



UNIVERSITÀ DEGLI STUDI DI SALERNO

Dipartimento di Informatica

Corso di Laurea Triennale in Informatica

TESI DI LAUREA

Studio sui Dark Pattern e sviluppo di un'estensione Chrome per il Dark Pattern Bait and Switch

RELATORE

Prof. Fabio Palomba

Dott. Giulia Sellitto

Università degli Studi di Salerno

CANDIDATO

Mario Lezzi

Matricola: 0512107631

Anno Accademico 2022-2023

Questa tesi è stata realizzata nel

sesa^{lab}
SOFTWARE ENGINEERING
SALERNO

The job's not finished

Kobe Bryant

Abstract

La crescente ubiquità delle interfacce digitali ha portato a un aumento delle preoccupazioni etiche riguardo alle pratiche di progettazione manipolative, conosciute come "dark pattern". Queste tattiche, intenzionalmente ingannevoli, mirano a influenzare il comportamento degli utenti online in modi che possono essere dannosi o fuorvianti. Questa tesi presenta una risposta pratica a questa sfida attraverso lo sviluppo di un'estensione Chrome dedicata, progettata per individuare e segnalare l'utilizzo del dark pattern 'Bait and Switch' durante l'interazione degli utenti con le pagine web. Il dark pattern 'Bait and Switch' propone una scelta dal risultato evidente all'utente, per poi provocarne uno indesiderato. L'estensione analizza il Document Object Model delle pagine web e informa l'utente sulla presenza di possibili dark pattern. I risultati indicano che l'estensione Chrome proposta è in grado di identificare dark pattern e informare l'utente sui possibili reindirizzamenti a pagine non desiderate. Tuttavia, i risultati del test, effettuato tramite un bot dedicato, evidenziano alcuni limiti dell'estensione, come la presenza di numerosi falsi positivi. Questi risultati sono un punto di partenza per gli sviluppi futuri.

Indice

Elenco delle Figure	iii
1 Introduzione	1
1.1 Contesto Applicativo	1
1.2 Motivazioni e Obiettivi	2
1.3 Struttura della Tesi	2
2 Background e stato dell'arte	4
2.1 Tassonomia dei dark pattern	4
2.1.1 Nagging	7
2.1.2 Obstruction	8
2.1.3 Sneaking	10
2.1.4 Bait and Switch	13
2.1.5 Interface Interferences	14
2.1.6 Forced Action	18
2.2 Influenza dei Dark Pattern	20
2.3 Implicazioni sulla privacy	21
3 Dark Pattern Identifier	23
3.1 Ricerca di un Dark Pattern identificabile	23
3.2 Algoritmo di detection	23

3.3	Implementazione algoritmo	24
3.3.1	Analisi elementi	24
3.3.2	Verifica dei risultati	24
3.3.3	Invio risultati	24
3.3.4	Architettura utilizzata	24
3.4	Sviluppo estensione Chrome	25
3.4.1	Interfaccia grafica e funzionamento	25
4	Valutazione dell'approccio	27
5	Conclusioni e Sviluppi futuri	30
5.1	Conclusioni	30
5.2	Sviluppi Futuri	31
	Bibliografia	32

Elenco delle figure

2.1	Tassonomia di Gray	7
2.2	Dark Pattern Nagging in Instagram	8
2.3	Dark Pattern Roach Motel in Amazon	9
2.4	Dark Pattern Price Comparison Prevention in Linkedin	9
2.5	Dark Pattern Intermediate Currency in FIFA 23	10
2.6	Dark Pattern Forced Continuity in PlayStation Store	11
2.7	Dark Pattern Hidden Costs in The Globe and Mail	12
2.8	Dark Pattern Sneak into Basket in name.com	13
2.9	Dark Pattern Bait and Switch in Windows 10	14
2.10	Dark Pattern Hidden Information in Greenpeace	15
2.11	Dark Pattern Preselection, esempio realizzato dal sito dapde.de . . .	16
2.12	Dark Pattern Toying with Emotion in booking.com	17
2.13	Dark Pattern False Hierarchy in Linkedin	17
2.14	Dark Pattern Disguised Ads in OnlyMP3	18
2.15	Dark Pattern Trick Questions fornito da darkpatterns.org	18
2.16	Dark Pattern Privacy Zuckering in Redis.com	19
2.17	Dark Pattern Gamification in FUT 23	20
3.1	Estensione Chrome non attiva	26
3.2	Estensione Chrome attiva	26

3.3	badge dell'estensione	26
4.1	bot per il testing in esecuzione	27
4.2	dark pattern presente su asuratoon.com	28
4.3	risultati su grafico a torta	29

CAPITOLO 1

Introduzione

1.1 Contesto Applicativo

La crescente digitalizzazione della società ha portato a un'ampia diffusione di servizi online e piattaforme digitali che facilitano la comunicazione, la transazione e l'accesso alle informazioni. Tuttavia, insieme a questi benefici, emergono anche sfide etiche legate alle pratiche di progettazione delle interfacce utente. In particolare, lo studio svolto in questa tesi è concentrato sui "dark pattern", un termine che si riferisce a pratiche di progettazione intenzionali volte a manipolare il comportamento degli utenti in modi che possono essere dannosi o fuorvianti.

Le interfacce digitali sono diventate il principale punto di interazione tra gli individui e il mondo online, che comprende servizi finanziari, piattaforme social, siti di e-commerce e altro ancora. In questo scenario, la progettazione delle interfacce gioca un ruolo cruciale nel plasmare l'esperienza degli utenti e influenzarne il comportamento. Tuttavia, alcune organizzazioni hanno adottato dark pattern per indirizzare gli utenti verso azioni che potrebbero non essere nel loro interesse.

Sul web sono riscontrabili siti di e-commerce che adottano un modello di design malevolo noto come 'Sneak into Basket', il quale comporta l'aggiunta non autorizzata di articoli al carrello dell'utente, costringendolo così a effettuare acquisti non deside-

rati. La registrazione a servizi di abbonamento online o newsletter risulta essere un processo agevole, richiedendo soltanto pochi clic in pochi secondi; tuttavia, la procedura di disiscrizione da tali servizi risulta spesso complessa. In queste circostanze, l'utente si trova di fronte a una situazione in cui l'ingresso è agevole, ma l'uscita è difficoltosa. Tale modello di design malevolo è noto come 'Roach Motel'.

Lo studio condotto in questa tesi fornisce informazioni dettagliate sui numerosi dark pattern presenti sulla rete, i quali influenzano le emozioni dell'utente attraverso l'uso di colori e immagini. Essi propongono azioni il cui risultato atteso è evidente, per poi mostrare un esito diverso, e così via. Tutti questi schemi condividono lo stesso obiettivo: manipolare le scelte dell'utente.

1.2 Motivazioni e Obiettivi

La motivazione principale di questa ricerca è affrontare la sfida dell'individuazione dei dark pattern, fornendo agli utenti uno strumento di difesa pratico. Attraverso l'implementazione di un'estensione Chrome, si cerca di aumentare la consapevolezza degli utenti riguardo alle pratiche ingannevoli, consentendo loro di prendere decisioni più informate durante la navigazione online.

La tesi si propone di sviluppare un'estensione Chrome efficiente e user-friendly per individuare il dark pattern di tipo Bait and Switch. L'obiettivo specifico include la progettazione di un algoritmo di rilevamento e la valutazione dell'efficacia dell'estensione, analizzando i cento siti più visitati in Italia nell'anno 2023 ed automatizzando il testing attraverso la realizzazione di un bot dedicato, il quale fornisce come output il numero di possibili dark pattern di tipo Bait and Switch presenti in ognuno dei suddetti siti web.

1.3 Struttura della Tesi

Di seguito è riportata la struttura della tesi

- **Background e Stato dell'arte** In questo capitolo viene fatta una descrizione dettagliata sulle diverse categorie e caratteristiche dei dark pattern esistenti.

- **Dark Pattern Identifier** Questo capitolo riporta i motivi della scelta del dark pattern da individuare, la descrizione dell'algoritmo di detection e i passi effettuati per la creazione dell'estensione.
- **Valutazione dell'approccio** In questo capitolo viene mostrato come è stata testata l'efficienza dell'estensione Chrome e i risultati ottenuti.
- **Conclusioni e Sviluppi Futuri** In questo capitolo vengono illustrati i limiti dell'estensione e i possibili sviluppi futuri.

CAPITOLO 2

Background e stato dell'arte

I dark pattern (noti anche come modelli di progettazione ingannevoli) sono modelli attentamente progettati e costruiti per indurre gli utenti a compiere azioni non volute e dannose, come abbonamenti indesiderati. Il termine dark pattern è stato coniato nel 2010 dal designer di UX londinese Harry Brignull, il quale ha classificato sul proprio sito `darkpatterns.org` i dark pattern. Harry Brignull così definì i dark pattern:

"La vera sfida per i designer è quella di creare interfacce utente che siano trasparenti, oneste e rispettose dell'utente. I dark pattern sono l'opposto di questo: sono opachi, ingannevoli e disonorevoli" [Brignull,2010]

2.1 Tassonomia dei dark pattern

L'approccio di Harry Brignull allo studio dei dark pattern si basa sulla sua esperienza come designer e sulla sua formazione in psicologia cognitiva. Brignull ha dedicato molto tempo e risorse alla ricerca dei diversi tipi di dark pattern e alla loro classificazione, con l'obiettivo di aiutare gli utenti a riconoscerli e a evitarli. Uno dei principali risultati del lavoro di Brignull è stato la creazione del sito web

www.darkpatterns.org, un catalogo online di diversi tipi di dark pattern che vengono utilizzati in molti siti web e applicazioni mobile. Il sito web include anche esempi di dark pattern in azione e suggerimenti su come evitarli. Il sito è stato lanciato nel 2010 ed è diventato una risorsa importante per gli utenti che desiderano evitare i dark pattern. Inoltre, Brignull ha anche pubblicato alcuni articoli e presentazioni in cui analizza in dettaglio i diversi tipi di dark pattern e le loro conseguenze per gli utenti. Ad esempio, in un articolo del 2011 intitolato "Dark Patterns: Deception vs. Honesty in UI Design" [1], Brignull descrive alcune delle tecniche più comuni utilizzate nei dark pattern. In generale, lo studio di Brignull sui dark pattern ha contribuito in modo significativo alla consapevolezza del pubblico sulle tecniche di progettazione ingannevoli e ha fornito agli utenti strumenti per proteggersi dalle pratiche commerciali sleali. Il sito di Brignull è suddiviso in due sezioni, una dedicata alla tassonomia realizzata dal designer e l'altra contenente le segnalazioni effettuate dagli utenti tramite twitter. La tassonomia di Brignull, contenuta nella sezione "Types of deceptives design", suddivide i dark pattern in 12 categorie distinte. Successivamente altri studiosi si sono impegnati nella ricerca di tecniche di progettazione di interfacce dannose e nella creazione di diverse tassonomie.

Conti e Sobiesk hanno presentato l'articolo "Malicious interface design: exploiting the user" [2] alla 19esima Conferenza Internazionale sul World Wide Web, il quale discute del concetto di design dell'interfaccia utilizzato per sfruttare gli utenti a scopi ingannevoli. L'articolo mette in evidenza come il design dell'interfaccia possa essere utilizzato per scopi malevoli, sfruttando le vulnerabilità degli utenti e le loro abitudini di utilizzo. Ad esempio, attraverso l'uso di tecniche di manipolazione psicologica e di design persuasivo, è possibile indurre gli utenti a compiere azioni non desiderate o a fornire informazioni personali sensibili. Inoltre, nell'articolo, viene presentata una tassonomia che classifica le tecniche utilizzate per realizzare il *Malicious interface design* in 11 categorie contenenti 20 sottocategorie. Di seguito sono elencate alcune delle più rilevanti:

- **Information obscuring:** le informazioni rilevanti per gli utenti vengono nascoste o presentate in modo da renderle difficili da individuare, ad esempio attraverso l'uso di colori o font poco visibili o di dimensioni troppo piccole.

- **Deception:** vengono utilizzate tecniche di inganno per indurre gli utenti a compiere azioni non desiderate, come cliccare su link dannosi o fornire informazioni personali, attraverso l'uso di design persuasivo o di messaggi di allarme falsi.
- **Social engineering:** in questa categoria vengono incluse le tecniche che sfruttano la psicologia umana per manipolare gli utenti e ottenere informazioni o accesso a sistemi protetti.
- **Obstruction:** questa categoria include le tecniche che rendono difficile o impediscono agli utenti di accedere a determinati servizi o funzionalità, ad esempio attraverso l'utilizzo di autenticazione eccessivamente complicata.
- **Forced Action:** questa categoria include le tecniche che inducono gli utenti a compiere azioni non volute o a fornire informazioni personali sensibili, attraverso l'utilizzo di design persuasivo o messaggi di allarme falsi.

La tassonomia più recente è stata proposta nel 2018 da David M.Gray *et al.* [3] alla Conference of Human Factors in Computing Systems. I lavori di ricerca di Gray si concentrano sulla comprensione e l'identificazione dei dark pattern. In particolare, Gray ha condotto uno studio nel 2018 in cui ha analizzato 11.000 siti web per identificare i dark pattern presenti. I risultati hanno mostrato che i dark pattern sono estremamente diffusi e possono essere suddivisi in diverse categorie, tra cui "misdirection" (tecniche che inducono gli utenti a compiere azioni non intenzionali), "obstruction" (tecniche che rendono difficile per gli utenti trovare informazioni o svolgere determinate azioni) e "forced action" (tecniche che inducono gli utenti a compiere azioni non volute). Successivamente, Gray ha condotto uno studio nel 2019 per esaminare come i dark pattern possano influenzare il comportamento degli utenti nell'ambito dell'acquisto online. L'obiettivo dello studio era quello di comprendere come i dark pattern possano indurre gli utenti a fare acquisti impulsivi e a prendere decisioni di acquisto che potrebbero non essere nella loro migliore intenzione. I risultati dello studio hanno evidenziato che l'utilizzo di dark pattern può portare a una riduzione della consapevolezza e della razionalità degli utenti nell'acquisto online. Inoltre, Gray ha anche contribuito alla definizione di una tassonomia dei dark pattern, basata su cinque categorie principali, **Nagging**, **Obstruction**, **Sneaking**,

Interface Interferences, Forced Action. La tassonomia di Gray è utile per comprendere le diverse tecniche di dark pattern e per identificare possibili vulnerabilità nelle interfacce utente.

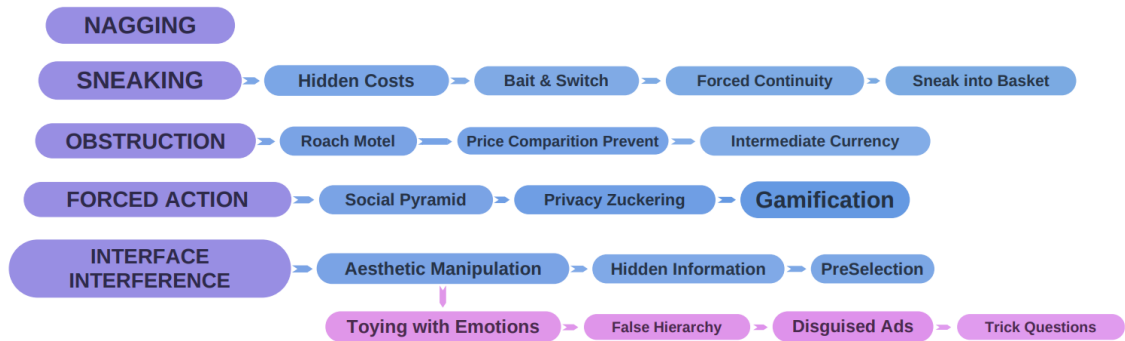


Figura 2.1: Tassonomia di Gray

2.1.1 Nagging

I dark pattern appartenenti alla categoria "Nagging" sono definiti come un leggero reindirizzamento delle azioni previste che possono durare per una o più interazioni. Il Nagging si manifesta spesso durante la normale interazione in cui l'attività desiderata dall'utente viene interrotta una o più volte da altre attività, non direttamente correlate a ciò su cui l'utente si sta concentrando. Il Nagging può includere pop-up che oscurano l'interfaccia utente, note audio che distraggono l'utente o altre azioni che interferiscono o distraggono in altro modo l'utente. Un esempio di Nagging è riportato in Figura 2.2, dove nell'app Instagram un pop-up per attivare le notifiche interrompe l'attività dell'utente. All'interno del pop-up non è presente un'opzione per dire "No", ma è visibile solo "Non adesso" quindi il pop-up verrà mostrato di nuovo in seguito.



Figura 2.2: Dark Pattern Nagging in Instagram

2.1.2 Obstruction

Un pattern "Obstruction" è un impedimento allo svolgimento di un compito, che rende un'interazione più difficile di quanto sia essenzialmente necessario. Brignull definisce tre dark pattern all'interno di questa categoria, ovvero **"Roach Motel"**, **"Price Comparision Prevention"** e **"Intermediate Currency"**.

Roach Motel

Il "Roach Motel" indica una situazione in cui è facile entrare ma da cui è difficile uscire. L'utente riesce facilmente ad iscriversi ad un determinato servizio, ma gli risulta particolarmente difficile disiscriversi o cancellare l'account. Ad esempio nella figura 2.3, è mostrato come sia difficile cancellare un account Amazon, dato che bisogna confermare più volte la cancellazione, obbligando l'utente ad un'ulteriore conferma entro cinque giorni tramite SMS.

Per inviare una richiesta di chiusura del tuo account Amazon ed eliminare i tuoi dati:

1. Vai a [Chiudi il tuo account Amazon](#).
2. Accedi all'account che desideri chiudere.
3. Rivedi i prodotti e i servizi associati al tuo account.
4. Se desideri continuare, seleziona un motivo nel menu a tendina, seleziona la casella accanto a **Sì, desidero chiudere definitivamente il mio account Amazon ed eliminare i miei dati** e fai clic su **Chiudi il mio account**.

Nota: Se disponi di più account, segui i passaggi sopra indicati per ciascuno di essi in modo da autorizzarci a intervenire su ciascuno degli account che desideri chiudere.

Una notifica di conferma verrà inviata all'indirizzo e-mail associato al tuo account o tramite SMS. Dovrai rispondere entro 5 giorni per verificare la tua richiesta.

Figura 2.3: Dark Pattern Roach Motel in Amazon

Price Comparison Prevention

Con qualsiasi tipo di acquisto, è sempre una bella sensazione sapere che le decisioni sono state prese in base ai dati disponibili. Con il Price Comparison Prevention, i rivenditori online rendono difficile per gli utenti confrontare il prezzo di un articolo con un altro. Questo modello è comune per i servizi che offrono diverse opzioni di packaging. I siti web di generi alimentari spesso cambiano anche il modo in cui vengono visualizzati i prezzi per lo stesso tipo di prodotto, ad esempio in base al peso, poi in base alla quantità. Di conseguenza, i clienti non dispongono di tutte le informazioni di cui hanno bisogno per prendere decisioni informate. In figura 2.4 viene mostrato un esempio preso da LinkedIn, i diversi piani e funzionalità vengono visualizzati l'uno di fianco all'altro, tuttavia i prezzi non sono visibili fino a quando non si fa clic su "Seleziona piano".

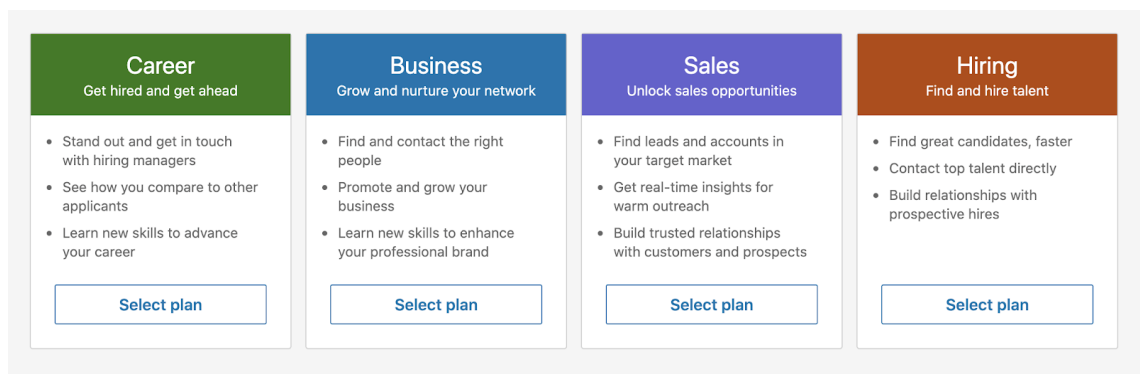


Figura 2.4: Dark Pattern Price Comparison Prevention in LinkedIn

Intermediate Currency

Il dark pattern Intermediate Currency induce l'utente a spendere denaro reale per l'acquisto di una valuta finta utile per l'acquisto di servizi o beni digitali. L'obiettivo di questo dark pattern è quello di separare gli utenti dal valore dei soldi effettivamente spesi per consentire loro di interagire con le valute in modo diverso. Questo pattern si manifesta tipicamente come un acquisto in-app per i videogiochi. In figura 2.5 viene mostrato un Intermediate Currency sul videogioco FIFA 23, il quale invita l'utente a spendere una somma di denaro reale per l'acquisto di "fifa points", ovvero una valuta utilizzata solo all'interno del gioco.

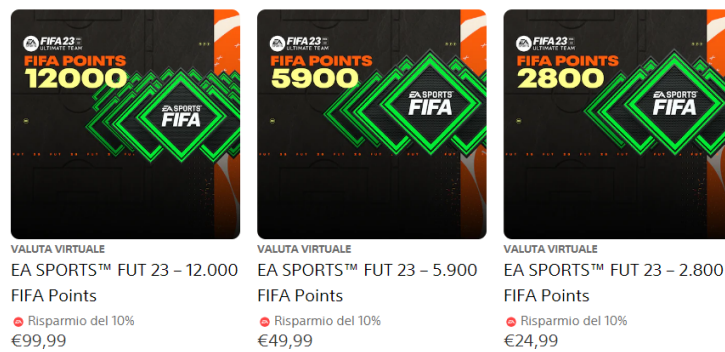


Figura 2.5: Dark Pattern Intermediate Currency in FIFA 23

2.1.3 Sneaking

I dark pattern appartenenti a questa categoria hanno l'obiettivo di nascondere, camuffare o ritardare le informazioni rilevanti per l'utente. Con lo Sneaking, l'utente non visualizza decisioni che probabilmente rifiuterebbe se ne fosse a conoscenza, come ad esempio pagamenti nascosti. La maggior parte dei design pattern ideati da Brignull sono di questo tipo. Questa categoria include tre sottocategorie : **Forced Continuity**, **Hidden Costs**, **Sneak into Basket** e **Bait and Switch**.

Forced Continuity

Questo dark pattern continuerà ad addebitare l'utente anche dopo la scadenza del servizio acquistato. Questo modello sfrutta gli utenti che non controllano la data di scadenza del servizio, sia per la prova gratuita che per l'uso a tempo limitato del

servizio a pagamento. Il Forced Continuity non ricorda agli utenti dell'imminente scadenza e li obbliga quindi ad effettuare il successivo pagamento. Un esempio di questo dark pattern è riportato in figura 2.6, la quale mostra come il sito "PlayStation Store" invita l'utente a pagare la prima mensilità del servizio "PS Plus", per poi attivare automaticamente il successivo pagamento, senza avvisare l'utente a ridosso della scadenza.

Scegli un piano di abbonamento

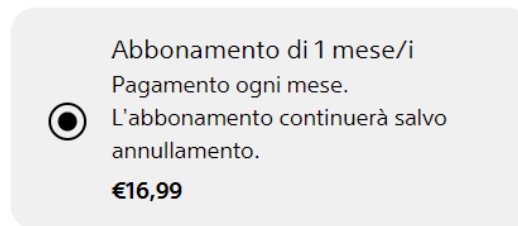


Figura 2.6: Dark Pattern Forced Continuity in PlayStation Store

Hidden Costs

l'Hidden Costs di Brignull fornisce all'utente una serie di costi per un determinato servizio. La particolarità di questo modello è quella di mostrare un prezzo iniziale per poi modificarlo in seguito ad ulteriori tasse, commissioni o costi di spedizione, facendo lievitare il prezzo inizialmente pubblicizzato. Ad esempio, la rivista "The Globe and Mail" utilizza questo dark pattern. Inizialmente offre la possibilità di abbonarsi al servizio settimanale pagando 1,99 dollari; se si sposta lo sguardo più in basso, è presente una descrizione della modalità di addebito che indica 7,96 dollari alla data di inizio dell'abbonamento, ed è diversa dal prezzo pubblicizzato di 1,99 dollari a settimana.

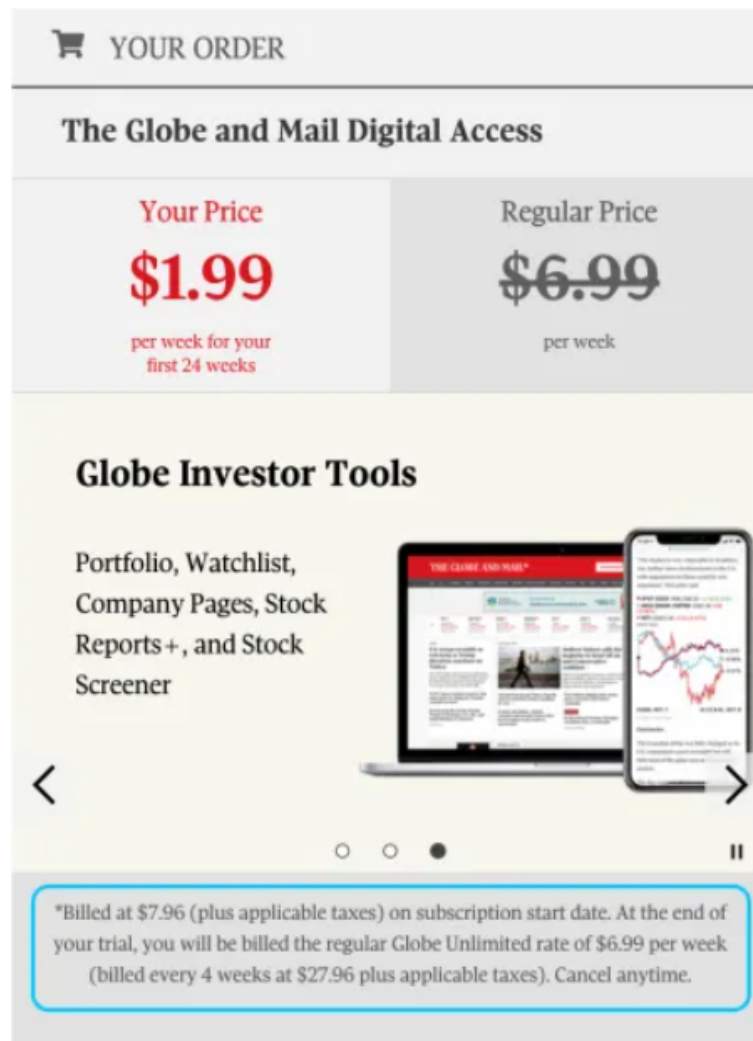


Figura 2.7: Dark Pattern Hidden Costs in The Globe and Mail

Sneak into Basket

Il modello "Sneak into Basket" aggiunge gli articoli non selezionati dall'utente al carrello online. Questo dark pattern invia prodotti al carrello degli utenti, spesso affermando che sono suggerimenti basati su altri articoli che hanno acquistato. Ciò può far sì che gli utenti acquistino inavvertitamente questi articoli senza saperlo prima del checkout. In figura 2.8 è raffigurato un esempio di sneak into basket presente sul sito *name.com*. Quando l'utente prova ad effettuare un acquisto, nell'ultimo passaggio, verrà aggiunta per impostazione predefinita al carrello la voce "Advanced Security + Privacy". Se l'utente fa clic sul passaggio successivo, la transazione includerà questo articolo e lo dovrà pagare.

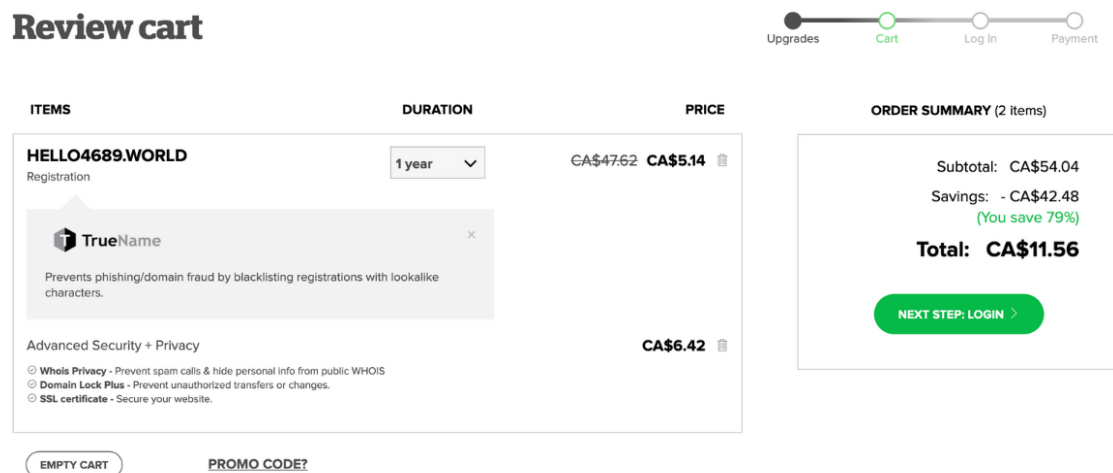


Figura 2.8: Dark Pattern Sneak into Basket in name.com

2.1.4 Bait and Switch

Con Bait and Switch l'utente sceglie un'azione che all'apparenza dà un risultato evidente, per poi provocare un altro indesiderato. Un esempio frequente di questo dark pattern è la "X" per la chiusura di un pop-up che, se cliccata, reindirizza l'utente su pagine indesiderate. In figura 2.9 è riportato un esempio di bait and switch, preso dal sito *darkpattern.org*. Questo esempio risale al 2016, dove agli utenti delle versioni precedenti di Windows, sono state mostrate finestre di pop-up. Con il passare dell'anno, Microsoft diventò sempre più aggressiva con i pop-up, e sempre più ingannevole dato che, premendo sul pulsante "X", gli utenti ottenevano il risultato opposto rispetto a quello aspettato. In questa versione di Windows, il significato del pulsante "X" non indicava "chiudi" ma "Sì, voglio aggiornare il mio computer a Windows 10". Questo specifico caso di Bait and Switch in Windows, provocò un'enorme reazione da parte dell'opinione pubblica.

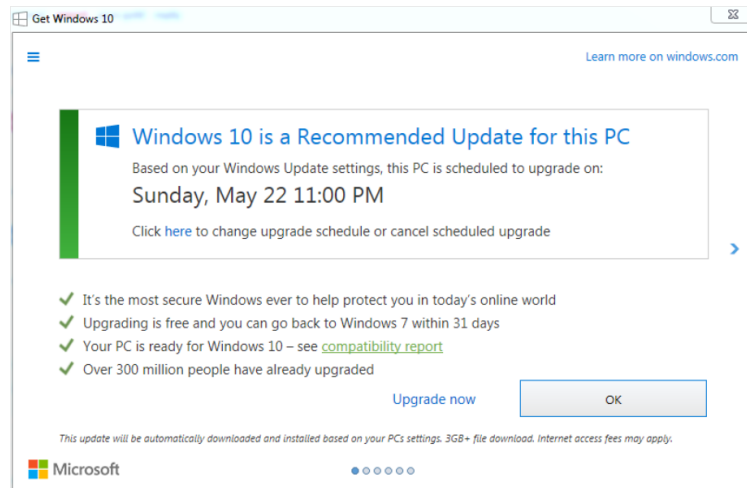


Figura 2.9: Dark Pattern Bait and Switch in Windows 10

2.1.5 Interface Interferences

Questa categoria comprende i dark pattern che manipolano l'interfaccia utente, privilegiando azioni specifiche rispetto ad altre, causando la confusione dell'utente. L'interface interferences utilizza numerosi inganni visivi e interattivi, ed è la strategia più diffusa. Questa categoria contiene tre sottotipi di dark pattern: **hidden information**, **preselection** e **aesthetic manipulation**.

Hidden Information

Le Hidden Information sono informazioni nascoste come opzioni rilevanti per l'utente, ma non rese subito accessibili. Possono manifestarsi come opzioni o contenuti nascosti attraverso stampa fine o testo scolorito. In figura 2.10 viene mostrata questa tecnica, in particolare sulla newsletter del sito *Greenpeace.it*: il link per disiscriversi è visualizzato con lo stesso font di un testo normale.

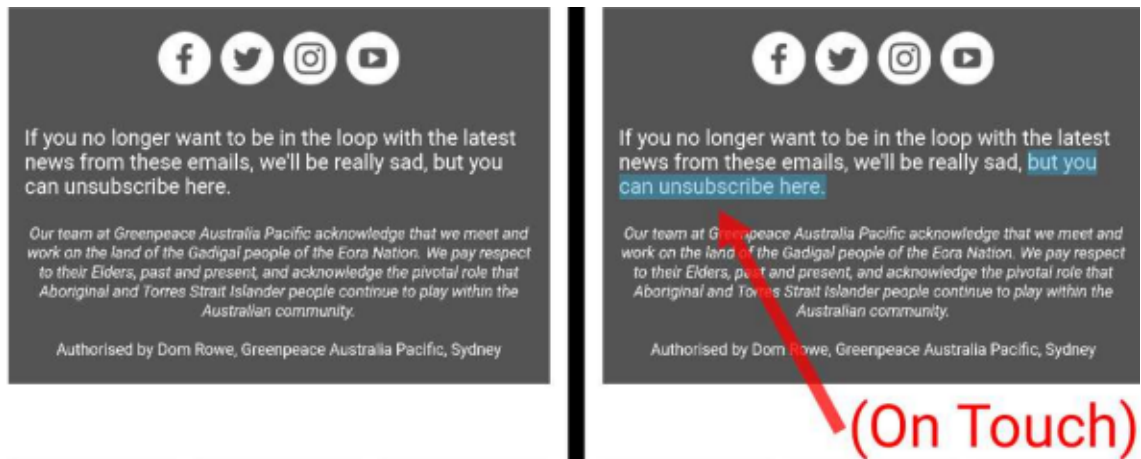


Figura 2.10: Dark Pattern Hidden Information in Greenpeace

Preselection

Il Preselection indica la presenza di un'opzione impostata come predefinita prima che l'utente possa effettivamente selezionarla. Questo dark pattern di solito appare come una selezione predefinita che il product owner vuole che l'utente selezioni. Questa selezione, ovviamente, è spesso contraria agli interessi dell'utente. Nell'esempio in figura 2.11, preso dal sito *dapde.de* è mostrato un uso del preselection. In questo esempio, l'abbonamento "risparmio" è già prelezionato al posto dell'ordine unico.

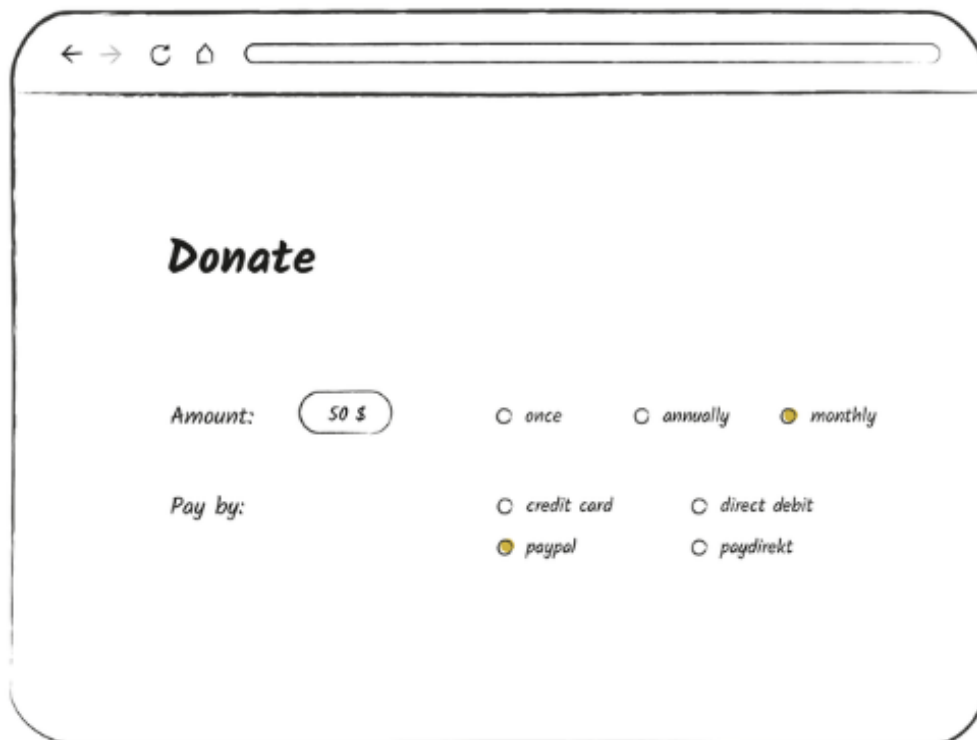


Figura 2.11: Dark Pattern Preselection, esempio realizzato dal sito dapde.de

Aesthetic Manipulation

L'aesthetic manipulation riguarda la manipolazione dell'interfaccia utente, in particolare la forma più che l'attenzione. Questa tipologia di dark pattern porta l'attenzione dell'utente su un elemento, per distrarlo e poi convincerlo a scegliere un altro elemento. Questo concetto è simile a quello espresso dalla "Misdirection" di Brignull. Aesthetic manipulation contiene ulteriori sottocategorie: **Toying with Emotion**, **False Hierarchy**, **Disguised Ads** e **Trick Question**.

Toying with Emotion

Si basa sull'utilizzo del linguaggio, dello stile, del colore o di altri elementi per evocare emozioni all'utente, al fine di persuaderlo ad effettuare una determinata azione. Il sito *booking.com* utilizza questa strategia, attraverso l'uso di colori e linguaggio che spingono l'utente ad affrettare la propria decisione, come mostrato in figura 2.12.



Figura 2.12: Dark Pattern Toying with Emotion in booking.com

False Hierarchy

Un dark pattern di questo tipo si basa sull'utilizzo di una gerarchia che dà precedenza visiva ad una o più opzioni rispetto ad altre, per convincere l'utente a selezionare una tra le prime opzioni. LinkedIn utilizza questa tecnica, come mostrato in figura 2.13, per mostrare l'opzione "prova premium gratis" nel menu "Account". Tipicamente questa opzione dovrebbe essere sotto alle altre.

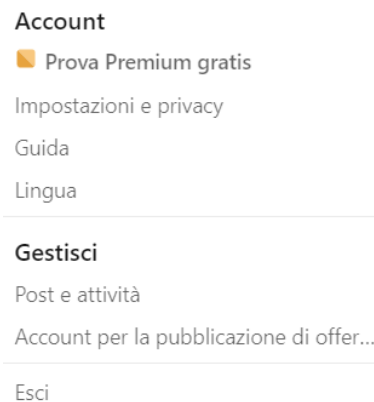


Figura 2.13: Dark Pattern False Hierarchy in LinkedIn

Disguised Ads

Il disguised ads definito da Brignull utilizza annunci nascosti da giochi interattivi o pulsanti per il download. Alcuni siti utilizzano questo pattern, facendo in modo che ad ogni click su qualsiasi parte del sito corrisponda il caricamento di un'altra pagina, rendendo l'intero sito un annuncio. Questo caso "estremo" di disguised ads è

mostrato in figura 2.14 : cliccando su una qualsiasi parte del sito, si apre un pop-up per il download.

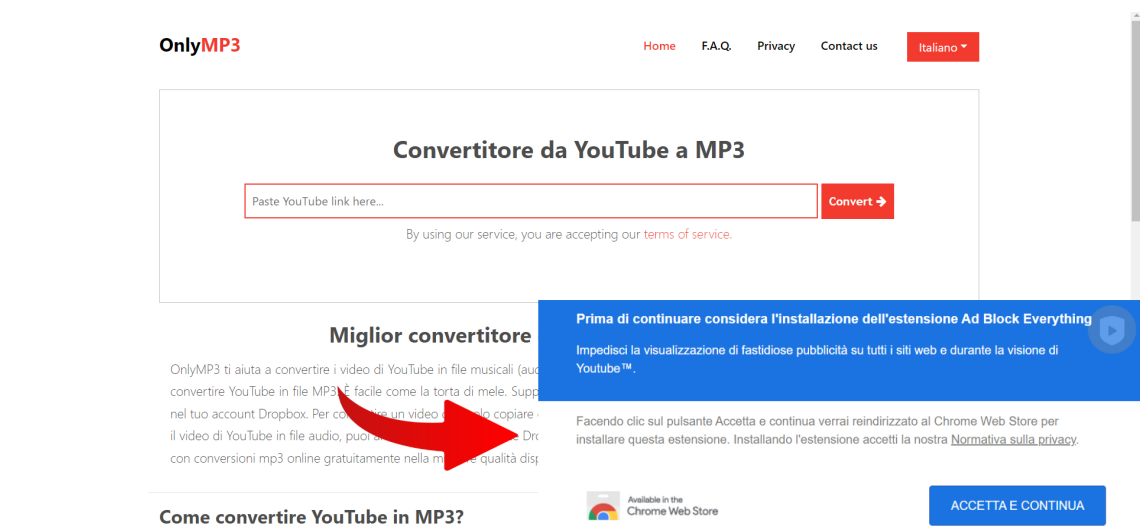


Figura 2.14: Dark Pattern Disguised Ads in OnlyMP3

Trick Questions

Il trick questions si basa sull'uso di domande trabocchetto, ovvero domande che sembrano intendere una cosa ma in realtà ne intendono un'altra, oppure utilizza una formulazione confusa delle domande, in modo da manipolare le scelte e le interazioni dell'utente. In genere viene mostrata una serie di caselle e vengono alternate in modo che spuntare la prima significa "opt out" e la seconda "opt-in", come l'esempio in figura 2.15, preso dal sito `darkpatterns.org`.



Figura 2.15: Dark Pattern Trick Questions fornito da `darkpatterns.org`

2.1.6 Forced Action

Questa categoria di dark pattern intende situazioni in cui gli utenti sono obbligati a compiere determinate azioni per accedere a determinate funzionalità di un sito.

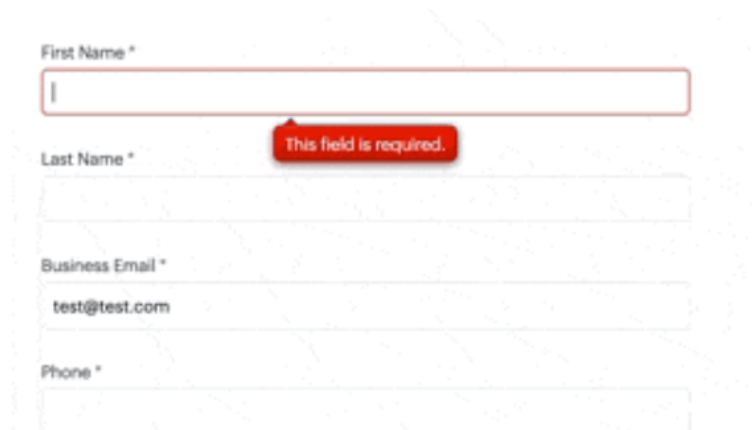
La categoria Forced Action include tre sottocategorie: **Social Pyramid, Privacy Zuckering, Gamification.**

Social Pyramid

Questo dark pattern è spesso utilizzato nei social media o nei giochi online. Gli utenti ottengono benefici extra invitando i loro amici ad utilizzare la piattaforma.

Privacy Zuckering

Il privacy zuckering è un dark pattern definito da Brignull, consiste nell'ingannare gli utenti e spingerli a condividere più dati personali di quelli che effettivamente intendono condividere; questo comporta la vendita delle informazioni a terze parti, incluse nei termini e condizioni o Privacy Policy dei siti web. Quando si prova a scaricare un ebook gratuito sul sito *Redis.com*, viene presentato un form che richiede di inserire il proprio indirizzo e-mail. Tuttavia, come mostrato in figura 2.16, il modulo si espande per includere ulteriori campi obbligatori. Questo cambiamento spinge l'utente ad inserire ulteriori informazioni non direttamente correlate al download dell'ebook.



The image shows a web form with the following fields and labels: "First Name *", "Last Name *", "Business Email *", and "Phone *". The "Business Email *" field contains the text "test@test.com". A red error message bubble with the text "This field is required." is positioned above the "Last Name *" field, indicating that this field is mandatory even though it was not initially shown as such.

Figura 2.16: Dark Pattern Privacy Zuckering in Redis.com

Gamification

Gamification indica una situazione in cui gli utenti sono costretti a svolgere ripetutamente le medesime azioni, al fine di sbloccare alcuni aspetti del servizio. L'esempio di Gamification più utilizzato è quello del "grinding", questo termine

indica il processo ripetuto di "uccisione di mostri" all'interno dei videogiochi, per ottenere punti esperienza e quindi far salire di livello il personaggio dell'utente. In figura 2.17 è mostrato un esempio di gamification, individuato sul videogioco FIFA23. In particolare, nella sezione "Division Rivals" dell'espansione FUT, il giocatore è spinto a giocare un numero elevato di partite (nell'esempio in figura fino a 90 partite), per ottenere premi utili a rinforzare la squadra dell'utente.



Figura 2.17: Dark Pattern Gamification in FUT 23

2.2 Influenza dei Dark Pattern

Nell'articolo di Di Geronimo *et al.*[4] del 2020 è presente uno studio sulla presenza dei dark pattern nelle applicazioni. Tra le 240 app studiate il 95 % conteneva uno o più dark pattern, 1787 in totale, con una media di 7,4 per applicazione.

Lo studio è stato condotto su un campione di 178 applicazioni mobile per Android e iOS, appartenenti a diverse categorie come giochi, produttività, social media, e-commerce e altre. Gli autori hanno utilizzato un approccio misto di analisi automatizzata delle app e valutazione umana, in cui gli utenti hanno valutato le app in base alla loro percezione di diversi schemi di design.

I risultati dello studio hanno mostrato che la maggior parte delle applicazioni mobile utilizzano almeno un tipo di UI Dark Pattern per influenzare le scelte degli utenti. Tra i diversi schemi di design analizzati, i ricercatori hanno identificato quelli che sono stati utilizzati più frequentemente, come la "False Hierarchy" (ovvero l'illusione di una scelta che in realtà è già stata preselezionata), il "Forced Action" (ovvero

l'obbligo di eseguire un'azione per proseguire l'utilizzo dell'app), la "Misdirection" (ovvero la manipolazione dell'attenzione dell'utente per nascondere o minimizzare alcune informazioni) e altri.

2.3 Implicazioni sulla privacy

I dark pattern sono tecniche di design che manipolano l'utente per compiere azioni che potrebbero non essere intenzionali. Possono avere implicazioni sulla privacy degli utenti in molteplici modi. In primo luogo, i dark pattern possono costringere gli utenti a condividere dati personali che altrimenti non avrebbero condiviso. In secondo luogo, i dark pattern possono spingere gli utenti ad accettare le politiche sulla privacy o i termini di servizio senza leggerli attentamente.

In terzo luogo, i dark pattern possono rendere difficile per gli utenti esercitare il loro diritto alla privacy, ad esempio impedendo loro di cancellare o modificare le loro informazioni personali.

In sintesi, i dark pattern possono avere implicazioni negative sulla privacy degli utenti, manipolando le loro scelte e facendo sì che condividano informazioni personali senza rendersene conto o senza il loro consenso. È importante che i designer, gli sviluppatori e le aziende adottino una prospettiva etica nella progettazione dei loro prodotti e servizi, evitando di utilizzare schemi manipolativi che mettono a rischio la privacy degli utenti.

Nel 2021, il California Consumer Privacy Act, ha vietato gran parte delle pratiche che utilizzano dark pattern, in particolare quelli che hanno l'effetto di compromettere le scelte degli utenti e quelli che coinvolgono i loro dati personali. Il Parlamento europeo ha approvato il Digital Service Act, una riforma del comparto digitale che punta a limitare chiunque svolga attività online, introducendo norme più stringenti riguardo all'uso di pubblicità e moderazione contenuti. Il regolamento europeo introduce requisiti rigidi per la rimozione di contenuti illegali, mentre per i contenuti dannosi ma legali, le piattaforme dovranno rispettare la libertà di espressione ma sono tenute a spiegare come personalizzano i contenuti per gli utenti. Le grandi piattaforme dovranno fornire un metodo alternativo non basato sui dati personali,

ad esempio Facebook dovrebbe ordinare i post in ordine cronologico e non in base a quelli che hanno più interazioni.

CAPITOLO 3

Dark Pattern Identifier

In base agli studi effettuati e analizzando i dark pattern individuabili all'interno di siti web, si è scelto di realizzare un'estensione Chrome in grado di identificare la presenza del dark pattern *Bait and Switch*. Successivamente verranno illustrate le fasi del lavoro svolto.

3.1 Ricerca di un Dark Pattern identificabile

La prima fase dello studio consiste nello scegliere un Dark Pattern facilmente identificabile all'interno di una pagina web. L'idea è stata quella di confrontare tutti i Dark Pattern e selezionare quelli che possono essere riconosciuti attraverso l'analisi del DOM (Document Object Model). Per la realizzazione dell'estensione è stato scelto il Dark Pattern *Bait and Switch*.

3.2 Algoritmo di detection

L'idea iniziale per detectare questa tipologia di design malevolo è stata quella di riconoscere tutte le immagini "piccole" contenute all'interno della pagina. Successivamente si è effettuato un ulteriore controllo per verificare la presenza di un

link all'interno di queste immagini, attraverso l'analisi del DOM. Per una maggior accuratezza sono stati analizzati anche elementi più piccoli della pagina, come ad esempio i bottoni. Di seguito sono illustrate le fasi per la realizzazione.

3.3 Implementazione algoritmo

L'algoritmo effettua un'analisi del DOM. Il Document Object Model presenta una struttura ad albero, dove ogni nodo contiene un elemento della pagina con le relative informazioni. L'algoritmo analizza i nodi di questo albero e individua potenziali dark pattern.

3.3.1 Analisi elementi

In questa fase viene effettuata una scrematura sugli elementi da analizzare. Nel caso della detection per *Bait and Switch*, vengono selezionati solo elementi di dimensioni contenute, come ad esempio piccole immagini, bottoni, ecc...

3.3.2 Verifica dei risultati

Dopo aver selezionato gli elementi "sospetti" si fa un ulteriore controllo per verificare se al di sotto di essi sono contenuti dei link ad altre pagine, in caso affermativo rende l'elemento della pagina un possibile dark pattern.

3.3.3 Invio risultati

I risultati ottenuti dai passaggi precedenti vengono inviati all'applicazione principale, in modo da rendere tutte le informazioni raccolte fruibili all'utente, all'interno dell'interfaccia grafica dell'estensione.

3.3.4 Architettura utilizzata

Per la realizzazione dell'algoritmo e dell'estensione sono stati utilizzati script comunicanti tra di loro attraverso API esterne. Nello specifico l'applicazione presenta la seguente struttura:

- HTML e CSS: questi file gestiscono lo stile e il layout utilizzati per la realizzazione dell'interfaccia grafica.
- Background Script: in questo script è contenuto il lato back-end dell'applicazione. Vengono gestite le operazioni in background e le operazioni di comunicazione tra gli script, inoltre contiene l'implementazione di un database interno, realizzato mediante l'API *IndexedDB*.
- Popup Script: Questo script si occupa della comunicazione con la UI, e comprende l'implementazione dell'interfaccia grafica. Il popup script viene eseguito ad ogni apertura dell'estensione.
- Content Script: Questo script permette di recuperare gli elementi del DOM, utilizzati poi per effettuare le operazioni citate precedentemente. Il content script viene eseguito al caricamento della pagina web corrente.

3.4 Sviluppo estensione Chrome

3.4.1 Interfaccia grafica e funzionamento

L'estensione web è totalmente user-friendly, infatti l'interfaccia consiste in una finestra che si apre all'attivazione dell'estensione. La suddetta finestra contiene un pulsante per l'attivazione; dopo aver avviato l'estensione, i possibili dark pattern all'interno della pagina vengono evidenziati da un box di colore rosso, e all'interno dell'estensione vengono rappresentati mediante una lista circolare il numero di dark pattern individuati e un link che richiama la pagina "nascosta", in modo da informare l'utente. Inoltre l'icona dell'estensione presenta un badge che tiene traccia del numero di possibili dark pattern rilevati.

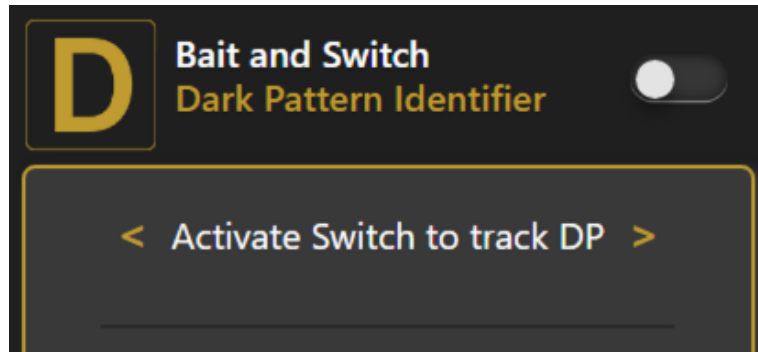


Figura 3.1: Estensione Chrome non attiva

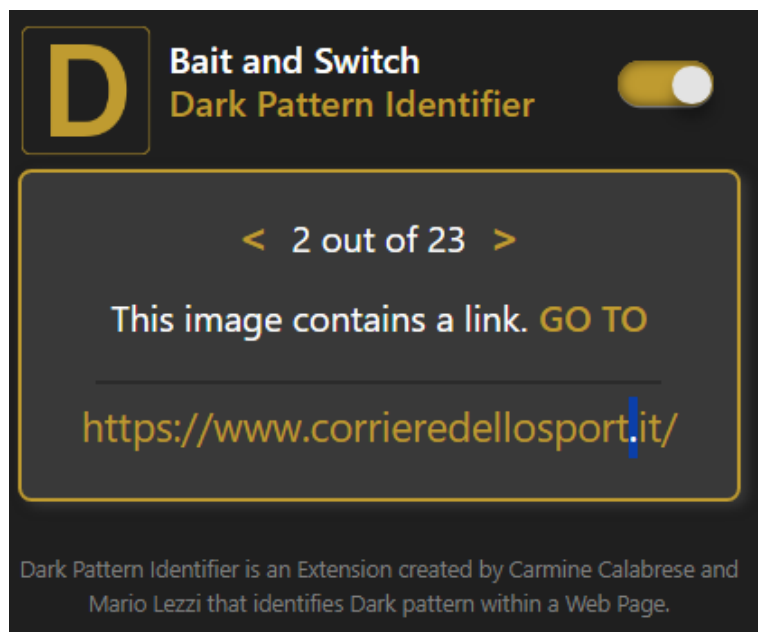


Figura 3.2: Estensione Chrome attiva

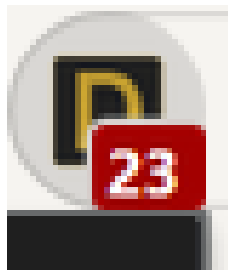
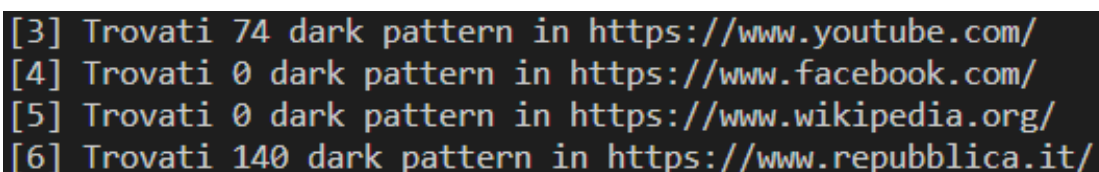


Figura 3.3: badge dell'estensione

CAPITOLO 4

Valutazione dell'approccio

Per valutare in modo accurato il corretto funzionamento dell'estensione Chrome, sono stati presi in considerazione i cento siti web più utilizzati in Italia nell'anno 2023. La procedura di analisi è stata focalizzata specificamente sulle homepage di ciascuno di questi siti. Al fine di automatizzare questo processo, è stato sviluppato un bot dedicato. Questo bot, utilizzando un file Excel contenente i cento link come punto di partenza, apre ciascun sito web identificato, apre l'estensione Chrome in modo sequenziale, raccoglie il numero visualizzato nel badge risultante e stampa il risultato ottenuto sulla console.



```
[3] Trovati 74 dark pattern in https://www.youtube.com/  
[4] Trovati 0 dark pattern in https://www.facebook.com/  
[5] Trovati 0 dark pattern in https://www.wikipedia.org/  
[6] Trovati 140 dark pattern in https://www.repubblica.it/
```

Figura 4.1: bot per il testing in esecuzione

Il test effettuato dal bot riporta quindi i risultati dell'estensione web applicata all'homepage di cento siti web. Dopo aver ottenuto questi risultati è stata svolta un'analisi più accurata, per verificare la precisione effettiva dell'estensione.

I risultati di questa analisi presentano un totale significativo di 2223 possibili dark pattern. Il 96% di tali casi è rappresentato da immagini, le quali contengono collegamenti interni ai rispettivi siti web. Questo risultato è particolarmente evidente nei siti che presentano caroselli di immagini contenenti notizie, evidenziando un tasso di possibili dark pattern notevolmente elevato in queste circostanze. La porzione rimanente, corrispondente al 4% dei risultati totali, sono quelli che più interessano lo studio effettuato fin qui. Tra gli 89 possibili positivi identificati, 83 di questi indirizzano l’utente verso pagine non desiderate. I restanti 6 casi, invece, rientrano nella categoria di dark pattern di tipo Bait and Switch.

I veri positivi riscontrati dall’analisi sono presenti nei seguenti siti: due su *asuratoon.com*, uno su *bing.com*, uno su *ilsole24ore.com*, uno su *libero.it* e uno su *fcinternews.it*. In tali casi, i dark pattern individuati conducono l’utente verso pagine differenti da quelle desiderate, principalmente promuovendo prodotto o abbonamenti. In particolare, va notato che uno dei sei casi ha portato l’utente verso una pagina bloccata e non disponibile.

Di seguito un’immagine riporta il dark pattern rilevato su *asuratoon.com* : l’utente viene reindirizzato su una pagina che pubblicizza fotovoltaici.

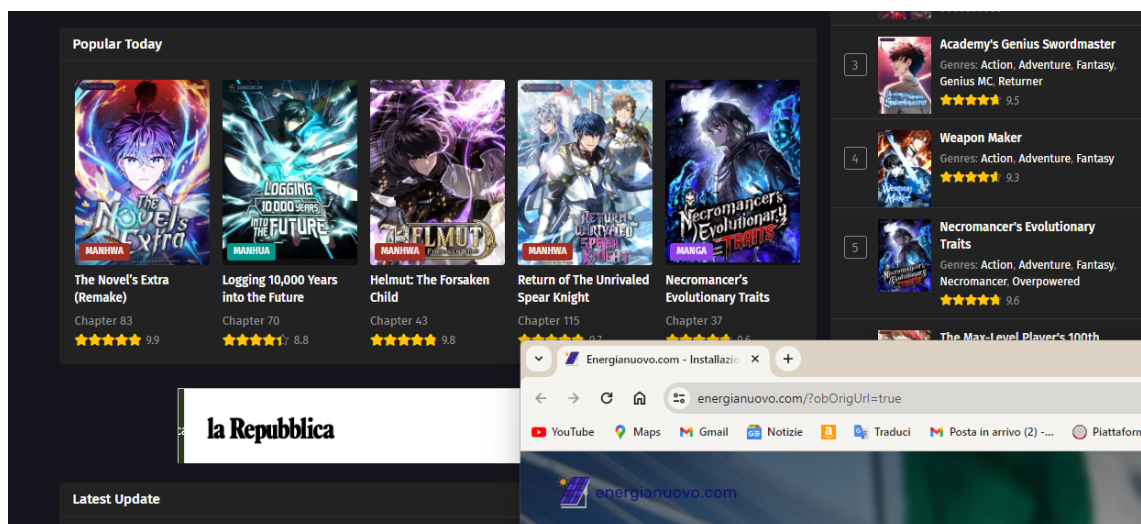


Figura 4.2: dark pattern presente su *asuratoon.com*

A seguito di questa analisi dettagliata, emerge che l’estensione Chrome riesce ad individuare con precisione piccole immagini che reindirizzano a pagine web differenti da quella inicial. Tuttavia, è importante notare una limitazione : l’estensione

fatica a riconoscere quando avviene un reindirizzamento verso pagine interne al sito stesso rispetto a un reindirizzamento verso pagine esterne completamente diverse dal sito web desiderato.



Figura 4.3: risultati su grafico a torta

Conclusioni e Sviluppi futuri

5.1 Conclusioni

L'obiettivo principale dello studio svolto era quello di realizzare un'estensione Chrome capace di informare e tutelare l'utente da design malevoli presenti sulle pagine dei siti web. L'approccio iniziale è stato quello di studiare, comprendere ed individuare le diverse categorie di dark pattern. Successivamente il focus è stato portato sull'identificare un dark pattern riconoscibile attraverso un'analisi del DOM, per poi implementare un algoritmo di detection da utilizzare nell'estensione. Il dark pattern che risponde a queste esigenze è il Bait and Switch. Dopo aver realizzato l'algoritmo, è stata realizzata l'interfaccia grafica dell'estensione, tenendo presente che il suo aspetto e funzionamento avrebbe dovuto rispondere alle esigenze dell'utente medio, il quale non ha una grande conoscenza dei design malevoli presenti in rete. L'estensione individua possibili dark pattern all'interno delle pagine web, in particolare analizza immagini o bottoni di dimensioni ridotte che contengono collegamenti ipertestuali. Una volta individuati tali elementi, li evidenzia con un box di colore rosso e informa l'utente, mostrando il link contenuto all'interno di essi. Un badge rosso sull'icona dell'estensione tiene informato l'utente sul numero di possibili dark pattern di tipo Bait and Switch presenti nella pagina corrente. Dopo aver completato

la realizzazione dell'estensione, è stata sottoposta a un processo di test, mediante l'utilizzo di un bot. I risultati del bot evidenziano un limite dell'estensione, ovvero un numero elevato di falsi positivi.

5.2 Sviluppo Futuri

Dopo avere testato e utilizzato l'estensione è emersa un'importante limitazione. L'estensione non è in grado di rilevare i falsi positivi, oltre gli effettivi dark pattern. Inoltre potrebbero essere aggiunte informazioni più specifiche sui dark pattern individuati, al fine di informare ulteriormente chi la utilizza. Un'altra limitazione riguarda il numero di dark pattern che l'estensione riesce ad individuare: dato che i siti web utilizzano immagini scalate, dopo un refresh della pagina, il numero di dark pattern rilevati potrebbe cambiare. Questi limiti dell'estensione sono una base di partenza per sviluppi futuri. In conclusione l'estensione fornisce uno strumento per navigare sul web in sicurezza, evitando di portare gli utenti a compiere azioni non desiderate e informarli sui possibili rischi.

Bibliografia

- [1] H. BRIGNULL, “Dark patterns: Deception vs.honesty in ui design,” *Smashing Magazine*, pp. 2–4, 2011. (Citato a pagina 5)
- [2] G. CONTI and E. SOBIESK, “Malicious interface design: Exploiting the user,” *Proceedings of the 19th international conference on World wide web*, pp. 271–280, 2010. (Citato a pagina 5)
- [3] C. M. GRAY, Y. KOU, B. BATTLES, J. HOGGATT, and A. TOOMBS, “The dark (patterns) side of ux design,” *Proceedings of the 2018 CHI conference on human factors in computing systems*, pp. 1–14, 2018. (Citato a pagina 6)
- [4] L. DI GIRONIMO, L. BRAZ, E. FREGNAN, F. PALOMBA, and A. BACCHELLI, “Ui dark patterns and where to find them: A study on mobile applications and user perception,” *Proceedings of the 2020 CHI conference on human factors in computing systems*, pp. 1–14, 2020. (Citato a pagina 20)

Ringraziamenti

Durante questi anni di studi ho avuto la fortuna di conoscere splendide persone che mi hanno accompagnato in questo percorso.

Ringrazio il mio relatore, il professore Fabio Palomba e la dottoressa Giulia Sellitto per avermi aiutato nella stesura di questa tesi, vi ringrazio per esservi mostrati disponibili sin dal primo momento.

Vorrei ringraziare On Gerà, che mi è stato vicino notte e giorno durante questi anni fin dal primo momento che ci siamo conosciuti, lo ringrazio per la splendida persona che è, sempre disponibile e generoso, e soprattutto milanista.

Ringrazio Andrea, il mio compagno di giochi all'università, con lui ho condiviso tanti bei momenti durante le nostre lunghe pause studio. Spero la nostra amicizia appena iniziata possa durare a lungo.

Ringrazio il Presidente, con lui ho condiviso la passione per i colori rossoneri, i video di Longoni e i viaggi in auto per andare all'Università, ti voglio tanto bene nonostante le tue teorie complottistiche su Maldini.

Un grazie Felice per le giornate passate insieme ad Atir, non le dimenticherò mai. Sei una delle persone più simpatiche e divertenti che abbia mai conosciuto.

Ringrazio Carmine per le giornate passate a studiare insieme i nostri ultimi esami, ti ringrazio per aver condiviso con me gli ultimi passi di questo percorso.

Ringrazio Biddau con cui ho condiviso splendidi momenti tra discussioni universitarie e non, purtroppo siamo stati poco tempo insieme durante questo percorso di studi

ma spero le nostre discussioni calcistiche possano continuare per molto tempo.

Ringrazio Raffaele e Rocco, due persone meravigliose e due amici d'oro che spero di ritrovare anche in futuro.

Un grazie speciale ai miei amici Renato e Alinei, vi ringrazio per essermi sempre vicino spero la nostra amicizia possa durare per sempre.

Ringrazio Marianna, mi sei stata sempre vicina durante questo percorso, mi hai sopportato, mi hai supportato, mi hai spronato nei momenti difficili e soprattutto hai sempre creduto in me, fin dal primo momento. Grazie per avermi sopportato quando il sabato sera rimanevo a casa per studiare e per avermi sempre spronato nei momenti più difficili di questo percorso, se li ho superati e anche grazie a te, grazie per tutto quello che fai per me.

Ringrazio Carmen, Liliana, Rossella e Giulio, siete i migliori cuginetti del mondo, vi voglio tanto bene.

Ringrazio la mia splendida famiglia, mia nonna, i miei zii Michele, Maria, Gianluca e Elvira, mio fratello e mio padre, ma soprattutto ringrazio la donna della mia vita, con cui amo litigare tutti i giorni, la donna che mi accompagna in ogni passo della mia vita, grazie di tutto mamma.

Questa tesi ha contribuito a piantare un albero in Kenya tramite il progetto Treedom.

<https://www.treedom.net/it/user/sesalab/event/sesa-random-forest>