

Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites

Accepted at [ACM CSCW 2019](#)

Dark patterns are user interface design choices that benefit an online service by coercing, steering, or deceiving users into making unintended and potentially harmful decisions. We conducted a large-scale study, analyzing ~53K product pages from ~11K shopping websites to characterize and quantify the prevalence of dark patterns.



[Read the paper \(final version\) »](#)



Please see the list of revisions [here](#).



Findings

- › We discovered 1,818 instances of dark patterns on shopping websites, which together represent 15 types of dark patterns.
- › These 1,818 dark patterns were present on 1,254 of the ~11K shopping websites (~11.1%) in our data set. Shopping websites that were more popular, according to Alexa rankings, were more likely to feature dark patterns.
- › We demonstrate which of the dark patterns that we discovered rely on consumer deception. In total, we uncovered 234 instances of deceptive dark patterns across 183 websites.
- › We identify 22 [third-party entities](#) that provide shopping websites with the ability to create dark patterns on their sites. Two of these entities openly advertise practices that enable deceptive messages.

Dark pattern categories

 **Sneaking** 
Attempting to misrepresent user actions, or delay information that if made available to users, they would likely object to.

 **Urgency** 
Imposing a deadline on a sale or deal, thereby accelerating user decision-making and purchases.

 **Misdirection** 
Using visuals, language, or emotion to steer users toward or away from making a particular choice.

 **Social proof** 
Influencing users' behavior by describing the experiences and behavior of other users.



Scarcity

Signaling that a product is likely to become unavailable, thereby increasing its desirability to users.



Obstruction

Making it easy for the user to get into one situation but hard to get out of it.



Forced Action

Forcing the user to do something tangential in order to complete their task.



Third parties that enable Social Proof Activity Notifications

Prevalence of third parties that enable Social Proof Activity Notifications are given below (based on our data set of 11K shopping websites and [Princeton Web Census crawls](#) of home pages of Alexa Top million websites). Where available, we list additional dark patterns the third parties claim to offer.

Third-party Entity	# Shopping Websites	# Alexa Top Million	Additional Dark Patterns
Beeketing	406	4,151	Pressured Selling, Urgency, Scarcity
Dynamic Yield	114	416	Urgency
Yieldify	111	323	Urgency, Scarcity
Fomo	91	663	--
Fresh Relevance	86	208	Urgency
Insider	52	484	Scarcity, Urgency
Bizzy	33	213	--
ConvertCart	31	62	--
Taggstar	27	4	Scarcity, Urgency
Qubit	25	73	Pressured Selling, Scarcity, Urgency
Exponea	18	180	Urgency, Scarcity
Recently	14	66	--
Proof	11	508	--
Fera	11	132	Pressured Selling, Scarcity, Urgency
Nice	10	80	--
Woocommerce Notification	10	61	--
Bunting	5	17	Urgency, Scarcity
Credibly	4	67	--

Convertize	3	58	Scarcity, Urgency
LeanConvert	2	0	--
Boost	1	3	--
Amasty	1	0	Pressured Selling, Scarcity, Urgency

Data and Code

The list of dark patterns can be downloaded [here](#) as a CSV file.

The [GitHub repository](#) contains crawler code, the crawled data, and the analysis scripts.

Revisions

Update (July 17, 2019): We have released our paper on [arXiv](#). The previous version can be found [here](#).

Update (July 1, 2019): In our previous release, we had marked all opt-out choices accompanied by checkboxes as Trick Questions dark patterns. Our classification was guided by the definition of Trick Questions provided by [Gray et al.](#) Since then we have narrowed our definition to only include opt-out choices that are misleading, such as when the user has to check a box and the text began with an affirmative statement about the undesirable practice. We have updated the paper and the CSV file (previous version of the paper and data can be found [here](#) and [here](#)). We have also made minor proofreading edits in the current version of the paper.

Citation

```
@article{Mathur2019DarkPatterns,
  title = {Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites},
  author = {Mathur, Arunesh and Acar, Gunes and Friedman, Michael and Lucherini, Elena and Mayer, Jonathan and Chetty, Marshini and Narayanan, Arvind},
  year = 2019,
  journal = {Proc. ACM Hum.-Comput. Interact.},
  publisher = {ACM},
  volume = 1,
  number = {CSCW},
  issue_date = {November 2019}
}
```

Links

- [Dark patterns \(Harry Brignull\)](#)
- [UXP2: Dark patterns @ Purdue University](#)

Contact

We are researchers from Princeton University and University of Chicago.

This study is part of the Princeton University's [WebTAP project](#).

Arunesh Mathur	amathur@cs.princeton.edu
Gunes Acar	gunes@princeton.edu
Michael Friedman	mjf4@princeton.edu
Elena Lucherini	elucherini@cs.princeton.edu
Jonathan Mayer	jonathan.mayer@princeton.edu
Marshini Chetty	marshini@uchicago.edu

