# PODVODNÁ SPRÁVA „AHOJ MAMI"

## KEĎ ÚTOČNÍK PREDSTIERA VAŠU RODINU

Jedným z najcitovo manipulatívnych typov podvodov súčasnosti je tzv. podvod „Ahoj mami" (z angl. Hi Mum scam). Útočník sa vydáva za blízku osobu – najčastejšie dieťa – a využíva prirodzený inštinkt rodičov okamžite pomôcť v núdzi. Nepýta sa na heslo, neinštaluje škodlivý kód a nepotrebuje prístup k zariadeniu. Stačí mu dôvera a emócia, ktorú cielene vyvoláva. Práve preto patrí tento typ podvodu medzi najúčinnejšie formy sociálneho inžinierstva.

Spolufinancovaný Európskou úniou

*Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.*

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

## Mechanizmus podvodu Ahoj mami

Útok zvyčajne začína príchodom krátkej SMS alebo správy cez aplikáciu WhatsApp. Správa znie nenápadne a familiárne: "Ahoj mami, mám nové číslo, ulož si ho." Odosielateľ sa identifikuje ako syn alebo dcéra, prípadne iná blízka osoba. Väčšina ľudí na takúto správu zareaguje prirodzene – odpovedá, prípadne sa opýta, čo sa stalo so starým číslom.

Reakcia obete je pre útočníka spustačom druhej fázy. Komunikácia sa presúva na WhatsApp alebo inú chatovú platformu, kde útočník naďalej udržiava rolu rodinného príslušníka. Vysvetlenie je vždy jednoduché a emocionálne uveriteľné: pokazený alebo stratený telefón, naliehavá oprava, neodkladná faktúra alebo iná situácia vyžadujúca okamžitú finančnú pomoc. Podstatou je vyvolať pocit urgentnosti, ktorý potlačí kritické myslenie.

Platbu útočník zvyčajne žiada formou bankového prevodu, zvyčajne na zahraničný účet. Tuzemský prevod by mohol odhaliť totožnosť príjemcu, preto podvodníci používajú účty v zahraničí, niekedy aj prostredníctvom tretích strán. Po uskutočnení prvého prevodu nasledujú ďalšie žiadosti – niečo sa pokazilo, platba neprišla, je potrebná ešte jedna transakcia. Takto sa suma škody postupne navyšuje.

Keď obeť začne mať pochybnosti a pokúsi sa zavolať späť na číslo, z ktorého prišla pôvodná správa, číslo je spravidla nedostupné alebo vôbec nezvoní. Ak obeť zavolá na pôvodné číslo svojho dieťaťa, zistí, že dieťa o ničom nevie. V tom momente je väčšinou už príliš neskoro a peniaze sú preč.

Niektoré sofistikovanejšie varianty podvodu kombinujú správu so vopred získanými informáciami z verejných profilov na sociálnych sieťach – meno dieťaťa, fotografia alebo životné udalosti – čo robí komunikáciu oveľa presvedčivejšou a sťažuje včasné odhalenie.

## Indikátory podvodu Ahoj mami

Včasné rozpoznanie podvodu závisí od schopnosti identifikovať varovné signály napriek emočnému tlaku, ktorý situácia vyvoláva. Prvým a najdôležitejším indikátorom je samotná správa z neznámeho čísla s tvrdením, že ide o blízkú osobu s novým číslom. Skutočné dieťa by v takejto situácii zavolalo, prípadne nové číslo overilo iným spôsobom.

Pozornosť si zaslúži aj tón a obsah komunikácie. Pre útočníkov nie je slovenský jazyk rodným, niekedy robia gramatické chyby, často používajú v rodine nezaužívané formulácie. Rodičia poznajú spôsob, akým ich dieťa píše – neobvyklé oslovenia, formálnosť alebo opačne príliš neformálne výrazy môžu byť signálom, že komunikujú s niekým iným.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Hlavným varovným signálom je požiadavka na okamžitý peňažný prevod, najmä na zahraničný účet. Legitímna núdzová situácia má vždy viac riešení – overenie situácie telefonátom na pôvodné číslo, kontakt cez iného príbuzného, prípadne osobné stretnutie. Urgentnosť a požiadavka konať hneď bez overovania sú charakteristické pre manipulatívne techniky sociálneho inžinierstva.

Opakované žiadosti o prevody s vysvetlením, že "niečo sa pokazilo" alebo platba neprišla, sú ďalším silným indikátorom podvodu. Legitímne transakcie sa pri správnom uskutočnení nezlyhávajú opakovane a nevyžadujú série ďalších prevodov. Napokon, nedostupnosť čísla pri spätnom volaní je posledným potvrdením, že šlo o útok.

## Ako sa chrániť pred podvodom Ahoj mami

Kľúčovým preventívnym opatrením je zavedenie jednoduchého rodinného overovacieho kódu alebo tajnej otázky. Ide o vopred dohodnuté slovo alebo frázu, ktorú pozná len rodina a ktorú môže v prípade pochybností použiť na overenie totožnosti. Útočník tento kód nepozná a nedokáže ho poskytnúť.

Pri žiadosti o zapísanie si nového čísla, ponechajte si v mobile aj pôvodné číslo rodinného príslušníka.

Pri každej žiadosti o peniaze od neznámeho čísla je nevyhnutné volať späť na pôvodné, dobre známe číslo danej osoby – nie na číslo, z ktorého prišla správa. Ak je číslo nedostupné, kontaktujte danú osobu iným kanálom alebo cez iného rodinného príslušníka. Nikdy nezasielajte peniaze na základe samotnej textovej komunikácie bez hlasového alebo osobného overenia.

Dôležité je tiež nastaviť súkromné profily na sociálnych sieťach a obmedziť viditeľnosť informácií o sebe a rodine pre neznámych používateľov. Útočníci zbierajú verejne dostupné informácie, aby podvod pôsobil dôveryhodnejšie. Čím menej informácií je verejne dostupných, tým ťažšie je zostaviť presvedčivú legendu.

Ak ste sa stali obeťou tohto podvodu, okamžite kontaktujte svoju banku s žiadosťou o zastavenie alebo vrátenie transakcie, a vec nahláste polícii. Aj keď vrátenie peňazí nie je vždy možné, nahlásenie pomáha orgánom sledovať vzorce podvodnej činnosti a chrániť ďalšie potenciálne obete.

Podvod „Ahoj mami" je príkladom útoku, ktorý nevyžaduje technickú sofistikovanosť – vystačí si s emocionálnou manipuláciou. Jeho účinnosť stojí na rýchlosti, urgentnosti a dôvere, ktorú rodičia prirodzene pociťujú voči svojim deťom. Spomalenie, overenie a kritické myslenie sú najúčinnejšou obranou. Každý by si mal pamätať, že skutočné dieťa pochopí, ak rodič pred poslaním peňazí zavolá a overí, čo sa deje.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberá žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti