

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **110** ze dne **10.6.2025**

Kryptoscamů přibývá. Jak je poznat?

Češi se stavějí ke kryptoměnám poměrně otevřeně, nemalá část plánuje jejich nákup. Méně zřejmá ale mohou být rizika.

Podle analýz Esetu se vloni počet investičních podvodů s kryptoměnami zvýšil o 335 %. A není divu, útočníci jdou vždycky tam, kde cítí peníze. Právě podvody související s investicemi patří podle policie mezi nejčastější zločiny v kyberprostoru.

„Kriminalita páchaná v kyberprostoru tvoří v současnosti přibližně 10,5 % celkového objemu trestné činnosti. Možná překvapivě se na předních příčkách z hlediska kvantity objevují právě útoky spojené s investováním – tedy podvodné nabídky výhodných investic, často do kryptoměn. Ročně evidujeme stovky takových případů, přičemž škody jdou řádově do stovek milionů korun,“ říká plk. Zuzana Pidrmanová, vedoucí odboru prevence Policejního prezidia ČR.

Krypto scam organizuje celý gang

Za celým schématem nestojí jeden nebo dva hackeři, jde o velmi promyšlené schéma, které vyžaduje organizovanou skupinu. Zastavit takové gangy je problematické, neustále se objevují nové falešné stránky a podvodné platformy.

Podvodníci kombinují lákavou reklamu na sociálních sítích, zmanipulované články v renomovaných médiích (jde o falešné stránky) s přesvědčivou manipulací a psychologickým nátlakem. V některých případech mají k dispozici i call centrum a mohou vyústit až k falešnému telefonátu s útočníkem, tzv. vishingu. Volající běžně hovoří velmi dobrou češtinou bez přízvuku.

„Pokud se lidé rozhodnou investovat do kryptoměn, doporučujeme využívat pouze prověřené platformy, které jsou členy České kryptoměnové asociace a prošly jejím certifikačním procesem,“ radí František Vinopala, předseda České kryptoměnové asociace.

Jak probíhají investiční podvody do bitcoinu?

Typicky na takový podvod narazíte na sociálních sítích, zpravidla ve formě placené inzerce. Útočníci si totiž umějí spočítat, že se jim clickbaitová reklama vyplatí.

Zpravidla jde o nabídku lákavé investice s pohádkovým zhodnocením, ještě častěji jde ale o trik „zbohatněte jako celebrita“. Velmi často je v inzerátu uvedeno, že se nějaká známá osobnost prokela a nyní čelí perzekuci, že umožnila Čechům zbohatnout. Zneužití takto byli například Tereza Pergnerová, Petr Kellner, Andrej Babiš i Petr Fiala. Bohužel i když se tyto osobnosti brání, mají jen málo možností, jak přimět útočníky podvod stáhnout.

Zneužití jmen známých osob není náhoda. Podle průzkumu dá na doporučení známé osobnosti desetina lidí.

„Pokud na reklamu člověk klikne, je přesměrován na webovou stránku, kde bývá falešný článek, který se tváří jako legitimní zpráva od nějakého známého média. Tato zpráva je zpravidla šokující a má za úkol manipulovat emocemi oběti a upoutat její pozornost. Na webové stránce je pak také falešný formulář. Jakmile do něj člověk zadá své údaje, kontaktuje ho následně někdo z podvodného call centra. Cílem

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **110** ze dne **10.6.2025**

podvodníků je samozřejmě vždy přimět oběť k převodu peněz," popisuje aktuální podvodný scénář Novotný.

Podvodníci vám pošlou peníze, aby vás okradli

Existují i varianty, kdy je formulář už součástí reklamy nebo naopak vede člověka přímo na krypto burzu, kde má možnost zadat zkušební investici. Celý proces působí velmi důvěryhodně.

„Falešné investiční portály působí na první pohled důvěryhodně, jsou plné pozitivních recenzí a ukazují neustále rostoucí zisky. Tyto zisky jsou ale smyšlené a oběť je ve skutečnosti nikdy nezíská zpět. Někdy je dokonce zpočátku malá částka vyplacena, aby byl podvod ještě důvěryhodnější a oběť investovala víc," varuje plk. Zuzana Pidrmánová. „Evidujeme i případy, kdy vás pachatelé oslovují skrze romantický vztah v online prostředí. Investici vám pak doporučuje osoba, které důvěřujete. Pachatelé mohou svou oběť dokonce znovu kontaktovat jménem například advokátní společnosti, tentokrát s legendou, že za úplatu dokážou investici zachránit, přičemž takto škoda jen dál narůstá.“

Češi podvody poznají bez problémů

V rámci průzkumu byl respondentům ukázán typický podvodný článek. Jen 4 % podvod neodhalila, 15 % si nebylo jistých. Ostatní uživatelé se dívali na text pečlivě kriticky vyhodnotili, že jde o podvod, protože:

- 32 % gramatické chyby
- 29 % rozporu informací v titulku článku s tématem obrázku
- 20 % důvodné podezření, že by spolu Andrej Babiš a Petr Fiala nespolupracovali

„Ideální je se zaměřit na kombinaci ukazatelů – zkontrolovat URL adresu webu, na kterém se nacházím, pořádně si celou stránku prohlédnout a mít zdravou skepsi k šokujícím sdělením," radí bezpečnostní analytik Ondřej Novotný.

Jak poznat scam?

Důležité je být obezřetný a vědět, že podvody existují. Narazit na ně mohou i děti nebo senioři, kteří mohou být důvěřivější. Jak tedy podvod poznat?

Nabídka je extrémně láková a musíte ji využít hned. Jde o nějaké tajemství, které známá osobnost nechtěně vyradila. URL adresa není přesná nebo neodpovídá médiu, ze které se vydává.

Zde je několik tipů, jak udržet vaše kryptoměny v bezpečí:

- Lákavou nabídku vždy nezávisle ověřte. Píše se o ní na oficiálních profilech nebo odborných médiích?
- Ověřte si adresu URL média, burzy nebo služby.
- Podívejte se, zda má vybraná burza certifikaci od České kryptoměnové asociace případně nějaké zahraniční autority.
- Nikdy nezadávejte osobní nebo platební údaje, pokud si nejste stránkou absolutně jistí.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **110** ze dne **10.6.2025**

- Nikdy nesdělujte po telefonu své přihlašovací údaje ani údaje k platební kartě.
- Stahujte si aplikace a programy jen oficiálních zdrojů.
- U kryptoměnových účtů si zapněte dvoufaktorové ověření.
- Aktualizuje operační systém zařízení a programy.
- Používejte na všech svých zařízeních spolehlivý antivirový program.

Co dělat, pokud jste se stali obětí scamu?

Pokud jste na nějaký podvod zareagovali a útočníkům zaplatili, neprodleně požádejte svou banku o zpětné zúčtování (chargeback). Vysvětlete bance situaci, tyto podvody znají, mapují. V některých případech lze získat peníze zpět. Podvod nahlaste na Policii ČR.

V některých případech požadují útočníci kopie dokladů nebo platebních karet. Což nemusí být překvapivé, dělají to i renomované banky, pokud komunikujete jen elektronicky. V takovém případě si nechte okamžitě vystavit nové doklady. Nebudete se tak muset obávat jejich případného zneužití.

Zdroj: AVcentrum ČR