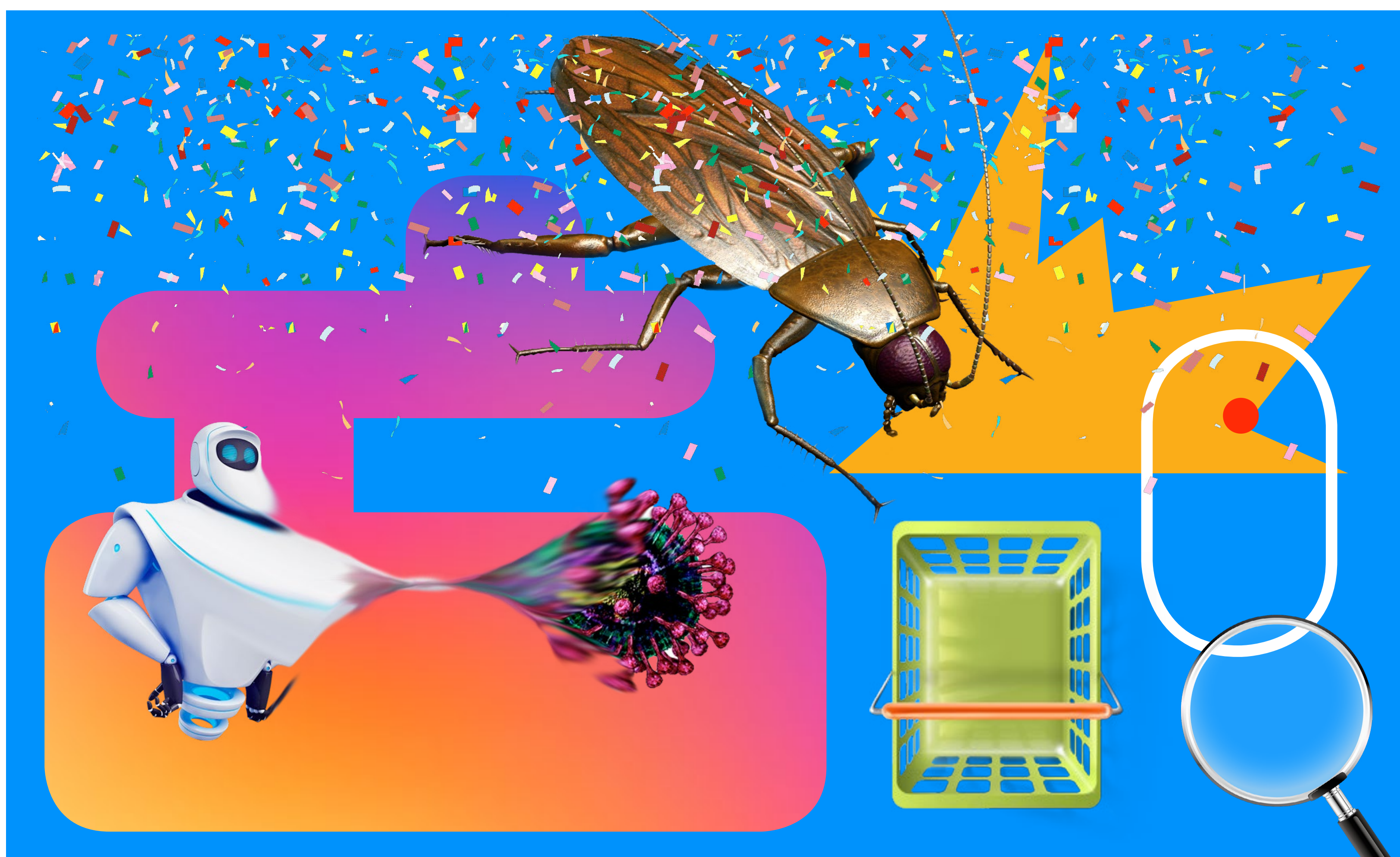


Dark patterns a na co si dát pozor při brouzdání internetem.



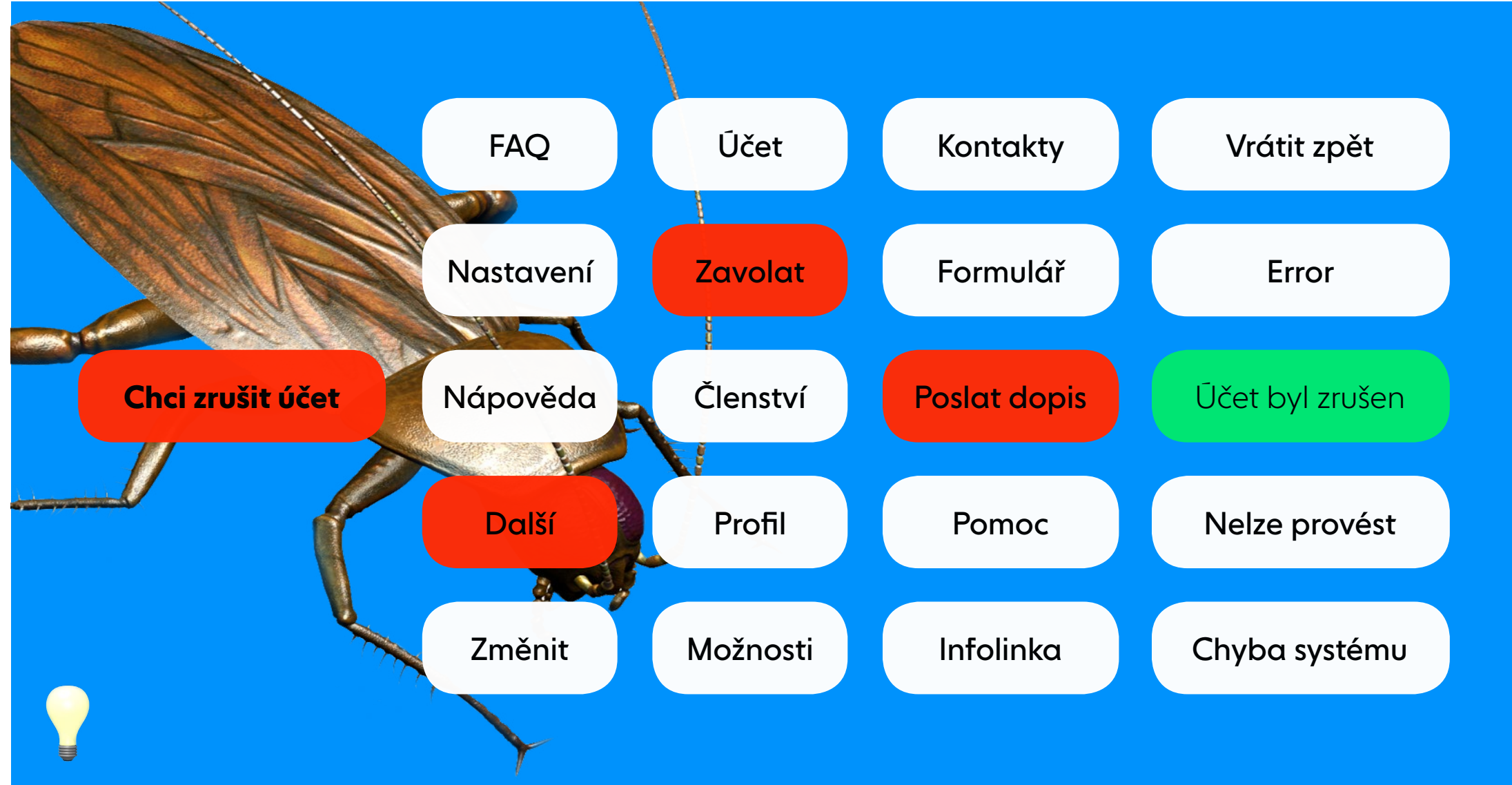
Dark patterns jsou manipulativní metody, obsahující kontrolovanou práci s jazykem, barvami, tvary, prostorem a hierarchií a zároveň chytře pracují s uživatelskými návyky, reflexí a intuicí návštěvníka (případně specifické skupiny návštěvníků) především při návštěvě webových stránek, ale i obecně v digitálním prostředí. Z hlediska designu jde o tenkou hranici mezi přesvědčováním a záměrnou manipulací, takže je v případě „chycení se“ těžké se dožadovat jasných pravomocí.

Tyto triky jsou jakýmsi digitálním ekvivalentem praktik u nás známých „šmejdů“, kteří neberou v potaz naše zájmy a rozhodnutí, ale psychologickými kličkami, oklikami a hledáním slabých míst, se nám snaží prodat informaci či produkt a dotlačit nás k rozhodnutí, které bychom pravděpodobně sami neprovedli. Do pastí se lze chytit velmi snadno jen pouhou nepozorností, či nedostatkem času...

Následující kategorie slouží jako přehled manipulativních metod, na které můžeme v digitálním prostředí narazit. Modré pozadí jsou interaktivní ukázky, oranžové jsou ilustrativní. Nejlepší obranou je o nebezpečí vědět a tím mu předcházet.

Švábí motel

Založení účtu je ve srovnání s jeho zrušením násobně náročnější a vyžaduje více úkonů — např. zrušení prémiového předplatného, nebo celkové zrušení účtu. Postup zrušení je často neintuitivní, je třeba se zorientovat v jeho umístění. V nejhorším případě je ke zrušení vyžadován osobní telefonát, osobní návštěva, nebo zaslání dopisu o zrušení.

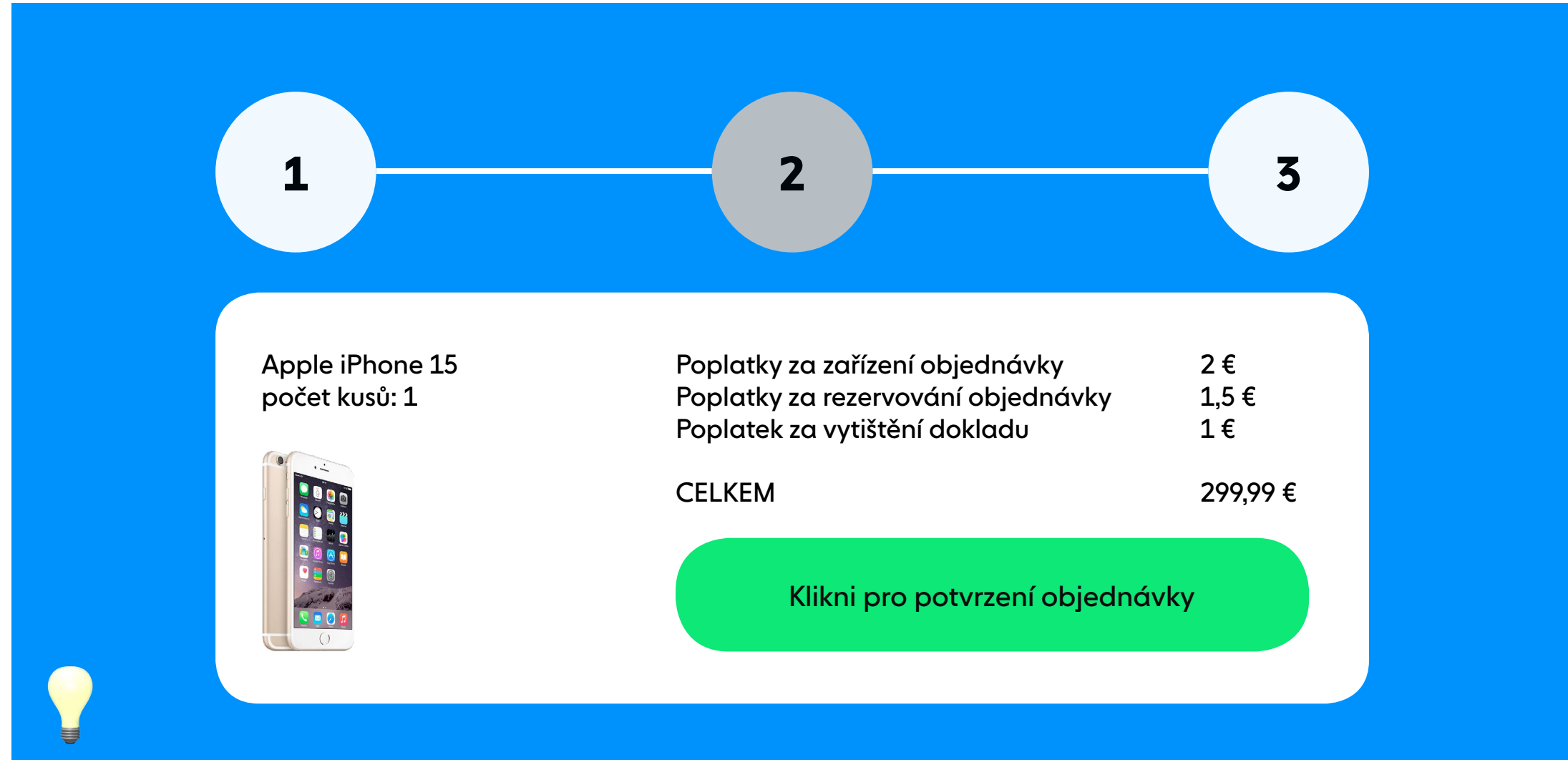


Privacy Zuckering

Jde o manipulaci k veřejnému sdílení mnohem více osobních informací, než jsme skutečně zamýšleli (pojmenováno podle gen. ředitele Facebooku Marka Zuckerberga). Příkladem je situace odstranění aplikace, kdy se zobrazí upozornění, že aplikace sice odstraní všechna data ze zařízení, avšak v cloudu data zůstanou.

Skryté poplatky

Obvykle tato situace nastane při on-line nakupování. V posledním kroku zjistíte, že vám jsou naúčtovány nečekané poplatky (např. poplatky za zařízení objednávky, za rezervaci), které nebyly v předchozích krocích zmíněny.



Skryté přeplatné

Účtování poplatků uživatelům pod záminkou jednorázového poplatku nebo bezplatné zkušební verze. Příkladem je registrace pro Netflix, kdy je použitý výrazný vizuální apel (barevný CTA button) k informování o účtování poplatků až po ukončení volného měsíce, zatímco doplňující informace o nepřerušených platbách jsou umístěné ve spodní části stránky malým a nevýrazným písmem.

Limitovaná nabídka (sociální tlak)

Vizuální upozorňování na to, že „v nejbližší době“ dojde k vyprodání nabídky, vypršení času, což vytváří tlak na rychlé dokončení objednávky. Ukázkovými případy jsou upozornění na rezervačních stránkách (Booking.com, Hotel.com): zbývají poslední dva pokoje. Na stránce je simulace sociální aktivity imaginárních zákazníků k vytvoření pulsující nákupní horečky. Pokud je součástí časomíra, po jejím uběhnutí se nic nestane.



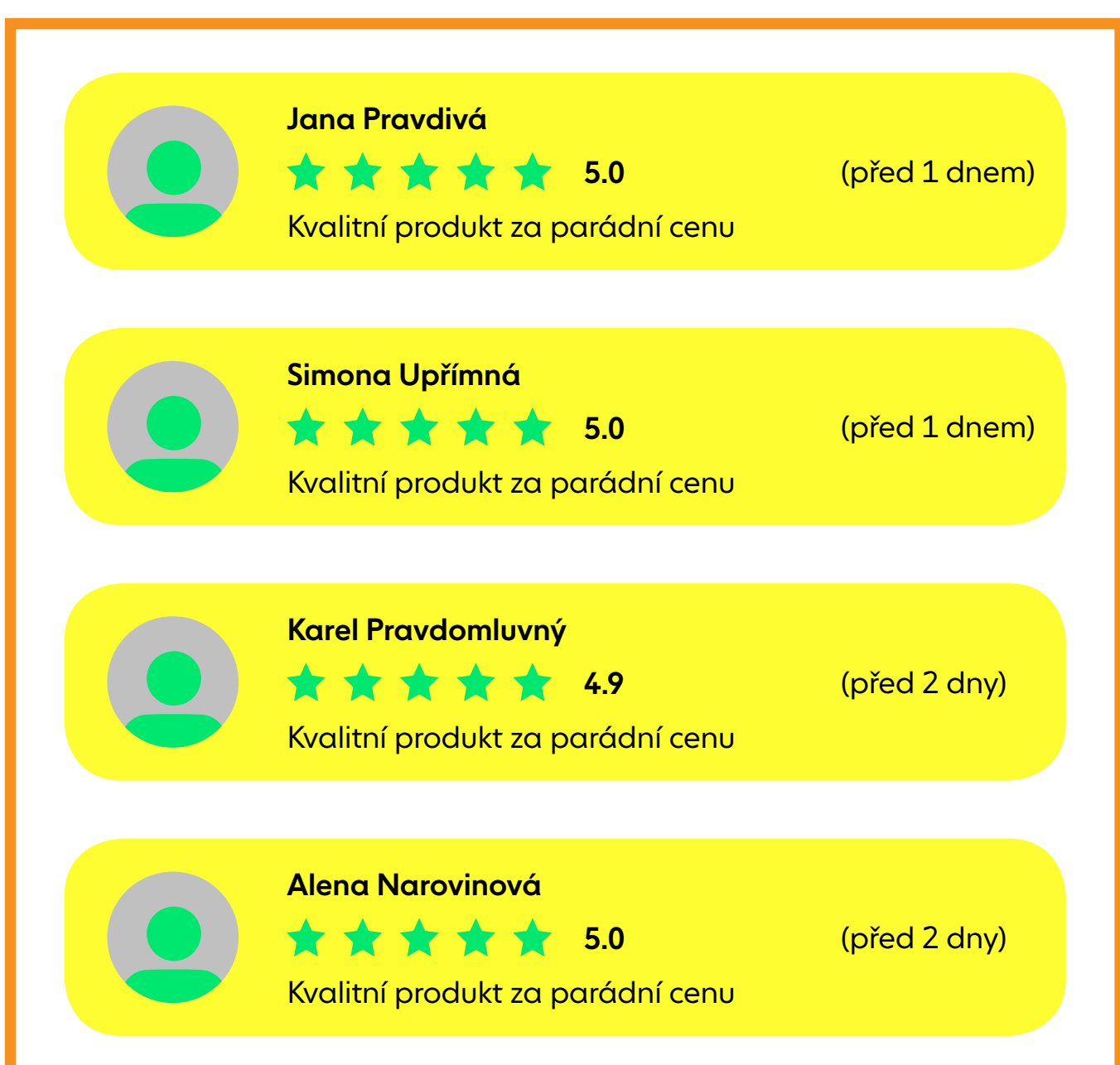
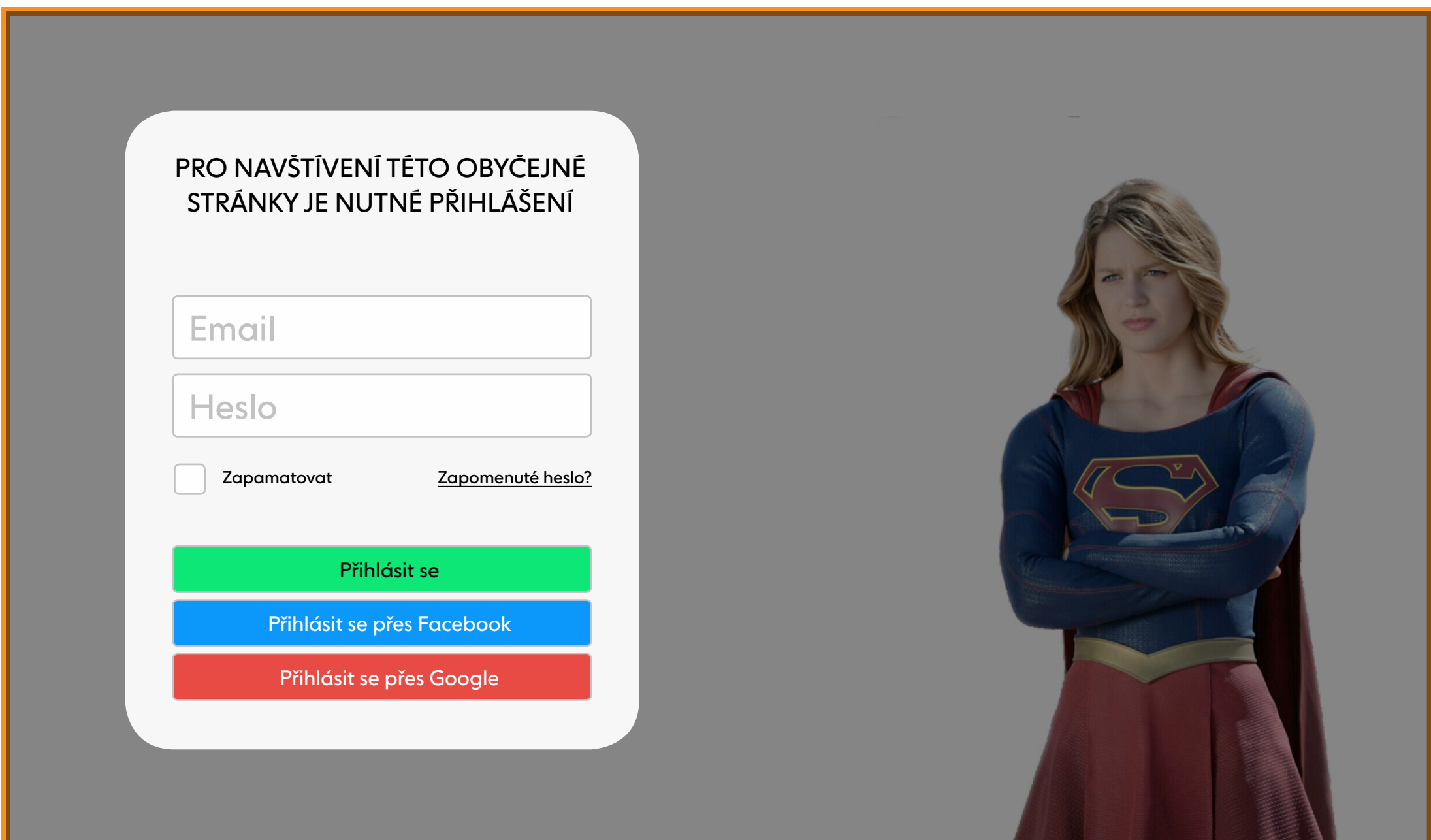
Klikni na tlačítko

Confirmshaming (sociální tlak)

Možnost odmítnutí je formulována takovým způsobem, aby uživatele zahanbila. Za pomoci zahanbujícího textu doplněného o emocionálně zabarvenou ilustraci (smutek, lítost, případně nenápadná urážka). Uživatel je donucen litovat svého rozhodnutí, aby si odhlášení/zrušení rozmyslel.

Nutnost přihlášení (sociální tlak)

Uživatel musí provést přihlášení, nebo si vytvořit nový účet (a tedy sdílet informace o jeho profilu), jen aby mohl navštívit webovou stránku. Některé soubory cookies fungují tak, že i v případě neodsouhlasení, nebo použití adblocku, nám neumožní na stránku vůbec vstoupit.

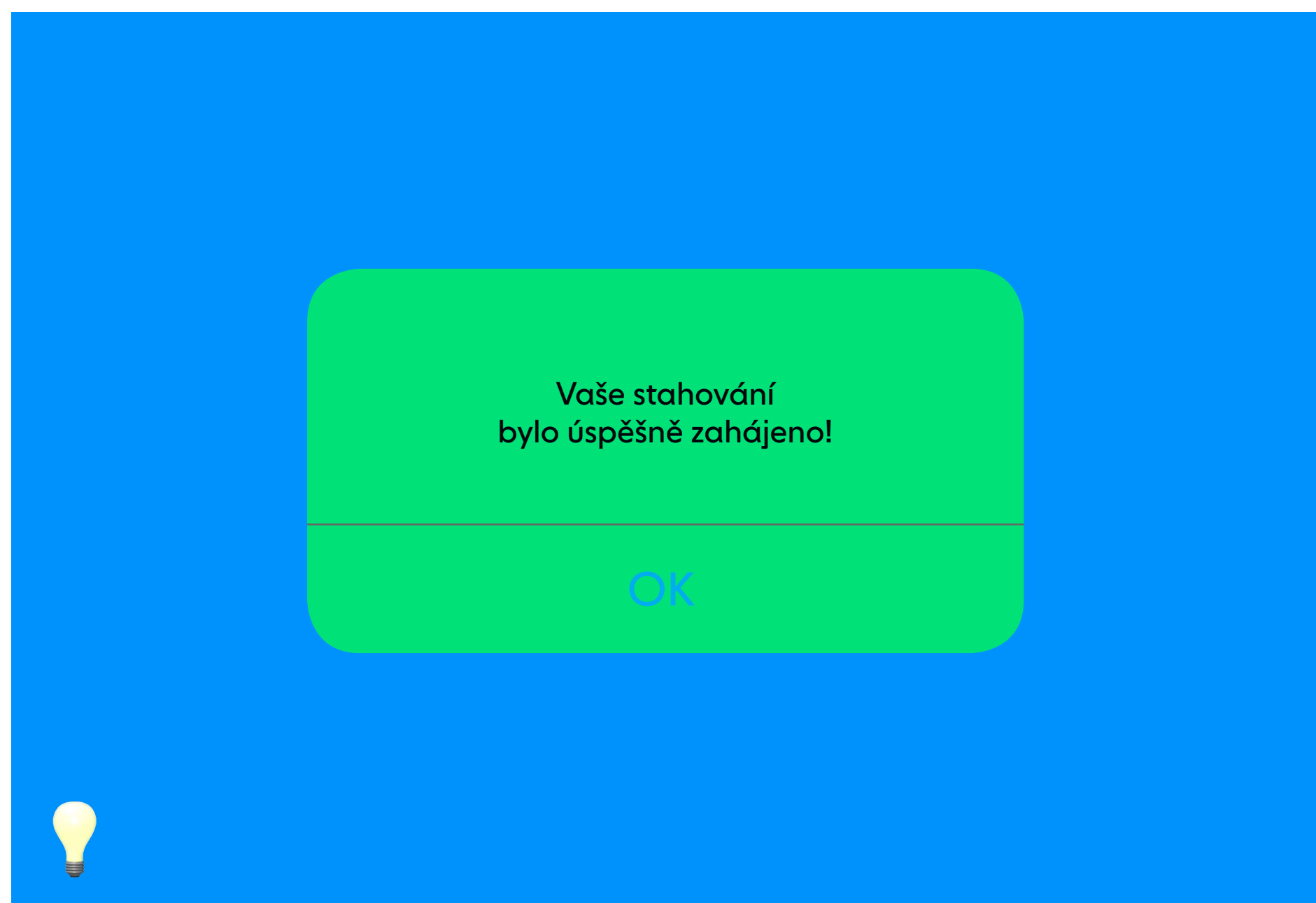


Falešné recenze (sociální tlak)

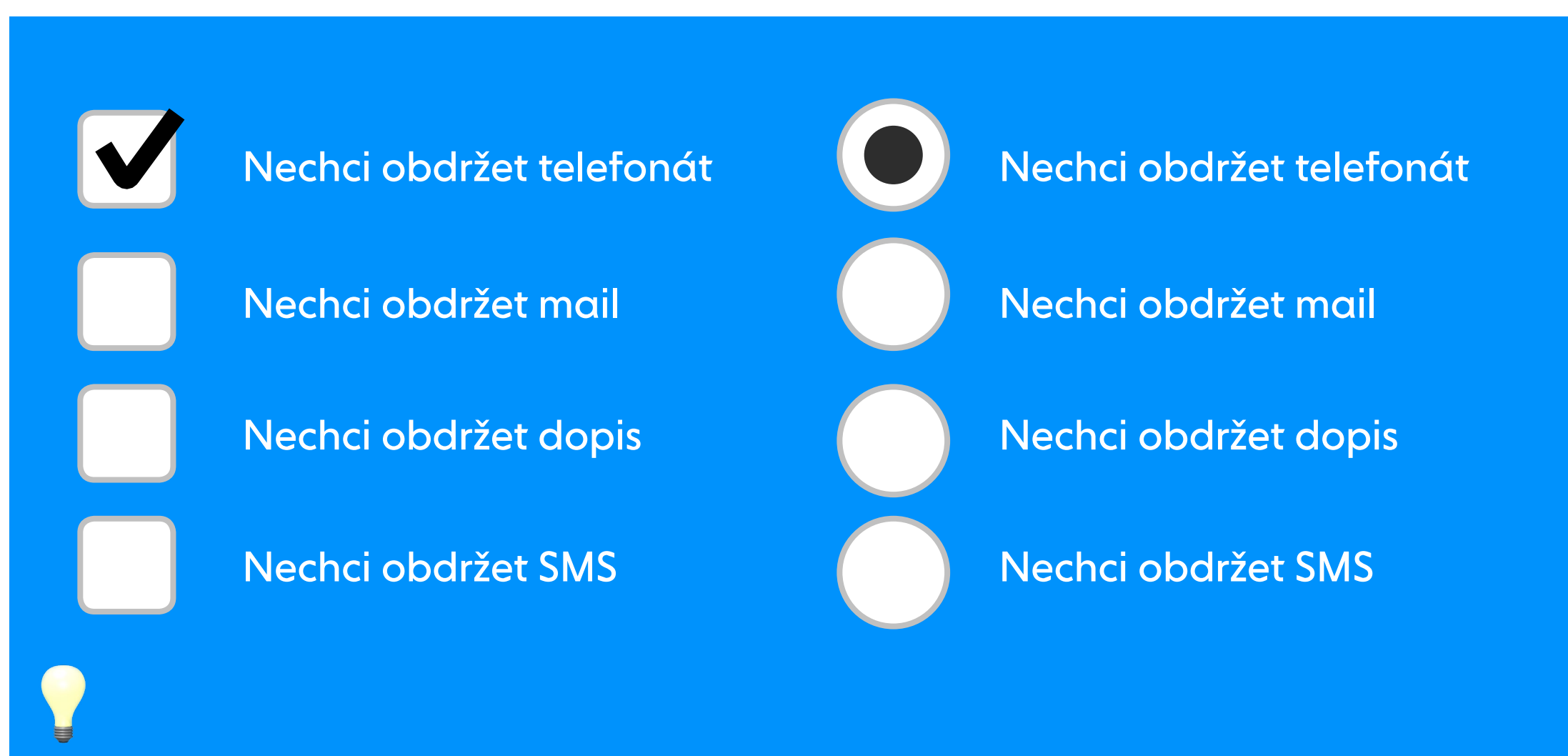
Ohlasy na stránce produktu jsou formulovány roboty, případně generovány tak, aby hodnotily produkt co nejvyšším počtem kladných hodnocení pod záminkou promování produktu. Dalším krokem je pak tzv. Blemishing effect (Pošpihující efekt), který zobrazuje několik negativních recenzí (může jít i o reálné recenze, ale umístěné na správné místo), které chytře podpoří prodej vybraných produktů.

Falešná CTA tlačítka (vizuální zmatení)

Reklamy jsou vizuálně maskovány jako nereklamní druh obsahu nebo navigace, aby přiměly návštěvníka na ně kliknout (CTA — Call To Action — tlačítko). Využívá se zde výrazného grafického jazyka k oklamání, nebo nasměrování uživatele jiným směrem (např. falešná tlačítka Confirm, OK, Download).



Najdi TO PRAVE tlačítko



Vyzkoušej si falešná přepínací tlačítka

Falešná volitelná tlačítka

Zaškrtávací políčka se zobrazují jako přepínací tlačítka (tzv. radio buttons), takže uživatel má na základě zkušenosti větší sklon vybrat pouze jednu možnost, která se hodí dotazujícímu subjektu.

Falešné novinové titulky (vizuální zmatení)

„Clickbait“ metody tváří se jako reálná a významná zpráva s vizualitou relevantního zdroje (BBC, ČT atp.). Cílem je odvést naši pozornost a v zájmu zjištění bližších informací se dostat na reklamní stránku, kterou jsme navštívit neplánovali.



Falešné přichozí zprávy (vizuální zmatení)

Součástí „clickbait“ metody se na stránce zobrazují vyskakující falešné notifikace, simulující přichozí zprávu, mail, nebo upozornění ze sociálních sítí atp. Po jejich otevření jste přesměrováni na reklamní stránku.



Falešný antivir

Paradoxním příkladem jsou antiviry, které po nainstalování přenesou vir (např.: malware/adware MacKeeper, nebo příliš agresivně se chovající Windowsový antivir Avast s automatickou volbou primárního antiviru bez uživatelského souhlasu).

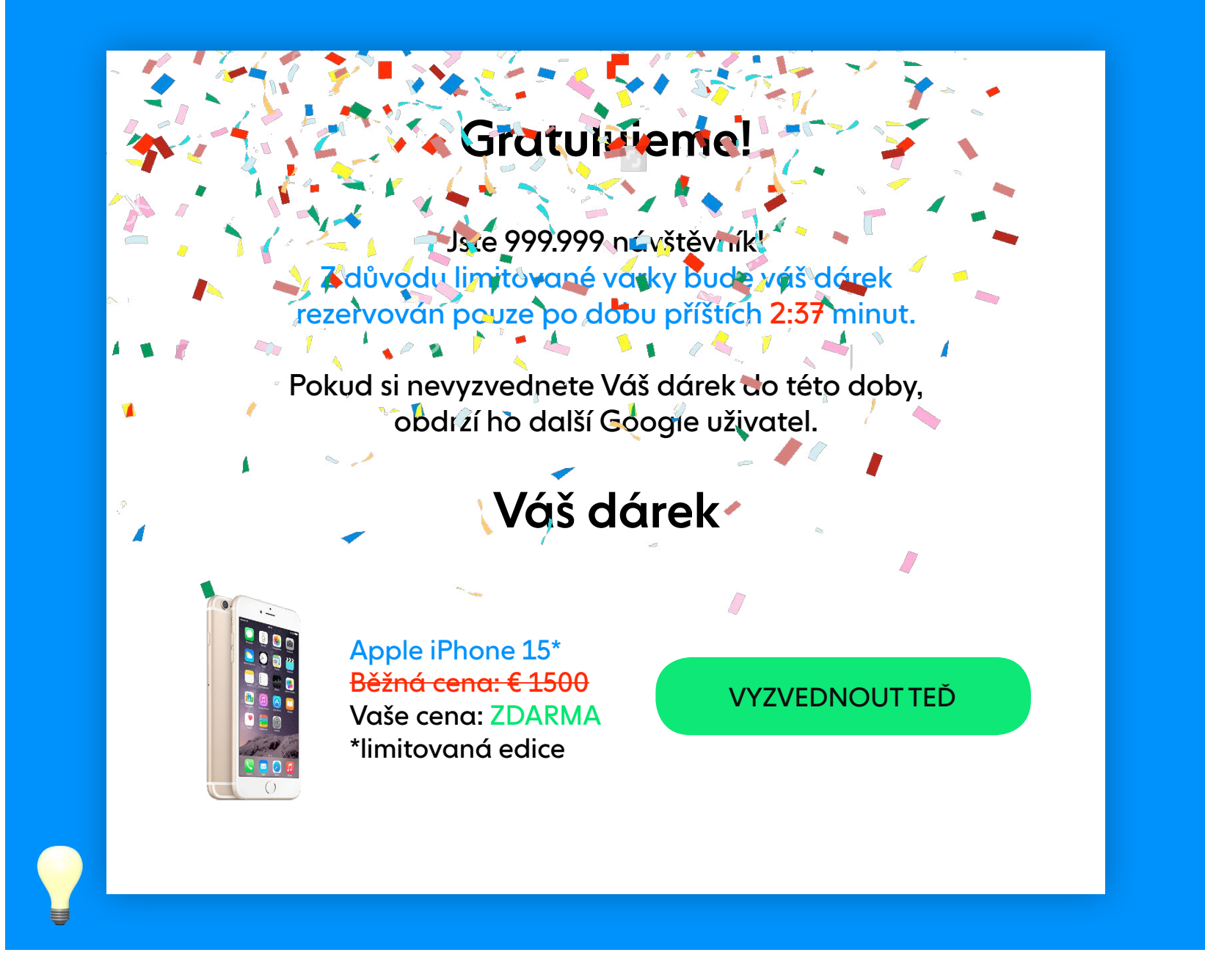


Žádné tlačítko zpět (vizuální zmatení)

Okna s upozorněním, která nenabízejí leave button — všechny možnosti vedou k potvrzení akce. Např.: uživatel Instagramu je pod tlakem, aby si zapnul oznámení, ovšem s možnostmi „Not now“ a „OK“. Spotify app nabízí pouze „Not now“. Možnost „Cancel“ není k dispozici a aplikace mu bude nadále nabízet upozornění, dokud potvrzení nepodlehne.

Hard click reklamní okno

Metoda, která ve formě adware/malware vyskakovacích oken nutí návštěvníka po kliknutí kamkoliv (zavřít, potvrdit, plocha reklamy) nalákat na reklamní sdělení. Klasickým příkladem, který už je spíše na ústupu (je už příliš rozeznatelný), je oznámení o výběru vaší IP adresy a získání odměny v podobě nového telefonu, sluchátek atp.).



Klikni kamkoliv



Přidat položku do košíku:

Prázdný košík (vizuální zmatení)

Bílá plocha jako „prázdné místo“ v online nákupním košíku chytře upozorňuje na nutnost „zaplnit“ košík dalšími položkami (např. Amazon). Ze stejného důvodu se například zvětšují nákupní vozíky v obchodech.

Nucené scrollování

Návštěvník je donucen scrollovat napříč desítkami produktů, než se dostane k místu, které potřebuje. (např. portál Megaknihy.cz vás v posledním kroku internetové objednávky donutí prohlédnout a scrollovat napříč obrovským množstvím produktů, abyste až na úplném konci mohli potvrdit objednávku).

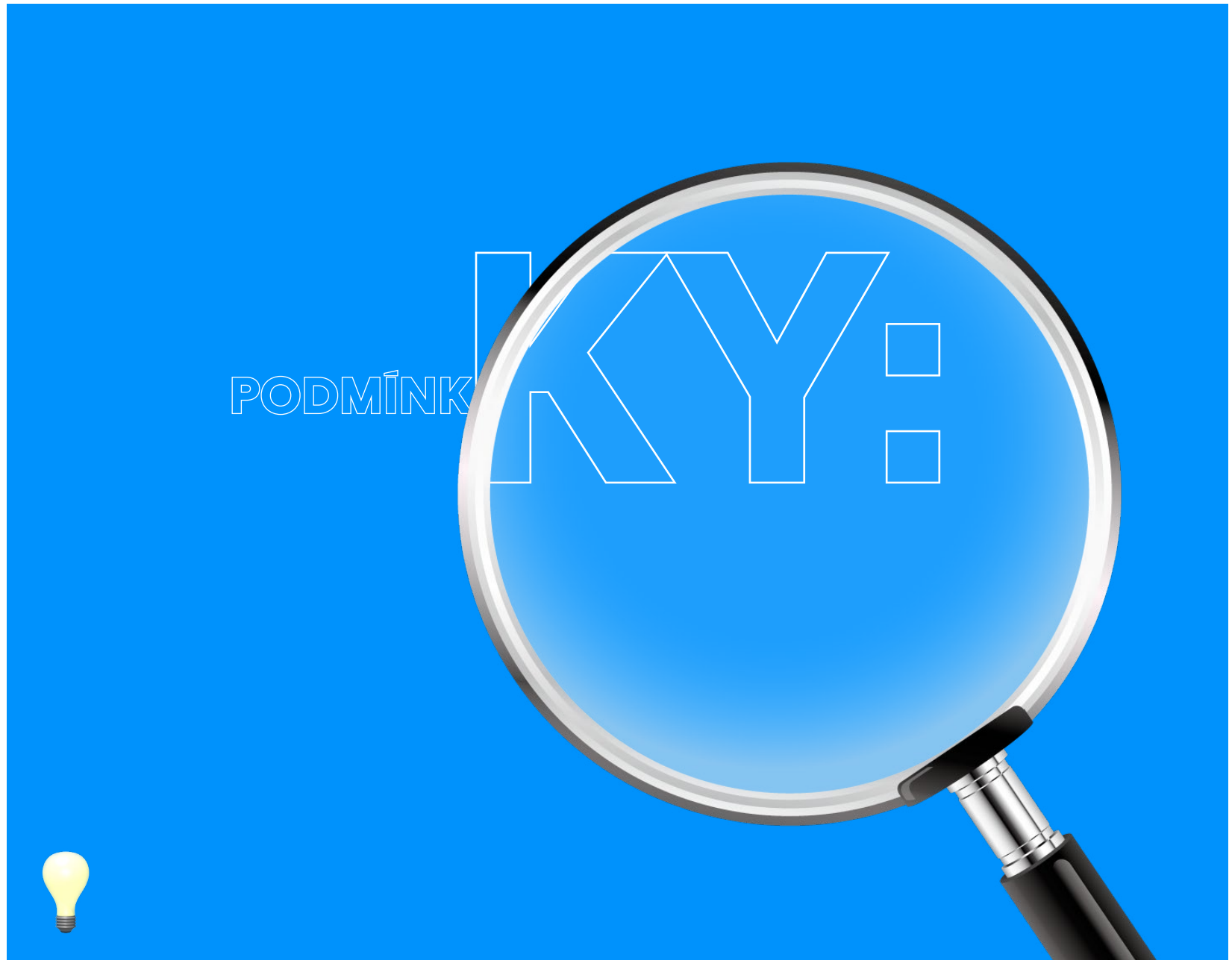


Scrollovat co to dělá



Gamification

Gamifikace je technika marketingu, která za pomoci herních mechanismů, designu a myšlení v neherním prostředí zvyšuje zájem, loajalitu a nadšení uživatelů. Jedná se o zábavnou metodu, která však může obsahovat jiné manipulativní prvky, na které je vhodné dát si pozor (skryté poplatky, či falešná CTA tlačítka).



Lupa ti pomůže přečíst nápis

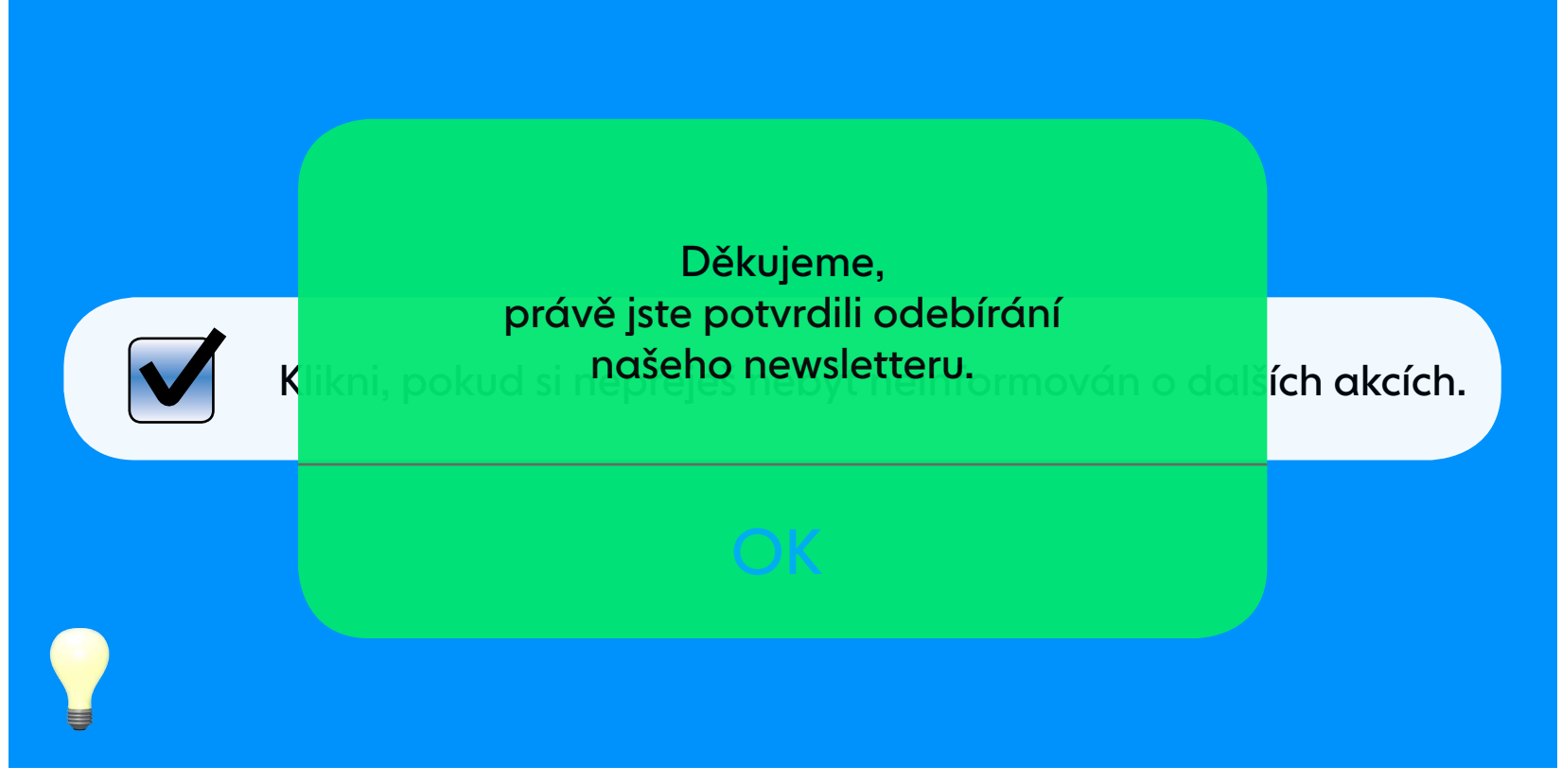
Neviditelné písmo

Důležité nápisy a texty jsou napsané nevýrazným, nebo částečně skrytým písmem. Výrazné nesrozumitelné jsou texty vysázené podobnou barvou jako je pozadí (šedá na bílé). Většinou jde o obchodní podmínky, Unsubscribe tlačítka ve spodních částech mailu, nebo X buttons k zavření okna. U nabídky produktů na e-shopu se ceny nepíší tak výrazně z důvodu, aby neodkládávaly zákaznickou pozornost (Amazon atp.).



Špatné UI

Navržené prostředí interface (to co na webu vidíme a na co klikáme), může být záměrně navrženo s manipulovatelným záměrem. Tlačítka na dotykových obrazovkách jsou miniaturní a bez prostoru kolem a návštěvníci mohou snadno kliknout na nabízenou reklamu. Příkladem je Exit full screen mode button na Youtube při přehrávání, který je malý a přímo hraničí s tlačítkem nabízeného dalšího videa, případně reklamního videa, na které spíš nechťně kliknu.



Kliknout, či nekliknout?

Přidružená slova

Součástí textu jsou jiná nesouvisějící slova, která podvědomě vnímáme jako součást hlavního textu. Slova jako „Zdarma“ nebo „0 Kč“ nás pak ovlivní v pocitu nižší ceny a lákavější nabídky.



Užitečné pluginy

Jak se manipulativním patternům bránit? Podstatné je především zamyšlení se nad prokázováním konsentu/souhlasu při návštěvě webové stránky a to, jakým způsobem je informace jazykově a vizuálně ohlášena.

Adblocker pro Google Chrome funguje automaticky po zvolení „Přidat do Chromu“. Je zde možnost nastavit si, zda chcete zobrazovat nenápadné reklamy, přidat seznam povolených pro své oblíbené weby nebo ve výchozím nastavení blokovat všechny reklamy. AdBlock je součástí programu Přijatelné reklamy, takže nenápadné reklamy nejsou ve výchozím nastavení blokovány aby podporovaly webové stránky. Věříme, že uživatelé by měli mít kontrolu nad tím, co vidí na webu, takže se můžete snadno odhlásit v nastavení AdBlock.*

[KE STAŽENÍ ZDE](#)

Přijetím cookies dáváme oprávnění k použití informací k přizpůsobení stránky a sledování našeho chování při jejím procházení. Problematické je neustálé vyskakování tohoto upozornění, které člověk v současném prostředí obvykle v rámci „otravnosti“ odklikne. Plugin „I don't care about cookies“, který v tomto ohledu nabízí NEUTRÁLNÍ volbu, tj. nebýt trackován, představuje zároveň tuto možnost vizuálně dostatečně srozumitelně a přívětivě.

[KE STAŽENÍ ZDE](#)

Plugin s názvem Rizikové weby detekuje rizikové weby a varuje uživatele před jejich návštěvou, před nákupy a používáním jejich služeb. Varování je zobrazeno pomocí popup okna, kde je možné přejít na odkaz s důvodem evidence webu. Dále je varování zobrazeno pod ikonou tohoto rozšíření. Varování je také zobrazeno, pokud odkaz na stránce vyhledávače (Google, Bing, Seznam.cz) odkazuje na rizikový web. Tuto aplikaci oficiálně podporuje ČOI (Česká Obchodní Inspekce).**

[KE STAŽENÍ ZDE](#)

* text je převzatý ze stránky Adblocker

** text je převzatý ze stránky Rizikové weby

ÚVOD

KATEGORIE

UŽITEČNÉ PLUGINY

UŽITEČNÉ ODKAZY

O PROJEKTU

Užitečné odkazy

<http://www.bezpecnyinternet.cz/>

<https://www.coi.cz/pro-spotrebitele/rizikove-e-shopy/>

<https://www.hoax.cz/hoax/aktuality/>

<https://webtransparency.cs.princeton.edu/dark-patterns/#revisions>

<https://www.nytimes.com/interactive/2015/12/04/business/media/bad-ads-list.html?mtrref=www.nytimes.com&assetType=REGIWALL>

<https://www.ghostery.com/>

<https://www.reddit.com/r/assholedesign/>

ÚVOD

KATEGORIE

UŽITEČNÉ PLUGINY

UŽITEČNÉ ODKAZY

O PROJEKTU

O projektu

Tato webová stránka je součástí diplomové práce
v Ateliéru Tvorby Písma a Typografie na pražské UMPRUM.

code: Jan Šindler
ux tester: XXXX, Šimon Trlifaj
konzultant: XXXXXXXXXX

© 2021

FB

IG

TW