Digital Dark Patterns

Sebastian Cyriac[1], Roshan Prakash[2], Sachin Tom[3]

[1]Mr. Sebastian Cyriac, Asst. Professor, Department of computer science, Santhigiri College of Computer Science, Vazhithala, Thodupuzha

sebastiancyriac@sathigiricollege.com

[2]Roshan Prakash, Santhigiri College of Computer Science, Vazhithala, Thodupuzha,

mca2022_roshanprakash@santhigiricollege.com

[3]Sachin Tom, Santhigiri College of Computer Science, Vazhithala, Thodupuzha,

mca2022_sachintom@santhigiricollege.com

***Abstract**: Dark Patterns are user interface designed elements with sole purpose of confusing or manipulating the consumers to take actions that they wouldn't have done willingly. ie, the designers knowingly confuse the users, makes it difficult for the customers to express their preferences, and manipulate the customers/users for the designers favor. The Dark Patterns can be found in certain web pages, pop ups and programs that include malware, freeware, shareware, etc... They typically are used to make online customers buy goods and services that they don't want or to exploit the cognitive biases or to share information that the user don't wish to disclose. There are several types of Dark Patterns that we dealt with in our day-to-day life. This article points out the Dark Patterns that we encounter with, unknowingly, and its power in manipulations. Also this article encounters various ethical issues related to the Dark Patterns.*

.1 Introduction:

Have you ever shopped on online end up buying more products that you never intended to or spend more than you budgeted? Have you ever felt the urge to sign up or to give information that you normally don't want? These days it's hard to determine the line between clever marketing and such deceptions. The element of user interface design that causes such confusions is called Dark Patterns.

Dark Patterns are digital designed elements that manipulate user/customer into making decisions that they wouldn't ordinarily make. The term 'Dark Patterns' is coined by UX designer '*Harry Brignull*' on 28th July 2010 with the registration of darkpatterns.org as "pattern library with the specific goal of naming and shaming deceptive user interfaces". Explanation of Dark Patterns by him quotes, 'When you use the web, you don't read every word, on every page. You skim read and make assumptions. And if a company wants to trick you into doing something, they can make advantage of this by making it look like it saying one thing when in fact it's saying another.' More broadly, dark patterns supplant "user values…in favor of shareholder value."

There are many different types of dark patterns that we're getting exposed to, in every day. Some of these Dark Patterns tricks us into sharing your personal data or sign up for subscriptions, others actively trying to take money from wallets

1.1.(a) Why dark patterns are bad?

A misleading design is created by products using dark patterns, a design that causes the consumer to make choices they do not want to make. In comparison to what product designers are attempting to do, this produces transparent prototypes that are user-centered.

1.1.(b) How dark patterns work?

While certain individuals assume that psychological techniques are dark patterns, most of them have little to do with psychology. They are cheap strategies that take advantage of the fact that web and app pages are ignored by individuals, instead of carefully reading the content. In the shortest possible time, people want to complete their task and at least choose the direction of defence by doing whatever the application requires. As a result, they can lose sight of the fact that the psychological dimensions of web interactions are the basis for some of the darker patterns. The transformation-effective patterns play on the FOMO (fear of missing out) sense of people to drive them to make a certain choice. Users feel like they don't have time for more study, and at that exact moment, they forces users to make their choice. Dark patterns, however, are simple tricks played on users to make them function in a manner they did not intend, but in benefit of design.

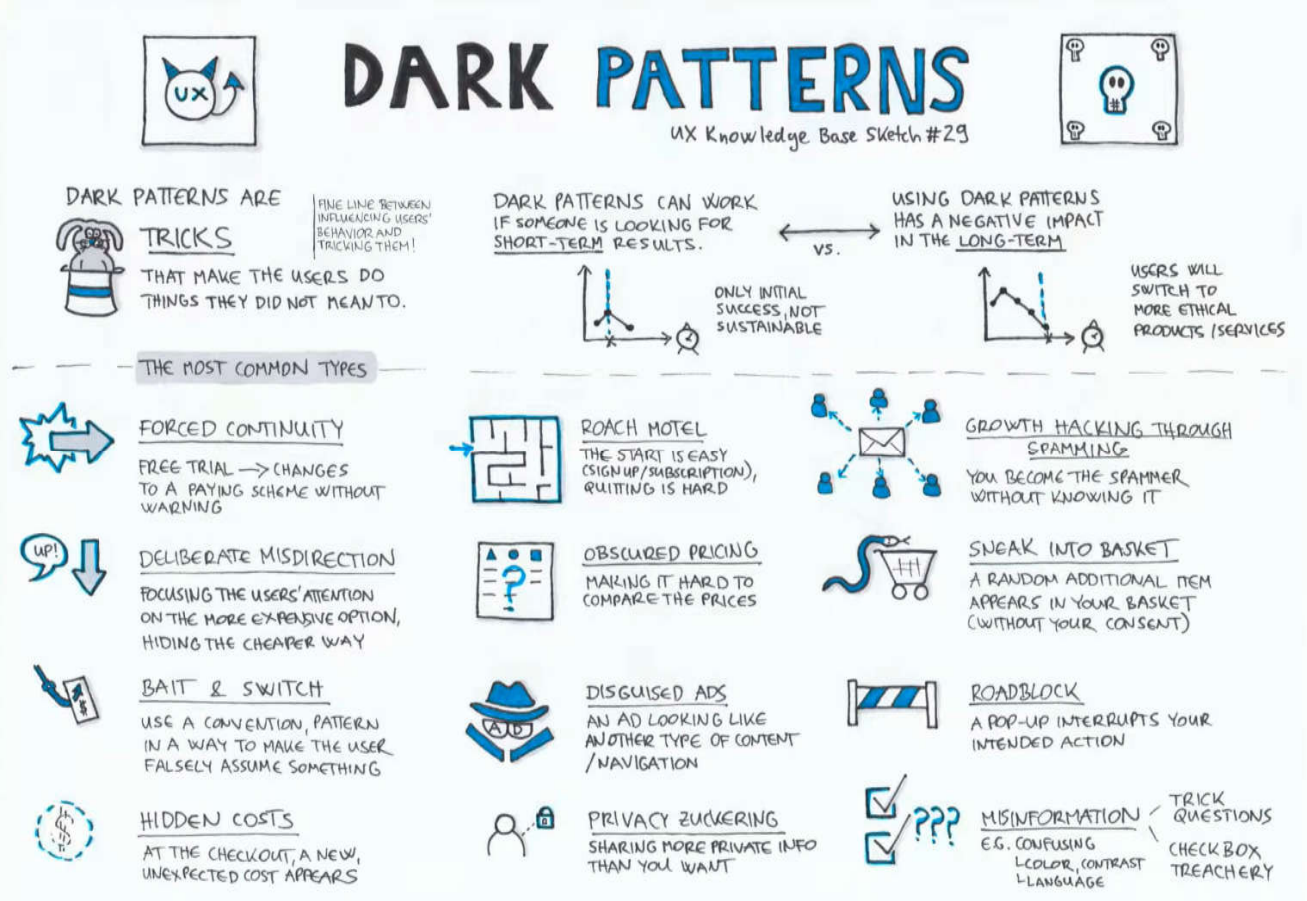

Figure 1.1

1.1.(c) Why products use them?

The explanation why corporations use these negative patterns is simple: money. The best conversion rates can be given by designs that use dark patterns. During A/B testing, such designs show outstanding performance.

But a design that provides the best conversion rate may not be the same one that provides the best user experience. They become disappointed and distrustful when users find out that a company has tried to cheat them. And a business will lose all the short-term advantages of Dark Patterns that it acquired, because consumers would leave goods they don't trust.

1.1.(d) Why are they more important to know now than ever?

For a typical internet user, all 12 dark pattern varieties manipulate them, irrespective of what pages or applications they use. The best defense that users have to get rid of such patterns is knowing them/ identifying them and their intention.

1.2 Types of Dark Patterns:

Harry Brignull categorized 12 types of dark patterns that should be aware of and to be avoided.

1.2.(a) Bait and Switch: The user assumes that their actions would have one outcome in this type of pattern, but instead, a completely different, undesirable outcome occurs.

Maybe Microsoft's misguided approach to getting people to upgrade their Windows OS to Windows 10 is the most popular example of bait and switch. Most users know that they can click the X at the top right corner to close the window when they see a pop-up window, and that they also say 'No' to the request in the pop-up by doing that.

Rather unexpectedly, though, on clicking the X in the Windows 10 dialog results in the update being initialized, a totally unexpected result for most users.

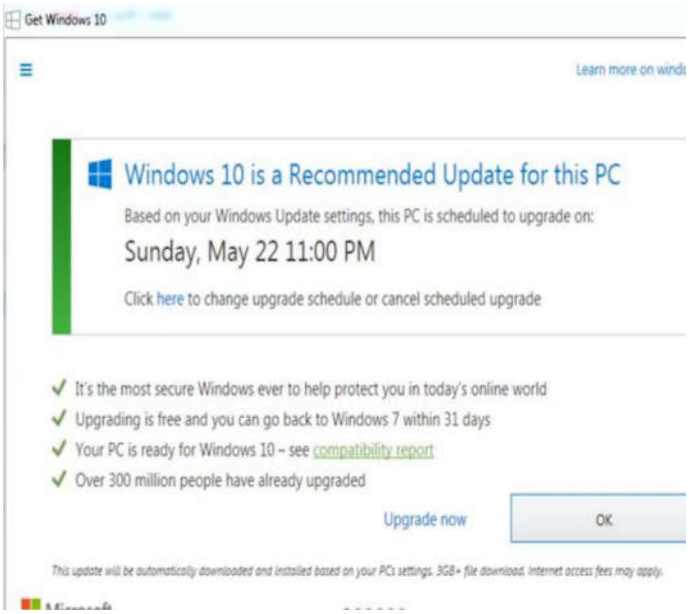

Figure 1.2.(a)

1.2.(b) Roach Motel: The design makes it very simple for you to get into a certain situation, but then it makes it very difficult for you to get out of it (e.g. a subscription). Attempting to delete a Facebook account is a perfect example of this. Not only it is more or less impossible to do, the only alternative shown is to deactivate the account, which is also incredibly hard to do.

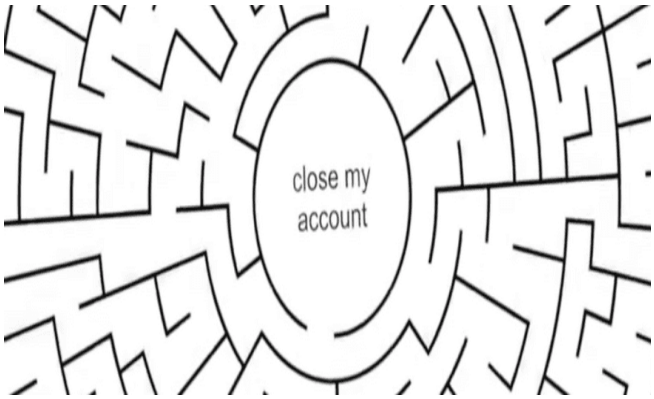

Figure 1.2.(b)

1.2.(c) Trick Questions: This pattern is based on the use of confusing language in questions (such as a double negative). As a consequence, the issue is much more difficult for users to understand.

Figure 1.2.(c)

Usually, as users register for a service, tricky questions appear. A number of checkboxes are shown, and the checkbox options are alternated, so ticking the checkbox means "opt out" while leaving it blank means "opt in".

1.2.(d) Sneak into basket: This dark pattern consists of an additional item being snuck during online shopping into the user's cart. There are usually two ways they add the unwanted item to the user's cart.

1. **The website adds an additional item automatically**. This method is seldom used on desktop users nowadays, since it is simpler for them to see when an additional item appears in their cart. But on mobile phones, this pattern is more widely used, since mobile users have less screen property and are often distracted, they can easily miss the additional item and only find the extra charge after checkout..
2. **Th The website tricks the user into inserting an additional item itself.** When a website pre-selects a choice that adds the object, this often happens.

1.2.(e) Privacy Zuckering: Privacy Zuckering is about having more personal data exchanged by the user than they actually intended. Harry Brignull called the dark pattern after CEO Mark Zuckerberg of Facebook. The details on what the business can do with the personal information of a user is found in the Terms of Service, and almost no one takes the time to read them. Facebook makes privacy management notoriously challenging.

1.2.(f) Price comparison prevention: Certain online retailers and subscription-based services make it difficult for the user to compare an item's price with another item. As a result, an effective decision can not be taken by users.

LinkedIn, which allows you to try out their Premium plans, is a good example of this, but does not tell you the cost. This makes it easier for users to mistakenly agree to a price that they are currently not prepared to pay.

1.2.(g) Intentional misdirection: When product developers attempt to guide consumers to an alternative that will result in more market value for the company, intentional misdirection occurs.

Ryanair's design is probably the most well-known example of deliberate misdirection. Users are asked to choose their country of residence when booking a trip, a mandatory issue. Therefore, the majority of users logically choose their country of residence. The problem, however, is actually related to the purchase of travel insurance; 'No travel insurance needed' is a choice between Latvia and Lithuania in the list of countries. Therefore, users who are not aware

of this will be fooled into buying travel insurance that is not necessarily compulsory. This deliberate money grab is a perfect way to destroy consumer morale.

1.2.(h) Hidden costs: Most of us are in a situation where we visit a website, see an item that we want, and are satisfied with the price at which it is listed. We go through a process of multi-phase checkout, and eventually get to the final step of confirming the order.

But then, to our surprise, we find that unforeseen costs, fees, shipping charges, and often more, have appeared on our order. And sometimes, even though we don't like the fact that the price has risen, we still decide to finish the order, because we have already spent a lot of time and money in the buying process.

1.2.(i) Friend spam: Asks your contacts for a favorable outcome under the pretense that it will be used (e.g. finding friends to join you), but then spams all your contacts in a message that appears to be from you.

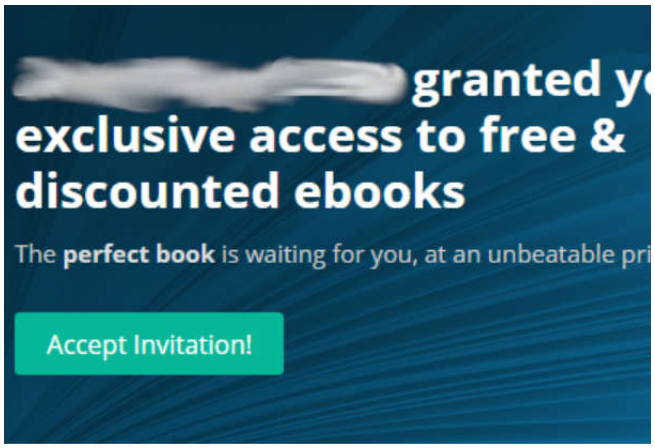

Figure 1.2.(i)

1.2.(j) Forced continuity: On many subscription-based services which offer a free trial, this pattern can be found. They are asked to enter their credit card information when users sign up for a free trial. Users start being paid automatically when the trial finishes if they don't remember to opt out.

Users aren't really provided a simple way to cancel the subscription in certain situations. They have to contact the office or even send a letter to get their subscription cancelled via regular mail.

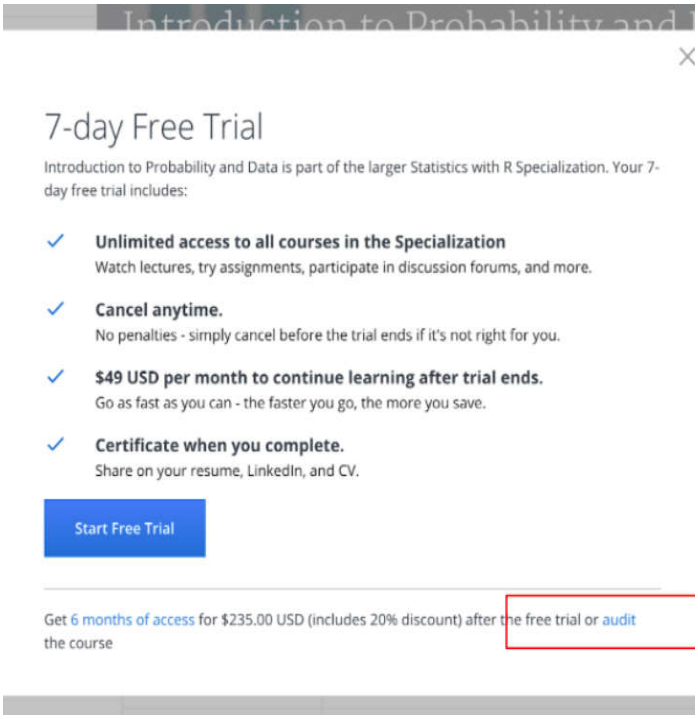

Figure 1.2.(j)

1.2.(k) Disguised ads: Usually, it's not difficult to separate ads from standard content. Ads are normally put on a page in unique locations, and users need just a fraction of a second to distinguish them from standard content.

Yet hidden commercials are a different story entirely. In order to get users to click on them, such advertisements are designed to look like normal content or navigation. Many pages on Softpedia, a common software download site, for instance, contain advertisements that look like software download call-to-action buttons. The buttons use exactly the same font that is used for the actual download buttons and the same dark blue color. It's quick to mistakenly press the wrong button as a result.

1.2.(l) ConfirmShaming: Confirmshaming is making the user into opt into something through shaming them if they don't. On the web today, this method is still popular, particularly as a way to get users to sign up for a mailing list. Users see two choices in a pop-up: the first in a bright color and a call to action, and the second in a subtle color, criticizing them for not making the 'right' choice. There are several examples of this trend found in real-world items in the blog Confirmshaming.

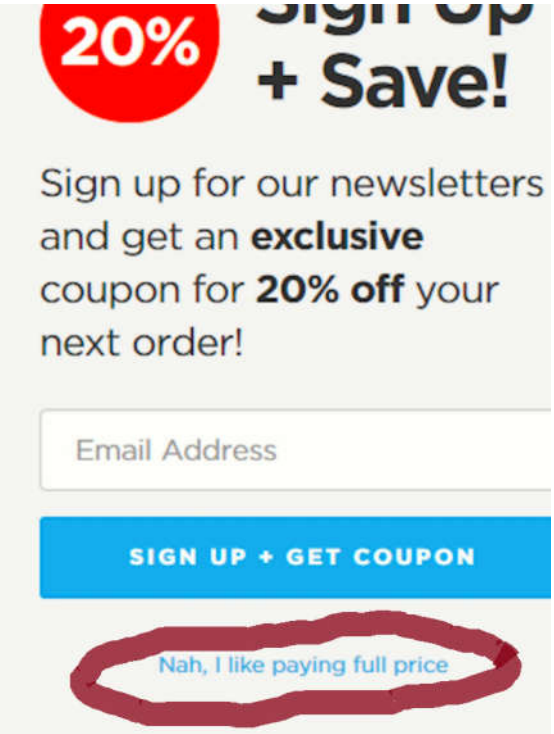

Figure 1.2.(I)

1.3 Dark Patterns As Critical—Ethical:

For a fundamental and simple cause, dark patterns have been developed: to deceive users. Dark Patterns are aimed at extracting personal data from consumers and website users while talking about privacy, which they will not offer willingly and that companies also do not necessarily use to provide their services.

As such, dark patterns are evil. But they can probably be used smartly and ethically to accomplish a positive purpose. Dark Patterns like prejudice or hacking can be engineered and enforced. As such, they are unethical and dangerous, but discrimination can be positive in ensuring that access to higher education and employment is provided to disadvantaged groups, and hacking can be ethical in checking the protection of networks and infrastructures or breaching criminal websites.

For example, a cookie consent banner may use ethical dark patterns if the choice to reject monitoring and marketing cookies is structured rather than the opposite in a way that users are pushed to click on it.

1.4 Dark Pattern – Solutions?

No easy solutions or alternatives to dark patterns are possible. Although dark patterns may offer short-term gains to a business, in the long term, such gains may cost users. Practising honest design is often easier. We should always put our users first when we design products. Strive to build transparent and user-focused goods, since the long-term battle for users can only survive.

They essentially have three choices when designers are faced with dark patterns:

1) **Let's go for it:** Are more subscribers or sales expected by the marketing department? Dark patterns are here to enable diligent designers to plan, design and execute them.

2) **No, thank you:** Designers refuse to use dark patterns on the websites that they develop and follow a balanced approach to design, i.e. all user choices are similarly provided. This is possibly the best approach from an ethical perspective, since it allows users complete freedom to make their free choices without any push. However, the most ethical solution is not always the most successful for bringing change when things get too dirty or corrupt.

3) **The fighting attitude:** In the website they are working on, programmers build and enforce ethical dark patterns to ensure that users are required to select the strictest privacy settings and that they send as little personal data as possible to the website provider.

In digital design and privacy, the last approach would be capable of shifting the paradigm: consumers would begin to trust providers not to collect excessive personal data for the sole purpose of trading and making extra money.

Design Responsibility and a Designer's Character

In shaping human behaviour for the better, designers should maintain ethics. Design must be sincere and sensitive, without being deliberately overwhelming, providing simple choices. The aim is to close the distance in understanding between what is being offered and what the client feels they are receiving. Instead of deceptively harvesting short-term gains, designers can lay the foundations for brand loyalty and organic, long-term growth.

1.5 Conclusion:

Slowly and slowly, Dark Patterns have evolved. But with time, they have been strengthened and are now often intended to deceive the more conscious user. Around a decade ago, computer scientists discovered dark patterns, and there is a sense in which what they have discovered is the current manifestation of something very old: sales

practices that challenge the boundaries of law and ethics. From looking backwards, there is a lot to be learned, but the size of dark patterns, their rapid proliferation, the possibilities of using algorithms to detect them, and the breadth of the numerous methods that have already developed mean that this is an environment where important legal innovation is needed.

References:

[1] https://www.darkpatterns.org/
[2] https://uxdesign.cc/dark-patterns-in-ux-design-7009a83b233c
[3] https://www.shopify.in/partners/blog/dark-patterns
[4] https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you

Author Profile:

Roshan Prakash pursuing the Master of Computer Application from Santhigiri Collegeof Computer Science, Vazhithala in 2020-2022

Sachin Tom pursuing the Master of Computer Application from Santhigiri Collegeof Computer Science, Vazhithala in 2020-2022

Sebastian Cyriac received the M.sc. professional degree in Computer Science. Currently working as Assistant Professor in Computer Science Department of Santhigiri College of Computer Sciences, Vazhithala.