Dark Patterns czym są i jak się przed nimi chronić?

1. Informacje ogólne

Dark patterns to techniki stosowane w projektowaniu interfejsów użytkownika, które mają na celu manipulowanie użytkownikami w taki sposób, aby podejmowali decyzje korzystne dla firmy. Są to subtelne, ale celowe zabiegi, które mogą prowadzić do niezamierzonych zakupów, subskrypcji czy udostępnienia danych osobowych. Dark patterns przybierają niejednolite formy – mogą jawić się użytkownikom jako ukryte informacje o możliwości rezygnacji z subskrypcji, brak informacji o kosztach wysyłki, automatyczne dodawanie produktów do koszyka. W praktyce najczęstszą sytuacją jest zasypywanie treściami i automatyczne przedłużanie subskrypcji bez zgody użytkownika. Współcześnie nie jest możliwe wskazanie skutecznej metody ochrony przed tego typu szkodliwymi wzorcami. Kluczowe jest jednak dla użytkowników Internetu przestrzeganie należytej ostrożności w trakcie korzystania z określonych platform internetowych.

2. Przykłady dark patterns

- **Przemyślana zgoda**: Ukrywanie opcji rezygnacji lub ustawienie jej w sposób, który sprawia, że użytkownik przypadkowo zgadza się na coś, czego nie chce.
- **Przekierowanie uwagi**: Skupianie uwagi użytkownika na jednym elemencie interfejsu, aby ukryć lub zminimalizować znaczenie innego, mniej korzystnego dla firmy elementu. **Przykład**: Przycisk „Kup teraz” jest duży i kolorowy, podczas gdy przycisk „Dowiedz się więcej” jest mały i szary.
- **Utrudniona rezygnacja**: Utrudnianie procesu anulowania subskrypcji, np. przez brak wyraźnej opcji anulowania lub konieczność wykonania wielu kroków.
- **Natarczywe pytania**: Stosowanie komunikatów, które sprawiają, że użytkownik czuje się winny, jeśli nie zgodzi się na pewne działania. **Przykład**: Okienka wyskakujące, które pytają „Czy na pewno chcesz zrezygnować z tej niesamowitej oferty?”, utrudniając proces zamknięcia.
- **Ukryte koszty**: Dodawanie opłat na końcu procesu zakupu, które nie były wcześniej wyraźnie widoczne. **Przykład**: Koszty wysyłki, które pojawiają się dopiero po wprowadzeniu danych karty płatniczej.

3. Jak się przed tym chronić?

1. **Uważne czytanie**: Zawsze należy dokładnie czytać każdy komunikat, który pojawia się podczas korzystania z aplikacji czy strony internetowej, szczególnie podczas zakupów czy rejestracji.
2. **Szukanie opinii**: Przed zakupem lub rejestracją należy zweryfikować opinie innych użytkowników na temat danej strony lub aplikacji.
3. **Należy korzystać z narzędzi blokujących reklamy**: Niektóre rozszerzenia przeglądarek internetowych mogą pomóc w blokowaniu elementów, które mogą być częścią dark patterns.
4. **Ostrożność przy subskrypcjach**: Zawsze należy sprawdzić, czy subskrypcje są automatycznie odnawiane i jakie są warunki ich anulowania.
5. **Należy korzystać z rozszerzeń do przeglądarek**: Istnieją rozszerzenia, które pomagają zidentyfikować i zablokować dark patterns, np. “Dark Reader”.
6. **Regularne przeglądanie ustawień prywatności**: Należy regularnie sprawdzać i aktualizować ustawienia prywatności na stronach internetowych i w aplikacjach, z których użytkownik korzysta.
7. **Edukacja i świadomość**: Należy czytać artykuły, blogi i raporty dotyczące nowych technik manipulacyjnych w projektowaniu interfejsów użytkownika.

8. **Zgłaszanie nieuczciwych praktyk**: Kiedy użytkownik zauważy praktyki dark patterns na stronie internetowej lub w aplikacji, powinien niezwłocznie zgłosić to odpowiednim organom, takim jak organizacje konsumenckie czy organy regulacyjne ds. ochrony danych osobowych.
9. **Ostrożność przy udostępnianiu danych osobowych**: Należy zawsze zastanowić się dwa razy przed podaniem swoich danych osobowych i sprawdzić, jak będą one wykorzystywane. Należy unikać rejestracji na stronach, które wymagają więcej informacji niż jest to konieczne do korzystania z ich usług.
10. **Regularne monitorowanie kont bankowych i kart kredytowych**: Śledzenie wszystkich transakcji może pomóc w szybkim zauważeniu i anulowaniu nieautoryzowanych subskrypcji. Np. sprawdzanie wyciągów bankowych co miesiąc w poszukiwaniu podejrzanych opłat.
11. **Znane przypadki i inicjatywy przeciw dark patterns:**

- **Apple iOS 14**: Wprowadzenie przez Apple w systemie iOS 14 wymogu uzyskiwania zgody użytkowników na śledzenie między aplikacjami jest krokiem w stronę większej transparentności i ochrony prywatności.
- **GDPR**: Ogólne Rozporządzenie o Ochronie Danych Osobowych (GDPR) w Unii Europejskiej wprowadziło surowe przepisy dotyczące zgody na przetwarzanie danych osobowych, co zmusza firmy do bardziej przejrzystych działań.
- **California Consumer Privacy Act (CCPA)**: Ustawa o ochronie prywatności konsumentów w Kalifornii daje użytkownikom większą kontrolę nad ich danymi i wymaga od firm informowania o zbieraniu i przetwarzaniu danych.

5. Jakie są konsekwencje stosowania „dark patterns”?

Stosowanie „dark patterns” może skutkować naruszeniem nie tylko przepisów o ochronie konsumentów, ale także o ochronie danych osobowych (w szczególności RODO).

Prezes UOKiK już postawił popularnym sklepom internetowym born2be.pl i renee.pl zarzut naruszenia praw konsumentów poprzez wprowadzanie konsumentów w błąd m.in. na skutek stosowania jednego z popularnych „zwodniczych interfejsów”. Te sklepy internetowe, przy użyciu zegara odliczającego czas do zakończenia promocji, sugerowały użytkownikom ograniczony czas na otrzymanie rabatu, podczas gdy asortyment sklepów był dostępny w promocji w sposób ciągły – promocje na tych samych warunkach następowały jedna po drugiej. Działanie sklepów stanowiło chwyt marketingowy, nie oferowano rzeczywistego rabatu klientom.

W przypadku, gdy działanie serwisu internetowego zakwalifikowane zostanie przez Prezesa UOKiK jako naruszające zbiorowe interesy konsumentów, przedsiębiorcę stosującego „dark patterns” w serwisie może spotkać m.in. kara finansowa w wysokości 10 proc. obrotu za rok poprzedni. Natomiast kiedy stosowane „dark patterns” naruszać będą przepisy RODO, Prezes UODO może ukarać przedsiębiorcę prowadzącego serwis m.in. karą finansową w wysokości do 20 000 000 euro lub 4 proc. całkowitego rocznego obrotu.

6. Podsumowanie

Dark patterns to nieuczciwe techniki stosowane w projektowaniu interfejsów użytkownika, mające na celu manipulowanie jego decyzjami. Aby się przed nimi chronić, warto być świadomym i ostrożnym podczas korzystania z Internetu, regularnie przeglądać ustawienia prywatności, edukować się na temat nowych zagrożeń i ostrzegać innych użytkowników. Stosowanie „dark patterns” może mieć poważne konsekwencje prawne, ale nie tylko. Stosowanie „dark patterns” jest sprzeczne z ideą etycznego projektowania i ochrony użytkowników. Przedsiębiorcy powinni unikać stosowania takich praktyk i zawsze dążyć do zapewnienia uczciwego i klarownego projektowania interfejsów.