

DALŠÍ METODY PODVODNĚKŮ

Stáda, 05 květen 2021

Kriminalisté desítky padě se škodami v řádu milionů korun. Policie České republiky v poslední době zaznamenala vzrůstající aktivitu skupiny osob, která využívá jednu z metod sociálního inženýrství a to takzvaný vishing. Jedná se o princip, který je založen na telefonních hovorech, kdy se volající (podvodníci) zpravidla představují jako pracovníci banky, kteří zjistili napadení vašeho bankovního účtu.

Tito domnívají pracovníci banky svými tvrzeními vystrašit osobu, která volá, pomocí jejich hlavní cíl je získat její peníze. Sdělení, že je nutné, aby finanční prostředky byly z vlastního účtu okamžitě převedeny na jiný účet s tím, že budou vyčleněny celkově v rámci následných vrátcení, což se samozřejmě nestane. Podvodníci tímto způsobem mohou vyvést i další citlivé údaje, které následně zneužijí.

Tento typ podvodu je nebezpečný zejména v tom, že falešně pracovníci bank mohou již před hovorem nejenom získat informace o osobách, které kontaktují, ale hlavně před hovorem u vás tak zvaný spoofing telefonního čísla, pomocí kterého dokážete napodobit jakkoliv telefonní číslo infolinek bank. Rovněž bylo zaznamenáno několik padě, pomocí kterých telefonicky kontaktují osoby, které vystupují jako policisté, s cílem ujistit o pravdivosti tvrzení ohledně napadení bankovního účtu a nutnosti provedení bankovního účtu dle předchozích instrukcí domnívají pracovníci bank.

Obecná zásady

Nereagujte na podobné hovory a v žádném případě nesdělujte k vašim osobním údajům citlivé údaje ani bezpečnostní údaje z vašich platebních karet, nebo předstoupit online bankovníctví. Nikdy nikomu nesdělujte a ani neposílejte bezpečnostní / autorizační kód, který vám předloží formou SMS zprávy. Myslete na to, že to někdo dokáže napodobit jakákoliv telefonní číslo, odesílatele SMS zprávy, ale třeba i e-mailovou adresu. Nikdy nikomu podezřelému neumožňujte vzdáleně do vašeho počítače. Sledujte a pečlivě tyto informace od vašich banky v internetovém bankovníctví. Před každým vstupem do internetového bankovníctví kontrolujte, zda odpověď domněna předloží strážníci. Toto platí vždy, kdy někdo kam zadává své osobní nebo předloží údaje. Aktualizovat software, antivirový program, firewall. Buďte neustále ostraženi proto že i vy se můžete stát cílem podobného podvodu jedním z nich. Buďte, nebo po takovémto podezřelém hovoru, si zaznamenejte údaje, které vám někdo sdělí (jména, e-mailové adresy, čísla účtů, odkazy na webovou stránku, apod.)

Nereagujte

na telefonní hovory, SMS zprávy, e-maily, kde se vás někdo pokouší vmanipulovat do situace, kde jsou vaše finanční prostředky v ohrožení a vy musíte udělat další kroky pro jejich ochranu. Kdyby byly vaše peníze v ohrožení, tak banka sama zareaguje a udělá další opatření. V případě pochybností vždy kontaktujte svou banku. Pokud vás shora naznačeným způsobem někdo kontaktoval, nehejte se rovněž obrátit na telefonní linku Policie České republiky na čísle 158 a celou zjevnost oznamte.

Zdroj: plk. Ondřej Moravský

tisková mluvčí, Policejní prezidium
ČER