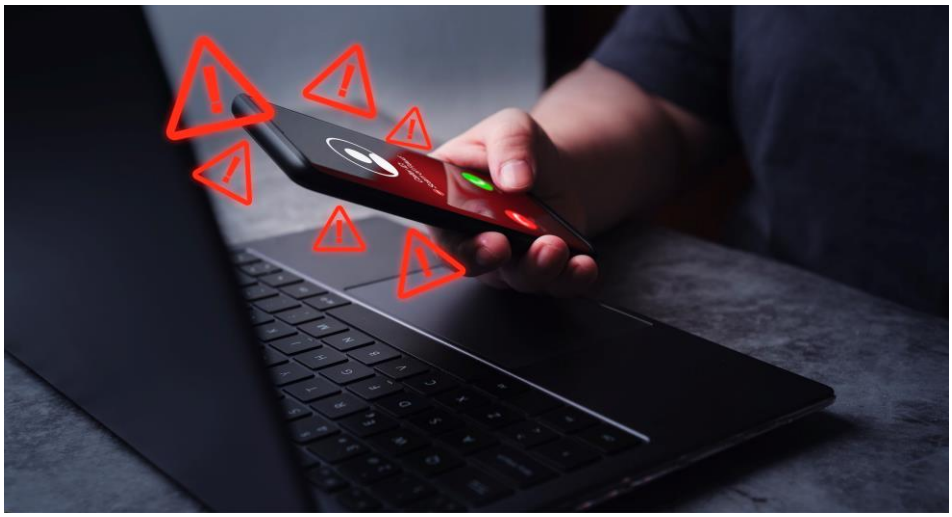
Tisková zpráva

U vkladomatu s igelitovou taškou a mobilem: Obětem falešných bankéřů jsme už zachránili statisíce korun, říká bezpečnostní manažer SSI Group

Praha, 27. srpna 2024 - **Je to docela obvyklý scénář. U vkladového automatu na virtuální měnu stojí člověk s mobilním telefonem v ruce, naplněnou igelitovou taškou, působí zmateně a pokouší se vložit hotovost do přístroje. Když někoho takového při obchůzce obchodním centrem vidí pracovníci ostrahy z SSI Group, už vědí, co dělat. Lidem, kteří se stali obětí kyberpodvodníků, pomohli zachránit statisíce korun.**



„Když se takového člověka zeptáme, proč to dělá, odpovědi většinou známe předem – prý se takto po upozornění z „banky" nebo „policie" snaží zachránit své úspory z napadeného účtu anebo chce pod vedením „svého bankéře" výhodně investovat," popisuje osobní zkušenost Daniel Knápek, Area manager ze společnosti SSI Group, která zajišťuje bezpečnostní služby v řadě obchodních center po celé republice.

„Potkáváme tam zejména seniory, ale stává se to i lidem v produktivním věku. Často nechtějí uvěřit, že toto je opravdu podvod a žádné peníze nezachrání ani nevydělají," dodává Daniel Knápek z SSI Group s tím, že společnost si předsevzala, že vzhledem k míře společenské nebezpečnosti tohoto podvodného jednání na něj bude veřejně upozorňovat.

Podle manažera prevence podvodů Partners Banky Petra Hrůzy zůstává princip podvodu stejný: Vylákat z klienta peníze a přimět ho co nejrychleji je převést pomocí vkladomatu do kryptoměny, případně odeslat do virtuální peněženky nebo na zahraniční účet.

Kontakt pro média

Evelýna Hrůzová
+420 731 466 749
hruzova@know.cz
www.knowcomm.cz

Michaela Němečková
+420 737 318 249
nemeckova@know.cz
www.knowcomm.cz

Podvodné legendy, kterými zločinci své oběti přesvědčují, se rychle vyvíjí a precizují. Mají ale společný základ. *„Volající, většinou s východním akcentem, kontaktuje oběť s tím, že dotyčný má někde investovány peníze, které se vysoce zúročily a je třeba je vybrat. To podmíní poplatkem, který se jim má i s údajným výdělkem zpětně vrátit. Nejen, že podvodník takto vyláká z obětí peníze, ale mnohdy také citlivé přístupové údaje a může dále zneužívat jejich bankovní identitu,"* dodává Hrůza s tím, že výjimkou nejsou ani lidé, kteří podlehli nátlaku podvodníků opakovaně.

Policie i banky přitom před tímto nebezpečím intenzivně varují už od roku 2020. *„Co výrazně zvyšuje úspěšnost pachatelů je fakt, že pachatel již před započetím telefonátu zná o oběti velké množství citlivých informací, které mohou pocházet z různých uniklých databází. Pachatelé se vydávají nejen za pracovníky bank, ale například i za policisty, pracovníky OAMP a NÚKIBu,"* upozornil mluvčí policejního prezidia Jakub Vinčálek.

Podrobnou statistiku těchto podvodů policie podle Vinčákla nevede. Česká bankovní asociace ale souhrnně sleduje škody způsobené kyberpodvody. Loni podle této statistiky zaznamenaly banky 69 685 napadených klientů s celkovou škodou 1,35 miliardy korun. Průměrná výše škody na jednoho klienta tak dosáhla 19 357 Kč.

Kontakt pro média
Evelýna Hrůzová
+420 731 466 749
hruzova@know.cz
www.knowcomm.cz

Michaela Němečková
+420 737 318 249
nemeckova@know.cz
www.knowcomm.cz