

Podvodníci mohou volat z vašeho telefonního čísla i čísla banky. Proč operátoři nezasáhnou?

 insmart.cz/spoofing-utoci-na-cesko-ctu-operatori/

V posledních dnech zaznamenávají čeští občané nárůst podvodných telefonátů využívajících metodu tzv. spoofingu. Prostřednictvím této techniky se podvodníci vydávají za legitimní instituce, jako jsou banky nebo policejní složky, a snaží se oběťmi vylákat citlivé údaje nebo je přesvědčit k finančním transakcím. Volat navíc mohou z libovolného českého čísla patřícímu komukoliv z nás, což činí podvod těžko rozeznatelným.

Někdy je na lince jen ticho a hovor je rychle ukončen, jindy se podvodníci vydávají za orgány činné v trestním řízení a tvrdí, že oběť je podezřelá z praní špinavých peněz. Velmi časté jsou případy, kdy volající maskující se za telefonní číslo banky tvrdí, že došlo k napadení vašeho bankovního účtu.

Číslo volajícího je stejně jako e-mail odesílatele snadné podvrhnout. Foto: Unsplash

V článku najdete: [skrýt](#)

Proč nezasáhnou operátoři?

Čeští operátoři jsou v současné situaci do značné míry bezmocní. Volání totiž přicházejí ze zahraničí a navíc nejčastěji s využitím VoIP služeb. **Operátor se zde musí spoléhat na identifikaci přicházející od zahraničních operátorů a volající tak mohou být maskováni libovolným českým číslem, což znesnadňuje jejich blokování.**

Problém tedy musí řešit sami uživatelé zvýšenou obezřetností. Pokud vám kdokoliv zavolá, nikdy byste neměli sdělovat citlivé údaje či provádět transakce na základě nevyžádaného telefonátu, a to ani v případě, že se volající vydává za důvěryhodnou instituci typu banka či policie.



Podvodníkům jde většinou o zisk. Stačí však dodržet několik jednoduchých pravidel a budete v bezpečí. Foto: Unsplash

Jak podvod funguje?

Spooing je metoda, při níž útočníci maskují své skutečné telefonní číslo, e-mailovou adresu nebo webovou stránku tak, aby se vydávali za legitimní subjekt. U telefonních podvodů hackeři využívají zahraničních tranzitních operátorů k propojení hovoru do České republiky. Náhodně či úmyslně vybírají telefonní čísla, která pak zneužijí k maskování své vlastní identity.

Než operátoři a ČTÚ vše vyřeší, **může se vám snadno stát, že vám bude volat někdo s číslem vašeho partnera či příbuzného a bude vás žádat o rychlé převedení peněz na účet.** Díky dostupnosti nástrojů využívajících umělé inteligence pak může dokonce mluvit také jejich hlasem. Pro takové situace je dobré mít domluvené tajné heslo a při podezření na podvod okamžitě zavěsit.

Řešení problému od ČTÚ přichází doslova za 5 minut 12. Sociální sítě se plní příběhy podvedených. Pokud vám bude volat někdo z banky, můžete si snadno vyžádat ověření hovoru, kdy vám je zaslána notifikace přímo do bankovní aplikace a vy tak máte jistotu, že skutečně mluvíte s někým z banky. Tuto možnost podporuje většina českých bank, operátorů a řady dalších služeb.

Jak zablokovat podvodníky? ČTÚ pracuje na dvojici řešení

Česká telekomunikační úřad (ČTÚ) pracuje na dvojici řešení, která by tento druh podvodů měla omezit. Prvním z nich je blokáce volání ze zahraničí, u nichž volající vystupuje pod českým číslem, které by ze zahraničí přicházet nemělo. To se týká např. právě policie či bank.

Toto opatření se však nefunguje na klasická mobilní čísla, která mohou být v roamingu a nelze na ně tuto logiku uplatnit. Druhým způsobem je zajištění, aby při volání iniciovaném v České republice bylo do signalizační zprávy vkládáno skutečné telefonní číslo provázané s daným účastníkem či službou elektronických komunikací. Právě manipulací s parametrem mobilní sítě známým pod zkratkou **CLI (Calling Line Identification)** bylo doposud možné podvod snadno provádět.



Čeští uživatelé se s podvody setkávají až překvapivě často. Nyní by mohly pomoci kroky ČTÚ. Foto: Redakce inSmart.cz

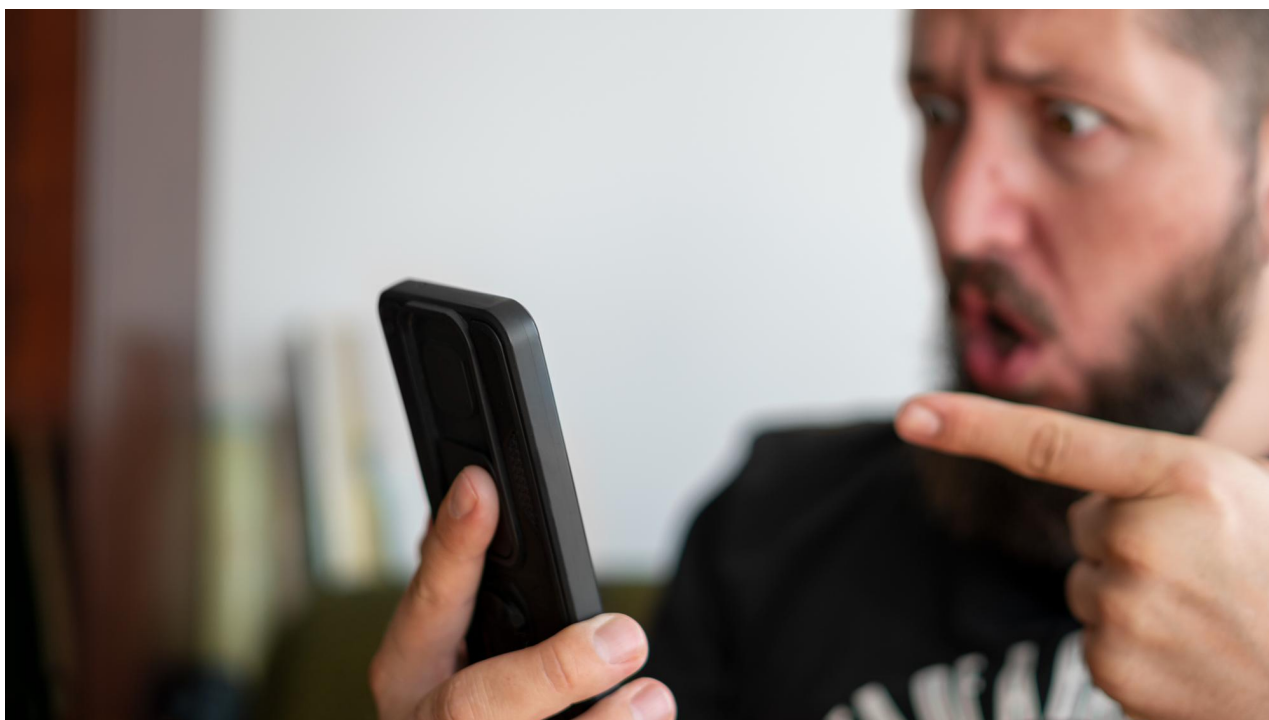
V České republice již fungování CLIP (Calling Line Identification Permission – povolení identifikace volajícího) omezil např. T-Mobile. Operátor se k problému vyjádřil následovně: „Společnost T-Mobile ve snaze zabránit narůstajícímu počtu případů nelegitimně spoofovaných hovorů s identifikací mobilních čísel naimplementovala na své straně ochranu, která zajišťuje pro koncové zákazníky sítě T-Mobile, že jejich číslo nemůže, ve většině případů, být při volání přes síť T-Mobile zneužito. Kontrola spočívá v tom, že se u A# patřící do sítě T-Mobile kontroluje, že hovor byl skutečně uskutečněn oprávněným volajícím.“

„Dále potvrzujeme tvrzení, že v případě, kdy se zákazník pokusí identifikovat ze své pobočkové ústředny umístěné mimo síť T-Mobile, tak i v tomto případě dojde k zamezení hovoru, neboť hovor není uskutečněn z dané SIM karty. Nesprávné označení hovoru –

tedy označení fixního volání mobilním číslem je v rozporu s číslovacím plánem a může, mimo spoofingu, vést i k nesprávné identifikaci a fakturaci na propojení," dodává T-Mobile.

Volá vám známé číslo? Může to být kdokoliv jiný

Přestože se čeští operátoři snaží proti vlně podvodných hovorů zakročit, zatím neúčinnější obranou zůstává obezřetnost samotných uživatelů. **Nikdy byste neměli sdělit žádné citlivé údaje nebo provádět jakékoliv transakce na základě telefonátu od někoho, koho jste sami nekontaktovali.** Změna podmínek všeobecného oprávnění by sice měla přinést zlepšení, úplné vymýcení tohoto typu podvodů však nebude jednoduché.



Volat vám může např. váš příbuzný, že potřebuje půjčit peníze. Číslo je správné, heslo sedí, ale ve skutečnosti je to někdo úplně jiný... Foto: Freepik

Zdroje: [ČTÚ](#), [Odorik](#)