NOVÝ TYP PODVODU

KURIÉRI BERÚ ĽUĎOM MOBILY, ABY IM VYBIELILI ÚČTY

Prázdniny prebiehajú v plnom prúde a prinášajú nové zážitky, zmenu prostredia a nové kontakty. Zmeny sa však neodohrávajú len v reálnom svete, ale aj v kybernetickom priestore. Útočníci opúšťajú anonymitu digitálneho prostredia a do svojich schém zapájajú aj priamy fyzický kontakt. Pod zámienkou vyplatenia fiktívneho zisku z kryptomien presviedčajú obete, aby prostredníctvom kuriéra odovzdali svoj mobilný telefón spolu s prístupovými kódmi.

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

Ide o variant už známeho investičného podvodu, ktorý sa začína telefonátom s informáciou, že obeť údajne zarobila na investovaní do kryptomien niekoľko tisíc eur. Na vyplatenie tohto fiktívneho výnosu je podľa páchateľov potrebná aplikácia s podporou NFC technológie.

Oproti doterajšej praxi podvodníci obeť už nenavigujú, aby si aplikáciu stiahla a nainštalovala sama. Namiesto toho sa profilujú ako mimoriadne proklientsky orientovaní a ponúknu, že inštaláciu vykonajú za klienta priamo v pobočke banky. Na to však potrebujú, aby im obeť poslala svoj telefón po nimi zabezpečenom kuriérovi.

Podvodná schéma sa navonok tvári ako výhodná ponuka na vyplatenie investičného zisku, v skutočnosti sa však snaží získať:

- mobilný telefón obete s nainštalovanou, funkčnou aplikáciou elektronického bankovníctva,
- PIN kód k internetbankingu,
- plný prístup k bankovému účtu, celoživotným úsporám a k možnosti čerpať úvery na meno obete.

Kuriér obeti na výmenu zvyčajne odovzdá náhradný mobilný telefón spolu s predplatenou SIM kartou. Na toto číslo podvodníci obeť následne kontaktujú, najmä ak majú podozrenie, že sa situácia nevyvíja v ich prospech – napríklad ak si obeť dodatočne uvedomí podvodný charakter komunikácie a pokúsi sa zmeniť si prístupové údaje k bankovej aplikácii.

Súčasťou manipulácie je aj presviedčanie obete, aby popri telefóne odovzdala aj PIN kód k internetbankingu. Vďaka tomu páchatelia nepotrebujú ani tvárovú biometriu obete, ani jej občiansky preukaz – kombinácia fyzického zariadenia a znalosti PIN kódu im postačuje na úplnú kontrolu nad účtom.

Indikátory podvodu

Prvým varovným signálom je už samotná požiadavka na odovzdanie telefónu tretej osobe. Žiadna banka ani legitímna investičná spoločnosť nikdy nevyžaduje, aby klient odovzdal svoje zariadenie kuriérovi alebo nahlas oznámil prístupový PIN kód akejkoľvek osobe mimo bankového kanála.

Typickým znakom je umelo vytváraný tlak. Ak obeť váha alebo odmietne mobil vydať, páchatelia nátlak stupňujú a tvrdia, že bez tohto kroku nie je možné výnos vyplatiť.

Kombinácia časovej tiesne, sľubu rýchleho zisku a osobného kontaktu robí z tohto podvodu mimoriadne presvedčivú a nebezpečnú kombináciu.

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

Ako sa chrániť

- Nikdy neodovzdávajte svoj mobilný telefón cudzej osobe, a to ani vtedy, ak tvrdí, že prichádza v mene banky, investičnej spoločnosti, technickej podpory alebo kuriérskej služby.
- Nikdy neposkytujte prístupové kódy. Heslá, PIN kódy ani autorizačné údaje do bankovníctva sú prísne tajné a banka ich od vás nikdy nebude žiadať telefonicky, cez kuriéra ani prostredníctvom tretej osoby.
- Neinštalujte si aplikácie na pokyn neznámej osoby, aj keď tvrdí, že je to potrebné na vyplatenie peňazí, overenie účtu alebo technické nastavenie mobilu.
- Neverte zázračným výnosom. Ak vám niekto telefonicky sľubuje rýchle vyplatenie výnosu z investičného alebo kryptoúčtu, o ktorý ste sami nežiadali, hovor okamžite ukončite.
- Overujte identitu volajúceho. Ak máte pochybnosti, kontaktujte banku výhradne cez oficiálne telefónne číslo uvedené na jej webovej stránke, nie cez číslo, ktoré vám poskytol volajúci.

Ak ste už mobil alebo prístupové kódy odovzdali, okamžite požiadajte o blokáciu elektronického bankovníctva a platobných kariet vašu finančnú inštitúciu na kontaktoch, ktoré si nájdete na oficiálnom webe, skontaktujte svojho mobilného operátora a nechajte si zablokovať dočasne SIM kartu a podajte trestné oznámenie na polícii.

Za úspechom tejto schémy nestojí len technická sofistikovanosť, ale predovšetkým psychológia. Útočníci cielene chcú využiť moment radosti z neočakávanej výhry – ten krátky okamih, keď sa racionálne uvažovanie vytráca pod tlakom eufórie z „ľahko nadobudnutých“ peňazí. Doba nikdy nie je taká zlá, aby sa neočakávaná výhra nehodila, a práve na tejto myšlienke podvodníci stavajú celú manipuláciu.

Skôr než podobnú ponuku začnete zvažovať, je užitočné položiť si jednoduchú otázku: ako často sa vo vašom okolí niekomu skutočne prihodila neočakávaná výhra alebo mimoriadny investičný zisk bez toho, aby si to sám aktívne a dlhodobo nezarobil? Ak je odpoveď „nikdy“ alebo „takmer nikdy“, možno je najvyšší čas začať byť voči podobným ponukám vážne podozrivý. Neočakávané zisky sú v reálnom svete výnimkou, nie pravidlom – a práve táto vzácnosť je dôvodom, prečo si zaslúžia oveľa väčšiu mieru nedôvery, než akú im bežne venujeme.

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