



Transitions



**Spolufinancováno
Evropskou unií**

Financováno Evropskou unií. Názory vyjádřené jsou názory autora a neodráží nutně oficiální stanovisko Evropské unie či Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za vyjádřené názory nenese odpovědnost. Informace o licenci k užití těchto materiálů jsou k dispozici na webových stránkách projektu LEVEL UP.
LEVEL UP – 101186597



**MYSLÍTE, ŽE MÁTE SILNÉ
HESLO?**



Spolufinancováno
Evropskou unií

JMÉNO DÍTĚTE, DATUM NAROZENÍ, 123456...



JAK VYPADÁ ŠPATNÉ HESLO?

- **lukas123**
- **qwerty**
- **heslo2023**
- **1.1.1975**
- **Předvídatelnost**
- **Krátkost**
- **Používání veřejně
dohledatelných údajů**



Zásady silného hesla

Level
Up

- ✓ Minimálně 12 znaků
- ✓ Velká a malá písmena
- ✓ Čísla a speciální znaky
- ✓ Neobsahuje osobní údaje
- ✓ Neopakuje se jinde

💡 **Bonus: Použít frázi → snadno zapamatovatelné a bezpečné**



Spolufinancováno
Evropskou unií

SCAMY A ONLINE BEZPEČNOST

TECHNIKA – VĚTA JAKO HESLO

„Můj pes Bobek sní každý den 3 kosti!“

➤ Heslo: MpBskd3k!

Tip: Použít vymyšlenou větu, kterou znáš jen ty. Ne ze známých písniček nebo citátů.



SKUPINOVÝ ÚKOL

Level



Vymyslete ve skupině silné a zapamatovatelné heslo podle právě představených zásad.

Mělo by být:

Bez jména, dat, místa

Minimálně 12 znaků

Kombinace znaků

VYTVOŘTE SKUPINKY 3-4 OSOBY

Doba na úkol: 7 minut



Spolufinancováno
Evropskou unií

SCAMY A ONLINE BEZPEČNOST

SDÍLENÍ A HODNOCENÍ

Kdo vymyslel NEJBENZPEČNĚJŠÍ heslo?



SPRÁVCE HESEL

- ✓ **Bitwarden (zdarma, bezpečný)**
- ✓ **1Password (placený, vhodný pro rodiny)**
- ✓ **Dashlane nebo NordPass (uživatelsky přívětivé)**

💡 **Tip: 1 hlavní heslo + správce hesel =
bezpečný přístup ke všemu**

SHRNUTÍ NA ZÁVĚR:

- **Nikdy nepoužívej stejné heslo 2x**
- **Nepoužívej jména, data, města**
- **Heslo = věta**
- **Zapamatuj si jen 1 heslo – zbytek spravuje správce hesel**





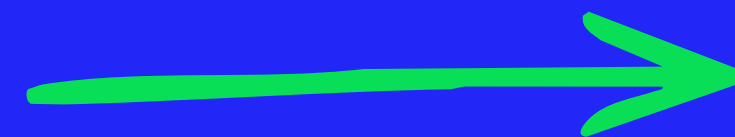
Transitions



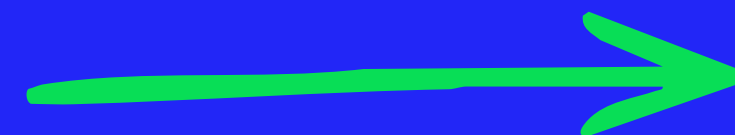
**Spolufinancováno
Evropskou unií**

Financováno Evropskou unií. Názory vyjádřené jsou názory autora a neodráží nutně oficiální stanovisko Evropské unie či Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za vyjádřené názory nenese odpovědnost. Informace o licenci k užití těchto materiálů jsou k dispozici na webových stránkách projektu LEVEL UP.
LEVEL UP – 101186597

plakát/ pracovní list do hodiny



var.1



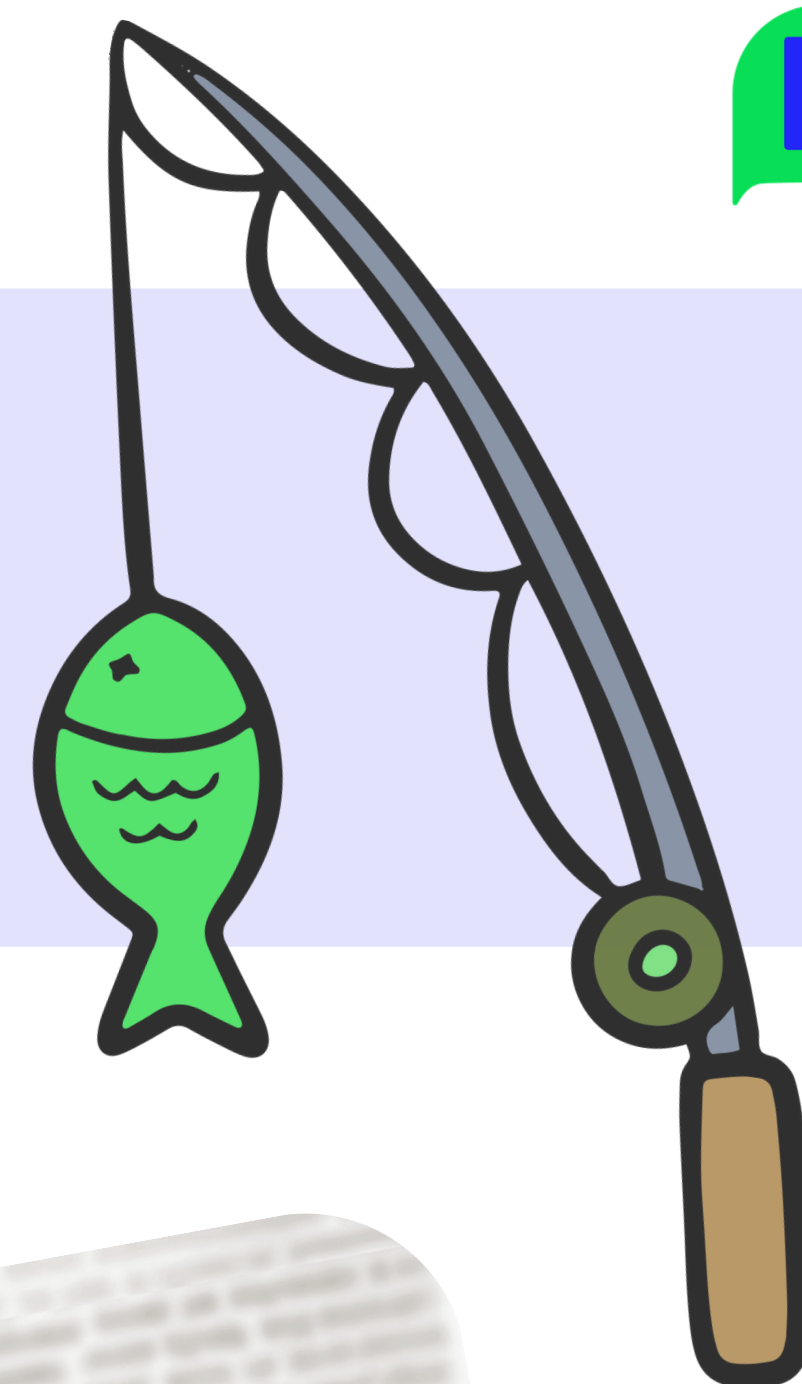
3 - BOJ O VAŠI POZORNOST

Level
Up

Kdo vás uloví?

Představte si, že jste „ryba“ v internetových mořích.

Který z těchto titulků by vás přiměl kliknout?



STEJNÁ UDÁLOST – RŮZNÉ TITULKY:

A

Ministerstvo představilo návrh změn v důchodovém systému.

B

ŠOK! Tohle vám vláda o důchodech neřekla!

C

Změny v důchodech: Co se navrhuje a koho se týkají.

D

Tohle vám vezme tisíce korun ročně! Podívejte se, co se chystá.

ÚKOL:

- Zakroužkujte titulek, na který byste nejspíš klikli.
- Seřadte titulky od nejvíce informativního po nejvíce manipulativní.
- Najděte alespoň 3 znaky, podle kterých poznáte clickbait.



Clickbait má za cíl přimět vás kliknout, ne informovat.
Manipulativní titulky (B, D): vyvolávají šok nebo strach, jsou neurčité („tohle“, „neřekla“), přehánějí!
Informativní titulky (A, C): říkají konkrétně, o čem článek je, nepoužívají silné emoce

Řešení



Spolufinancováno
Evropskou unií

Financováno Evropskou unií. Názory vyjádřené jsou názory autora a neodráží nutně oficiální stanovisko Evropské unie či Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za vyjádřené názory nenese odpovědnost. Informace o licenci k užití těchto materiálů jsou k dispozici na webových stránkách projektu LEVEL UP.

LEVEL UP – 101186597

Transitions

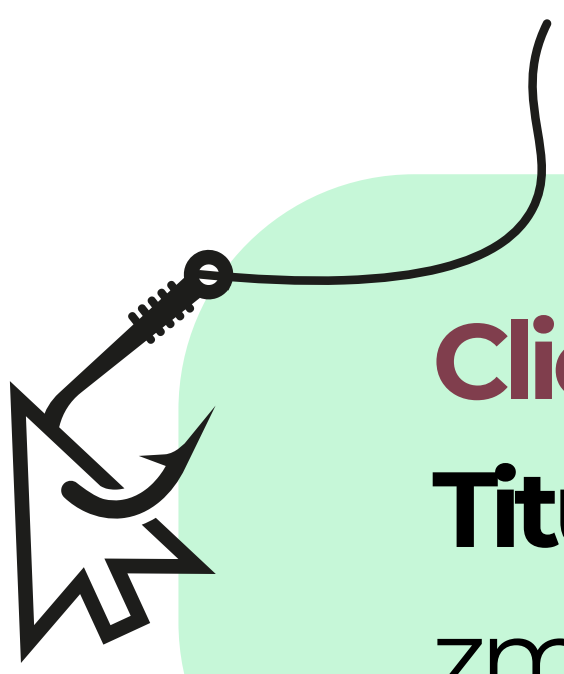
Proč je o naši pozornost takový zájem?

Na internetu platíme pozorností (bohužel nic není zadarmo). Čím déle se díváme, tím více reklam vidíme, tím více peněz někdo vydělá. Naše pozornost je zboží, které se prodává inzerentům.

Proto jsou weby a sociální sítě navrženy tak, aby nás udržely co nejdéle.

A nejspolehlivější způsob? Silné emoce – zvědavost, pobouření, strach, vztek.

SLOVNÍČEK:



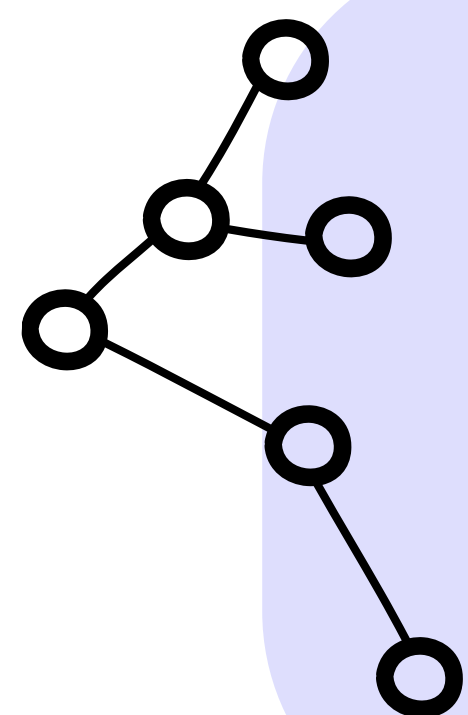
Clickbait (návnada na kliknutí)

Titulek, který slibuje víc, než článek splní. "Neuvěříte, co se stalo potom!" "Toto změní váš pohled na..." Cílem je donutit vás kliknout – **obsah je pak často zklamáním.**



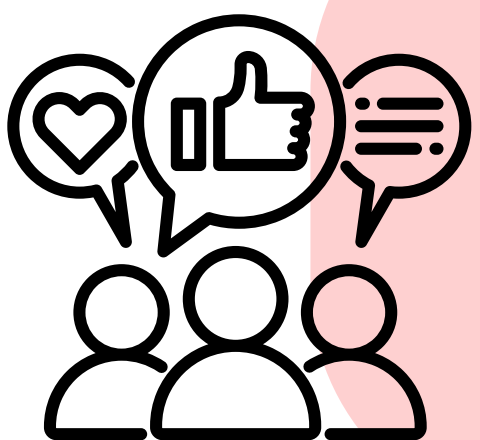
Ragebait (návnada na vztek)

Obsah záměrně vytvořený tak, aby vás naštval. Provokativní tvrzení, urážlivé názory – čím více vás to rozcílí, tím spíše budete reagovat, sdílet, hádat se. **A tím více pozornosti to získá.**



Algoritmus

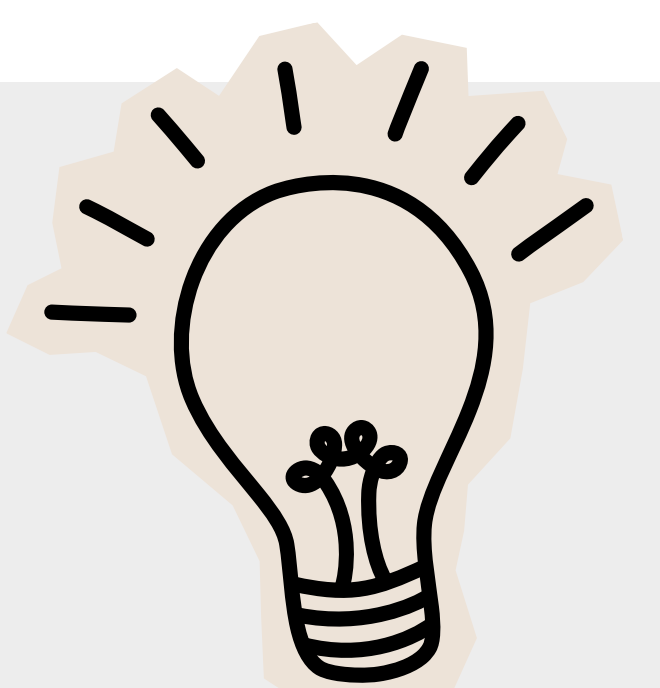
Program, který rozhoduje, co uvidíte. Sleduje, na co klikáte, co vyhledáváte a co vás zaujme. Když si například něco vyhledáte nebo na něco kliknete, **začne vám podobné příspěvky ukazovat častěji.** Ne proto, že jsou pravdivé nebo užitečné – ale proto, aby vás udržel online.



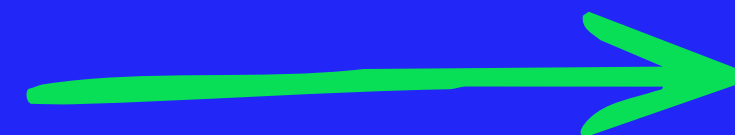
Engagement (zapojení)

Každé kliknutí, lajk, komentář, sdílení. Čím více engagementu, tím více algoritmus obsah šíří. Negativní reakce fungují stejně dobře jako pozitivní – **někdy i lépe.**

Co s tím? Než kliknete, zeptejte se: **Proč mě to tak táhne? Slibuje mi to něco? Chce mě to naštvat?** Titulek, který vyvolává silnou emoci, je často navržen právě k tomu – ne k informování.



var.2





Úkol

Co je na této zprávě podezřelé?
Najděte a zakroužkujte alespoň 3 varovné znaky.



< Zpět

Přesunout ▾

Označit ▾

Spam ▾

Smazat

Odpovědět

Odpovědět všem

Přeposlat

^

v

ps

podpora@secure-cloud247.com

Komu: mujemail@seznam.cz

27. 2. 2026, 14:37

Přejít na přílohy

Předmět: OKAMŽITÁ AKCE: Váš účet bude zablokován!

☆

Shrnout e-mail



Vážený zákazníku,

z důvodu bezpečnostní aktualizace byl váš účet dočasně omezen.
Pokud neprovedete ověření do 24 hodin, dojde k **trvalému zablokování přístupu** a ztrátě vašich dat.

Klikněte na odkaz níže a potvrďte své přihlašovací údaje:

www.cloud-overeni-uctu.com/login-verification

- Pro ověření zadejte:
- e-mail
 - heslo
 - telefonní číslo
 - ověřovací kód z SMS

Děkujeme za spolupráci.
Technická podpora

Na další stránce zjistíte, co jsou právě tyto varovné signály,
a níže se můžete podívat na řešení úkolu.



Řešení – Ukázka obsahovala tyto podezřelé znaky:

- 1) Podezřelá e-mailová adresa - Odesílatel: podpora@secure-cloud247.com
- Nepůsobil jako oficiální doména známé firmy. Seriózní firmy používají jasně identifikovatelnou doménu (např. @nazevfirmy.cz).
- 2) Obecné oslovení – „Vážený zákazník“: Skutečně služby obvykle oslovují jménem, pokud mají váš účet.
- 3) Vytváření nátlaku a strachu - „Do 24 hodin bude účet trvale zablokován.“ Podvodníci vytvářejí časový tlak, aby člověk jednal bez přemýšlení.
- 4) Podezřelý odkaz - www.cloud-overeni-uctu.com/login-verification
- Doména neodpovídá názvu známé služby. Často obsahuje slova jako „verify“, „login“, „secure“, ale není to oficiální web.
- 5) Žádost o citlivé údaje - Požadavek na: heslo, telefon, ověřovací kód z SMS
- Zadná seriózní instituce po vás nebude chtít heslo ani ověřovací kód e-mailem.

1

Podezřelý odesílatel

E-mailová adresa nevypadá oficiálně - i když se o to mnohdy snaží a liší se třeba jen pár písmeny.

(např. banka-info@xyz123.com místo @csob.cz).

U SMS se může místo běžného čísla zobrazit podivný název.

i **Nejste si jistí? Kontaktujte firmu sami – přes oficiální web, ne přes odkaz ve zprávě.**

2

Tlak na rychlé jednání

- „Vaše zásilka bude vrácena.“
- „Účet bude zablokován do 24 hodin.“
- „Reagujte ihned!“

i **Podvodníci chtějí, abyste jednali rychle a pod stresem.**
Seriózní instituce vám dávají čas situaci ověřit.

3

Podezřelý odkaz

Na počítači můžete zjistit, kam odkaz vede: Přesuňte šipku myši nad tlačítko (neklikajte). Dole v okně prohlížeče se zobrazí skutečná webová adresa.

i **Jestli máte podezření, na odkaz neklikajte a navštivte web firmy přímo zadáním adresy do prohlížeče.**

4

Žádost o citlivé údaje

Banka ani jiná seriózní instituce po vás nikdy nebude chtít:

- heslo, PIN, celé číslo platební karty, ověřovací kódy z SMS, přístupové údaje e-mailem nebo telefonicky.

i **Pokud tyto údaje někdo požaduje, jde o podvod.**

5

Falešný zájemce o váš inzerát

Komunikuje přes zprávy a chce platit „přes kurýra“ nebo vám posílá odkaz k vyplnění údajů? Nebo píše lámanou češtinou?

i **Budte obezřetní. Nikdy nezadávejte údaje o kartě kvůli přijetí platby..**

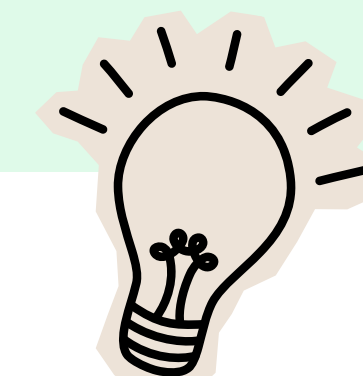
6

Podvodné telefonáty (vishing)

Volá vám „banka“, „policie“ nebo „vnuk v nouzi“?

Zavěste a zavolejte sami na oficiální číslo instituce (a číslo klidně rovnou zablokujte).

i **Existují i aplikace (např. „Můžu to zvednout?“), které upozorní na známá podvodná čísla.**



NEZAPOMEŇTE

Podvodné zprávy většinou nepřicházejí jen jednou.
Často jsou součástí celého „řetězce“ zpráv během několika dní či týdnů.

Typicky obsahují:

- varování, že vám bude zablokován účet,
- informaci, že je vaše úložiště plné,
- výzvu k „okamžité aktualizaci“ nebo „ověření účtu“,
- časově omezenou nabídku.

Dobrá zpráva je, že ověřit si informaci zabere jen chvíli – když víte, na co si dát pozor.



Spolufinancováno
Evropskou unií

Transitions