

Nový typ podvodného navolávání - Kombinace smishingu a vishingu

19.10.2023 - Veronika Hyšplerová | Policie ČR

Může se to stát každému, proto je potřeba být obezřetný.

I přesto, že jsme včera prostřednictvím sociálních sítí varovali před nejnovějším a nejpropracovanějším způsobem podvodného jednání, tak již ústečtí policisté evidují jeden případ.

O co vlastně jde?

Nejprve vám přijde SMS zpráva ohledně státního příspěvku. Kliknutím na odkaz a následném vyplnění citlivých přihlašovacích údajů na podvodném webu, umožníte pachateli přístup do vašeho bankovníctví, což mu samotní nevědomky potvrdíte. Pachatel následně zadá transakci na připravený bankovní účet a čeká, zda mu to v rámci manipulace odsouhlasíte v rámci více faktorového ověření. V případě, že odsouhlasíte, tak jsou z vašeho účtu okamžitě odcizeny finanční prostředky. V případě, že transakci nepotvrdíte, tak vám obratem volá pachatel, který se vydává za pracovníka vaší banky s tím, že máte napadený účet a musíte okamžitě všechny své peníze převést na „bezpečný“ účet, který vám nadiktuje. Tím, že má pachatel přístup do vašeho bankovníctví, tak zná i citlivé informace o vaší osobě, včetně zůstatku na účtu a faktu, že jste reagovali na podvodnou SMS zprávu.

Náš 27letý poškozený vyplnil všechny formuláře, potvrdil nespecifikovanou platbu ve výši 4.990 korun, která místo, aby mu byla připsána, coby „státní příspěvek“, tak mu byla odčerpána. Následně jej kontaktoval údajný pracovník banky s tím, že jeho účet byl napaden a že je potřeba následovat všechny jeho instrukce. Bohužel poškozený ze strachu z toho, že přijde o své finance tak veškeré instrukce splnil a ve čtyřech platbách přišel o 102.498 korun. Ve výsledku o 107 498 korun.

Banky takto nikdy nepostupují. Ministerstvo práce nikdy takového SMS zprávy s odkazem neposílá. Celé je to podvod. V případě podezření na napadení vašeho účtu okamžitě kontaktujte svou banku.

<https://www.policie.cz/clanek/novy-typ-podvodneho-navolavani-kombinace-smishingu-a-vishingu.aspx>