

Podvodník byl přesvědčivý

3.1.2024 - Štěpánka Schwarzová | Policie ČR

Důvěřivý muž přišel vložením peněz do bitcoinmatu o více než 700 000 korun.

Velmi přesvědčivý byl neznámý pachatel, který v druhé polovině prosince telefonicky kontaktoval muže z Táborska s tím, že se představil jako pracovník jedné banky a poškozeného se dotazoval, zda souhlasí s podmínkami úvěru, o který si zažádal osobně v bance. Poškozený však o žádný úvěr nežádal a hovor ukončil. Následně mu zavolala jemu neznámá žena z jiného telefonního čísla, která mu sdělila, že je z bezpečnostního oddělení banky s tím, že pokud chce zabránit tomu, aby si na něj někdo vzal neoprávněně úvěr, tak si musí nainstalovat aplikaci Viber do mobilního telefonu pro další zabezpečenou komunikaci, což muž v obavě o své peníze učinil. Zároveň mu na jeho email přišel falešný email, ve kterém ho jeho banka informovala o tom, že mu chce někdo zpronevěřit osobní údaje a zneužít přístup do jeho účtu. Další falešný email přišel od policie, ve kterém obdržel muž propustku z práce z důvodu občanské povinnosti. Pak už veškrá komunikace probíhala přes Viber, kde dostal muž instrukce o tom, že musí dojet do své banky v Českých Budějovicích, ze které má vybrat více než 250 000 korun a následně je má vložit do bitcoinmatu pomocí zasláných QR kódů. Toto muž udělal. Další den ho neznámý pachatel poslal do pobočky banky v Táboře, kde opět vybral peníze, tentokrát více než 400 000 korun a tyto opět vložil do bitcoinmatu. Následně s mužem přestal pachatel komunikovat. Ten tak přišel o více než 700 000 korun.

Případem se intenzivně zabývají policisté z obvodního oddělení v Sezimově Ústí, kteří po pachateli trestného činu podvodu pátrají. Zároveň upozorňují na neustále se opakující případy internetových podvodů. Je potřeba být maximálně obezřetní. Podvodníci se snaží využít strach poškozených o své finanční prostředky, kdy je přesvědčí o tom, že je potřeba peníze "bezpečně" uložit v bitcoinmatu. Dávejte vždy pozor např. na emailové adresy, ze kterých s vámi pachatel komunikuje, většinou obsahují písmena či znaky navíc a je možné podle toho poznat, že jsou falešené. V tomto případě to např. bylo: info@csob.**gs**.cz. Pokud máte jakékoliv pochybnosti, kontaktujte infolinku vaší banky či přímo vašeho bankéře, kteří vám potvrdí vaši domněnku, že se skutečně jedná o podvodné jednání. Nedávejte podvodníkům šanci, hlídejte si své peníze.

<https://www.policie.cz/clanek/podvodnik-byl-presvedcivy.aspx>