
SCAMULATOR
Prvý cyber podvod, ktorý ťa obohatí.
SLOVENSKÁ sporiteľňa

INSIGHT

Keď sa človek stane obeťou podvodu, nezabudne na ten pocit do konca života. Už nikdy neklikne na podozrivý link, nikomu neprezradí svoje bankové údaje a je v strehu vždy, keď mu píše kuriér, polícia či jeho vlastná banka. Okradnúť sa nechá len raz.

IDEA

Aby sa mladí ľudia nemuseli poučiť tak draho, dáme im ten prvý raz zažiť bezpečne a bez následkov.

V spolupráci s etickými hackermi vytvoríme **Scamulator – simulátor cyber podvodu** na báze AI, ktorý ich prevedie celým zážitkom. Keď sa potom stretnú so skutočným podvodníkom, budú pripravení mu čeliť.

Situáciu zámerne preženieme, aby sme zanechali ponaučenie, ale nevyvolali paniku z reálneho útoku.

Umelá inteligencia nám pomôže každý útok ušiť na mieru používateľovi.

SCAMULATOR

Prvý cyber podvod, ktorý ťa obohatí.

EXEKÚCIA

Ako funguje Scamulator?

1. Na microsite používateľ zadá svoje **meno**, **číslo**, **e-mailovú adresu** a **súhlas s podmienkami**. Stlačí štart.

2. Po spustení simulátora okamžite dostane mail, že bol pokus prihlásiť sa do jeho schránky z podozrivej krajiny. Zbadá typické tlačidlá „áno, som to ja“ a „**nie som to ja**“. Tlačidlo “**áno**” sa stlačí samé.

3. Príde ďalší mail: „**Vaše heslo bolo zmenené**“. A za ním ďalší: „**Budete odhlásení.**“

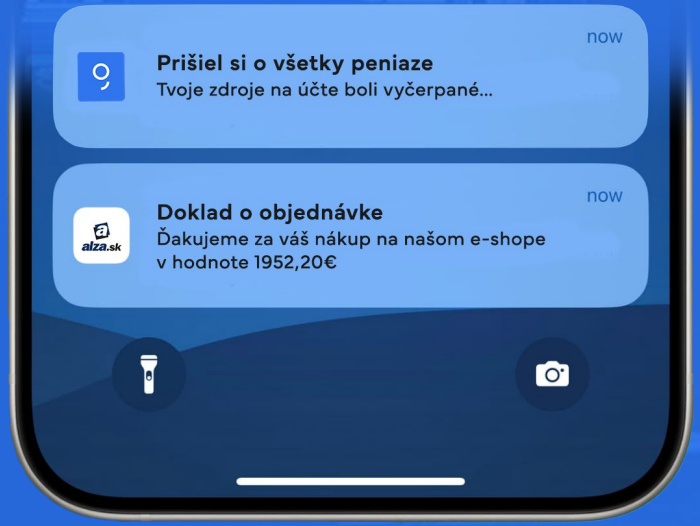
4. Vtom pípne SMS-ka s informáciou, že evidujeme pokus o aktiváciu Georga na novom zariadení. Pre potvrdenie treba použiť priložený kód. Hneď na to ďalšia SMS – „**Ďakujeme za potvrdenie prihlásenia.**“

EXEKÚCIA

5. Vzápätí George* v rýchlom slede vypľuje otravný počet notifikácií. O viacerých platbách kartou, o prečerpaní limitu na kreditke, o prijatej žiadosti o spotrebný úver. Napokon príde notifikácia „**Prišiel si o všetky peniaze.**“

6. Po rozkliknutí notifikácie sa aj samotný Goerge najprv zobrazí s glitch efektom, ktorý pripomína hacknutie. Zážitok okoreníme sériou SMS-iek s textom „**Ďakujeme za váš nákup.**”

7. Potom zákazníka konečne upokojíme mailom, SMS aj notifikáciou o úspešnom dokončení Scamulatora a zaradení do súťaže.* Odkážeme ho späť na web, kde mu vysvetlíme typické znaky cyber útoku a predstavíme zásadu neveriť, nepanikáriť a neklikať.



*Pokiaľ sa do simulátora zapojí neklient, namiesto Georga mu budú chodiť notifikácie alebo pop-up okná priamo na stránke.

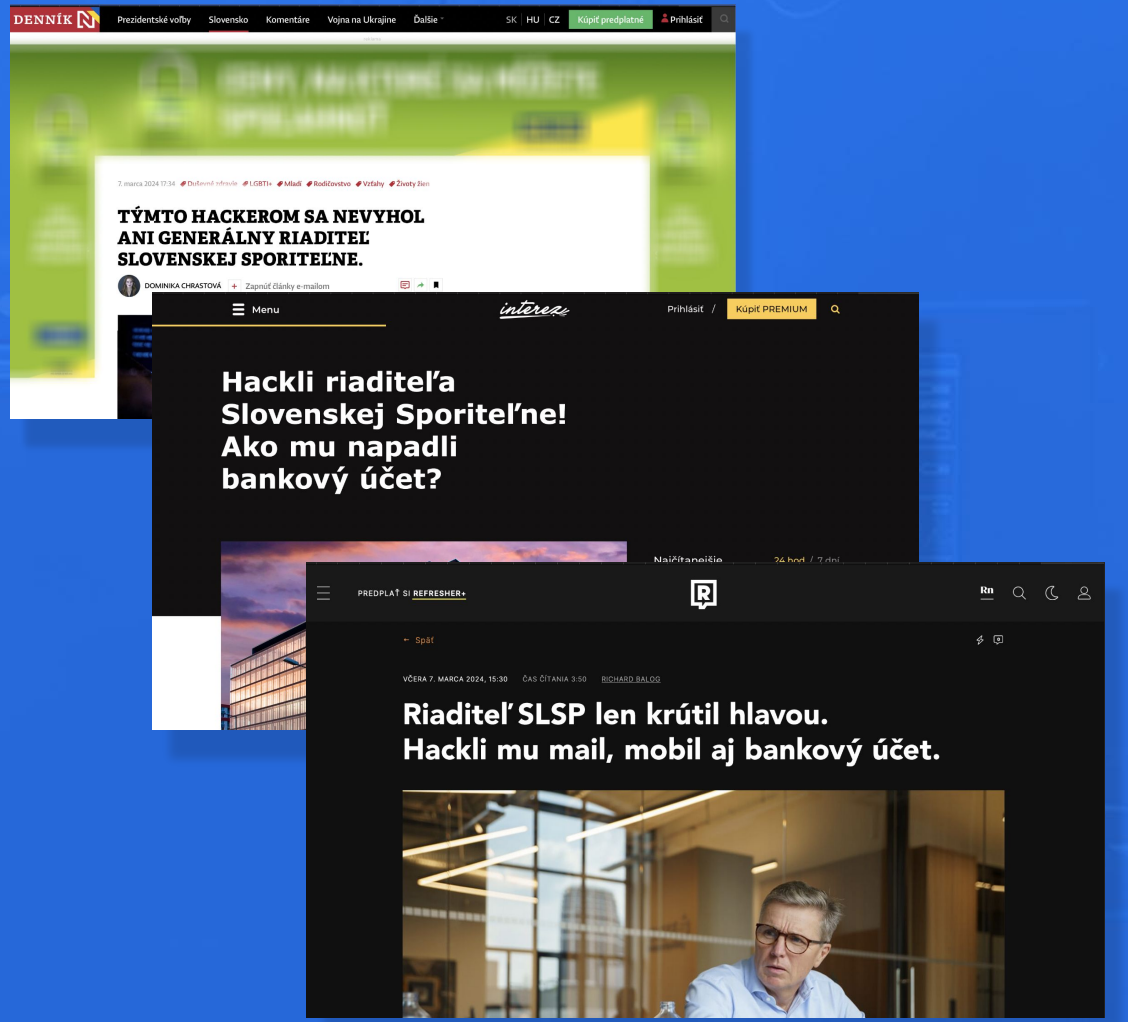
*Zážitok môžeme gamifikovať ešte viac, ak pripravíme rôzne scenáre s typickými cyber podvodmi – záujemca z bazáru, volanie polície, správy od kuriéra, vyhrážanie sa nahými fotkami a pod. Za prejdenie viacerých z nich potom môže hráč získať vyššiu odmenu.

KAMPAŇ

Na verejnosť vypustíme správu: **„Hackli riaditeľa Slovenskej Sporiteľne! Napadli mu osobný bankový účet“**.

V texte správy vysvetlíme, že pán Krutil si skúšal **Scamulator** a bol taký podobný realite, akoby sa naozaj stal obeťou útoku. Takýto chytľavý nadpis si rýchlo získa mediálnu pozornosť.

Prvé články si zaplatíme, ale rátame s organickým šírením správy aj v ďalších médiách.

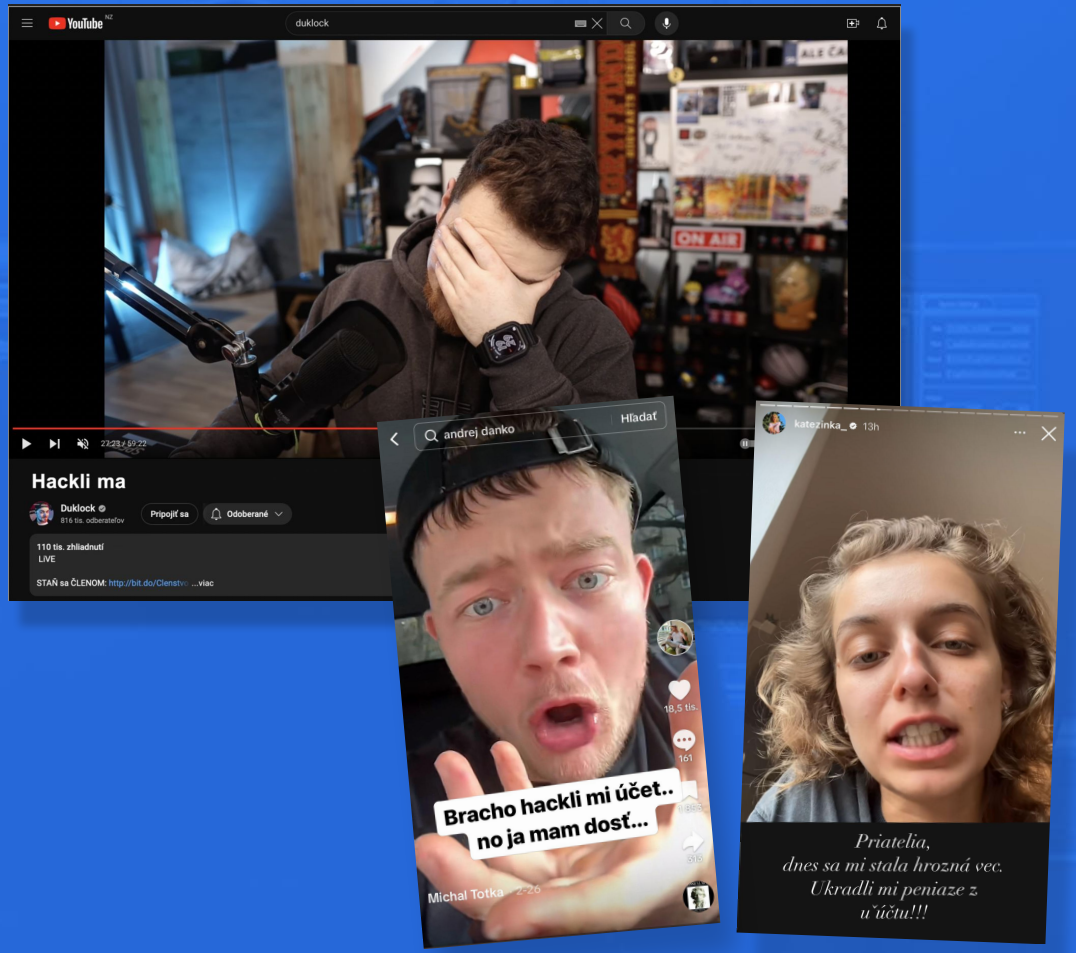


KAMPAŇ

Do kampane pridáme aj influencerov. Na streame a svojom youtube bude obľúbený streamer Duklock riešiť, ako ho **hackli**.

Na Instagrame a TikToku sa k téme pridajú aj **Katezinka** a **Michal Totka**.

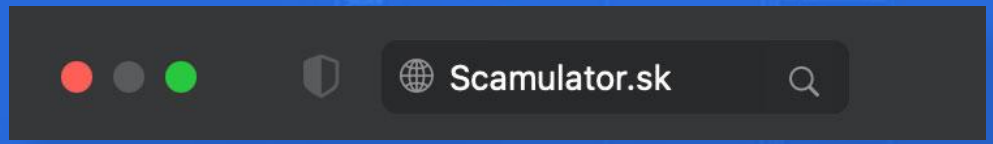
Vo videách divákov prevedú svojím zážitkom zo simulátora.



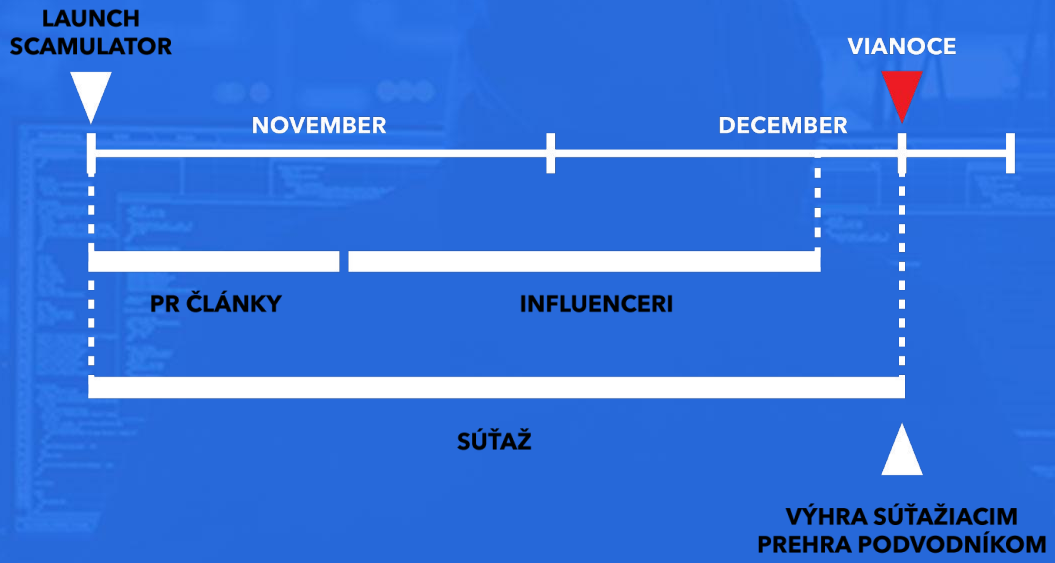
KAMPAŇ

Všetky výstupy budú odkazovať na kampaňovú microsite so simulátorom, informáciami o cyber podvodoch a o digitálnej bezpečnosti v SLSP.

Za úspešné **dokončenie simulátora bude používateľ zaradený do súťaže** o vecné ceny ako iPhone či hernú konzolu s doručením pod stromček.



TIMEPLAN & BUDGET



Produkcia

Vývoj Scamulatora **12 000** – *Microsite* **5 000** – *Odmeny do súťaže* **3 000**

Médiá

Influenceri **10 000** – *PR články* **9 000** – *Podpora súťaže cez vlastné social* kanály **2 000**


ĎAKUJEME