

Dark patterns: what to look for

16 patterns, grouped under the 5 strategies of Gray et al.'s (2024) ontology. For each one, what to check in the interface. The guide is for spotting whether a pattern is there, not for grading it.

Sneaking

Hiding, disguising or delaying information that, if the person saw it in time, would lead them to decide differently (Gray et al., 2024, p. 17).
2 patterns

Sneak into basket

How to check: Add a single product and read the cart line by line before paying. Go back through the previous steps and look for ticked boxes you did not tick.

By text? **No**

Drip pricing or hidden costs

How to check: Write down the price shown on the product page and compare it with the total on the last step before paying. Every difference should have been disclosed from the start.

By text? **Partly**

Obstruction

Making a task harder than it needs to be in order to dissuade the person (Gray et al., 2024, p. 17).
2 patterns

Roach motel

How to check: Compare the two paths: how many steps and which channel it takes to sign up, and how many it takes to leave. If you cannot find how to leave in the interface, look in the terms and conditions: that is often where “by phone only” lives (Mathur et al., 2019, p. 21; SERNAC, 2021, p. 30).

By text? **Partly**

Price comparison prevention

How to check: Try to compare two equivalent options. If you have to take notes by hand, open each one or work out unit prices to do it, there is a barrier. Whether the barrier is deliberate cannot be proven from the outside; record it as a finding with that caveat.

By text? **No**

Interface interference

Manipulating the interface to privilege some actions over others (Gray et al., 2024, p. 17).
3 patterns

Visual interference

How to check: Compare the options within the same decision: size, color, contrast and position. If one looks disabled, click it.

By text? **No**

Trick questions

How to check: Read every checkbox out loud and ask what happens if you tick it and what happens if you don't. Mathur et al. only count as a trick question an opt-out box that opens with an affirmative statement. Those that open by offering the opt-out (“Tick here to opt out of...”) are recorded separately, as concerning but not deceptive (note 9, p. 17).

By text? **Partly**

Pressured selling

How to check: Check which variant is selected when you open the product page. If it is the most expensive one, note it. Also check whether a pop-up interrupts the way to the cart.

By text? **Partly**

Forced action

Requiring an additional action, such as signing up or handing over data, before the person can continue (Gray et al., 2024, p. 18).
2 patterns

Forced registration

How to check: Try to complete the task without an account. If a window appears, look for a way to close it without signing up. Ask what data each step actually needs.

By text? **Partly**

Forced continuity or hidden subscription

How to check: Before paying, look for three things: whether it renews, how much it will charge and when. If any of them is not visible, note it. Asking for a card is not enough to call it a dark pattern; SERNAC treats it as a signal (p. 29), but the proof is that the renewal is not disclosed.

By text? **No**

Social engineering

Presenting options or information that lean on social pressure or cognitive biases to get the person to act (Gray et al., 2024, p. 19).
7 patterns

Countdown timer

How to check: Note the time the clock reaches zero and come back afterwards, and again the next day. It is deceptive if it **resets with the same offer** or if **the offer is still available** after it expired (Mathur et al., 2019, p. 15).

By text? **Partly**

Test for deception

Limited-time message

How to check: Look for the end date in the fine print, in the promotion's conditions and on the terms page. Mathur et al. only counted it when it was in none of those places (pp. 15–16).

By text? **Partly**

Low-stock message

How to check: Come back several times over a few days and note the number. It is suspicious if it drops on a fixed schedule, changes when you reload the page, or the message appears on almost every product (Mathur et al., p. 20).

By text? **Partly**

Test for deception

High-demand message

How to check: Check whether the message changes with the product. Mathur et al. found that 38 of 47 appeared the same whatever the product or the cart contents (p. 21).

By text? **Partly**

Activity messages

How to check: Look at the page source: Mathur et al. found numbers generated at random and messages hard-coded so that they never changed (pp. 18–19). Also check which script draws the message: many come from third-party providers, and some openly advertised fake orders (pp. 22–24).

By text? **Partly**

Test for deception

Testimonials of uncertain origin

How to check: Two tests from Mathur et al. (p. 19): see whether the site has a form for submitting testimonials, and search Google for the exact text of one. They found the same testimonials on another site under different names.

By text? **Partly**

Confirmshaming

How to check: Read the decline option without looking at the other one. If it describes the person (“I like paying more”) rather than the action (“no, thanks”), it is confirmshaming. This one needs no proof of deception: you can see it.

By text? **Partly**