

Podvodníci dělají z brigádníků bílé koně. Pak je připraví o peníze

22.7.2024 - Petr Lesenský | Lesensky.cz

Léto je obdobím prázdninových brigád. Mezi seriózními nabídkami na přivýdělek se však často objevují i ty, které mají za cíl člověka napálit a připravit o peníze.

Jednou z nových metod, před nimiž varují finanční instituce, je snaha podvodníků udělat z brigádníků takzvané bílé koně a prát přes jejich účty nelegálně nabyté prostředky. Kromě ztráty úspor hrozí obětem i trestní stíhání.

Podvod s falešnými nabídkami brigád obvykle začíná posláním SMS nebo zprávy na WhatsApp či jinou aplikaci. Odesílatel se v ní často vydává za zástupce personální agentury či konkrétní společnosti. V první fázi je úkolem brigádníka obvykle lajkovat dle instrukcí různé příspěvky na sociálních sítích, za což obdrží drobnou odměnu na svůj účet.

Následně však podvodníci rozšiřují náplň práce. „Vaším úkolem bude přeposílat ‚výdělky‘ dalším ‚zaměstnancům‘ firmy. Za přeposlání ‚výdělků‘ samozřejmě dostanete provizi, abyste nepřišli zkrátka. V tuto chvíli se stáváte bílým koněm. Jste součástí řetězce, kdy přes váš účet podvodníci legalizují výnosy z trestné činnosti,“ popisuje **Lukáš Kropík**, mluvčí České spořitelny.

Odpovědnost za vzniklé škody

Bílý kůň má před zákonem povinnost vydat všechny prostředky, o které se obohatil – tedy odměnu, kterou od podvodníka obdržel. Zároveň je však odpovědný i za vydání částek, které z účtu vybral nebo přeposlal podle instrukcí podvodníka. Za dané jednání hrozí peněžitý trest, propadnutí věci, propadnutí majetku, zákaz činnosti a v krajním případě i trest odnětí svobody. „Pokud obdržíte neznámé peníze na svůj účet, nahlase to přímo bance, neboť je musíte vrátit,“ upozorňuje Lukáš Kropík.

Ve finální části podvodu se falešný zaměstnavatel obvykle pod záminkou výhodné investice pokusí vylákat od „brigádníka“ vyšší finanční částku z jeho účtu. Kromě trestního stíhání tak může člověk v případě neopatrnosti čelit i realitě ztráty úspor.

Podle **Petra Doudy**, mluvčího společnosti Randstad, lze většinu podvodných zpráv nabízejících falešné brigády při vyšší ostražitosti rozeznat. Často se totiž prozradí lámanou češtinou, gramatickými chybami nebo podivnou předvolbou náležející obvykle asijským či africkým zemím. Zviklat by člověka neměla ani situace, kdy se podvodník představí jako zaměstnanec agentury zprostředkovávající práci. „Agentura práce nikdy nežádá osobní údaje nebo informace o platební kartě prostřednictvím textových zpráv. Rovněž nikdy nepožaduje peníze za zprostředkování zaměstnání,“ doplňuje Petr Douda.

Oběťmi jsou lidé ve středním věku

I přes pokračující osvětu počty obětí kyberkriminality každoročně rostou. Podle České bankovní asociace zaznamenaly banky v roce 2023 celkem 69 685 napadených klientů s celkovou škodou 1,35 miliardy korun. Průměrná výše škody dosáhla 19 357 korun.

„Řada lidí se domnívá, že typickými oběťmi podvodníků bývají senioři. Podle dat však nejčastěji přicházejí o peníze lidé ve středním věku, mezi 36 a 44 lety. Ve větší míře jde o ženy, muži však

bývají okradeni o vyšší částky," popisuje **Jan Nedělník** ze společnosti Konecta Czech, Hungary a Slovakia, která působí v oblasti zákaznického servisu a spolupracuje s řadou bankovních institucí.

Falešní bankéři a investiční poradci

Kromě triků s lákavými brigádami využívají podvodníci desítky dalších metod, jak vymámit z důvěřivých lidí peníze. V oblibě jsou scénáře s falešnými investičními poradci, kteří pod záminkou výhodného zhodnocení financí nabádají k transakcím na falešné účty či platformy. K odcizení peněžních prostředků často využívají i takzvaný vzdálený přístup, kdy se prostřednictvím aplikace po souhlasu oběti dostanou přímo do uživatelského rozhraní daného člověka.

Podobně funguje i taktika falešného bankéře. Ten se obvykle snaží vybrané oběti namluvit, že byl její účet napaden. Pro záchranu úspor klienta vyžaduje podvodník přístupové údaje do internetového bankovníctví či jej za pomoci důmyslných lží lanaří k vložení úspor do bitcoinmatů a k jejich poslání na cizí účty.

„Zástupci bankovních společností nikdy od klientů nepožadují jejich přihlašovací údaje ani nevstupují do účtů zákazníků prostřednictvím vzdálených přístupů. Pokud má tedy člověk při kontaktu s někým, kdo se představí jako zástupce jeho banky, jakékoli pochybnosti, měl by konverzaci ihned přerušit,“ uzavírá Jan Nedělník.

<https://www.dychame.cz/podvodnici-delaji-z-brigadniku-bile-kone-pak-je-pripravi-o-penize>