Současné trendy podvodníků - vishing a spoofing !!!!!

Kriminalisté řeší desítky případů se škodami v řádu milionů korun.

Policie České republiky v posledních týdnech zaznamenala vzrůstající aktivitu skupiny osob, které využívají jednu z metod sociálního inženýrství a to takzvaný Vishing. Jedná se o princip, který je založený na telefonních hovorech, kdy se v tomto případě osoby volajících zpravidla představují jako pracovníci banky, kteří zjistili napadení bankovního účtu. Tito domnělí pracovníci banky svými tvrzeními vystraší osobu, které volají, přičemž jejich hlavním cílem je získat její peníze. Sdělí, že je nutné, aby finanční prostředky byly z vlastního účtu okamžitě převedeny na jiný účet s tím, že budou po vyřešení celé věci následně vráceny, což se samozřejmě nestane. Uvedené osoby tímto způsobem mohou vylákat i další citlivé údaje, které následně zneužijí. Tento typ podvodného jednání je nebezpečný zejména v tom, že falešní pracovníci bank mohou již před hovorem nejenom znát různé informace o osobách, které kontaktují, ale hlavně při hovorech užívají tak zvaný spoofing telefonního čísla, při kterém dokážou napodobit jakékoliv telefonní číslo, včetně infolinek bank. Rovněž bylo zaznamenáno několik případů, při kterých telefonicky kontaktují další osoby, které vystupují jako policisté, s cílem ujistit o pravdivosti tvrzení ohledně napadení bankovního účtu a nutnosti převodu peněz na „bezpečný" bankovní účet dle předchozích instrukcí domnělých pracovníků bank.

Obecné zásady:

- Nereagujte na podobné hovory a v žádném případě nesdělujte k Vaší osobě žádné citlivé údaje ani bezpečnostní údaje z vaší platební karty, nebo přístupové údaje k online bankovnictví.
- Nikdy nikomu nesdělujte a ani nepřeposílejte bezpečnostní / autorizační kód, který Vám přišel formou SMS zprávy.
- Myslete na to, že útočník dokáže napodobit jakékoliv telefonní číslo, odesílatele SMS zprávy, ale třeba i e-mailovou adresu.
- Nikdy nikomu podezřelému neumožňujte vzdálený přístup do Vašeho počítače.
- Sledujte a pečlivě čtěte informace od Vaší banky v internetovém bankovnictví.
- Při každém vstupu do internetového bankovnictví kontrolujte, zda odpovídá doména přihlašovací stránky. Toto platí vždy, když někam zadáváte své osobní nebo přihlašovací údaje.
- Aktualizovat software, antivirový program, firewall.

- Buďte neustále ostražití, protože i vy se můžete stát cílem podobného podvodného jednání.
- Během, nebo po takovémto podezřelém hovoru, si zaznamenejte údaje, které Vám útočník sdělil (jména, e-mailové adresy, čísla účtů, odkazy na webové stránky, apod.)

Policie ČR varuje:

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

plk. Ondřej Moravčík
tiskový mluvčí, Policejní prezidium ČR
23. dubna 2021