0.685 and 0.697, respectively. While a Cronbach's alpha of 0.7 is generally considered the threshold for acceptable reliability, recent methodological reviews suggest that values around 0.70 or greater are widely regarded as desirable [117]. Given that the alpha values for these two constructs are close to 0.7, we chose to retain them in our analysis.

After confirming the measurement validity, we compared the means of the constructs between the treatment and control groups using Mann-Whitney U Test. Two constructs, i.e., *Enjoyment* and *Aesthetic Appeal* were significantly higher in the treatment group compared to the control group. For *Enjoyment*, the average score for the treatment group was 4.46, compared to 4.19 for the control group. The p-value of 0.002, which is below 0.05, provides significant evidence that participants found DPTrek more enjoyable than web-based static content learning. Additionally, the treatment group had an average score of 4.00 for *Aesthetic Appeal*, while the control group scored 3.60, with a p-value less than 0.05, indicating that participants found DPTrek more visually appealing.

However, no such differences were observed in other constructs. Although the means for *Perceived Usability*, *Attitude of Coping with DPs*, *Risk of DPs*, and *Future Behavioral Intention* were higher in the treatment group, these differences were not statistically significant. Interestingly, the means for *Confidence* and *Reward* were lower in the treatment group, though not significantly, suggesting that DPTrek was not effective in improving participants' confidence or sense of reward.

In summary, through a series of comparisons between the treatment and control groups, DPTrek is shown to be more effective in enhancing participants' ability to cope with DPs, improving their understanding of DP consequences, and providing a more enjoyable and aesthetically appealing learning experience, compared to web-based static content learning.[1]

4.2 Before-After Comparison in Treatment Group

As the treatment group underwent the four phases of EL in DPTrek, we compared the accuracy of coping with DPs across experience, experimentation and DP coping test through Wilcoxon signed-rank tests [35]. Additionally, we reported statistics from reflection phase to show how participants reflected on their observations.

As shown in Figure 7, participants' accuracy in coping with DPs significantly improved from experience to experiment and the DP coping test. This trend is evident in both the overall comparison and for each DP category. The increasing trend is further supported by the Wilcoxon Signed-rank test (Table 5), as the comparisons between experience and experiment, and between experience and the DP coping test, are both statistically significant. However, the difference between experiment and the DP coping test is not significant, with a slight decrease in accuracy as shown in Figure 7. Overall, this indicates that DPTrek is effective in improving participants' ability to cope with DPs throughout the EL process.

Table 6 and Figure 8 highlight variations in participants' responses for different DP categories during the reflection phase, the second step in EL. When asked about their observations in the experience phase, 96.8% successfully identified the DPs and their

[1] On average, the treatment group took 23.1 minutes to complete DPTrek, while the control group took 20.8 minutes to complete the web-based static content learning. The time was measured from the moment participants clicked on the first module to just before the DP coping test. No significant difference was found in the time spent (T-test Statistic = 186.5, p-value = 0.872), allowing us to rule out learning time as a potential confound.

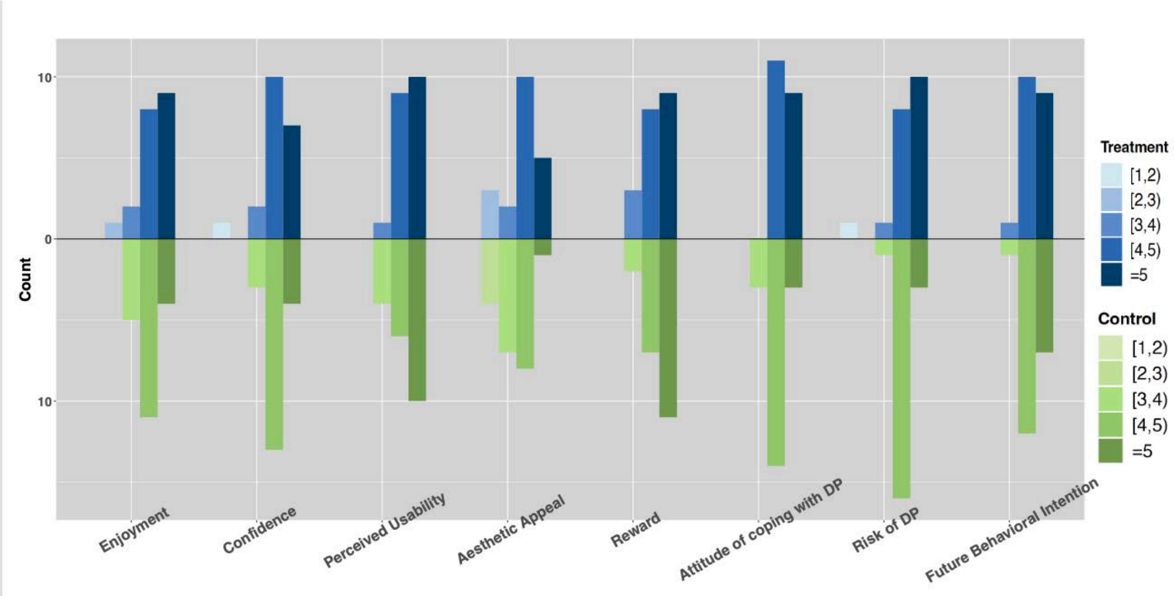


Figure 6: Distribution of survey-based subjective evaluation between treatment (top) and control (bottom) groups

Table 4: Descriptive statistics, measurement validity and Mann-Whitney U Test results of survey-based subjective evaluation

Construct	Treatment Mean	Control Mean	Cronbach's Alpha	Test Statistic	P-value	Significance
Enjoyment	4.46	4.19	0.909	286.0	0.002	Significant
Confidence	4.26	4.37	0.869	184.0	0.929	Not Significant
Perceived Usability	4.65	4.49	0.706	190.5	0.763	Not Significant
Aesthetic Appeal	4.00	3.60	0.861	267.0	0.010	Significant
Reward	4.49	4.56	0.878	167.0	0.680	Not Significant
Attitude of Coping with DPs	4.63	4.41	0.685	228.0	0.161	Not Significant
Risk of DPs	4.57	4.33	0.810	231.5	0.124	Not Significant
Future Behavioral Intention	4.72	4.47	0.697	232.5	0.114	Not Significant

Table 5: Wilcoxon Signed-rank test results for before-after comparison in the treatment group

	Test Statistic	P-value	Significance
Experience Vs Experiment	0.0	0.000	Significant
Experience Vs Test	2.0	0.001	Significant
Experiment Vs Test	46.5	0.238	Not Significant

associated consequences. In reflecting on their feelings towards DPs, "Annoyed" was the most frequently reported emotion (46.3%), particularly in the *Nagging* (84.2%) and *Forced Action* (52.6%) categories. The average intensity of "Annoyed" was consistently high, reaching 3.94 in the *Nagging* category and 4.10 in the *Forced Action* category. "Concerned" was also a common response, especially in the *Sneaking* and *Obstruction* categories. In contrast, emotions such as "Indifference" and "Intrigued" were less frequently reported and generally associated with lower average intensity scores. These findings suggest that while participants generally exhibited negative feelings towards DPs, specific categories like *Nagging* and *Forced Action* evoked stronger and more negative emotional reactions.

Lastly, we collected participants' reflections on how frequently participants encounter the presented DPs in their daily lives, as shown in Figure 9. The analysis reveals varying levels of frequencies across different DP categories. *Obstruction* and *Interface Interference* are the most prevalent, with many participants reporting frequent encounters with these patterns. Specifically, *Obstruction* is identified as a serious issue, with a substantial proportion of participants encountering it "always" (31.6%) or "often" (42.1%). Over half of the participants experience *Interface Interference* "often" (52.6%). Similarly, *Nagging* is frequently reported, with 15.8% of participants experiencing it "always" and 31.6% "often." In contrast, *Forced Action* and *Sneaking* show a more varied distribution, with a lower percentage of participants encountering them "always" (10.5%). These findings highlight significant variations in the frequency of different DPs, indicating their diverse impact on user experiences. The prevalence of "often" (37.9%) and "sometimes" (26.3%) across categories suggests that DPs are a common issue affecting many users regularly.

In summary, through a before-and-after comparison across the stages of experiential learning within the treatment group, we observed a significant improvement in participants' ability to cope with DPs from the experience to the experiment/test stage. Participants expressed negative feelings toward DPs, especially to Nagging and Forced Actions, and reported frequent encounters with DPs in their daily lives.

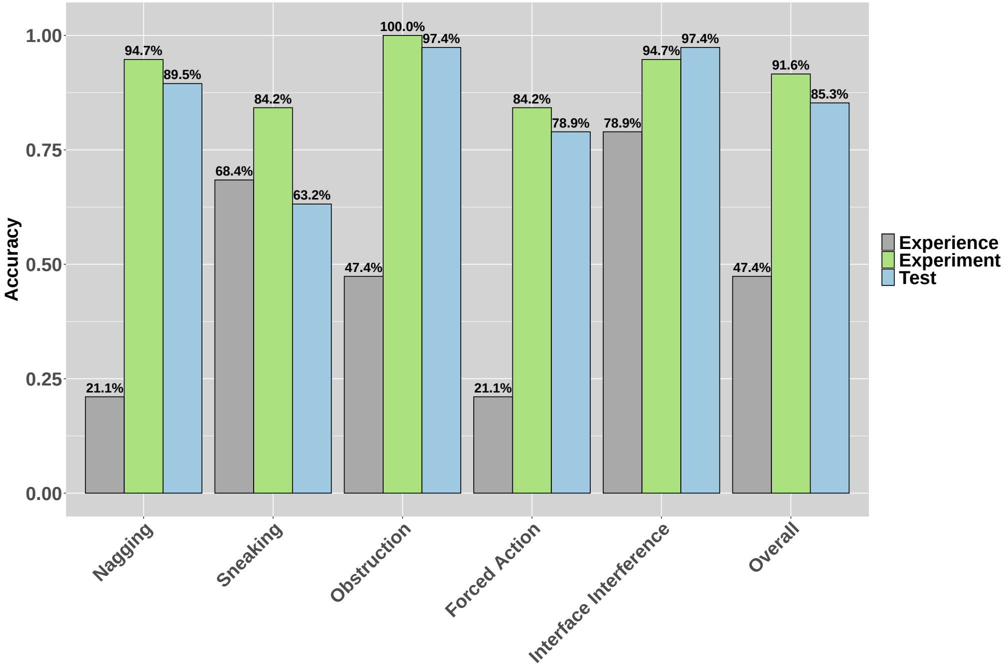


Figure 7: Before-after accuracy of DP coping test in the treatment group

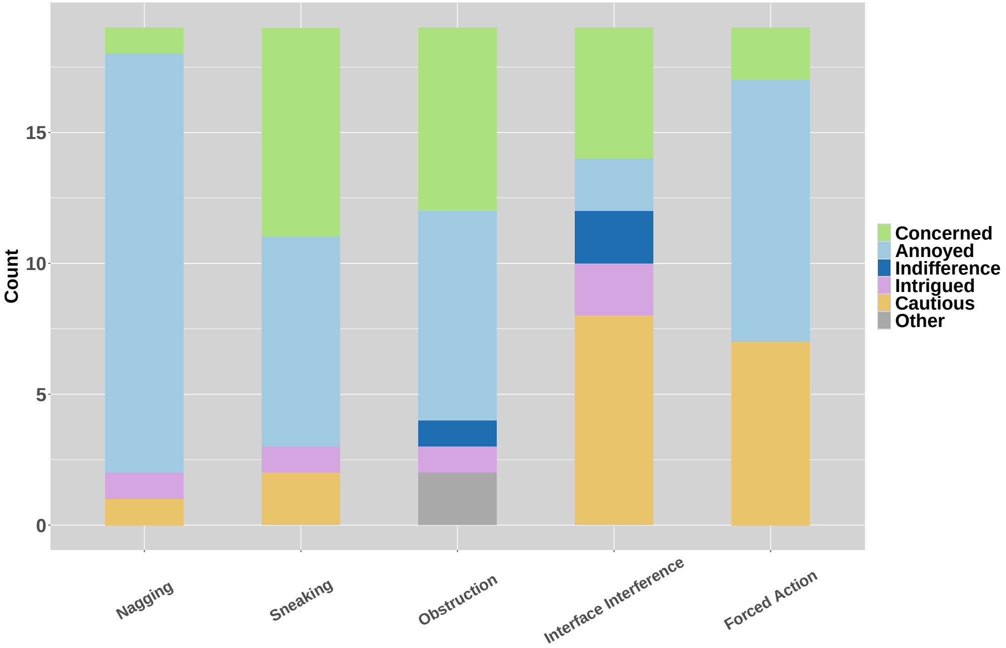


Figure 8: Feeling distribution in the observation phase (treatment group only)

5 Qualitative Results

We identified several key aspects from participants' feedback in the exit interviews regarding the effectiveness of DPTrek, covering both positive and negative impacts.

5.1 Positive Impacts of DPTrek

Improving understandings of DPs. A notable number of participants (P1, P3, P7, P12, P13) mentioned that DPTrek significantly increased their awareness of DPs. Several participants emphasized

Table 6: Average degree of feelings towards each DP category in the observation phase (treatment group only)

	Nagging	Sneaking	Obstruction	Interface Interference	Forced Action
Concerned	4.00	3.75	3.43	3.00	4.50
Annoyed	3.94	3.25	3.00	3.00	4.10
Indifference	/	/	3.00	1.50	/
Intrigued	4.00	2.00	2.00	2.00	/
Cautious	4.00	3.00	/	3.12	2.86
Other	/	/	3.50	/	/

Note: "/" indicates that the corresponding feeling is not reported by participants.

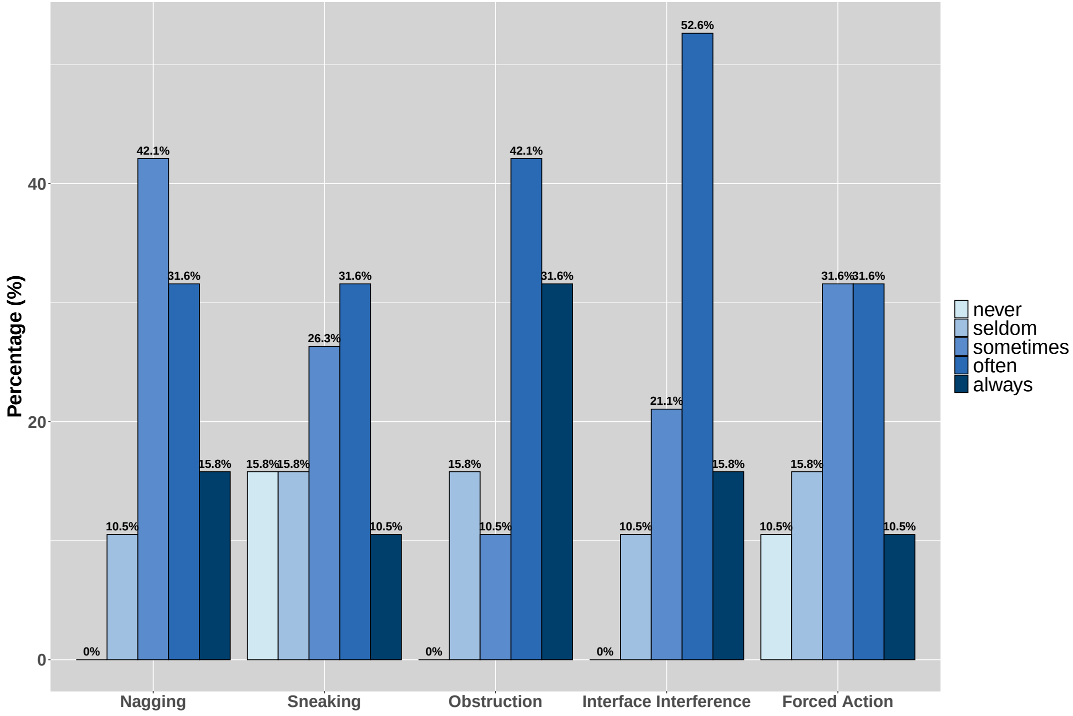


Figure 9: Frequency distribution of DP encounters

how the training made them more vigilant, enabling them to recognize potential risks in their daily online activities, which could help them avoid losses in the future. For instance, P1 specifically highlighted the increased awareness of *Sneaking*, making people more cautious when browsing shopping websites:

> *"I learned that people need to be aware of these dark patterns in their everyday lives. If they pay attention to what they're doing, they can avoid the consequences of extra charges that might appear on their accounts in the near future."*

Participants (P2, P5, P6, P31) also reported that DPTrek had a significant impact on teaching them how to avoid DPs. They mentioned that DPTrek underscored the risks associated with DPs, prompting them to adopt careful examination of web pages and interactive elements are crucial in avoiding misleading tactics. For example, P2 reflected:

> *"The training showed me the importance of double-checking and being more careful, especially when something seems off, like discrepancies on a receipt."*

Gaining hands-on experience in coping with DPs. Participants (P2, P6, P7, P12, P13) highly appreciated the use of real-world examples in DPTrek, stating that these cases enhanced their understanding of the application of the concepts. By showcasing real-world examples from familiar platforms such as social media and online shopping websites, DPTrek helped participants relate the material to their own experiences, obtaining practical skills to identify DPs in real life. For instance, P12 mentioned:

> *"The definitions are useful, but seeing these patterns in real-life examples makes it easier to identify them."*

5.2 Negative Feedback on DPTrek

Despite the positive impact of DPTrek, participants also identified several areas that need further improvement.

Coping strategies lack practicality. While the training helped raise awareness and instructed useful strategies to cope with DPs, several participants (P2, P3, P22, P38) questioned the practicality of the coping strategies provided, i.e., "leaving the website" and "reporting the website", as they might not be a viable option when users really need to use the websites. Instead, they expressed a desire to learn more effective strategies to avoid DPs while still being able to complete their transactions. For instance, P3 noted:

> *"Sometimes you really need to buy something, and just leaving the website isn't a practical solution."*

Memorizing DP categories is challenging. Several participants expressed difficulty in remembering the specific names of DPs (P2, P10, P11). They found the terms unfamiliar and challenging to retain, particularly since these are not words commonly used in everyday conversations. P10 mentioned that while they understood the concepts, matching the names to their respective DP categories was difficult. P2 also noted that these terms are not typically part of daily language, making them harder to memorize, while P11 found the names confusing even though the concepts themselves were well understood. For instance, P11 commented:

> *"I understand the concepts deeply, but the names of the dark patterns are somewhat confusing."*

Classifying DPs is challenging. While participants grasped the general concepts of DPs, some (P6, P7, P21, P29) found it difficult to classify specific patterns into different categories. For instance, P6 explained:

> *"Yeah, they are easy to understand but can be a bit confusing, especially when differentiating between obstruction and forced action."*

Education places the burden on users. One participant (P22) believed that while the training improved users' knowledge, relying solely on user education was not sufficient. They stressed that addressing DPs and associated privacy issues required top-down measures, such as the implementation of laws and regulations, rather than placing the burden entirely on users to avoid these patterns:

> *"It might be more effective to regulate companies designing dark patterns rather than just teaching users how to avoid them. Even if users are educated on avoiding things like cookie permissions, those who design dark patterns can always come up with new tactics."*

In summary, participants believed DPTrek enhanced their understanding of DPs and provided valuable hands-on experience in coping with them. However, they also noted that some coping strategies lacked practicality, certain DP categories were difficult to memorize, and they expressed a desire for regulatory measures to alleviate the educational burden on end users.

6 Discussion

EL-based DP education is effective. Overall, our results demonstrate that DP education is beneficial and that DPTrek is particularly effective for this purpose. DPTrek excels in teaching users how to handle DPs while browsing websites, compared to those learning through Web-based Static Content Learning. Additionally, there was a notable enhancement in DP coping skills from before to after DPTrek. Moreover, quiz results show that DPTrek more effectively improves participants' understanding of DP consequences. Interview feedback also highlights that participants valued the real-world DP examples used in DPTrek. These findings suggest that the EL-based approach, like DPTrek, is effective in developing practical skills for managing DPs. Given that DPs are characterized by psychological manipulation, lack of transparency, misleading impressions, and complicated processes [60], traditional educational methods, such as fact-based instruction, may fall short in fully conveying the complexity and manipulative nature of DPs, or in encouraging learners to take its potential harm seriously. The EL-based approach addresses this gap by enabling learners to develop practical skills through hands-on experience, reflection, conceptualization, and experimentation. By immersing learners in simulated scenarios that demonstrate the consequences of dark patterns and providing practical strategies for navigating them, EL offers a more comprehensive understanding of how to recognize and counteract DPs. Therefore, we propose EL as an effective educational approach for teaching about DPs in the future.

The effectiveness of EL-based DP education has broader implications for informal cybersecurity and privacy education. Many everyday cyber threats involve psychological manipulation, misleading information, disguises, deceptive tactics, and a lack of transparent consequences. For example, phishing attacks exploit users by employing various disguises and deceptive tactics to appear legitimate, tricking users into divulging personal information or clicking malicious links [68]. Many software applications obscure key data-sharing information within lengthy privacy policies, leading users to unknowingly grant access without realizing the consequences of data sharing [90]. Current education methods for addressing these cyber threats largely rely on "Fact-and-Advice" approaches [8, 41, 74, 120], storytelling [39, 54, 66, 99, 104], and games [10, 33, 121]. They lack personal relevance to learners, are detached from their contexts, and do not incorporate experiential components [62, 101, 107, 108]. For instance, "Fact-and-Advice" methods may not resonate with learners' personal experiences, while storytelling provides indirect experiences without active participation or emotional engagement. Although gamified education simulates and contextualizes cyber threats, its game-like nature does not allow learners to experience the real-world consequences of incorrect cybersecurity decisions. For instance, most phishing games involve losing points or lives when learners fall for phishing emails [10, 113, 121], while others provide warnings explaining potential consequences of phishing [28, 121]. These are not the true consequences that would occur in real-world phishing incidents. Given these issues, learners may not always be able to effectively apply cybersecurity knowledge into their real-world situations, nor develop the critical thinking skills necessary to evaluate the implications of cyber threats in their daily lives.

Based on observations from our study, an EL-based approach holds significant potential for enhancing the application of cybersecurity knowledge and fostering critical thinking. By allowing users to experience and reflect on the entire process of receiving, interacting with, and facing the simulated consequences of DPs (e.g., simulated email notifications of extra payments or advertisements), learners can deepen their understanding of DP consequences and therefore critically assess the impact on their situation. Therefore, we believe that EL-based approaches present a promising alternative for advancing cybersecurity and privacy education more broadly. We suggest that future cybersecurity and privacy education should incorporate such experiential components to enhance learners' understanding not only of how to interact with cyber threats but also of their real-world consequences (e.g., a simulated scenario of financial or identity loss from phishing, or a simulated data breach incident). This will enable learners to critically assess the associated risks, raise awareness of the seriousness of the threats, and make informed decisions that align more effectively with their real-world situations.

A user-friendly DP taxonomy is needed. One common theme emerging from our findings is that participants generally found the DP categories difficult to memorize and understand. For instance, in Figure 4 in Section 4.1.2, we show that participants are better at understanding the consequences of DPs, but they have difficulties mapping the DP examples to the correct categories. The exit interviews also reveal that memorizing DP categories is challenging because the names of the categories are not everyday words. Classifying DPs is hard because participants perceived overlaps between categories. This difficulty largely stems from the fact that the DP taxonomy used in our study was created based on HCI expert encoding from the perspectives of UX designers rather than users [60]. In fact, most available taxonomies are developed by domain experts, such as those leveraging observations from cognitive science [85], based on input from hackers [36], or through ad-hoc discussions among researchers [61]. Currently, no DP taxonomy has been specifically developed for public users or based on their perceptions.

A user-friendly DP taxonomy offers two key benefits. First, it enables learners to apply coping strategies learned for one DP to other DPs within the same category. DPs of the same type may be presented differently across various types of websites. For example, sneaking manifests as hidden fees or preselected add-ons on shopping websites, but as hidden policies in promotional offers (e.g., auto-renewal or price increase after 1 year) on internet/phone/TV service websites. Despite these differences in presentation, the coping strategies remain consistent within each DP category. For instance, the above two different presentations of sneaking both require a careful review to identify hidden items or policies. Thus, if users can accurately categorize DPs with varying presentations across different websites, even those they have not encountered during DPTrek, they can effectively map the corresponding coping strategies to the identified DP category. Second, DPs are evolving rapidly, with new variations constantly emerging to exploit user vulnerabilities. Recent FTC report shows that more companies are using DPs to trick consumers into buying products and sharing personal information [53]. While DPTrek or other DP education programs cannot cover all emerging DP cases, teaching learners to effectively categorize these patterns into existing taxonomy categories can enable the transfer of coping strategies to novel instances. Additionally, if learners find an emerging DP does not fit within any existing category, it serves as a signal for researchers and practitioners to raise awareness and investigate the coping strategies. Thus, a user-friendly DP taxonomy is important and beneficial to DP education given the evolving digital landscape. We suggest further research on building DP taxonomies should potentially include input from end users and evaluate the ease of user understanding.

Lack of practical solutions to mitigate DPs. Our findings indicate that *Nagging* and *Forced Action* are particularly challenging for users to completely avoid. In *Nagging*, users are persistently reminded to take an action. Even if users reject the action, the reminder typically reappears after a while. In *Forced Action*, users are compelled to complete a specific action to gain or maintain access to certain functionality. While DPTrek provides coping strategies, namely reporting the website or ceasing to use it, participants found the strategies impractical, as in some cases, they need to use the website and cannot simply report or abandon it. Consequently, they are forced to accept the DPs. At present, no practical coping strategies exist that allow users to both avoid these DPs and continue using the websites. Prior research has proposed solutions such as rewriting the UIs associated with DPs [42, 43, 73] or providing notifications for suspicious DPs on UIs [25]. Unfortunately, these solutions face challenges such as high implementation workload, scalability concerns, robustness issues, and the risk of voiding software warranties [42, 43].

While DPTrek effectively educates users to be more aware of these DPs and their consequences, addressing DPs requires efforts beyond end-user education. The implementation of laws and regulations targeting DPs is essential for systematically mitigating DPs, particularly those that users find difficult to opt out of. Additionally, practitioners, including website designers and developers, should be educated on ethical UI design principles and incentivized to avoid DPs in their design. Ideally, practical solutions should not solely rely on user education or third-party interventions but should be integrated into platforms (e.g., operating systems, browsers, or software marketplaces) to provide inherent, centralized, and robust mitigation against DPs. These efforts would not only address DPs that currently lack practical end-user coping strategies, but also alleviate the educational burden on users, who are otherwise required to constantly learn about and remain vigilant against potential DPs in their daily lives. Ultimately, users expect to enjoy the services provided by websites while simultaneously avoiding the harms of DPs. We anticipate that a comprehensive DP mitigation solution will emerge through collaborative efforts encompassing the legislation, UI design, and user education, alongside a deeper understanding of how to balance these legislative, technical, and educational initiatives to achieve a long-term, viable solution to DPs.

7 Limitations

One limitation of this study is the lack of diversity among participants. Most participants are aged 18-25, have relatively high education levels, and come from STEM majors. Although we did not require participants to be affiliated with our institution, the majority (36 out of 38) were from our institution, potentially sharing similar educational backgrounds. This might introduce biases into the study that affect the generalizability of the findings to a broader population. For example, the evaluation results from participants with relatively high education levels may not represent the effectiveness of DPTrek for the general public. Additionally, the cybersecurity culture at our institution might make the sample more security-conscious than average. In future research, we plan to explore the effectiveness of education across a more diversified set of participants, such as across different age groups, education levels, and other demographic factors. Also, this study is based on the most widely adopted DP taxonomy [60]. However, there are other taxonomy variants, such as those proposed by [36, 61, 85]. Future research could examine how these different taxonomies impact experiential learning in DP education. The study incorporates some DP cases in the learning phases of DPTrek (i.e., experience and experiment) and uses other DP variants in the same category for the DP coping test, which indicates that participants acquire some extent of skills to identify and cope with DP variants after learning. However, assessing the long-term effectiveness of the intervention and participants' ability to handle evolving and other new DPs will require a broader and more rigorous evaluation, which we leave for future research.

8 Conclusion

Today's online users face widespread exposure to dark patterns (DPs) – unethical user interface designs that deceive them into making unwanted decisions, compromising their privacy, security, financial safety, and more. This study explores effective educational interventions for teaching users about DPs by developing DPTrek, an experiential learning (EL) platform that educates users through simulated real-world DP cases. We conducted a series of quantitative and qualitative evaluations, including DP coping tests, quizzes, subjective surveys, and interviews, which indicate that DPTrek effectively enhances users' ability to identify and manage DPs. The study also highlights critical concerns for future DP education and research, such as the challenges posed by user-unfriendly taxonomies and the lack of practical solutions to mitigate DPs.

References

[1] [n. d.]. Federal Trade Commission. https://www.ftc.gov/. Accessed: 2024-09-11.

[2] [n. d.]. Free Online Survey Maker Tool - Qualtrics. https://www.qualtrics.com/free-account/. Accessed: 2024-09-11.

[3] 2007. The Mann - Whitney U: A Test for Assessing Whether Two Independent Samples Come from the Same Distribution. https://api.semanticscholar.org/CorpusID:59357756

[4] 2018. Dark Patterns. https://darkpatterns.uxp2.com/.

[5] 2023. Microsoft Security – Cybersecurity | Microsoft. https://www.microsoft.com/en-us/security?rtc=1 Accessed: 2023-06-20.

[6] Ritu Agarwal and Elena Karahanna. 2000. Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS quarterly* (2000), 665–694.

[7] I Ajzen. 2002. Constructing a TPB questionnaire: Conceptual and methodological considerations. *University of Massechusetts Amherst, Office of Information Technologies* (2002).

[8] Elham Al Qahtani, Lipsarani Sahoo, Yousra Javed, and Mohamed Shehab. 2022. " Why would Someone Hack Me out of Thousands of Students": Video Presenter's Impact on Motivating Users to Adopt 2FA. In *Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies*. 139–150.

[9] Eirik Albrechtsen and Jan Hovden. 2010. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security* 29, 4 (2010), 432–445.

[10] Nalin Asanka Gamagedara Arachchilage, Steve Love, and Konstantin Beznosov. 2016. Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior* 60 (2016), 185–197.

[11] Shahryar Baki and Rakesh M Verma. 2022. Sixteen Years of Phishing User Studies: What Have We Learned? *IEEE Transactions on Dependable and Secure Computing* 20, 2 (2022), 1200–1212.

[12] Victoria Simpson Beck, Stephanie K Boys, Hannah J Haas, and Karen N King. 2017. How do you use experiential learning to bridge the classroom and the real world? *New Directions for Teaching and Learning* 2017, 151 (2017), 97–115.

[13] Kristian Beckers and Sebastian Pape. 2016. A serious game for eliciting social engineering security requirements. In *2016 IEEE 24th International Requirements Engineering Conference (RE)*. IEEE, 16–25.

[14] Federal Reserve Board. 2008. Consumer Compliance Handbook: Section 5 of the FTC Act. https://www.federalreserve.gov/boarddocs/supmanual/cch/200806/ftca.pdf. Accessed: 2024-08-26.

[15] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proc. Priv. Enhancing Technol.* 2016, 4 (2016), 237–254.

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

[17] H Brignull, M Leiser, C Santos, and K Doshi. 2010. Dark Patterns. https://twitter.com/darkpatterns Accessed: 2024-08-26.

[18] H Brignull, M Leiser, C Santos, and K Doshi. 2010. Deceptive patterns – user interfaces designed to trick you. https://www.deceptive.design/

[19] H Brignull, M Leiser, C Santos, and K Doshi. 2015. Forced email collection. https://www.deceptive.design/types/forced-action

[20] H Brignull, M Leiser, C Santos, and K Doshi. 2015. Sneaking cart. https://www.deceptive.design/types/sneaking

[21] H Brignull, M Leiser, C Santos, and K Doshi. 2020. Executive-committee of the Belgian DPA (GBA) v. Rossel & Cie. https://www.deceptive.design/cases/executive-committee-of-the-belgian-dpa-gba-v-rossel-cie

[22] H Brignull, M Leiser, C Santos, and K Doshi. 2021. Deliberation of the Restricted Committee concerning Google LLC and Google Ireland Limited. https://www.deceptive.design/cases/deliberation-of-the-restricted-committee-concerning-google-llc-and-google-ireland-limited#:~:text=Outcome,the%20French%20Data%20Protection%20Act

[23] H Brignull, M Leiser, C Santos, and K Doshi. 2021. Preselection deceptive pattern. https://www.deceptive.design/types/preselection

[24] H Brignull, M Leiser, C Santos, and K Doshi. 2022. Deliberation of the restricted formation SAN-2022-027 concerning TikTok. https://www.deceptive.design/cases/deliberation-of-the-restricted-formation-san-2022-027-concerning-tiktok

[25] Zhaoxin Cai, Yuhong Nan, Xueqiang Wang, Mengyi Long, Qihua Ou, Min Yang, and Zibin Zheng. 2023. DARPA: Combating Asymmetric Dark UI Patterns on Android with Run-time View Decorator. In *2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 480–493.

[26] 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*. 1–20.

[27] Tom Chothia, Sam Holdcroft, Andreea-Ina Radu, and Richard J Thomas. 2017. Jail, Hero or Drug Lord? Turning a Cyber Security Course Into an 11 Week Choose Your Own Adventure Story.. In *ASE@ USENIX Security Symposium*.

[28] Gokul CJ, Sankalp Pandit, Sukanya Vaddepalli, Harshal Tupsamudre, Vijayanand Banahatti, and Sachin Lodha. 2018. Phishy-a serious game to train enterprise users on phishing awareness. In *Proceedings of the 2018 annual symposium on computer-human interaction in play companion extended abstracts*. 169–181.

[29] Federal Trade Commission. [n. d.]. Restore Online Shoppers' Confidence Act. https://www.ftc.gov/legal-library/browse/statutes/restore-online-shoppers-confidence-act. Accessed: 2024-08-26.

[30] Federal Trade Commission. 2011. Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises. https://www.ftc.gov/news-events/news/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep-privacy-promises. Accessed: 2024-08-26.

[31] Federal Trade Commission. 2019. FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook. Accessed: 2024-08-26.

[32] Federal Trade Commission. 2021. FTC to Ramp Up Enforcement Against Illegal Dark Patterns That Trick or Trap Consumers into Subscriptions. https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions. Accessed: 2024-08-26.

[33] Benjamin D Cone, Cynthia E Irvine, Michael F Thompson, and Thuy D Nguyen. 2007. A video game for cyber security training and awareness. *computers & security* 26, 1 (2007), 63–72.

[34] Benjamin D Cone, Michael F Thompson, Cynthia E Irvine, and Thuy D Nguyen. 2006. Cyber security training and awareness through game play. In *Security and Privacy in Dynamic Environments: Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006), 22–24 May 2006, Karlstad, Sweden 21*. Springer, 431–436.

[35] WJ Conover. 1999. *Practical nonparametric statistics.* John Wiley & Sons, Inc.

[36] Gregory Conti and Edward Sobiesk. 2010. Malicious interface design: exploiting the user. In *Proceedings of the 19th international conference on World wide web*. 271–280.

[37] James Crabb, Christopher Hundhausen, and Assefaw Gebremedhin. 2024. A Critical Review of Cybersecurity Education in the United States. In *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1*. 241–247.

[38] Lee J Cronbach. 1951. Coefficient alpha and the internal structure of tests. *psychometrika* 16, 3 (1951), 297–334.

[39] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. 2014. The effect of social influence on security sensitivity. In *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*. 143–157.

[40] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I Hong. 2018. Breaking! A typology of security and privacy news and how it's shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–12.

[41] Sanchari Das, Shrirang Mare, and L Jean Camp. 2020. Smart storytelling: Video and text risk communication to increase mfa acceptability. In *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*. IEEE, 153–160.

[42] Siddhartha Datta, Konrad Kollnig, and Nigel Shadbolt. 2022. GreaseVision: Rewriting the rules of the interface. *arXiv preprint arXiv:2204.03731* (2022).

[43] Siddhartha Datta, Konrad Kollnig, and Nigel Shadbolt. 2022. Mind-proofing your phone: Navigating the digital minefield with greaseterminator. In *Proceedings of the 27th International Conference on Intelligent User Interfaces*. 523–536.

[44] Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. 2013. Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 915–928.

[45] Deceptive Design. 2023. French Data Protection Act, Article 82. https://www.deceptive.design/laws/french-data-protection-act-article-82. Accessed: 2024-08-26.

[46] Deceptive Design. 2023. Section 6:3:3A of the Dutch Civil Code: Unfair Commercial Practices. https://www.deceptive.design/laws/section-6-3-3a-of-the-dutch-civil-code-unfair-commercial-practices. Accessed: 2024-08-26.

[47] 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*. 1–14.

[48] Ersin Dincelli and InduShobha Chengalur-Smith. 2020. Choose your own training adventure: designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. *European Journal of Information Systems* 29, 6 (2020), 669–687.

[49] Feng Dong, Haoyu Wang, Li Li, Yao Guo, Tegawendé F Bissyandé, Tianming Liu, Guoai Xu, and Jacques Klein. 2018. Frauddroid: Automated ad fraud detection for android apps. In *Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 257–268.

[50] Yasmine El-Glaly, Weishi Shi, Samuel Malachowsky, Qi Yu, and Daniel E Krutz. 2020. Presenting and evaluating the impact of experiential learning in computing accessibility education. In *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering: Software Engineering Education and Training*. 49–60.

[51] Federal Trade Commission. 2021. Age Learning, Inc. (ABCmouse). https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3186-age-learning-inc-abcmouse Accessed: 2024-08-26.

[52] Federal Trade Commission. 2021. Bringing Dark Patterns to Light: FTC Workshop. https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop Accessed: 2024-08-26.

[53] Federal Trade Commission. 2022. FTC Report Shows Rise in Sophisticated "Dark Patterns" Designed to Trick and Trap Consumers. https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers.

[54] Chris Fennell and Rick Wash. 2019. Do stories help people adopt two-factor authentication? *Studies* 1, 2 (2019), 3.

[55] Valentina Fietta, Mirko Franco, Erika De Santis, Merylin Monaro, Claudio E Palazzi, and Ombretta Gaggi. 2024. Safe Digital Teens: an App to Address Technology-Related Risks for Adolescents. In *Proceedings of the 2024 International Conference on Information Technology for Social Good*. 333–341.

[56] Susanne Furman, Mary Frances Theofanos, Yee-Yin Choong, and Brian Stanton. 2011. Basing cybersecurity training on user perceptions. *IEEE Security & Privacy* 10, 2 (2011), 40–49.

[57] Mark Gondree and Zachary NJ Peterson. 2013. Valuing security by getting [d0x3d!]: Experiences with a network security board game. In *6th Workshop on Cyber Security Experimentation and Test ({CSET} 13)*.

[58] John R Goodall, Wayne G Lutters, and Anita Komlodi. 2009. Developing expertise for network intrusion detection. *Information Technology & People* 22, 2 (2009), 92–108.

[59] Colin M Gray, Shruthi Sai Chivukula, and Ahreum Lee. 2020. What Kind of Work Do" Asshole Designers" Create? Describing Properties of Ethical Concern on Reddit. In *Proceedings of the 2020 acm designing interactive systems conference*. 61–73.

[60] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3174108

[61] JOHANNA GUNAWAN, AMOGH PRADEEP, DAVID CHOFFNES, WOODROW HARTZOG, and CHRISTO WILSON. 2021. A Comparative Study of Dark Patterns Across Mobile and Web Modalities. (2021).

[62] Julie M Haney and Wayne G Lutters. 2018. "It's Scary... It's Confusing... It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security.. In *SOUPS@ USENIX Security Symposium*. 411–425.

[63] Stephen Hart, Andrea Margheri, Federica Paci, and Vladimiro Sassone. 2020. Riskio: A serious game for cyber security awareness and education. *Computers & Security* 95 (2020), 101827.

[64] Stephanie D Hight. 2005. The importance of a security, education, training and awareness program, November 2005. *City of Raleigh* (2005), 1–5.

[65] Sebastian Hobert, Asbjørn Følstad, and Effie Lai-Chong Law. 2023. Chatbots for active learning: A case of phishing email identification. *International Journal of Human-Computer Studies* 179 (2023), 103108.

[66] David Michael Hull, Sebastian Walter Schuetz, and Paul Benjamin Lowry. 2023. Tell me a story: The effects that narratives exert on meaningful-engagement outcomes in antiphishing training. *Computers & Security* 129 (2023), 103252.

[67] Zaidat Ibrahim, Clara Caldeira, and Chia-Fang Chung. 2024. Supporting Experiential Learning in People with Gestational Diabetes Mellitus. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–16.

[68] Lance James. 2005. *Phishing exposed*. Elsevier.

[69] Keith S Jones, Akbar Siami Namin, and Miriam E Armstrong. 2018. The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. *ACM Transactions on Computing Education (TOCE)* 18, 3 (2018), 1–12.

[70] Jin Kang and Audrey Girouard. 2022. Impact of UX internships on human-computer interaction graduate students: a qualitative analysis of internship reports. *ACM Transactions on Computing Education (TOCE)* 22, 4 (2022), 1–25.

[71] Mari Karjalainen and Mikko Siponen. 2011. Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems* 12, 8 (2011), 3.

[72] David A Kolb. 2014. *Experiential learning: Experience as the source of learning and development.* FT press.

[73] 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*. 1–8.

[74] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. 2010. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)* 10, 2 (2010), 1–31.

[75] UXP2 Lab. 2024. Dawn of War III: Required Secondary Subscription. https://darkpatterns.uxp2.com/pattern/required-secondary-subscription/.

[76] UXP2 Lab. 2024. Google Location Services: Spam. https://darkpatterns.uxp2.com/pattern/google-location-services-spam/.

[77] UXP2 Lab. 2024. Instagram - No Option for No. https://darkpatterns.uxp2.com/pattern/instagram-no-option-for-no/.

[78] UXP2 Lab. 2024. Quora: Automatic Opt-In. https://darkpatterns.uxp2.com/pattern/quora-automatic-opt-in/.

[79] Kees Leune and Salvatore J Petrilli Jr. 2017. Using capture-the-flag to enhance the effectiveness of cybersecurity education. In *Proceedings of the 18th Annual Conference on Information Technology Education*. 47–52.

[80] Danyang Li. 2022. The FTC and the CPRA's regulation of dark patterns in cookie consent notices. *The University of Chicago Business Law Review* 1, 1 (2022), 19.

[81] Bin Liu, Suman Nath, Ramesh Govindan, and Jie Liu. 2014. {DECAF}: Detecting and characterizing ad fraud in mobile apps. In *11th USENIX symposium on networked systems design and implementation (NSDI 14)*. 57–70.

[82] Jamie Luguri and Lior Jacob Strahilevitz. 2021. Shining a light on dark patterns. *Journal of Legal Analysis* 13, 1 (2021), 43–109.

[83] Maximilian Maier. 2019. Dark patterns–An end user perspective.

[84] SM Hasan Mansur, Sabiha Salma, Damilola Awofisayo, and Kevin Moran. 2023. Aidui: Toward automated recognition of dark patterns in user interfaces. In *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)*. IEEE, 1958–1970.

[85] 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 (2019), 1–32.

[86] 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*. 1–18.

[87] Patricia R McCarthy and Henry M McCarthy. 2006. When case studies are not enough: Integrating experiential learning into business curricula. *Journal of Education for business* 81, 4 (2006), 201–204.

[88] Thomas Mejtoft, Erik Frängsmyr, Ulrik Söderström, and Ole Norberg. 2021. Deceptive design: cookie consent and manipulative patterns. In *34th Bled eConference-Digital support from crisis to progressive change, Online, June 27-30, 2021*. 397–408.

[89] Marisa Meyer, Victoria Adkins, Nalingna Yuan, Heidi M Weeks, Yung-Ju Chang, and Jenny Radesky. 2019. Advertising in young children's apps: A content analysis. *Journal of developmental & behavioral pediatrics* 40, 1 (2019), 32–39.

[90] Abraham Mhaidli, Selin Fidan, An Doan, Gina Herakovic, Mukund Srinath, Lee Matheson, Shomir Wilson, and Florian Schaub. 2023. Researchers' experiences in analyzing privacy policies: Challenges and opportunities. *Proceedings on Privacy Enhancing Technologies* (2023).

[91] Thomas Howard Morris. 2020. Experiential learning–a systematic review and revision of Kolb's model. *Interactive learning environments* 28, 8 (2020), 1064–1077.

[92] Carol Moser, Sarita Y Schoenebeck, and Paul Resnick. 2019. Impulse buying: Design practices and consumer needs. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–15.

[93] Pradeep K Murukannaiah, Chinmaya Dabral, Karthik Sheshadri, Esha Sharma, and Jessica Staddon. 2017. Learning a privacy incidents database. In *Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp*. 35–44.

[94] National Initiative for Cybersecurity Careers and Studies. 2022. *Workforce Framework for Cybersecurity NICE Framework*. https://niccs.cisa.gov/workforce-development/nice-framework

[95] United States Court of Appeals for the Ninth Circuit. 2018. 16-17197 - FTC v. AMG Capital Management, LLC, et al. https://www.govinfo.gov/content/pkg/USCOURTS-ca9-16-17197/pdf/USCOURTS-ca9-16-17197-0.pdf. Accessed: 2024-08-26.

[96] Marc Olano, Alan Sherman, Linda Oliva, Ryan Cox, Deborah Firestone, Oliver Kubik, Milind Patil, John Seymour, Isaac Sohn, and Donna Thomas. 2014. {SecurityEmpire}: Development and evaluation of a digital game to promote cybersecurity education. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*.

[97] OpenAI. 2024. ChatGPT: GPT-4 Language Model. https://chat.openai.com. Accessed: 2024-09-09.

[98] James Parker, Michael Hicks, Andrew Ruef, Michelle L Mazurek, Dave Levin, Daniel Votipka, Piotr Mardziel, and Kelsey R Fulton. 2020. Build it, break it, fix it: Contesting secure development. *ACM Transactions on Privacy and Security (TOPS)* 23, 2 (2020), 1–36.

[99] Katharina Pfeffer, Alexandra Mai, Edgar Weippl, Emilee Rader, and Katharina Krombholz. 2022. Replication: Stories as Informal Lessons about Security. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 1–18.

[100] Lynette Pretorius. 2018. Experiential and self-discovery learning in digital literacy: Developing the discernment to evaluate source reliability. *College & Undergraduate Libraries* 25, 4 (2018), 388–405.

[101] Petri Puhakainen and Mikko Siponen. 2010. Improving employees' compliance through information systems security training: an action research study. *MIS quarterly* (2010), 757–778.

[102] R Core Team. 2023. *R: The R Project for Statistical Computing*. https://www.r-project.org/

[103] Emilee Rader and Rick Wash. 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity* 1, 1 (2015), 121–144.

[104] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*. 1–17.

[105] Jenny Radesky, Alexis Hiniker, Caroline McLaren, Eliz Akgun, Alexandria Schaller, Heidi M Weeks, Scott Campbell, and Ashley N Gearhardt. 2022. Prevalence and characteristics of manipulative design in mobile applications used by children. *JAMA network open* 5, 6 (2022), e2217641–e2217641.

[106] George E Raptis, Christina Katsini, Andrew Jian-Lan Cen, Nalin Asanka Gamagedara Arachchilage, and Lennart E Nacke. 2021. Better, funner, stronger: a gameful approach to nudge people into making less predictable graphical password choices. In *Proceedings of the 2021 CHI conference on human factors in computing systems*. 1–17.

[107] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. 2016. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 272–288.

[108] Andrew Reeves, Dragana Calic, and P Delfabbro. 2021. "Get a red-hot poker and open up my eyes, it's so boring" 1: Employee perceptions of cybersecurity training. *Computers & security* 106 (2021), 102281.

[109] Children's Advertising Review. 2021. Self-Regulatory Guidelines for Children's Advertising. https://bbbnp-bbbp-stf-use1-01.s3.amazonaws.com/docs/default-source/caru/caru_advertisingguidelines.pdf. Accessed: 2024-08-26.

[110] Fred B Schneider. 2013. Cybersecurity education in universities. *IEEE Security & Privacy* 11, 4 (2013), 3–4.

[111] Roland W Scholz, Regula Steiner, and Ralf Hansmann. 2004. Role of internship in higher education in environmental sciences. *Journal of Research in Science Teaching: The Official Journal of the National Association for Research in Science Teaching* 41, 1 (2004), 24–46.

[112] Amazon Web Services. 2024. *Amazon Simple Storage Service (S3) Documentation*. Accessed: 2024-09-09.

[113] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. 2007. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security*. 88–99.

[114] Adam Shostack. 2014. Elevation of privilege: Drawing developers into threat modeling. In *2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*.

[115] Lori Simons, Lawrence Fehr, Nancy Blank, Heather Connell, Denise Georganas, David Fernandez, and Verda Peterson. 2012. Lessons Learned from Experiential Learning: What Do Students Learn from a Practicum/Internship?. *International Journal of Teaching and Learning in Higher Education* 24, 3 (2012), 325–334.

[116] Valdemar Švábenský, Jan Vykopal, and Pavel Čeleda. 2020. What are cybersecurity education papers about? a systematic literature review of sigcse and iticse conferences. In *Proceedings of the 51st ACM technical symposium on computer science education*. 2–8.

[117] Keith S Taber. 2018. The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in science education* 48 (2018), 1273–1296.

[118] Anne Clara Tally, Jacob Abbott, Ashley M Bochner, Sanchari Das, and Christena Nippert-Eng. 2023. Tips, Tricks, and Training: Supporting Anti-Phishing Awareness among Mid-Career Office Workers Based on Employees' Current Practices. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–13.

[119] U.S. Congress. 2022. S.3330 - Deceptive Experiences To Online Users Reduction (DETOUR) Act. https://www.congress.gov/bill/117th-congress/senate-bill/3330 Accessed: 2024-08-26.

[120] Rick Wash and Molly M Cooper. 2018. Who provides phishing training? facts, stories, and people like me. In *Proceedings of the 2018 chi conference on human factors in computing systems*. 1–12.

[121] Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, and Erik Andersen. 2019. What. hack: engaging anti-phishing training through a role-playing phishing simulation game. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

[122] Tingmin Wu, Wanlun Ma, Sheng Wen, Xin Xia, Cecile Paris, Surya Nepal, and Yang Xiang. 2021. Analysis of trending topics and text-based channels of information delivery in cybersecurity. *ACM Transactions on Internet Technology (TOIT)* 22, 2 (2021), 1–27.

[123] Heng Xu, Tamara Dinev, Jeff Smith, and Paul Hart. 2011. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems* 12, 12 (2011), 1.

[124] José P Zagal, Staffan Björk, and Chris Lewis. 2013. Dark patterns in the design of games. In *Foundations of Digital Games 2013*.

[125] Olga A Zielinska, Rucha Tembe, Kyung Wha Hong, Xi Ge, Emerson Murphy-Hill, and Christopher B Mayhorn. 2014. One phish, two phish, how to avoid the internet phish: Analysis of training strategies to detect phishing emails. In *Proceedings of the human factors and ergonomics society annual meeting*, Vol. 58. SAGE Publications Sage CA: Los Angeles, CA, 1466–1470.

[126] Wenting Zou, Amanda Purington Drake, Philipp K Masur, Janis Whitlock, and Natalie N Bazarova. 2024. Examining learners' engagement patterns and knowledge outcome in an experiential learning intervention for youth's social media literacy. *Computers & Education* 216 (2024), 105046.

A Additional Tables

Table 7: Simulated DP cases and their use in DPTrek

DP Category	DP Case Description	Phase in Study	Consequences	Successful Strategies
Nagging	The user is pressured to turn on notifications, with no clear option to opt out. [77]	DPTrek-Experience	Receiving promotional notifications.	1. Reject using such application 2. Report such application
	Users are asked to sign up for notifications with no clear rejection option. [17]	DPTrek-Experiment		
	Persistent reminders to update the app pressure the user to install updates. [17]	DP Coping Test		
	Repeated location access prompts, only allowing dismissal if permission is given. [76]	DP Coping Test		
Sneaking	Unwanted magazine subscriptions added to shopping baskets. [20]	DPTrek-Experience	Unintended financial loss.	1. Reject using such application 2. Report such application 3. Be careful and remove extra items
	Items added to the shopping cart without user consent. [82]	DPTrek-Experiment		
	A 20% gratuity was added automatically to a restaurant bill. [17]	DP Coping Test		
	Hidden consent for non-essential cookies led to privacy violations. [21]	DP Coping Test		
Obstruction	Google made refusing cookies harder than accepting them. [22]	DPTrek-Experience	Pop up ads	1. Reject using such application 2. Report such application 3. Stay persistent through additional steps to deny consent or refuse options.
	The cookie banner made accepting cookies easier than denying them. [24]	DPTrek-Experiment		
	Misleading account settings made it harder to cancel subscriptions. [17]	DP Coping Test		
	Confusing wording in iOS 6 obscured the option to disable ad tracking. [17]	DP Coping Test		
Interface Interference	The Trump campaign used preselected recurring donations. [23]	DPTrek-Experience	Automatic selection leads to unintended email.	1. Reject using such application 2. Report such application 3. Uncheck default options.
	A default 20% tip was applied without clear notice. [17]	DPTrek-Experiment		
	ChatGPT users unknowingly allowed data usage for training. [17]	DP Coping Test		
	Preselected cookie options tricked users into accepting all cookies. [82]	DP Coping Test		
Forced Action	Users were forced to subscribe to a newsletter to create an account. [75]	DPTrek-Experience	Forced to receive emails and SMS.	1. Reject using such application 2. Report such application
	LinkedIn forced users to provide email addresses during registration. [19]	DPTrek-Experiment		
	Booking websites required personal information for registration. [17]	DP Coping Test		
	Marketing email opt-ins were hidden in terms and conditions. [78]	DP Coping Test		

Table 8: Participants' demographic information

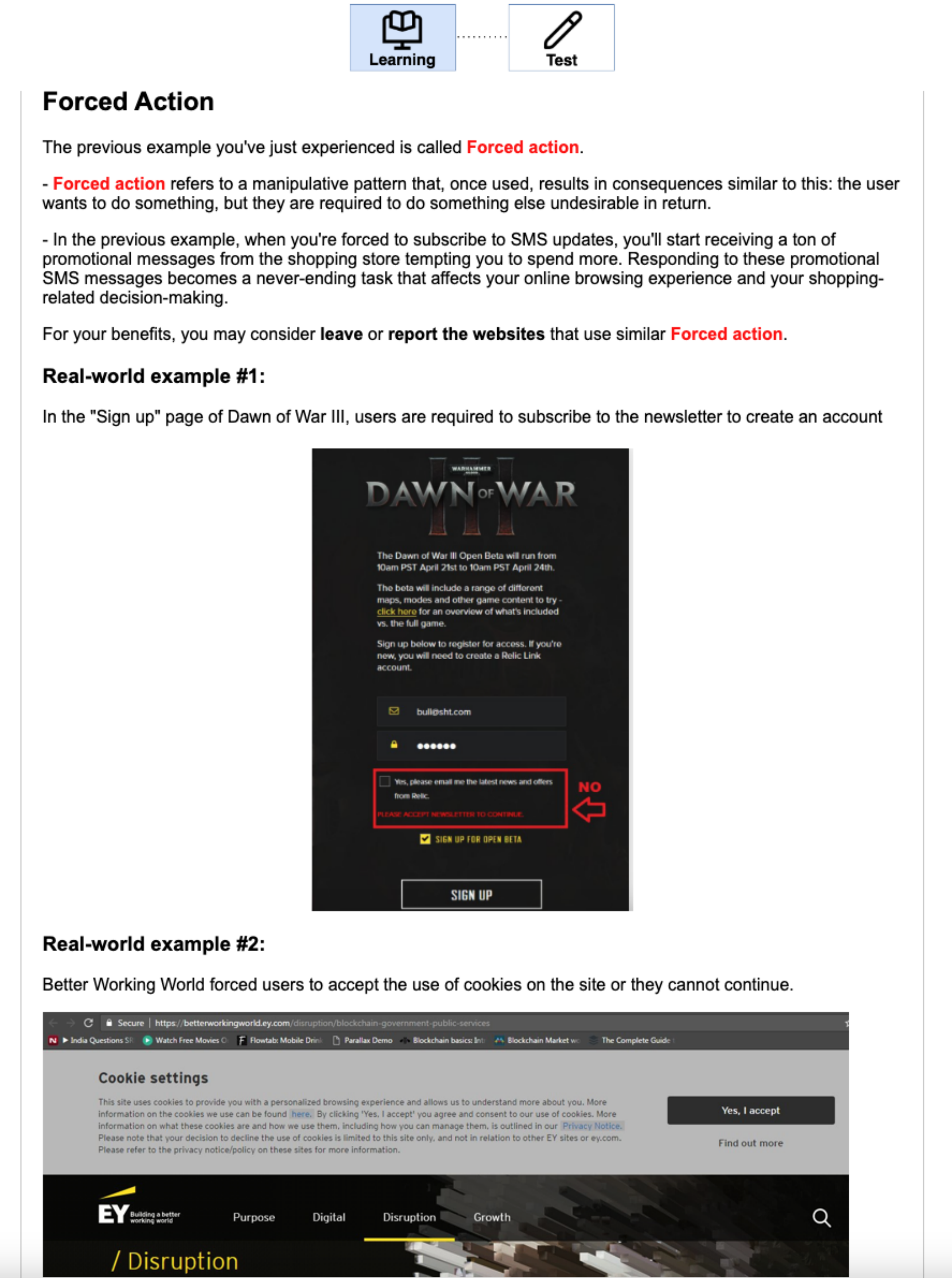
ID	Age	Gender	Race	Major	Education
Treatment Group					
1	51-60	Female	Caucasian	Intelligence Management	Master
2	23-25	Male	Caucasian	Cyber Security & Privacy	Master
3	31-35	Female	Asian	Education	Ph.D
5	23-25	Male	Asian	Computer Science	Master
6	18-22	Female	Asian	Computer Science	Master
7	26-30	Male	Asian	Computer Vision	Master
10	23-25	Male	Asian	Computer Science	Master
11	18-22	Female	Asian	Computer Science	Master
12	26-30	Female	African American	Psychology	Master
13	18-22	Male	Asian	Computer Science	Master
16	26-30	Male	Asian	Computer Science	Master
17	23-25	Male	Asian	Computer Science	Master
22	31-35	Male	Asian	Psychology	Ph.D
24	23-25	Female	Asian	Chinese	Master
25	23-25	Female	Asian	Computer Science	Master
27	23-25	Male	Asian	Computer Engineering	Master
30	18-22	Male	Asian	Computer Science	Bachelor
31	23-25	Female	Asian	Electrical Engineering	Master
38	23-25	Male	Asian	Mechanical Engineering	Master
Control Group					
4	18-22	Female	Asian	Computer Science	Master
8	23-25	Male	Asian	Computer Science	Master
9	26-30	Male	Asian	Psychology	Bachelor
14	23-25	Female	Asian	Computer Science	Master
15	18-22	Female	Asian	Computer Science	Master
18	23-25	Female	Asian	Computer Science	Master
19	26-30	Male	Asian	Computer Science	Master
20	23-25	Male	Caucasian	Computer Science	Bachelor
21	23-25	Female	Asian	Computer Science	Master
23	23-25	Male	Asian	Business Administration	Bachelor
26	26-30	Male	African American	Electrical Engineering	Master
28	23-25	Male	Asian	Computer Engineering	Bachelor
29	35-40	Female	Asian	Modeling & Simulation	Master
32	18-22	Male	Asian	Computer Science	Bachelor
33	23-25	Male	Hispanic	Film	Some College
34	23-25	Male	Asian	Computer Vision	Master
35	23-25	Female	Asian	Mathematics	Master
36	23-25	Male	Asian	Computer Science	Master
37	18-22	Female	African American	Psychology	Bachelor

Table 9: Constructs and items in the survey-based subjective evaluation of DPTrek

Construct	Items
Enjoyment [6, 66]	I had fun in the training. I found the training enjoyable. The actual process of the training was pleasant. The training experience was pleasurable.
Confidence [66]	I am confident of my ability to make sense of the dark pattern modules in the training materials. I am confident that I can identify different categories of dark patterns in real life. I believe that I can deal with dark patterns if I see them in the future.
Perceived Usability [6, 65].	I felt frustrated while taking this training. I found this training confusing to learn. Using this training was taxing.
Aesthetic Appeal [65]	This training was attractive. This training was aesthetically appealing. This training appealed to my senses.
Reward [65]	Taking this training was worthwhile. My experience with this training was rewarding. I felt interested in this training experience.
Attitude of Coping with DPs [7]	Coping with dark Pattern is unnecessary. Coping with dark pattern is wise. Coping with dark pattern is useful. Coping with dark pattern is not helpful. Coping with dark pattern is rewarding.
Perceived Risk of DPs [123]	In general, it would be risky to fall into dark patterns. There would be a high potential for loss if I fall into dark patterns. There would be too much uncertainty associated with falling into dark patterns. Dark patterns would create many unexpected problems.
Future Behavioral Intention [6]	I plan to take the training if such training is available in the future. I intend to continue to take the training if such training is available in the future. I expect the training to continue if such training is available in the future.

Table 10: Exit interview questions

Questions
What is your understanding of dark pattern now? Have you encountered this dark pattern before? Can you please describe the experience? Can you describe how it was displayed on the website? How did you notice it? How did you feel about it? How did the dark pattern influence your browsing experience? What do you think the company's objective is in designing such dark patterns? Have you tried to get rid of it? If no, why not? If yes, how did you get rid of it? Was it successful? If no, why not successful? If yes, any problem with your strategy? How do you feel about the training? And why? What did you learn from the training? What problems did you find in the training? What strategies did you learn today to identify dark patterns? What strategies did you learn to minimize the consequences of dark patterns? What difficulties did you encounter during the training? What can we do to improve the training? Any new concepts you learned from this training today? Do you remember the 5 categories of DPs? If no, why not? If yes, do you find them easy or difficult to understand? Which one is easy and which one is difficult? Do you think you understand the definitions of the 5 categories? If no, why not? If yes, do you find them easy or difficult to understand? Which one is easy and which one is difficult?



Forced Action

The previous example you've just experienced is called Forced action.

- Forced action refers to a manipulative pattern that, once used, results in consequences similar to this: the user wants to do something, but they are required to do something else undesirable in return.

- In the previous example, when you're forced to subscribe to SMS updates, you'll start receiving a ton of promotional messages from the shopping store tempting you to spend more. Responding to these promotional SMS messages becomes a never-ending task that affects your online browsing experience and your shopping-related decision-making.

For your benefits, you may consider **leave** or **report the websites** that use similar Forced action.

Real-world example #1:

In the "Sign up" page of Dawn of War III, users are required to subscribe to the newsletter to create an account

The Dawn of War III Open Beta will run from 10am PST April 21st to 10am PST April 24th.

The beta will include a range of different maps, modes and other game content to try - click here for an overview of what's included vs. the full game.

Sign up below to register for access. If you're new, you will need to create a Relic Link account.

bull@sht.com

●●●●●●

□ Yes, please email me the latest news and offers from Relic.

PLEASE ACCEPT NEWSLETTER TO CONTINUE.

☑ SIGN UP FOR OPEN BETA

Real-world example #2:

Better Working World forced users to accept the use of cookies on the site or they cannot continue.

Secure | https://betterworkingworld.ey.com/disruption/blockchain-government-public-services

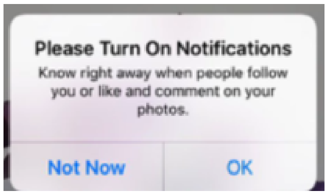
Cookie settings

This site uses cookies to provide you with a personalized browsing experience and allows us to understand more about you. More information on the cookies we use can be found here. By clicking 'Yes, I accept' you agree and consent to our use of cookies. More information on what these cookies are and how we use them, including how you can manage them, is outlined in our Privacy Notice. Please note that your decision to decline the use of cookies is limited to this site only, and not in relation to other EY sites or ey.com. Please refer to the privacy notice/policy on these sites for more information.

Figure 10: An example of learning material

B DP Knowledge Quiz (the correct answers are bolded)

Example 1



Please Turn On Notifications

Know right away when people follow you or like and comment on your photos.

Figure 11: Quiz Image 1

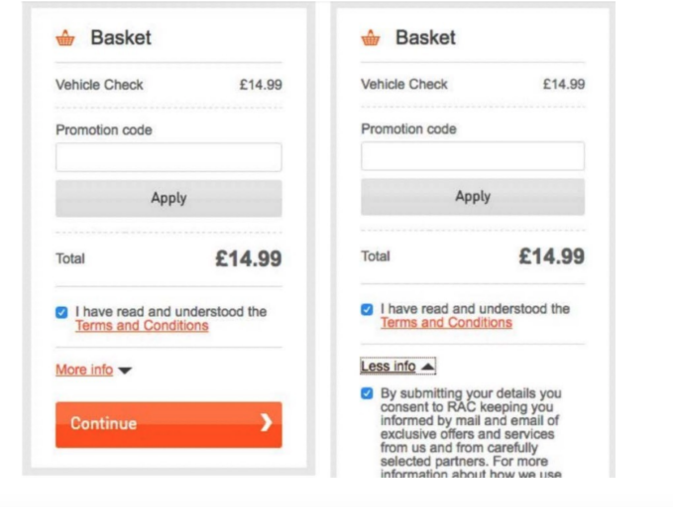
Q1: What will happen in this example?

- A. If I click 'Not Now', the notification will pop up again and again
- B. If I choose 'OK', I will receive tons of messages
- **C. Both A and B**
- D. Neither A nor B
- E. I don't know

Q2: To which kind of dark pattern does this example belong?

- A. Forced Action
- B. Obstruction
- C. Interface Interference
- D. Sneaking
- **E. Nagging**
- F. I don't know

Example 2



Basket

Vehicle Check £14.99

Promotion code

Total £14.99

☑ I have read and understood the Terms and Conditions

Basket

Vehicle Check £14.99

Promotion code

Total £14.99

☑ I have read and understood the Terms and Conditions

☑ By submitting your details you consent to RAC keeping you informed by mail and email of exclusive offers and services from us and from carefully selected partners. For more information about how we use

Figure 12: Quiz Image 2

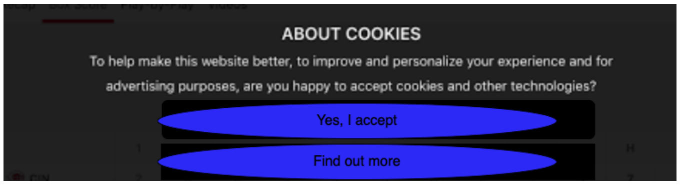
Q3: What will happen in this example?

- A. If I click 'Continue', I will not receive mail and email about exclusive offers
- **B. If I click 'Continue', I will receive mail and email about exclusive offers**
- C. Clicking 'More info' won't tell me that I will receive mail and emails after paying
- D. All of the above
- E. I don't know

Q4: To which kind of dark pattern does this example belong?

- A. Forced Action
- B. Obstruction
- C. Interface Interference
- **D. Sneaking**
- E. Nagging
- F. I don't know

Example 3



ABOUT COOKIES

To help make this website better, to improve and personalize your experience and for advertising purposes, are you happy to accept cookies and other technologies?

Figure 13: Quiz Image 3

Q5: What will happen in this example?

- A. I can continue browsing if I don't click 'Yes, I accept'
- B. If I click 'Yes, I accept', I will leave the website
- **C. If I click 'Yes, I accept', I might see personalized ads on the websites**
- D. If I click 'Yes, I accept', my browsing data won't be collected
- E. I don't know

Q6: To which kind of dark pattern does this example belong?

- **A. Forced Action**
- B. Obstruction
- C. Interface Interference
- D. Sneaking
- E. Nagging
- F. I don't know

Example 4

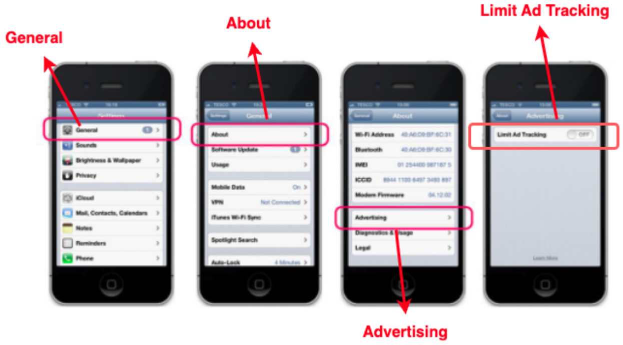


Figure 14: Quiz Image 4

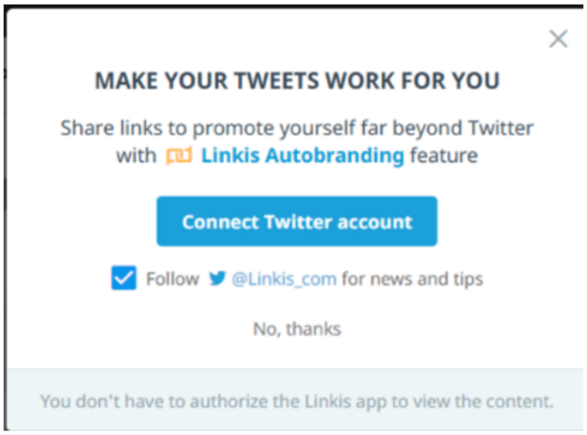
Q7: What will happen in this example?

- **A. If I want to stop personalized ads, I need to go through at least four pages in the app.**
- B. I can stop personal ads in only one page
- C. In the 'General' settings, I can not find the way to stop personalized ads
- D. I cannot stop personal ads
- E. I don't know

Q8: To which kind of dark pattern does this example belong?

- A. Forced Action
- **B. Obstruction**
- C. Interface Interference
- D. Sneaking
- E. Nagging
- F. I don't know

Example 5



MAKE YOUR TWEETS WORK FOR YOU

Share links to promote yourself far beyond Twitter with Linkis Autobranding feature

Connect Twitter account

☑ Follow @Linkis_com for news and tips

No, thanks

You don't have to authorize the Linkis app to view the content.

Figure 15: Quiz Image 5

Q9: What will happen in this example?

- **A. If I click 'Connect Twitter Account', Linkis_com promotion ads will appear in my Twitter account.**
- B. If I click 'Connect Twitter Account', Linkis_com promotion ads will not appear in my Twitter account.
- C. I will receive news and tips if I uncheck the 'Follow Linkis_com for news and tips' option.
- D. None of the above.
- E. I don't know.

Q10: To which kind of dark pattern does this example belong?

- A. Forced Action
- B. Obstruction
- **C. Interface Interference**
- D. Sneaking
- E. Nagging
- F. I don't know