

Umelá inteligencia zvyšuje sofistikovanosť podvodov cez telefón. O2 chráni zákazníkov a štartuje edukačnú kampaň „Otázka za milión“

V Bratislave, 2. septembra 2025

Vďaka mobilnému telefónu a internetu dnes vybavíme takmer všetko: platby, nákupy, komunikáciu s bankou či úradmi. Práve preto sú aj jedným z cieľov pre podvodníkov. O2 spúšťa osvetovú kampaň Otázka za milión, ktorá učí ľudí rozpoznať manipuláciu pri telefonátoch a online komunikácii, vysvetľuje úlohu umelej inteligencie pri moderných sofistikovaných podvodoch a ponúka konkrétny, rýchly spôsob overenia identity – osobnú „bezpečnostnú otázku“, ktorú poznáte len vy a vaši najbližší. Na stránke rozpoznai.o2.sk si ju viete vygenerovať, otestovať sa v kvíze a prejsť si najčastejšie typy podvodov aj tipy, ako sa proti nim brániť.

S pokusom o podvod sa už stretol takmer každý kto vlastní mobilný telefón. Podvodníci pritom menia svoje scenáre – raz sa vydávajú za vojaka hľadajúceho lásku, inokedy za personalistku s „neodolateľnou“ pracovnou ponukou, falošného kuriéra či bankára, príbuzného, ktorý stratil telefón, alebo známeho žiadajúceho hlas v tanečnej súťaži. **Zostať ostražitý a zachovať si kritické myslenie je v takýchto situáciách jednou z najdôležitejších zručností a práve na ich posilnenie sa O2 zameriava vo svojej edukačnej kampani.**

Podvody v digitálnom svete dnes patria medzi rastúce formy kriminality a denne ohrozujú tisíce Slovákov, ktorí môžu prísť o peniaze či citlivé údaje. Podľa Europolu patria mobilné a online podvody medzi najvýnosnejšie kriminálne aktivity v Európe aj vo svete, pričom zločinecké skupiny na nich ročne zarábajú miliardy Eur ([Europol, 2023](#)). To, že mobilné podvody predstavujú pre páchateľov lákavý zdroj nelegálnych ziskov potvrdzujú aj dáta Polície Slovenskej republiky. Od roku 2021 do prvého polroka 2025 bolo zaznamenaných 786 dokonaných skutkov so škodou presahujúcou 7,5 milióna Eur, pričom priemerná škoda na jedného poškodeného dosiahla takmer 9.600 Eur. **Pokiaľ ide o najčastejšie scenáre, v roku 2024 dominoval tzv. family scam, pri ktorom sa podvodník vydáva za vnuka alebo tvrdí, že vnuk potrebuje naliehavú pomoc. Druhým najčastejším scenárom bolo zneužitie autority, konkrétne vydávanie sa za policajta ([MV SR, 2025](#)).**

Zasiahnutí podvodmi boli v posledných rokoch prevažne seniori, no podvodníci cieľia na ľudí rôzneho veku. Kým tzv. family scam vylákal peniaze najmä od starších ľudí, na romantické zoznámenia reagovali ženy v strednom veku a investičným podvodom podľahli ľudia vo veku 30 až 50 rokov. Netreba pritom zabúdať, že časť prípadov zostáva nenahlásená a nezaznamenaná ([MV SR, 2025](#)).

Operátori zablokujú denne až 70-tisíc podvodných telefonátov

Z pohľadu infraštruktúry podniká O2 už dnes rozsiahle kroky na technickú ochranu zákazníkov priamo v sieti. Väčšinu hrozieb vedia operátori odfiltrovať bez dopadu na zákazníka, no existujú aj

také, s ktorými je boj náročnejší. Podvodníci totiž neustále menia svoje techniky. Kedysi volali z exotických čísiel, ktoré si ľudia zvykli nezdvíhať, dnes sa však dokážu vydávať za slovenské číslo. Takto funguje **metóda tzv. spoofingu**, pri ktorej je volanie realizované s falošnou identitou domáceho telefónneho čísla.

„Operátori nepoznajú obsah komunikácie, ktorú si zákazníci vymieňajú. Zjednodušene povedané neodpočúvajú volania zákazníkov a nečítajú obsah SMS správ. Preto je pre nich veľmi náročné vyhodnotiť, ktoré volanie je korektné, a ktoré realizujú podvodníci. Platí zásada, že nemôžeme zablokovat' žiaden korektný hovor, ktorý realizujú naši zákazníci,“ **hovorí technologický riaditeľ O2 Slavomír Pšenák.**

Medzioperátorskou spoluprácou však dokážu počty podvodných volaní v spoofingu radikálne znížiť. *„Už od minulého roka máme s iným operátorom implementovaný špeciálny jednoúčelový online mechanizmus slúžiaci na overenie volania, ktoré sa prezentuje číslom zapojeným v našej alebo partnerovej sieti. Doterajšie štatistiky počtu podvodných volaní sú alarmujúce. Každý šiesty hovor, ktorý týmto mechanizmom skontrolujeme vyhodnocujeme ako pokus o podvodné volanie a k zákazníkovi sa nedostane. Za posledných 90 dní sme spolu s partnerom vyhodnotili a zablokovali viac ako 6 miliónov takýchto volaní zo zahraničia, čiže približne 70-tisíc volaní denne, alebo takmer 50 takýchto volaní za minútu,“* **dodáva Slavomír Pšenák.**

O2 svojim zákazníkom ponúka aj **službu O2 Security**, ktorá chráni pred podvodnými stránkami či vírusmi, pokiaľ je telefón pripojený na mobilných dátach v ich sieti. **Od jej spustenia zablokovala služba už takmer 2,1 milióna rizikových hrozieb**, čím prispela k ochrane mobilnej komunikácie a dát zákazníkov, ktorí ju majú aktivovanú.

Umelá inteligencia robí podvody nebezpečnejšími

Podvodné volanie s hlasom blízkej osoby či správy s bezchybnou slovenčinou s logom banky je dnes mimoriadne ťažké odlíšiť od skutočnej komunikácie. **Umelá inteligencia totiž nielen výrazne napomáha digitalizácii procesov, ale zásadne mení aj charakter podvodov.** Umožňuje totiž generovať obsah vo veľkom rozsahu a v kvalite, ktorá pôsobí uveriteľne, a to bez veľkých technických zručností. Automatizované nástroje dokážu napodobniť hlas konkrétnej osoby, vytvoriť vizuálne či textové podvody v slovenčine bez jazykových chýb a zároveň pripraviť útoky vo veľkej rýchlosti a objeme.

Čo sa týka špecificky syntézy reči, najnovšie AI modely potrebujú len niekoľko sekundovú nahrávku, aby dokázali „naklonovať“ daný hlas. *„Hoci stále platí, že veľké jazykové modely aj generátory reči najlepšie fungujú pre angličtinu, mnohé z nich už zvládnu obstojne aj slovenčinu. Aktuálne výskumy pritom ukazujú, že ľudia vo všeobecnosti majú problém rozpoznať, či ide o skutočný alebo AI generovaný obsah. V prípade reči sa úspešnosť pohybuje okolo 60%; najťažšie rozpoznateľné sú text a obrázky (obe okolo 50 %). Výskumy však zároveň ukazujú, že schopnosť ľudí správne rozlíšiť AI generovaný obsah sa zvyšuje pomocou tréningu,“* **upresňuje Róbert Móro z Kempelenovho inštitútu inteligentných technológií (KlnIT).**

Medzi najčastejšie využívané techniky patrí klonovanie hlasu, deepfake videá či obrázky a texty, ktoré dokáže AI tvoriť takmer bezchybne. Napriek tomu existujú znaky, ktoré môžu pomôcť detegovať či ide o obsah vytvorený umelou inteligenciou.

Typ obsahu	Čo si všímať
Text	gramatické a štylistické chyby, nezvyčajné tvary slov, zvláštne formulácie

Typ obsahu	Čo si všímať
Obrázok	nezrovnalosti v detailoch, nerealistické osvetlenie a tieň, nelogické pozadie či objekty, ktoré k sebe „nesedia“
Video	pohyby úst nesedia s hovoreným slovom, neprirodzené pohyby očí, trhané prechody, zmeny výzoru, nelogické detaily v pozadí
Hlas	neprirodzená melódia reči a pauzy, dôraz na jednotlivé slová

S rastúcim vývojom technológií bude kritické myslenie a ostražitosť jednotlivcov ešte dôležitejšia. „V budúcnosti môžu pribúdať personalizované útoky, pri ktorých podvodníci využijú údaje z verejných statusov na sociálnych sieťach alebo správy získané phishingom na „personalizáciu“ obsahu. Týmto spôsobom dokážu vytvoriť odpovede napodobňujúce váš štýl vyjadrovania a pôsobiť ešte uveriteľnejšie. Čoraz častejšie sa môžu objavovať aj podvody využívajúce AI modely, ktoré dokážu viesť autonómne konverzácie v chate či telefonáte alebo v reálnom čase meniť tvár vo videu (tzv. face swap),“ **dodáva odborník na umelú inteligenciu Róbert Móro.**

Obete podvodov nie sú iba menej technologicky zdatní ľudia

Umelá inteligencia a technické vymoženosti dávajú podvodníkom do rúk silné nástroje, no tie samy osebe nestačia. Na úspech potrebujú spoluprácu človeka, najmä jeho pozornosť a dôveru. **To, či človek „naletí“ podvodníkom, nezávisí od veku, vzdelania či iných demografických znakov.** Rozhodujúce je skôr jeho aktuálne rozpoloženie a spôsob, ako sa rozhoduje. **Podvodníci cielene pracujú s emóciami obete a dokážu ju zmanipulovať** aj v situáciách, keď by inak reagovala racionálne.

„Podvodníci sa nás snažia dostať do stavu emocionálnej destabilizácie – či už negatívnej, napríklad keď vyvolajú strach o našich blízkych, alebo pozitívnej, keď nám volajú s oznamom o výhre alebo zhodnotení našej investície. Vždy im však ide o to, aby sme konali rýchlo a bez rozmýšľania. Akonáhle vychladneme, nastúpi racionálne uvažovanie a začneme si všímať nezrovnalosti,“ **vysvetľuje klinický psychológ a súdny znalec RNDr. Mgr. Dušan Kešický.**

„Platí, že čím viac času trávime vo virtuálnom svete, tým sa znižuje naša obozretnosť. „Dnes sú už podvodné techniky natoľko sofistikované, že nikto nemôže s istotou tvrdiť: mne sa to nikdy nestane. To je ilúzia,“ **dodáva psychológ.**

Otázka za milión: jednoduchý a efektívny trik na podvodníkov

Vzhľadom na rastúcu sofistikovanosť podvodov si O2 uvedomuje, že popri technickej ochrane je dôležitá aj edukácia a prevencia, a preto spúšťa kampaň „Otázka za milión“. **Jadro kampane je postavené na jednoduchom, no účinnom triku pri jednom z najrozšírenejších podvodov – keď sa niekto vydáva za vášho blízkeho.** V kampani O2 predstavuje tzv. otázku za milión – osobnú otázku, ktorú poznáte iba vy a vaši najbližší. Vďaka nej si môžete rýchlo a spoľahlivo overiť, či na druhej strane naozaj s vami komunikuje ten, za koho sa vydáva, alebo ide o podvodníka.

„Útočníci dnes dokážu zavolať či poslať hlasovú správu s imitáciou hlasu a jazykového prejavu, dokonca sa môžu dostať priamo do vašej spoločnej konverzácie. Na dohodnutú otázku, na ktorú pozná odpoveď iba konkrétna osoba, však reagovať nedokážu a práve vtedy máte jasný signál, že ide o pokus o podvod,“ **hovorí Lucia Petrášová, riaditeľka úseku značky a komunikácie O2.**

O₂

Otázka za milión

Ako sa volal pes babky Majky?

Pripravte si kontrolnú otázku, ktorá vás môže ochrániť pred AI podvodníkmi.

rozpoznai.o2.sk

„V O2 stojíme na strane zákazníka a našou úlohou je pripraviť ho na novú éru mobilných podvodov. Preto kladieme dôraz na edukáciu – veríme, že ľudia si vďaka nej osvoja nové zručnosti a budú sa vedieť v kritickej chvíli správne rozhodnúť,“ vysvetľuje **Lucia Petrášová**.

Ako sa chrániť pred mobilnými podvodmi

Podvodníci často vytvárajú časový tlak („hneď, inak prídete o peniaze“), falošnú autoritu (bankár, polícia, kuriér) a emóciu (strach/šok či eufória). V takom momente je dobré aktivovať jednoduché pravidlá:

- Zvýšiť opatrnosť a prerušiť konverzáciu (napríklad zložiť a zavolať späť na oficiálne číslo banky/inštitúcie)
- Pripraviť si „otázku za milión“ a overiť si tak s kým komunikujete
- Nezdierať PIN kódy, heslá, prístup do bankovníctva, či iné citlivé údaje
- Neklikať na podozrivé odkazy a neotvárať neznáme prílohy
- Všímať si jazyk, gramatiku a logiku správy

„Univerzálny recept, ako sa podvodom úplne vyhnúť, neexistuje. Kľúčové je, aby téma zostávala prítomná v povedomí ľudí. Ak o podvodoch pravidelne hovoríme, čítame o nich a pripomíname si ich, máme väčšiu šancu rozpoznať podozrivú situáciu včas. Aj preto majú význam kampane, ktoré konkrétne techniky podvodníkov približujú a udržiavajú túto tému živú,“ uzatvára **psychológ Dušan Kešický**.

Kampaň O2 bude komunikovaná v online priestore a na sociálnych sieťach. **Nový edukačný spot si môžete pozrieť tu:** <https://youtu.be/zljrPtwdhbQ> Všetky materiály sú sústredené na internetovej stránke **rozpoznai.o2.sk** – od generátora bezpečnostnej otázky, cez kvíz na rozpoznávanie AI obsahu, až po prehľad vzorových situácií a odporúčaní pre bežných ľudí aj firmy.

Všetky tlačové správy nájdete na www.spolocnost.o2.sk/tlacove-centrum/tlacove-sprawy.

O spoločnosti O2 Slovakia, s.r.o.

o2 je na Slovensku najrýchlejšie rastúcim mobilným operátorom. Od začiatku svojho pôsobenia, prináša revolučné riešenia, otvorenú komunikáciu a férovosť pre všetkých zákazníkov bez rozdielu. S jednoduchým portfóliom produktov systematicky mení pravidlá mobilnej komunikácie. Ako prvý priniesol na Slovensko skutočne neobmedzený program na volania a SMS, ako prvý uviedol komerčnú testovaciu prevádzku LTE siete, či ponúkol platby mobilom prostredníctvom NFC technológie. Vysokú kvalitu poskytovaných služieb zohľadňuje aj získanie certifikátu QMS podľa normy ISO 9001.

Senior PR špecialistka
Dominika Hovorková Ertelová
media@o2.sk

O2 Slovakia, s.r.o.
Pribinova 40, 811 09
Bratislava, Slovakia
+ 421 2 620 20 100
www.o2.sk

IČO : 47 259 116
spoločnosť zapísaná v Obchodnom
registri Mestského súdu Bratislava III,
oddiel Sro, vložka č. 160894/B