

Pozor na podvodné jednání s kryptoměnou

20.1.2026 - Tomáš Macura | Policie ČR

Nový trik podvodníků využívá terminály v trafikách. Peníze mizí v kryptoměnách.

Policie České republiky upozorňuje občany na nový, rafinovaný způsob podvodného jednání, který kombinuje psychologický nátlak, lákavou nabídku investic a anonymní platby přes terminály v prodejnách GECO.

Tento nový model podvodu, často spojovaný s investičními platformami, kombinuje manipulativní techniky známé jako „scam“ s využíváním hotovostních platebních terminálů v síti prodejen GECO. Právě zapojení fyzických poboček trafik dodává celému podvodu pro oběti falešný pocit legitimacy a bezpečnosti.

Celý mechanismus začíná velmi nenápadně, obvykle lákavou reklamou na sociálních sítích nebo nevyžádaným telefonním hovorem od domnělého investičního experta. Pachatelé se představují jako profesionální makléři a slibují nereálné zhodnocení úspor. Jakmile oběť projeví zájem, podvodník ji instruuje k provedení první investice. Na rozdíl od běžných bankovních převodů však pachatel zašle oběti specifický platební kód a nasměruje ji na nejbližší pobočku trafiky GECO. Zde má oběť obsluhu ukázat obdržení kódu a zaplatit požadovanou částku v hotovosti.

Ve skutečnosti tento kód neslouží k dobití investičního účtu, ale k nákupu kryptoměn nebo dobití anonymních platebních prostředků, ke kterým má přístup výhradně pachatel. V momentě, kdy obsluha trafiky kód načte a přijme hotovost, jsou finance okamžitě a nevratně převedeny do digitální podoby v anonymní peněženke. Pro policii je následné trasování takto převedených prostředků extrémně náročné, neboť transakce probíhá mimo standardní bankovní systém a identita příjemce zůstává skryta za šifrováním kryptoměnové sítě.

Popsané jednání nese všechny znaky fenoménu zvaného scam. Podvodníci se v průběhu komunikace snaží vyvolat časový nátlak a často oběti přesvědčují k instalaci programů pro vzdálenou správu počítače, jako jsou AnyDesk, TeamViewer či Hoptodesk, pod záminkou pomoci s nastavením účtu. Tímto krokem však získávají plnou kontrolu nad zařízením oběti i jejím internetovým bankovníctvím. Důležitým varovným signálem je také požadavek na další platby ve chvíli, kdy se oběť pokusí své domnělé zisky vybrat. Pachatelé si v takové situaci vymýšlejí fiktivní poplatky za převod, daně nebo provize, které mají za cíl z oběti odčerpat další finanční prostředky.

Policie ČR důrazně varuje před investováním prostřednictvím subjektů, které nemají licenci České národní banky. Před jakoukoli platbou v trafice si položte otázku, zda plně kontrolujete cílovou peněženku, kam peníze směřují. Pokud vás k platbě instruuje kdokoli po telefonu nebo chatu, jde s největší pravděpodobností o podvod. V případě, že se občan již stal obětí takového jednání, měl by okamžitě přerušit kontakt s pachatelem, zajistit účtenky z terminálů i historii komunikace a věc neprodleně nahlásit na nejbližší služebně Policie ČR nebo na lince 158.

Varovné signály v komunikaci:

- **Časový nátlak:** Podvodníci často spěchají a tvrdí, že "výhodná nabídka platí jen dnes".
- **Příslib nereálných zisků:** Slibují pohádkové zbohatnutí s nulovým rizikem.
- **Zneužití známých jmen:** Reklama používá loga ČEZ, bank, nebo tváře celebrit.
- **Špatná čeština nebo neobvyklá jména:** I když dnes už používají AI pro překlad, stále se mohou objevovat gramatické chyby nebo nepřirozený slovosled.

- **Komunikace přes aplikace:** Místo oficiálních e-mailů vás nutí komunikovat přes WhatsApp, Telegram nebo Messenger.
- **Instalace programů pro vzdálený přístup k vašemu počítači:** Nabídne vám „pomoc“, kdy se zmocní vašeho zařízení a ovládá ho vzdáleně.

Pokud vás někdo po telefonu nebo přes internet navádí k tomu, abyste vzali hotovost a šli ji někam vložit přes terminál nebo automat, **VŽDY JDE O PODVOD!**

por. Bc. Tomáš Macura
preventista ÚO Nymburk
20. ledna 2026

<https://policie.gov.cz/clanek/pozor-na-podvodne-jednani-s-kryptomenou.aspx>