Průzkum ESET: Češi chtějí nakupovat kryptoměny, podceňují ale kybernetická rizika

16.4.2025 - Lucie Mudráková, Vítězslav Pelc | ESET software

Zhruba polovina Čechů a Češek plánuje nákup kryptoměn, necelá třetina je už vlastní nebo někdy vlastnila. Kromě složitosti a finanční rizikovosti se bojí také kybernetických rizik, třetina však netuší, jaká rizika by to měla být. Vyplývá to z nového průzkumu společnosti ESET. Podle bezpečnostních expertů se můžeme v Česku aktuálně setkávat s podvodem, při kterém útočníci využívají různé techniky manipulace, včetně falešného obsahu, který vydávají za články ve známých médiích. Cílem je oběť kontaktovat a přimět ji k nákupu falešných služeb, zboží nebo k investicím.

Podle nejnovějšího průzkumu společnosti ESET mají Češi obecně kladný vztah ke kryptoměnám. Necelá třetina dotázaných nějakou kryptoměnu již vlastní nebo někdy vlastnila (27 %). Jedná se především o uživatele ve věku 18-30 let a z Prahy, nejvíce se středoškolským a vysokoškolským vzděláním. Téměř polovina dotázaných by si kryptoměny v budoucnu ráda pořídila (45 %), z toho 9 % z nich co nejdříve během pár měsíců. Popularita kryptoměn však láká i různé kybernetické podvodníky a útočníky. Podle poslední zprávy ESET Threat Report H2 2024 narostl v období od června do listopadu 2024 počet investičních podvodů o více než 335 % mezi prvním a druhým pololetím roku 2024. Mezi zeměmi s největším počtem detekcí se objevila také Česká republika. Ve stejném období byl zaznamenán také růst počtu útoků na kryptoměnové peněženky, především na platformě macOS.

„I když z dat můžeme vidět, že Češi jsou v pozitivním a negativním postoji ke kryptoměnám rozděleni prakticky na dvě stejné skupiny, obecně lze říct, že s kryptoměnami ve svém životě počítají – zhruba polovina uvažuje o jejich nákupu. Nejčastěji je chtějí lidé v běžném životě využívat jako alternativu ke spoření, uvedlo to 30 % dotázaných. Vnímají ale i kybernetická rizika. Na otázku, co je pro ně důvodem si kryptoměny nepořídit, uváděla čtvrtina z nich vedle přílišné finanční rizikovosti a složitosti také obavu, že by byli následně příliš vystaveni kybernetickým podvodům a útokům," komentuje výsledky průzkumu Ondřej Novotný, kyberbezpečnostní analytik z pražské pobočky společnosti ESET. „Bohužel ale u otázky, o jaká konkrétní kybernetická rizika by se mělo jednat, čeští uživatelé a uživatelky spíše tápou, a to není dobrá zpráva. V případě kybernetických podvodů s tématikou investic se jedná o propracované podvodné scénáře, kdy útočníci zapojují více než jen jednu útočnou techniku. Součástí podvodů je například i manipulovaný vizuální obsah, který má oběti přilákat ke kliknutí na škodlivé odkazy. Podvodné webové stránky vnímá jako největší nebezpečí 16 % dotázaných, zatímco phishing jen 8 %, deepfake podvody 5 % a škodlivé kódy, tzv. cryptostealery, jen 3 % dotázaných. Třetina dotázaných uvedla, že netuší, co je největším rizikem pro kryptoměny," dodává Novotný.

„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. „Tato trestná činnost je dnes doménou organizovaných skupin, které velmi dobře vědí, jak účinná tato legenda je. Nejenže se neustále objevují nové podvodné platformy, ale stále přibývají i nové oběti. Pachatelé totiž kombinují lákavou nabídku s velmi přesvědčivou manipulací a psychologickým nátlakem. V kontextu těchto

případů varujeme veřejnost, že jakákoliv online investice je vždy riziková a neměla by být činěna pod tlakem nebo na základě emocí. Je důležité investovat pouze prostředky, o které si lze dovolit přijít, pečlivě si prověřit platformu i zprostředkovatele, a v případě nejistoty raději neinvestovat vůbec," dodává plk. Zuzana Pidrmanová.

„Rostoucí sofistikovanost online podvodů nás nutí klást důraz na vzdělávání uživatelů a prevenci. I když některé útoky stále prozrazují hrubé chyby, jiné využívají pokročilé techniky sociálního inženýrství a působí velmi věrohodně. Právě proto je důležité být obezřetný, nedůvěřovat nevyžádaným kontaktům a nepodléhat emocím, jako je strach nebo touha po rychlém zisku. Kryptoměny dávají lidem svobodu – a s ní přichází i zodpovědnost chránit sebe i své investice. Pokud se lidé rozhodnou investovat do kryptoměn, doporučujeme využívat pouze prověřené platformy, které jsou členy České kryptoměnové asociace a prošly jejím certifikačním procesem," říká František Vinopala, předseda České kryptoměnové asociace.

Podle bezpečnostních expertů, kteří kybernetické podvody s tématikou investic do kryptoměn dlouhodobě sledují, začínají současné podvody často na sociálních sítích. Mohou vyústit až k falešnému telefonátu s útočníkem, tzv. vishingu. Kromě investic do kryptoměn mohou podvodníci nabízet také falešné služby a zboží.

„Podvody, které v současnosti sledujeme, začínají většinou tzv. clickbaitovou reklamou na sociálních sítích. Pokud na ni 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. Podvod může mít také několik dalších variant. Formulář k zadání údajů může být přímo součástí reklamy na sociálních sítích. Útočník může oběť kontaktovat také rovnou na sociálních sítích prostřednictvím chatu a následně v komunikaci pokračovat buď po telefonu nebo e-mailu. Cílem podvodníků je samozřejmě vždy přimět oběť k převodu peněz," popisuje aktuální podvodný scénář Novotný.

„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. Na podvodnou investiční příležitost můžete narazit nejen v rámci lákavých reklam, ale můžete být přímo osloveni v rámci agresivních telefonátů. 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," vysvětluje plk. Zuzana Pidrmanová.

Řada podvodných reklam a novinových článků může podle expertů z ESETu využívat jmen známých osobností nebo firem. I to podle nich přispívá k úspěšnosti podvodů. Na otázku, k jakému zdroji informací se lidé obrací, pokud uvažují o nákupu kryptoměn, více než desetina (14 %) odpověděla, že dá na doporučení známé a respektované osobnosti či organizace z oblasti politiky nebo byznysu. A to si útočníci dobře uvědomují a zneužívají toho. Třetina lidí (30 %) se obrací na odborná média a pětina sleduje geopolitický vývoj a vývoj na kryptoměnových trzích (23 %). Zdrojem informací jsou pro ně také přátelé a rodina (22 %) a kolegové v práci (19 %).

„Respondentům jsme v rámci průzkumu zobrazili i ukázku falešného zpravodajského článku, který útočníci využívají v rámci popsaných útoků. Překvapilo nás, že 15 % dotázaných při pohledu na obrázek nevědělo, zda by se mohlo jednat o falešnou zprávu či nikoli. Považujeme to za varovný ukazatel toho, jak úspěšné tyto podvody mohou být," říká Novotný a dodává: „Třetina respondentů,

32 %, označila obsah za podvodný z důvodu gramatických a stylistických chyb a další necelá třetina, 29 %, uvedla, že je to prokazatelný podvod kvůli rozporu informací v titulku článku s tématem obrázku. Pětina dotázaných pak uvedla, že by je na podvod upozornilo důvodné podezření, že by spolu Andrej Babiš a Petr Fiala nespolupracovali. Ve všech případech dotázaní udělali to, co dlouhodobě doporučujeme – zastavit se, pořádně si zprávu přečíst a kriticky zhodnotit, na co se to vlastně dívám a zda to dává smysl. Přesto se největší část dotázaných odkazovala na chyby v gramatice, s čímž si ale nástroje umělé inteligence pravděpodobně již brzy zase o něco lépe poradí. Ideální je se tak zaměřit na kombinaci ukazatelů – zkontrolovat URL adresu webu, na kterém se nacházím, pořádně si celou stránku prohlédnout a mít zdravou skepsi k šokujícím sdělením."

Při podezření, že se setkali s deepfake obsahem vygenerovaným pomocí umělé inteligence, by nejvíce lidí zkontrolovalo nejdříve oficiální profily dotyčné osobnosti či organizace na sociálních sítích, zda na podvodný obsah sami neupozorňují (29 %). Pětina dotázaných pak uvedla, že by se ze všeho nejdříve zaměřila na samotné prvky obsahu – zda osoba ve videu působí reálně, zda sedí pohyb rtů s tím, co říká, nemá trhané pohyby či zda mrká (23 %). Další pětina (18 %) by pak nejdříve zkontrolovala, zda na nepravost videa neupozornili jiní uživatelé nebo média a desetina lidí (11 %) by hledala informaci, že se jedná o obsah vygenerovaný pomocí AI (11 %). Pětina lidí však odpověděla, že by neudělala ani jednu z kontrol zmíněných výše (19 %).

„Pokud jsme mluvili o opatrnosti při prohlížení statického obsahu na internetu, který mohou zmanipulovat útočníci, u videa by naše kontrola měla být pečlivější, protože snáze můžeme varovné prvky přehlédnout. S vývojem nástrojů schopných generovat deepfake obsah bude pravděpodobně stále těžší všímat si nesrovnalostí v projevu osoby ve videu, zatím to však může být stále jeden z dobrých ukazatelů nepravdivého obsahu. Opět je ale důležité především nepodlehnout šokujícím sdělením. Cílem útočníků je působit na naše emoce, jako je strach, zvědavost a soucit. A u investičních podvodů bychom si měli pamatovat, že když něco zní až příliš senzačně a jednoduše, nebude to pravda," dodává Novotný.

Jak v případě škodlivých kódů, tak i u internetových podvodů hraje v obraně roli celkový přístup k naší online bezpečnosti. Týká se to nejen správy našich hesel, stahování aplikací z internetu, ale také například toho, zda využíváme na svých zařízeních kyberbezpečnostní software.

Nejčastěji se v otázkách kyberbezpečnosti uživatelé a uživatelky v Česku spoléhají na vícefázové ověření – pro přihlášení ke svým účtům ho využívá více než polovina dotázaných (51 %). Dále si lidé nejčastěji dávají také pozor, odkud stahují aplikace do svých zařízení (43 %) a zda pravidelně svá zařízení a aplikace aktualizují (42 %).

„Na základě dat z průzkumu můžeme vidět, že se stále liší poměr lidí, kteří využívají bezpečnostní software na svém počítači, 33 %, a těmi, kteří mají bezpečnostní program i na svém chytrém telefonu, 23 %. Chytré telefony jsou přitom v našem každodenním životě prakticky nepostradatelné a uchováváme v nich celou řadu osobních a citlivých dat. Konkrétně u většinově zastoupených chytrých telefonů s operačním systémem Android pravidelně sledujeme nezanedbatelná kybernetická rizika. Rozhodně bych pak uživatelům a uživatelkám doporučil zvážit pořízení spolehlivého bezpečnostního softwaru i pro jejich smartphony," říká Novotný. „Jen třetina dotázaných, 32 %, pak tvoří pro každý svůj účet unikátní heslo. V případě, že využíváme jedno heslo pro více účtů a přes všechnu opatrnost jej zadáme do nějakého falešného formuláře, otevíráme útočníkům dveře k několika svým účtům. Jen pětina lidí pak využívá specializované šifrované programy pro bezpečnou správu hesel, které nám přitom mohou pomoci uchovávat dostatečně složitá hesla bez toho, aniž bychom si je museli bokem někam zapsat nebo pamatovat. Správci hesel dnes také bývají součástí kvalitních bezpečnostních řešení," dodává Novotný z ESETu.

Sběr dat byl realizován prostřednictvím aplikace Instant Research agentury Ipsos ve dnech od 13. do

18. března 2025 na 1039 respondentech v České republice.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost najdete například v online magazínu Dvojklik.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide. Nejčastějším rizikům pro děti na internetu se věnuje iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET, v podcastu TruePositive a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio řešení od ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři výzkumná a vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/pruzkum-eset-cesi-chteji-nakupovat-kryptomeny-podcenuji-ale-kyberneticka-rizika