GETTY IMAGES

'Dark patterns' on the Internet: how companies are tricking their users

What are dark patterns on the Internet and how are users getting affected by it? How are Big Tech firms using this to downgrade the user experience? What do Internet users lose due to these unethical interface designs?

Sahana Venugopal

The story so far:

Some Internet-based firms have been tricking users into agreeing to certain conditions or clicking a few links. The unsuspecting users would not have accepted to such terms or clicked urls (uniform resource locator), but for the deceptive tactics deployed by tech firms. Such acceptances and clicks are flooding inboxes of the users with promotional emails they never wanted, making it hard to unsubscribe or request deletion. These are examples of "dark patterns," also known as "deceptive patterns."

What are dark patterns?

Such patterns are unethical user interface designs that deliberately make your Internet experience harder or even exploit you. In turn, they benefit the company or platform employing the designs.

By using dark patterns, digital platforms take away a user's right to full information about the services they are using and their control over their browsing experience.

The term is credited to UI/UX (user interface/user experience) researcher and designer Harry Brignull, who has been working to catalogue such patterns and the companies using them since around 2010.

How do companies use dark patterns?

Social media companies and Big Tech firms such as Apple, Amazon, Skype, Facebook, LinkedIn, Microsoft, and Google use dark or deceptive patterns to downgrade the user experience to their advantage.

Amazon came under fire in the EU for its confusing, multi-step cancelling process in Amazon Prime subscription. After communicating with consumer regulators, Amazon this year made its cancellation process easier for online customers in European countries.

In social media, LinkedIn users often receive unsolicited, sponsored messages from influencers. Disabling this option is a difficult process with multiple steps that requires users to be familiar with the platform controls.

As Meta-owned Instagram pivots to video-based content to compete against TikTok, users have complained that they are being shown suggested posts they did not wish to see and that they were unable to permanently set preferences.

Another dark pattern on the application is sponsored video ads getting scattered between reels and stories users originally opted to view, tricking them for several seconds before they can see the small "sponsored" label.

Google-owned YouTube nags users to sign up for YouTube Premium with pop-ups, obscuring final seconds of a video with thumbnails of other videos – a way of disrupting what should have been an otherwise smooth user experience.

What do users stand to lose because of dark patterns?

Dark patterns endanger the experience of Internet users and make them more vulnerable to financial and data exploitation by Big Tech firms. Dark patterns confuse users, introduce online obstacles, make simple tasks time-consuming, have users sign up for unwanted services/products, and force them to pay more money or share more personal information than they intended.

In the U.S., the Federal Trade Commission [FTC] has taken note of dark patterns and the risks they pose. In a report released in September this year, the regulatory body listed over 30 dark patterns, many of which are considered standard practice across social media platforms and e-commerce sites.

These include "baseless" countdowns for online deals, conditions in fine print that add on to costs, making cancellation buttons hard to see or click, making ads appear as news reports or celebrity endorsements, auto-playing videos, forcing users to create accounts to finish a transaction, silently charging credit cards after free trials end, and using dull colours to hide information that users should know about.

In one instance, the FTC report outlined its legal action against Amazon in 2014, for a supposedly "free" children's app that fooled its young users into making in-app purchases that their parents had to pay for.

"Once the account holder downloaded the app and children began playing the game, unbeknownst to the account holder, kids could rack up multiple charges, ranging from $0.99 to $99.99 each, by tapping buttons, with no account holder involvement. These purchases were disguised as play," stated the release.

The case was settled after Amazon agreed to refund over $70 million.

However, dark and deceptive patterns don't just stop with laptops and smartphones. The FTC report has warned that as augmented reality (AR) and virtual reality (VR) platforms and devices grow in usage, dark patterns will likely follow users to these new channels as well.

Internet users who are able to identify and recognise dark patterns in their daily lives can choose more user-friendly platforms that will respect their right to choose and privacy.