Prevalence and User Perception of Dark Patterns: A Case Study on E-Commerce Websites of Bangladesh

Yasin Sazid and Kazi Sakib
Institute of Information Technology, University of Dhaka, Dhaka, Bangladesh

Keywords: Dark Patterns, Data Analysis, Dataset, Bangladesh, E-Commerce, User Perception, Categorization.

Abstract: Dark patterns are deceptive design tactics that impact user decision-making. Such tactics can harm user's finances, privacy, and lifestyle. Researchers have explored dark patterns from different perspectives in recent times. However, most of the work have been conducted in western countries. As dark patterns involve people and their psychology, explorations in other cultural contexts may generate novel insights. We carried out such a study in the local context of Bangladesh, focusing on the prevalence and user perception of dark patterns. We first examined Bangladeshi e-commerce websites for dark patterns using a combination of automated methods such as GPT-3's in-context learning and a novel segmentation algorithm, along with manual validation to address any limitations of the automated techniques. We also surveyed Bangladeshi university students about exposure, awareness, and concern regarding dark patterns. Based on the findings of both explorations, we ranked six dark pattern categories and subsequently divided them into two novel groups with distinct traits. We also found that educational background in technology make users more aware and concerned about dark patterns. 18.3% of the websites we analyzed in this study contained dark patterns, indicating prevalence of such design practices in e-commerce websites of Bangladesh.

1 INTRODUCTION

Dark patterns (DP) are user interface design tactics that deceive users to alter their decision-making by abusing knowledge of psychology (Gray et al., 2018). For example, 'Forced Action' is such a dark pattern where users are forced to perform an undesirable action to access some other functionality. Such design tactics can harm users financially, privacy-wise, and even in the form of addiction (Mathur et al., 2021). As a result, it is imperative to characterize and investigate these tactics thoroughly.

Existing research on dark patterns and user perception has primarily focused on Europe and the United States. However, research efforts in other local contexts may generate novel insights because of cultural and linguistic differences (Hidaka et al., 2023). Thus, further efforts are needed to analyze dark pattern data as well as user perception in a local context like Bangladesh.

As a developing country, Bangladesh has rapidly embraced digitalization. As a result, its e-commerce sector has experienced significant growth in recent years as well. However, this growth also brings the risk of dark patterns that can harm the increasing number of online users. Studying dark patterns in the e-commerce industry of Bangladesh can help us understand how much local users are exposed to these manipulative design tactics. Understanding local user perception regarding dark patterns is also an important area to explore.

Dark patterns can have varying representations in user interfaces, making it difficult to identify and analyze related data on a large scale. As identification methods of dark patterns are still in the early stages, there have been only a few efforts in collecting and analyzing dark pattern data on a large scale. Mathur et al. conducted the first exploration of textual dark pattern data in a large sample of 11,000 shopping websites, extracting 1,818 instances of dark pattern texts (Mathur et al., 2019). Yada et al. extended their exploration to extract 1,178 non dark pattern texts from the same websites (Yada et al., 2022).

Understanding user perception of dark patterns is another relevant area of research, as these design tactics abuse user psychology. Geronimo et al. found that users struggle to recognize dark patterns, emphasizing the need for improved awareness mechanisms (Geronimo et al., 2020). Bongard-Blanchy et al. discovered that users can identify dark patterns but are

Sazid, Y. and Sakib, K.
Prevalence and User Perception of Dark Patterns: A Case Study on E-Commerce Websites of Bangladesh.
DOI: 10.5220/0012734900003687

In *Proceedings of the 19th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2024)*, pages 238-249
ISBN: 978-989-758-696-5; ISSN: 2184-4895

often unaware of their harmful consequences, with demographic factors influencing user perception as well (Bongard-Blanchy et al., 2021). Gray et al. revealed that users can sense manipulation, even without precise terminology to describe such experience (Gray et al., 2021). Maier found that users may initially react negatively to dark patterns but eventually get normalized to them, suggesting awareness alone might not be enough as a countermeasure (Maier, 2019). Hidaka et al. revealed that Japanese applications contain fewer instances of dark patterns compared to the United States (Hidaka et al., 2023). This finding emphasizes the necessity to analyze dark pattern data and user perception in different local contexts. No such exploration has been done yet in the local context of Bangladesh.

In this study, we analyzed the prevalence of dark patterns in e-commerce websites of Bangladesh. Member companies of the E-Commerce Association of Bangladesh (e-CAB) were selected to be analyzed to show the prevalence of dark patterns. We were able to analyze 715 websites and HTML contents from relevant webpages of those websites were extracted. A novel page segmentation algorithm was used to identify candidate dark pattern texts from the HTML contents. It was developed with a more relaxed inclusion criteria for candidate dark patterns compared to the segmentation algorithm developed by Mathur et al., resulting in improved detection of dark patterns (Mathur et al., 2019). Detection and classification of dark patterns involved a combination of automated and manual techniques. In-context learning capabilities of GPT-3 were used to detect dark patterns from the candidate texts according to our previous work (Sazid et al., 2023). A manual review was carried out to remove the false positives and classify the texts into different dark pattern categories.

We complemented our work on the prevalence of dark patterns with an empirical study on user perception of dark patterns. A survey was conducted with Bangladeshi university students of two groups - one with a background in technology education and the other without such a background. Participants were presented with user interface design instances of different dark pattern categories and then exposure, awareness, and concern ratings were collected for each dark pattern category.

We found 931 instances of dark patterns, 99 of which were unique instances. These dark pattern instances were classified into six common dark pattern categories, including 'Misdirection', 'Urgency', 'Scarcity', 'Social Proof', 'Obstruction', and 'Forced Action'. The 931 dark pattern instances belonged to 131 different websites, which is roughly 18.3% of the 715 e-commerce websites analyzed in this study. Average ratings of awareness and concern across all dark pattern categories show that users are aware of the influences of dark patterns and are concerned about such design tactics in general. Based on the findings from the user perception survey and the prevalence data across dark pattern categories, we divided the categories into two distinct groups - 'Passive Dark Patterns' containing 'Social Proof', 'Urgency', and 'Scarcity' categories and 'Active Dark Patterns' containing 'Forced Action', 'Obstruction', and 'Misdirection' categories. We found distinct characteristics of these two groups in terms of prevalence, user awareness, and concern. User perception survey also revealed that users with a background in technology education were more aware and concerned about dark patterns than users with no such background.

The main contributions of this study can be summarized as follows:

- Analysis of the prevalence of dark patterns in e-commerce websites of Bangladesh
- Novel page segmentation algorithm that extracts candidate dark pattern texts from HTML contents of webpages
- Collection of a dark pattern dataset containing 99 unique text instances labelled with different dark pattern categories
- Ranking dark pattern categories in terms of user exposure, awareness, and concern
- Novel grouping of dark pattern categories according to their approach of abusing user psychology
- Revealing the influence of technology education (i.e., computer science or related fields) on user awareness and concern regarding dark patterns

2 RELATED WORK

Dark patterns have attracted a lot of attention from researchers in recent times. Researchers have worked on the definition and classification of dark patterns (Gray et al., 2018) (Mathur et al., 2019), explored legal and policy-making perspectives (Luguri and Strahilevitz, 2019), and studied user perception of dark patterns (Geronimo et al., 2020). Detection techniques (Mansur et al., 2023) (Stavrakakis et al., 2021) and data collection efforts (Mathur et al., 2019) regarding dark patterns have also been explored. This section provides an overview of past literature on taxonomy, data collection and analysis, and user perception of dark patterns.

2.1 Taxonomy of Dark Patterns

Dark patterns have versatile representations in user interfaces, making it very challenging to define and classify them under a holistic taxonomy. Brignull et al. first defined the term 'dark patterns' as a set of "tricks used in websites that make a user do things that the user did not mean to" (Brignull et al., 2023). Researchers since have tried to define and classify dark patterns in various ways. Gray et al. classified dark patterns into five distinct categories based on user experience - 'Nagging', 'Obstruction', 'Sneaking', 'Interface Interference' and 'Forced Action' (Gray et al., 2018). Some researchers have classified dark patterns specifically based on privacy (Jarovsky, 2022) (Bösch et al., 2016). Other researchers have also studied dark patterns found on social media (Roffarello and Russis, 2022) and video streaming platforms (Chaudhary et al., 2022).

Mathur et al. mentioned seven broad categories of dark patterns in their work (Mathur et al., 2019). These dark pattern categories are briefly discussed below:

- **Urgency** refers to the category of dark patterns that enforce a time limit on a sale or offer, prompting users to make decisions and purchases quickly.
- **Misdirection** refers to the category of dark patterns that employ visuals, language, and emotions to influence users towards or away from specific choices.
- **Social Proof** refers to the category of dark patterns that accelerate user decision-making and purchases, by showing the actions and behaviours of other users.
- **Scarcity** refers to the category of dark patterns that indicate the limited availability or high demand of a product, thereby increasing its perceived value and desirability.
- **Obstruction** refers to the category of dark patterns that intentionally complicate a specific action beyond what is necessary to discourage users from taking that action.
- **Forced Action** refers to the category of dark patterns that require users to perform an additional action, which is often undesirable, to accomplish some other tasks.
- **Sneaking** refers to the category of dark patterns aimed at misrepresenting user actions or concealing/delaying information that users would probably oppose if they were aware of it.

2.2 Dark Pattern Related Data

Dark pattern data collection efforts rely heavily on the successful detection of such deceptive tactics in websites. However, it is a challenging task, especially without a holistic definition and classification of dark patterns. This is also a relatively new field of research, and detection methods are yet to be matured. As a result, there have been very few efforts to collect dark pattern data on a large scale. Another challenge in such data collection efforts is determining the appropriate format (image, video, text, etc.) to represent dark patterns.

Researchers have collected dark patterns in various formats, including video recordings (Geronimo et al., 2020), screenshots (Mansur et al., 2023), extracted features (Soe et al., 2022), and textual data (Yada et al., 2022) from user interfaces, each with its own advantages and disadvantages. Geronimo et al. prepared a comprehensive video dataset comprising screen recordings of mobile application usage (Geronimo et al., 2020). The dataset contains 15 videos, accompanied by classifications of identified dark patterns at different timestamps within the videos. Mansur et al. created a dark pattern dataset containing 501 instances by manually labelling user interface screenshots collected from different sources (Mansur et al., 2023). Soe et al. analyzed dark patterns in cookie banners of 300 news websites (Soe et al., 2020). For each cookie banner, they manually extracted a set of features (location within the page, clarity of options, site works after rejecting cookies or not, number of clicks needed to reject all cookies, etc.) in terms of dark patterns. However, data collection and analysis efforts using video recordings, screenshots, or manually extracted features are quite challenging to carry out on a large scale. Alternatively, textual data collection and analysis are more convenient in terms of scalability.

Mathur et al. collected the first large-scale textual dark pattern data (Mathur et al., 2019). They analyzed more than 11,000 e-commerce websites and extracted meaningful text segments using their page segmentation algorithm. Even though they collected text segments using automated techniques, dark pattern detection and classification were carried out manually, which is a time-consuming task. To ease the manual labelling of a large number of text segments, they used hierarchical clustering in their work. They found 1,818 instances of dark pattern texts from 1,254 websites, which was roughly 11.1% of all analyzed websites in their work. Yada et al. extended this textual dataset of dark patterns by adding 1,178 non dark pattern texts from the same websites (Yada et al., 2022).

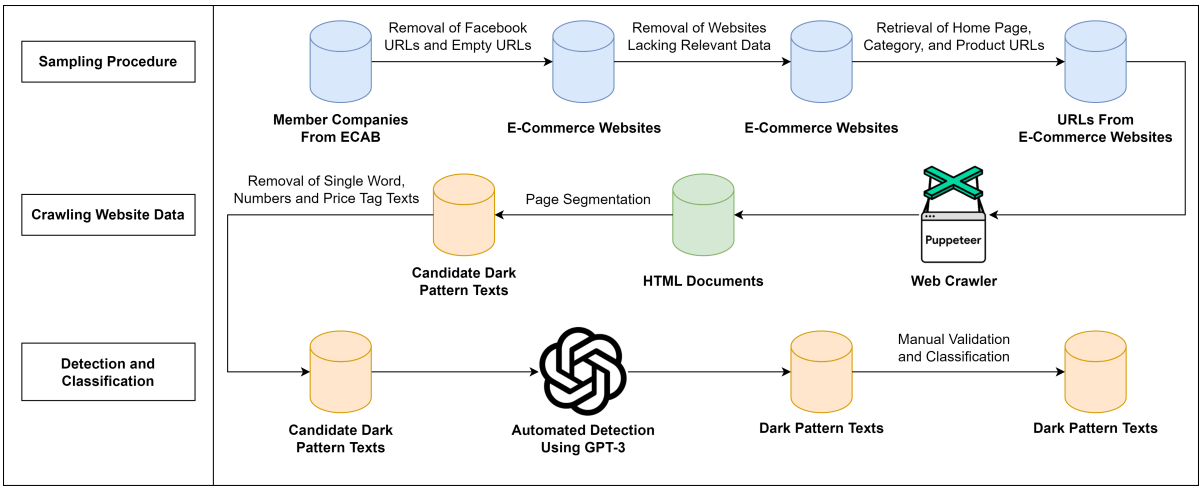


Figure 1: Overview of Dark Pattern Data Collection.

2.3 User Perception of Dark Patterns

As dark patterns abuse user psychology and manipulate their decision-making, user perception regarding the phenomenon is a significant area of research. Geronimo et al. studied user awareness and their ability to recognize dark patterns found within popular mobile applications (Geronimo et al., 2020). Their efforts revealed that users often struggle to identify dark patterns, highlighting the necessity to improve user awareness mechanisms. Bongard-Blanchy et al. investigated user awareness, and their capability to recognize and resist dark patterns (Bongard-Blanchy et al., 2021). They found that users can recognize dark patterns even though they are often unaware of the actual harmful consequences. Their study also identified that demographic factors such as age and educational background can influence user perception of dark patterns.

Gray et al. conducted a survey on English and Mandarin Chinese-speaking participants to explore users' experiences of feeling manipulated by digital technologies, their emotional responses to such experiences, and their awareness of manipulative design practices (Gray et al., 2021). Their findings indicate that users often have a sense that something is "off" or manipulative, even when they lack the precise language to describe it. Maier investigated how users perceive, experience, and respond to dark patterns (Maier, 2019). His findings suggest that while users may initially be angered by dark patterns, they often become accustomed to them over time. This leads to the normalization of these deceptive design practices. His work also highlights that awareness mechanisms alone may not be sufficient to safeguard users from dark patterns.

Most research efforts in analyzing dark patterns and related user perception have been mainly conducted in Europe and the United States. Hidaka et al. termed these works as coming from the 'Western context' and argued that the 'Eastern context' might be different because of cultural and language differences (Hidaka et al., 2023). Their work also revealed fewer dark patterns in Japanese applications (i.e., the Eastern context) compared to the Western context. Thus, further efforts are needed to analyze dark pattern data as well as user perception in a local context like Bangladesh. Such efforts are especially crucial for local policy-making that can protect users from the harmful consequences of dark patterns.

3 DARK PATTERNS IN E-COMMERCE OF BANGLADESH

In this study, we extracted dark patterns from e-commerce websites of Bangladesh to analyze the local context and show the prevalence of such design tactics in local e-commerce websites. We started our exploration by defining a sampling frame for local e-commerce websites, followed by automated crawling of relevant website data. The crawled textual data was then processed using a combination of automated and manual methods to retrieve dark pattern texts across different categories. Figure 1 provides an overview of the different stages of data collection carried out for this purpose. The resulting dataset of dark patterns and other technical artifacts associated with this study are publicly available on GitHub[1].

[1]https://github.com/bsse1006/dark-patterns-bangladesh

3.1 Sampling Procedure

The sampling frame for this study is derived from the membership list of the E-Commerce Association of Bangladesh (e-CAB)[2], which is a Bangladeshi local organization that has 2,000+ e-commerce companies as members. The members' list of e-CAB is the largest available representative sample of Bangladeshi e-commerce companies. Thus, we considered this list as our sampling frame for this study.

Upon inspecting the members' list of e-CAB available online at 'https://e-cab.net/member-list', we found a general pattern in webpage URLs associated with each e-CAB member profile - 'https://e-cab.net/company-profile/<member id>', where <member id> refers to the numbers '0001' to '2238' which are distinct member id numbers associated with each e-CAB member companies. We used the Javascript library 'puppeteer' to crawl the 'company name' and 'website URL' data for each e-CAB member company from their associated member profile pages using this general URL pattern. As some member profile pages were unavailable, we were able to collect data for 2,216 member companies of e-CAB. Two exclusion criteria were applied to these 2,216 instances of data - (1) 104 companies were removed because their associated 'website URL' data contained URLs of Facebook pages, not of company websites, and (2) 57 companies were removed for not having any specified 'website URL' at all. After excluding these companies, we considered a total of 2,055 e-commerce websites for further inspection.

3.2 Crawling Website Data

We crawled the e-commerce websites to extract text segments from them. We first manually examined all the websites to collect and store relevant URLs, followed by automatically crawling the HTML contents from those URLs. Subsequently, we applied a page segmentation algorithm to the HTML contents to identify text segments for further inspection.

3.2.1 URL Retrieval

We tried to manually visit the home or landing page of all of the 2,055 company websites. However, 650 websites were unreachable. We inspected the remaining 1,405 websites to collect two additional URLs alongside the home page URL from each website. For product-based companies, we navigated to one category page and one product page per website. And for service-based companies, we navigated to the offered services page and the portfolio page. In this way, we manually inspected all the websites and tried to collect URLs of the home page, one category/services page, and one product/portfolio page. Two exclusion criteria were applied - (1) websites that were static pages with no further navigation available, and (2) websites that lacked relevant information. These exclusion criteria reduced the number of websites to 715 and 2,119 URLs were collected from these websites.

3.2.2 HTML Data Retrieval

We again used the Javascript library 'puppeteer' to crawl the 2,119 URLs and retrieve the whole HTML content associated with each URL. Some websites detected our 'puppeteer' crawler as a bot and restricted it from accessing the original HTML content. We used the 'puppeteer-extra-plugin-stealth' library to bypass this bot detection. This library conceals certain properties from outgoing HTTP requests that can flag the requests as coming from a bot. HTML contents of 51 URLs could not be retrieved because of connection and navigation problems. We were able to collect the HTML contents of the remaining 2,068 URLs.

3.2.3 Candidate Dark Pattern Extraction

Text segments need to be extracted from HTML contents that we call 'Candidate Dark Patterns'. For this purpose, we needed a segmentation algorithm to analyze webpages and identify candidate dark patterns. Mathur et al. proposed such a segmentation algorithm, where segments are defined as visible HTML elements that contain no other block-level elements and at least one text element (Mathur et al., 2019). Using this algorithm led to the discovery of very few dark patterns in the HTML contents. We explored the causes and found that the algorithm was too restrictive, discarding potential dark pattern texts.

We modified the segmentation algorithm to make the inclusion criteria as relaxed as possible. We defined segments as any visible HTML element that is a leaf (i.e., does not contain any child elements) and contains text content. However, we exclude paragraph elements from this definition, as they usually represent longer blocks of descriptive text that are not relevant to our analysis. Details of our page segmentation algorithm are illustrated in Algorithm 1.

This version of the segmentation algorithm resulted in the discovery of both, increased candidate dark patterns and subsequently increased dark patterns. So we used this algorithm to extract candidate dark pattern texts from the HTML contents obtained in the previous step. 770,570 texts was extracted from the 2,068 HTML contents under analysis.

[2]https://e-cab.net

Algorithm 1: Page Segmentation.

```
Input: HTML Document
Output: List of Text Segments
Function extractTextSegments(page):
    ignoredElements ← ["p", "script",
      "style", "noscript", "br", "hr"];
    segmentsList ← [];
    foreach element in page do
        if element is not in ignoredElements
          and element is visible and element
          does not contain any child elements
          then
            innerText ← element.innerText;
            segmentsList.append(innerText);
        end
    end
    return segmentsList;
```

3.3 Detection and Classification

It is a time-consuming task to detect dark patterns by manually reviewing the large set of 770,570 texts. Thus, we employed a combination of automated and manual approaches to detect and classify dark pattern texts from the candidate texts. Dark pattern texts were first detected using an automated approach leveraging machine learning, followed by a manual review of each text and associated URLs to remove the false positives and classify the remaining texts into different dark pattern categories.

3.3.1 Data Preprocessing

We removed candidate dark pattern texts that consisted of only numbers or a single word. We also removed price tag texts containing the local currency sign, using regular expressions. This preprocessing reduced the set of candidate dark pattern texts by 43% to 435,536 texts. Removing the duplicates would reduce the set even further. However, multiple websites or multiple webpages within the same website can contain the same dark pattern text. Thus, removing duplicates would deny us the real scenario of dark patterns in the e-commerce websites of Bangladesh. As a result, we opted not to remove the duplicates in this step.

3.3.2 Automated Dark Pattern Detection

We used machine learning to automatically classify the candidate texts as 'dark pattern' or 'not dark pattern'. Yada et al. provided some baseline machine learning models that could be used for this purpose (Yada et al., 2022). Initially, we used their best-performing model ($RoBERTa_{large}$), trained on 1,178 dark pattern and the same number of non dark pattern texts provided in their dataset. The hyper-parameters were set according to their work. However, this approach resulted in a large number of false positives. As a result, the subsequent manual verification would be time-consuming, undermining the purpose of automated detection. Upon inspecting for causes behind high false positives, we found the model to be vulnerable to data overfitting.

Our previous work developed an automated detection technique that could detect dark patterns without the need for training data, thus eliminating the concern regarding data overfitting (Sazid et al., 2023). This approach utilized the in-context learning capabilities of GPT-3 to detect dark pattern texts. The best-performing model from this work was the few-shot model where two example texts per category were used along with the category definitions to engineer prompts for GPT-3. This approach was able to detect six common categories of dark pattern texts successfully - 'Misdirection', 'Urgency', 'Scarcity', 'Social Proof', 'Obstruction', and 'Forced Action'. As the approach using in-context learning resulted in a very low rate of false negatives (under 10%) in our previous work, we reused this approach to detect dark pattern texts from the candidate texts obtained in the previous step. To optimize resource usage, we only considered the unique texts in this step. We also treated texts with numerical variations (e.g., 'Only 4 left in stock' and 'Only 1 left in stock') as duplicates, ensuring that similar texts are not processed by GPT-3 separately. There were 91,585 such unique texts among the set of 435,536 candidate texts. Our automated approach detected 2,185 out of those 91,585 texts as dark patterns.

3.3.3 Manual Dark Pattern Classification

We manually reviewed each of the 2,185 dark pattern texts to check whether they were really instances of dark patterns or not. We discarded 2,086 instances as they did not belong to any dark pattern category considered in this study. We reviewed each of the remaining 99 instances to classify them into the six dark pattern categories. During the review, if the textual data was insufficient for labelling, we manually visited the associated URL to gather context about the text. This resulted in a dataset of dark patterns containing 99 unique text instances labelled with their respective dark pattern categories. As we only considered the unique texts in the previous step, we revisited the set of 435,536 candidate texts to extract and label the duplicates matching the 99 unique dark pattern texts. Numerical variations were also treated as

similar texts in the previous step. Thus, we labelled all such groups of texts with the same dark pattern category. After considering the duplicates and numerical variations, the final set of dark patterns consisted of 931 instances.

4 EMPIRICAL STUDY ON USER PERCEPTION

We conducted an empirical study to analyze user perception regarding the presence of dark patterns in e-commerce websites of Bangladesh. The goal was to analyze and rank the dark pattern categories according to users' exposure, awareness about influence, and concern. We also wanted to see if there is any difference in user perception based on whether they had an educational background in technology or not.

4.1 Study Design

An open survey was conducted, directed primarily at Bangladeshi university students. Participants were first asked about their general understanding of the ability of user interface designs to influence user's decision-making, followed by the frequency of their usage of e-commerce websites and applications. Later, participants were presented with six user interface design instances containing dark patterns from the six categories mentioned in the previous section. Presenting only dark pattern instances could bias the participants in favour of a negative perception regarding the design instances. To counteract that possibility, four non dark pattern design instances were also presented in the survey. The ten user interface design instances presented in this survey are illustrated in Figure 2. Participants were presented with these design instances in a random order and three ratings were measured for each design. 'Exposure' rating was measured based on whether the participant had ever encountered such a design or not (0 = never encountered, 1 = encountered). To measure 'Awareness' and 'Concern' ratings, the following two statements were presented respectively:

- This kind of design can influence users to do something that users normally would not do.
- I am worried about the influence of this kind of design on users' decision-making and choices.

Participants were instructed to rate their agreement on a 5-point Likert scale (from 1 = strongly disagree to 5 = strongly agree). In addition, demographic information (age, sex, and educational background) was collected from the participants. All questions in the survey were mandatory.

4.2 Participants

We collected responses from 68 participants. The demographics of the participants were as follows: 45 male, 23 female. Their age ranged from 19 to 27 years (mean 22.57, SD 1.47). Participants were divided into two groups based on their educational background - 36 participants had an educational background in computer science or related fields and the other 32 had no such background in technology education. Our thinking behind such grouping is that participants with an educational background in technology might have a different perception regarding dark patterns than the ones without such a background.

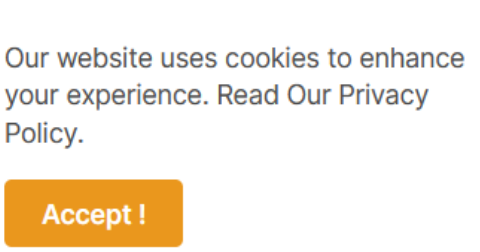
5 RESULTS

This section analyzes and discusses our findings regarding the prevalence of dark patterns in e-commerce websites of Bangladesh as well as the user perception survey.

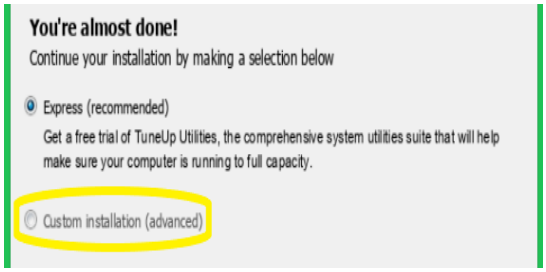
5.1 Prevalence of Dark Patterns

We analyzed the collected 931 dark pattern texts to showcase the prevalence of dark patterns in e-commerce websites of Bangladesh. These dark pattern texts were found across 131 websites, constituting approximately 18.3% of the 715 analyzed e-commerce websites. This is a much higher rate compared to the work of Mathur et al., who found dark patterns in 11.1% of their analyzed websites (Mathur et al., 2019). The increased rate can be credited to our use of a more relaxed page segmentation algorithm than theirs, resulting in improved detection of dark patterns. It is important to note that we exclusively analyzed the home page, one category/services page, and one product/portfolio page per website and our analysis only focused on the texts of these pages. Given the scope of our exploration, this finding serves as a conservative estimate. As a result, it can be said that the actual prevalence of dark patterns in the e-commerce websites of Bangladesh is even higher.

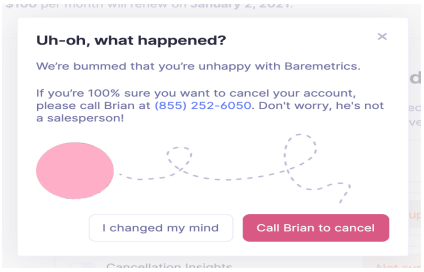
Figure 3 illustrates the frequency of each dark pattern category. 'Social Proof' and 'Urgency' had the highest number of instances among all the categories with 466 and 271 occurrences respectively. 165 instances belonged to the 'Scarcity' category while 'Forced Action' and 'Misdirection' had 23 and 6 occurrences respectively.



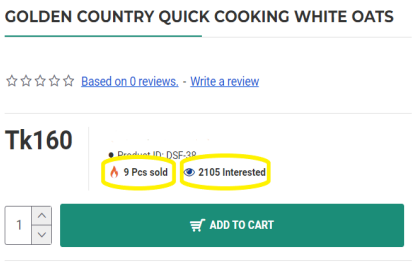
(a) Forced Action.



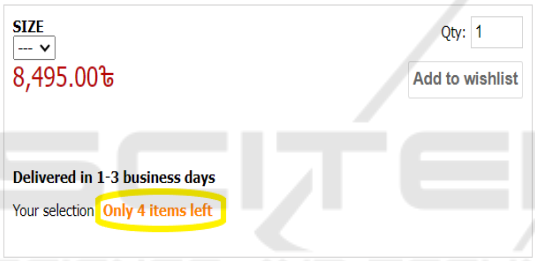
(b) Misdirection.



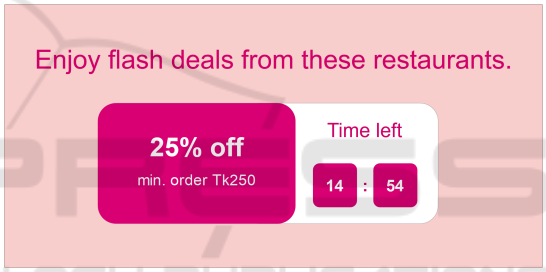
(c) Obstruction.



(d) Social Proof.

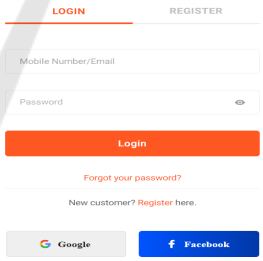


(e) Scarcity.

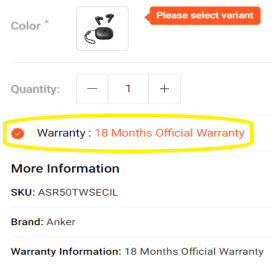


(f) Urgency.

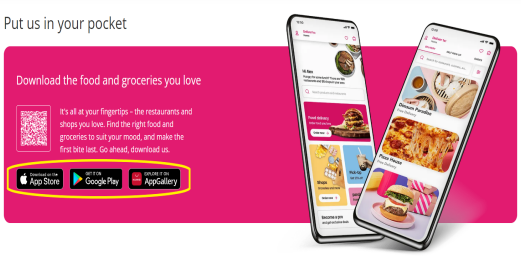
(g) Not Dark Pattern.



(h) Not Dark Pattern.



(i) Not Dark Pattern.



(j) Not Dark Pattern.

Figure 2: User Interface Design Instances Used in This Study.

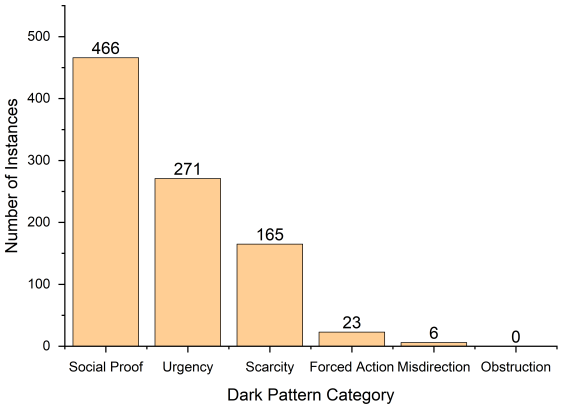


Figure 3: Instances Across DP Categories.

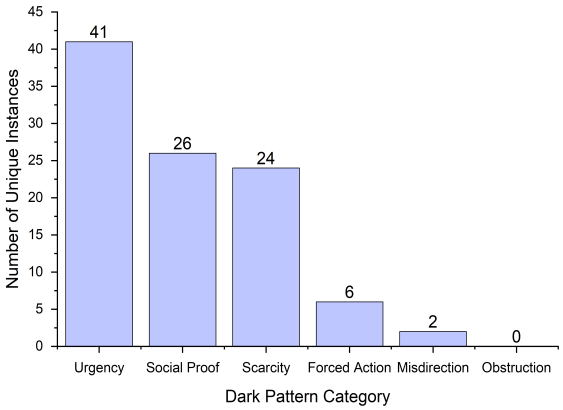


Figure 4: Unique Instances Across DP Categories.

Figure 4 illustrates the number of unique instances across each dark pattern category. 'Urgency' tops the other categories in this regard, with 41 unique instances. 'Social Proof' and 'Scarcity' had 26 and 24 unique instances respectively while 'Forced Action' and 'Misdirection' had only 6 and 2 respectively. No instance of the 'Obstruction' category was found in the study. We compared this prevalence of unique dark pattern texts across categories with the findings of Mathur et al., who also gathered unique instances of dark pattern texts in their work (Mathur et al., 2019). While the rankings of dark pattern categories in terms of prevalence do not perfectly align between the two studies, two distinct groups emerge. Both analyses indicate that 'Urgency', 'Social Proof', and 'Scarcity' (Group A) had the highest number of unique instances, while 'Forced Action', 'Misdirection', and 'Obstruction' (Group B) had relatively fewer unique instances. As a result, we can say that Group A dark patterns were more prevalent in our analysis than Group B dark patterns.

Figure 5 also confirms such a grouping of dark pattern categories in terms of prevalence across websites. 'Urgency', 'Scarcity', and 'Social Proof' had the more prominent presence, with occurrences on 78, 28, and 26 websites respectively. 'Forced Action', 'Misdirection', and 'Obstruction' were much less prominent, with occurrences on only 7, 2, and 0 websites respectively. Interestingly, 121 of the 131 websites were associated with a single dark pattern category, with the remaining 10 being associated with at most two dark pattern categories.

Figure 6 illustrates the frequency of dark patterns across the 131 websites. Most of the websites present only 1, 2, or 3 unique instances of dark patterns, whereas very few websites present larger quantities. The highest number of unique dark pattern texts on a single website is 10.

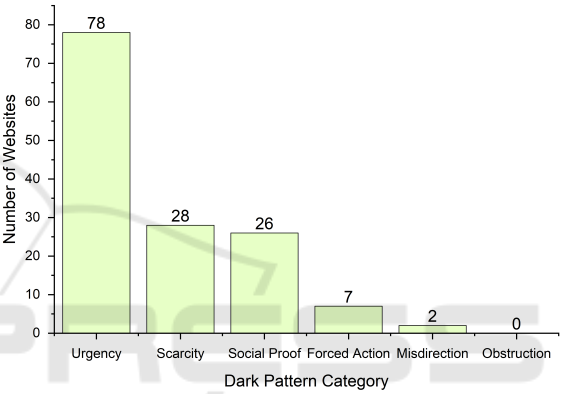


Figure 5: Websites Across DP Categories.

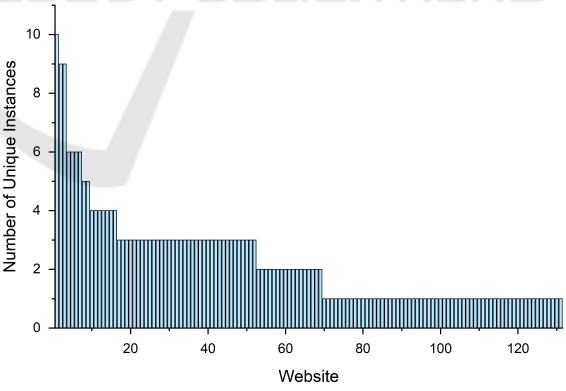


Figure 6: Unique Instances Across Websites.

5.2 User Perception of Dark Patterns

Based on the survey responses, we ranked and grouped the dark pattern categories in terms of exposure, awareness, and concern. We also carried out Mann-Whitney U test to see if there was any difference in user perception based on educational background in technology.

Table 1: Dark Pattern Category Rankings Based on User Perception.

Rank	Exposure		Awareness		Concern	
	DP Category	Mean Rating (%)	DP Category	Mean Rating (1 to 5)	DP Category	Mean Rating (1 to 5)
1	Forced Action	94.12	Urgency	4.21	Obstruction	3.81
2	Urgency	88.24	Scarcity	3.99	Forced Action	3.78
3	Scarcity	86.76	Social Proof	3.96	Urgency	3.56
4	Social Proof	77.94	Obstruction	3.96	Scarcity	3.44
5	Misdirection	73.53	Forced Action	3.81	Social Proof	3.22
6	Obstruction	30.88	Misdirection	3.65	Misdirection	3.17

5.2.1 Ranking Dark Pattern Categories

Survey data was analyzed to rank different categories of dark patterns based on users' ratings of exposure, awareness of their influence, and concern regarding them. The rankings were determined by calculating the mean ratings of exposure, awareness, and concern for each dark pattern category by averaging all participant responses. The resulting rankings are provided in Table 1. Notably, participants consistently rated their awareness and concern regarding dark patterns above the neutral value of 3, indicating a general awareness of the potential influences of dark pattern design instances and significant concern about them. However, the category rankings of awareness and concern do not perfectly align with each other, suggesting that participants were not necessarily more concerned about a design simply because they perceived it to be more influential, and vice versa.

5.2.2 Grouping Dark Pattern Categories

Exposure, awareness, and concern ratings produce further evidence in favour of our grouping of dark pattern categories in the previous section. There is a clear distinction in the ratings between the two groups of dark patterns. Participants were more exposed to Group A dark patterns than Group B, except for 'Forced Action'. Such a contrast in the exposure ratings makes more sense as they align directly with the prevalence of these two groups explained in the previous section. Participants found Group A containing 'Urgency', 'Scarcity', and 'Social Proof' categories more influential than Group B containing 'Misdirection', 'Obstruction', and 'Forced Action'. The reverse tendency is found in concern ratings as participants found Group B more concerning than Group A, except for 'Misdirection'.

The contrast between awareness and concern ratings across the two groups of dark pattern categories can be explained by how these design instances manifest themselves in user interfaces. Group A dark patterns get users' attention to certain actions using the attraction of limited sales or discounts, and the rarity or credibility of a product. Even though they can create a sense of hurry among users, the user experience is not necessarily unpleasant, resulting in less concern. On the other hand, Group B dark patterns make users feel uncomfortable as they get controlled, forced, or deceived by the user interface. As a result, users are more concerned about this group of dark pattern categories. According to this finding, we name Group A dark patterns as 'Passive Dark Patterns' and Group B dark patterns as 'Active Dark Patterns':

Passive Dark Patterns: This group of dark patterns consists of 'Urgency', 'Social Proof', and 'Scarcity' categories. All of these techniques use users' 'fear of missing out' (FOMO) and create a sense of attraction in users to take certain actions. They rely on social conformity and the perception of limited availability (time or quantity) to motivate users to take action quickly. The main identifying factor of these dark patterns is that they entice and attract users, rather than forcing them. Because of their subtle presentation in user interfaces, they do not seem abnormal to users, even when users think they have a high influence on their decision-making. As passive dark patterns have been 'normalized' to users, finding countermeasures for this group of dark patterns is more difficult and necessitates legal and policy conversations regarding marketing and advertisement strategies in general.

Active Dark Patterns: This group consists of 'Forced Action', 'Misdirection', and 'Obstruction' categories. These techniques manipulate user behavior through deception, obstacles, or coercion. These design instances forcefully drive users to act in ways that are against their wishes or interests. The main identifying factor of these dark patterns is that they mislead or force users to make certain choices. As a result, users often feel uncomfortable while encountering these dark patterns. These techniques undermine user autonomy and can lead to a negative user

Table 2: Results of Mann-Whitney U Test ($n1$=36, $n2$=32).

Variable	Mann-Whitney U Statistic	P Value	H_0 Rejected
Exposure	614	0.3184	No
Awareness	790	0.0042	Yes
Concern	739	0.0225	Yes

experience. Thus, this group of dark patterns does not fall into traditional marketing or advertisement strategies. Legal and policy regulations over design principles of online platforms can have a significant impact on counteracting these dark patterns.

Two deviations are visible in Table 1 from our analysis regarding the grouping of dark pattern categories - 'Forced Action' in the case of exposure ratings and 'Misdirection' in the case of concern ratings. We argue that these deviations are due to participant bias or misunderstanding about the particular design instances used in both cases. As shown in Figure 2a, participants were presented with a cookie banner featuring solely an 'Accept' button without a corresponding 'Reject' button, as an example of 'Forced Action'. The heightened frequency of responses indicating high exposure to 'Forced Action' could stem from participants' familiarity with cookie banners rather than the dark pattern design featuring only an 'Accept' button and lacking a 'Reject' button. As shown in Figure 2b, participants were presented with an installer interface containing two choices where one was recommended and the other was blurred, as an example of 'Misdirection'. Participants could have perceived such a recommendation as a helpful thing and not considered situations where such preselection and design interference could go against their interests; leading to less concern about this category.

5.2.3 Impact of Technology Education on User Perception of Dark Patterns

Mann-Whitney U test was used to see if there was any difference in user perception between participants who had an educational background in technology and participants who did not have such a background. For this purpose, ratings of exposure, awareness, and concern across all dark pattern categories were averaged to get mean exposure, awareness, and concern ratings for each participant, which were the three variables used in hypothesis testing. For each one of the three variables, the null and alternative hypotheses were as follows (CS = participants with an educational background in technology, NCS = participants with no educational background in technology):

- H_0: Ratings from CS participants are lower than or equal to that of NCS participants
- H_a: Ratings from CS participants are greater than that of NCS participants

Table 2 presents the results from the one-tailed Mann-Whitney U test (level of significance, α = 0.05). While the null hypothesis could not be rejected for exposure, it was rejected for awareness and concern; indicating statistically significant evidence that participants with an educational background in technology are more aware and concerned about dark patterns than participants without such a background.

6 THREATS TO VALIDITY

This section discusses the potential threats that may affect the validity of the study.

Threats to External Validity: The selection of the e-CAB members' list as the sampling frame poses an external validity threat as not all e-commerce websites of Bangladesh are members of e-CAB. However, this is the largest possible representative sample of e-commerce websites originated in Bangladesh. Analyzing a few URLs per website also poses a threat, as other URLs may produce different results. However, e-commerce websites generally have similar user interface designs across category/services pages and product/portfolio pages. That is why we considered one instance of each of these webpage types, along with the homepage. The survey participants in our empirical study were university students. Thus, the findings may differ for other age groups and educational levels.

Threats to Internal Validity: Survey participants could have made assumptions about which responses were socially desirable for this study, posing a threat to the internal validity. However, we mitigated this bias by communicating to the participants that there were no 'right' answers. Random ordering of the user interface design instances also poses a threat to the internal validity.

Threats to Construct Validity: The automated detection and manual classification techniques used in the study may affect the construct validity. Our automated detection approach may have missed some dark pattern data as false negatives. However, we carried out the manual classification with great care to reduce the remaining threats as much as possible. There would always be a possibility for survey participants to misunderstand questions or appropriate contexts. To mitigate this threat, we carried out a physical survey instead of a remote one. As a result, we were able to provide clear explanations and instructions about the survey to the participants.

7 CONCLUSION

This study marks the first exploration into dark patterns in the local context of Bangladesh. We combined automated and manual methods to collect textual dark pattern data from the websites of member companies of the E-Commerce Association of Bangladesh (e-CAB). We analyzed 715 websites and exposed dark patterns in 18.3% of those websites, which is 7.2% higher than in previous research using a similar approach. We also surveyed 68 university students about their perception of dark patterns. Based on our findings from both explorations, we divided dark pattern categories into two distinct groups - 'Passive Dark Patterns' and 'Active Dark Patterns'. Most of the dark pattern instances found in this study belonged to 'Passive Dark Patterns'. Our analysis also revealed that users with a background in technology education are more aware and concerned about dark patterns than other users. Further research is needed to analyze the reasons and consequences of dark patterns, local developer perspectives, and potential regulatory frameworks in the context of Bangladesh.

ACKNOWLEDGEMENTS

This study is supported by the fellowship from the ICT Division, Government of Bangladesh – No.: 56.00.0000.052.33.001.23-09, date: 04.02.2024.

REFERENCES

Bongard-Blanchy, K., Rossi, A., Rivas, S., Doublet, S., Koenig, V., and Lenzini, G. (2021). " i am definitely manipulated, even when i am aware of it. it's ridiculous!"-dark patterns from the end-user perspective. In *Designing Interactive Systems Conference 2021*, pages 763–776.

Bösch, C., Erb, B., Kargl, F., Kopp, H., and Pfattheicher, S. (2016). Tales from the dark side: privacy dark strategies and privacy dark patterns. *Proc. Priv. Enhancing Technol.*, 2016(4):237–254.

Brignull, H., Leiser, M., Santos, C., and Doshi, K. (2023). Deceptive patterns – user interfaces designed to trick you. https://www.deceptive.design/.

Chaudhary, A., Saroha, J., Monteiro, K., Forbes, A. G., and Parnami, A. (2022). "are you still watching?": Exploring unintended user behaviors and dark patterns on video streaming platforms. In *Designing Interactive Systems Conference*. ACM.

Geronimo, L. D., Braz, L., Fregnan, E., Palomba, F., and Bacchelli, A. (2020). UI dark patterns and where to find them. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM.

Gray, C. M., Chen, J., Chivukula, S. S., and Qu, L. (2021). End user accounts of dark patterns as felt manipulation. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–25.

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., and Toombs, A. L. (2018). The dark (patterns) side of UX design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM.

Hidaka, S., Kobuki, S., Watanabe, M., and Seaborn, K. (2023). Linguistic dead-ends and alphabet soup: Finding dark patterns in japanese apps. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pages 1–13.

Jarovsky, L. (2022). Dark patterns in personal data collection: Definition, taxonomy and lawfulness. *SSRN Electronic Journal*.

Luguri, J. and Strahilevitz, L. (2019). Shining a light on dark patterns. *SSRN Electronic Journal*.

Maier, M. (2019). Dark patterns–an end user perspective.

Mansur, S. M. H., Salma, S., Awofisayo, D., and Moran, K. (2023). AidUI: Toward automated recognition of dark patterns in user interfaces. In *2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE)*. IEEE.

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., and Narayanan, A. (2019). Dark patterns at scale. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–32.

Mathur, A., Kshirsagar, M., and Mayer, J. (2021). What makes a dark pattern... dark? In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM.

Roffarello, A. M. and Russis, L. D. (2022). Towards understanding the dark patterns that steal our attention. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*. ACM.

Sazid, Y., Fuad, M. M. N., and Sakib, K. (2023). Automated detection of dark patterns using in-context learning capabilities of gpt-3. In *2023 30th Asia-Pacific Software Engineering Conference (APSEC)*, pages 569–573. IEEE.

Soe, T. H., Nordberg, O. E., Guribye, F., and Slavkovik, M. (2020). Circumvention by design-dark patterns in cookie consent for online news outlets. In *Proceedings of the 11th nordic conference on human-computer interaction: Shaping experiences, shaping society*, pages 1–12.

Soe, T. H., Santos, C. T., and Slavkovik, M. (2022). Automated detection of dark patterns in cookie banners: how to do it poorly and why it is hard to do it any other way. *arXiv preprint arXiv:2204.11836*.

Stavrakakis, I., Curley, A., O'Sullivan, D., Gordon, D., and Tierney, B. (2021). A framework of web-based dark patterns that can be detected manually or automatically.

Yada, Y., Feng, J., Matsumoto, T., Fukushima, N., Kido, F., and Yamana, H. (2022). Dark patterns in e-commerce: a dataset and its baseline evaluations. In *2022 IEEE International Conference on Big Data (Big Data)*. IEEE.