International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Dark Patterns in UI: User Awareness and Ethical Implications

Anusha Sanghavi

ITM SLS Baroda University
Guided by: Prof. Shivangi Matieda

Abstract- In today's rapidly evolving digital landscape, the prevalence of dark patterns in user interfaces (UI) presents substantial ethical challenges and heightens the need for user awareness. Dark patterns are manipulative design tactics that exploit cognitive biases, misleading users into making decisions that may not align with their best interests. As highlighted in recent research, a majority of users are aware of these deceptive techniques; however, they often struggle to effectively combat them due to various barriers such as a lack of awareness, cognitive biases, and the allure of short-term benefits (Singh V et al.). Furthermore, the ability to recognize these patterns is often limited by unclear interface information and pervasive marketing strategies that blend seamlessly with harmful designs (Zahratunnisa HS et al.). This underscores an urgent need for improved consumer education and ethical design practices, fostering a digital ecosystem that prioritizes transparency and user empowerment in the face of manipulative tactics."

I. Introduction

The rise of persuasive technology has reshaped how digital platforms engage with users. While UI design traditionally aims to improve usability and enhance user experience, it has increasingly been exploited to manipulate user behavior through what are known as dark patterns. These deceptive designs, while legal in many jurisdictions, raise critical ethical concerns and have become widespread across websites, apps, and software.

Dark patterns refer to interface designs crafted to trick users into actions they might not have taken intentionally. Common examples include:

- Fake download buttons: Designed to mimic legitimate actions but redirect users to ads or malicious content.
- Sneak into basket: Adding items to a user's cart without consent.
- Roach motel: Easy to get into a situation (e.g., signing up), but hard to get out (e.g., unsubscribing or deleting an account).
- Confirmshaming: Guilt-tripping users into opting into something.
- Forced continuity: Making it difficult to cancel free trials.

These patterns exploit psychological principles, such as decision fatigue, scarcity, and fear of missing out (FOMO).

Real-World Examples

- Misleading download buttons: Many users intending to download files end up redirected to gambling websites or prompted to install unsafe applications.
- Account deletion obstacles: Social media platforms like Instagram simplify account creation but impose multiple steps for account deletion, discouraging users from leaving.
- Pre-ticked checkboxes: Websites automatically select additional purchases or subscriptions.
- Pop-ups and fake system alerts: Trick users into clicking or providing
personal information.

Instagram
Phone number, username, or email
Password
Log In
OR
Log in with Facebook
Forgot password?
Don't have an account? Sign up
Get the app
App Store
Google Play
ABOUT HELP PRESS API JOBS PRIVACY TERMS
LOCATIONS TOP ACCOUNTS HASHTAGS LANGUAGE

Fig 1.1 Login Page of Instagram

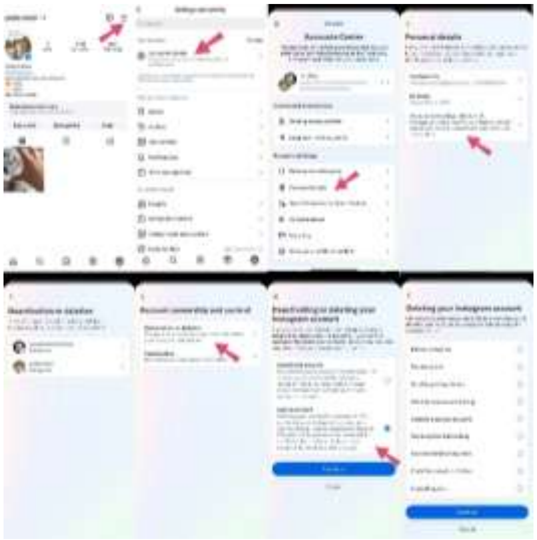


Fig 1.2 Steps to delete account on Instagram

II. VICTIMS, SCAMS, AND USER VULNERABILITY IN THE AGE OF DECEPTIVE INTERFACES

The rise of dark patterns in user interface design has not only influenced digital decision-making but has also become a gateway for large-scale scams that exploit trust, familiarity, and urgency. Real-world incidents demonstrate how manipulative design—paired with deceptive communication—can lead to financial loss, identity theft, and compromised personal data.

3.1 Phishing Through Familiarity: The PayPal Incident

In late 2023, cybercriminals launched a sophisticated phishing campaign targeting PayPal users. Fake websites were crafted to closely mimic the legitimate PayPal login page, using domain names like "paypaysecurity.com" and "paypa1.com." These URLs were carefully designed to deceive users at a glance, exploiting the visual similarity to the official domain.

The attack was supported by email notifications warning users of suspicious account activity, prompting them to log in immediately. Once redirected to the fraudulent sites, victims unknowingly submitted their credentials, which hackers used to hijack accounts, initiate unauthorized transactions, and access linked bank details. Though exact loss figures remain undisclosed, a similar scam in 2020 saw reported damages exceeding $8 million. This case underlines how even minor UI choices—such as the design of a login page or the layout of a warning message—can significantly impact user trust and behavior.

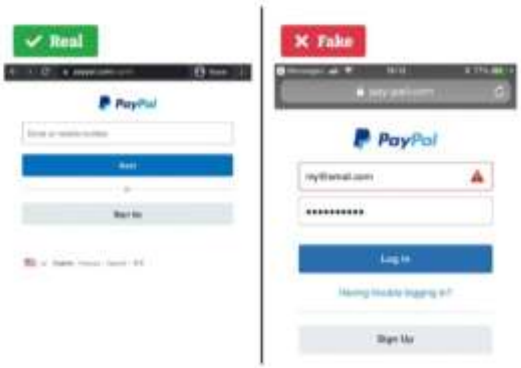
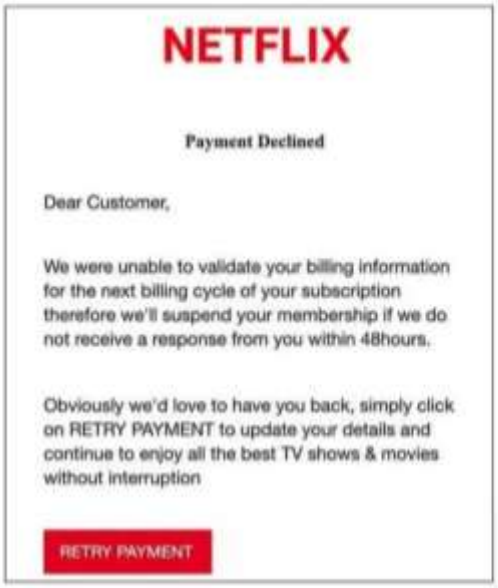


Fig 3.1.1 Real and Fake PayPal Website

3.2 Streaming into Trouble: Netflix Scam Campaigns

Streaming platforms have also become targets for deceptive campaigns. In late 2023, a phishing scheme involving fake Netflix portals began circulating via email. These messages warned users that their accounts were at risk of suspension due to failed payment issues. Embedded within the emails were links directing users to counterfeit Netflix login pages that replicated the original interface with astonishing accuracy.

Once logged in, users unknowingly handed over personal identification information (PII), including billing addresses, credit card numbers, and passwords. The scam leveraged urgency—common in dark pattern design—by suggesting the account would be locked within 24 hours unless immediate action was taken. This type of manipulation preys on fear and the psychological discomfort of losing access to entertainment or essential services.



NETFLIX

Payment Declined

Dear Customer,

We were unable to validate your billing information for the next billing cycle of your subscription therefore we'll suspend your membership if we do not receive a response from you within 48hours.

Obviously we'd love to have you back, simply click on RETRY PAYMENT to update your details and continue to enjoy all the best TV shows & movies without interruption

RETRY PAYMENT

Fig 3.2.1 Fake Netflix Interface

These examples illustrate how dark patterns, when combined with phishing and social engineering, amplify the risk of digital exploitation. Users are not only misled—they are systematically deceived through the very interfaces designed to serve them. As online scams become increasingly sophisticated, recognizing and addressing these deceptive patterns becomes a crucial step toward user protection and ethical design.

of critical remarks. In that cases don't get disheartened and try to improvise the maximum.

III. COMBATING DARK PATTERN

Tackling the widespread use of dark patterns requires a multi-faceted approach, involving ethical design practices, industry responsibility, and government regulation. As deceptive UI elements become more sophisticated, the response must evolve to ensure digital experiences prioritize user rights, consent, and transparency.

4.1 Ethical UI Design Principles

Ethical UI design is rooted in honesty, user empowerment, and usability. A few foundational principles—when consistently applied—can significantly reduce user manipulation.

• Clarity

A transparent interface ensures that users understand what will happen when they take an action. For instance, a clear call-to-action on a subscription page should differentiate between starting a free trial and enrolling in a paid plan.

• Choice Architecture

This principle refers to the way options are structured to guide users toward a decision. Ethical design ensures all choices—especially those that may not benefit the business—are given equal prominence.

• Reversibility

Ethical interfaces make it easy for users to undo actions such as subscribing, signing up, or deleting data. A process that is easy to enter should be just as easy to exit.

4.2 Industry and Policy-Level Recommendations

Ethical UI cannot rely solely on individual developers or companies; systemic interventions are necessary to prevent widespread abuse of dark patterns.

• Standardized UI Guidelines

Developing international standards for ethical interface design can help reduce the ambiguity around what constitutes a dark pattern. These guidelines should define acceptable design practices, especially around consent, subscriptions, privacy, and personalization.

•Auditing and Transparency Reports

Large platforms should be held accountable for the way they design interfaces. Regular audits by independent third parties—alongside public usability and ethics reports—can help detect the use of dark patterns.

• Legal Frameworks

Government action plays a vital role in curbing unethical design. Regulatory frameworks should penalize companies found guilty of deliberately misleading users. These laws should also encourage complaint mechanisms and empower users to report suspicious UI behavior.

By aligning design practices with ethical principles, establishing clear guidelines, and implementing enforceable laws, the digital ecosystem can move toward a future where users feel empowered, not exploited. Combating dark patterns is not just a matter of design—it's a matter of digital rights and human dignity.

IV. CONCLUSION

In an age where digital interactions govern many aspects of our lives—from communication and banking to entertainment and healthcare—the design of user interfaces plays a critical role in shaping our experiences, behaviors, and even decisions. While good UI design aims to simplify, guide, and support user goals, the rising use of dark patterns reveals a more troubling side of this influence.

Dark patterns exploit cognitive biases, urgency, and confusion to manipulate users into making decisions that often benefit companies at the expense of the user's interests. These manipulative tactics—ranging from fake download buttons to complex account deletion flows—are not simply poor design choices but are intentional strategies that undermine trust, autonomy, and transparency.

Our analysis has shown how such deceptive design practices are deeply embedded across industries, from e-commerce and streaming platforms to financial services and tech support scams. The real-world examples of PayPal phishing, fake Apple support sites, and Netflix clone portals illustrate how easily users can be victimized when design is weaponized for malicious purposes.

Despite growing awareness, many users remain vulnerable due to lack of digital literacy, the sophistication of scams, or the normalization of deceptive patterns. Even when users recognize that something feels off, they often lack the time or resources to respond critically or protect themselves.

The ethical implications of these practices cannot be overstated. When businesses prioritize conversion rates over consumer consent, they create a digital environment that erodes user agency and fosters distrust. A short-term gain for businesses may translate into long-term harm for users and the broader digital ecosystem.

To address this, ethical UI design must become a standard rather than an exception. Interfaces should be clear, reversible, and designed to present all choices fairly. Clarity in design allows users to make informed decisions. Reversibility ensures that users can undo actions without friction. Balanced choice architecture prevents users from being coerced into undesired outcomes.

Beyond design principles, systemic solutions are essential. Regulatory bodies must step in to define, identify, and penalize the use of dark patterns. Legislation like the California Privacy Rights Act (CPRA) and guidelines from the European Union are important steps, but global consensus and enforcement are needed. Transparency reports, independent audits, and user reporting mechanisms should become routine practices for digital platforms.

Moreover, digital literacy programs should be promoted to empower users to recognize and respond to deceptive tactics. Schools, communities, and organizations must educate people not only about the benefits of digital tools but also about the risks that come with poorly regulated design.

The responsibility lies with all stakeholders—designers, companies, regulators, and users—to ensure the internet remains a place of choice, not coercion. As we look to the future, the fight against dark patterns is not just a technical or legal issue; it is a human one. Ethical design has the potential to restore balance, rebuild trust, and protect the dignity of every digital citizen.

Let us choose design that respects, empowers, and defends the user—because manipulation has no place in the future of technology

REFERENCES

[1] Memcyco. (2024, March 5). 5 recent examples of fake websites to watch out for. Memcyco. https://www.memcyco.com/5-recent-examples-of-fake-websites/

[2] ExpressVPN. (2024). List of scam shopping websites and how to identify them.https://www.expressvpn.com/blog/list-of-scam-shopping-websites/?srsltid=AfmBOorIHlQbWcdUvJsyZmxTYTX1TVnE20jTrsQ1n73xI3BC8sh2DLTQ

[3] Pritchard, J. (2023, October 30). Watch out for these top internet scams. Investopedia. https://www.investopedia.com/articles/personal-finance/040115/watch-out-these-top-internet-scams.asp

[4] Mathur, A., Acar, G., Friedman, M. G., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2020). Dark

Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. Proceedings of the ACM on Human-Computer Interaction, 4(CSCW2), 1–32. https://doi.org/10.1145/3415211

[5] Laws of UX. (n.d.). Key principles that drive user behavior. https://lawsofux.com/

.

AUTHORS

First Author – Anusha Sanghavi, Bachelor in Computer Science and Technology, ITM SLS Baroda University, sanghavi29anusha@gmail.com.

.