Zdařilý pokus o podvod. Kyberšmejdi zneužívají autentické formuláře pojišťovny

8.4.2026 - Viktorie Plívová | Všeobecná zdravotní pojišťovna ČR

Vidina vráceného přeplatku na zdravotním pojištění může důvěřivce přijít draho. Podvodníci se v nové vlně e-mailů odvolávají na roční vyúčtování a lákají na vyplacení loňských přeplatků. Věrně přitom napodobují webové formuláře skutečně používané Všeobecnou zdravotní pojišťovnou. Příjemce je formálním oslovením vyzván k vyplnění údajů na přiloženém odkazu.

Podobu rozesílaných průvodních e-mailů i dotyčného formuláře najdete níže a video s podobou podvodu ke shlédnutí.

„Průvodní e-mail, který příjemce obdrží, i následný formulář vypadají velmi autenticky. Vizuálem i dalšími prvky působí důvěryhodně. Celým procesem vede příjemce k vyplnění bankovních údajů, samozřejmě opět pouze po přístupu k jeho účtu. Podvodníci tentokrát odkazují na domnělé roční vyúčtování a vzniklý přeplatek,“ říká **Jan Svoboda**, ředitel Odboru bezpečnosti VZP, a nabádá k obezřetnosti: *„VZP tímto způsobem přeplatky nevrací, po klientech přihlášení k bankovním účtům nikdy nevyžaduje. Opět zdůrazňuji, že každý, kdo takový e-mail obdrží, by neměl na nic klikat, a pokud to ze zvědavosti udělá, rozhodně by neměl nic vyplňovat. Vystavuje se vysokému riziku, že přijde o peníze z účtu, jako se tomu již v řadě případů stalo při podobných útocích kyberšmejdů nejen na klienty zdravotních pojišťoven.“*

Podvodný e-mail je uveden jako „oznámení o evidovaném přeplatku“ ve výši 12 407,50 Kč. Je zde i informace, že peníze jsou připravené k výplatě, a nechybí číslo jednací, pod nímž se údajný přeplatek eviduje, či datum vyhotovení.

„V posledních dnech rozesílané e-maily s údajným přeplatkem jsou velmi zdařilé a mimořádně uvěřitelné. Klienti by měli vždy bedlivě sledovat, zda jsou skutečně na webové stránce VZP, a také věnovat pozornost e-mailovým adresám, ze kterých zprávy dostávají. E-maily přicházejí z různých na první pohled nedůvěryhodných adres, například „nico.azedo-estradas@schueler-bkvie.de“, formuláře se následně otvírají například na webu „waha-audit.ps“. Už z toho je patrné, že se jedná o podvod,“ doplňuje **Jan Svoboda**. Jediná oficiální doména pro komunikaci s VZP ČR je **vzp.cz**.

VZP na zneužívání svého jména kyberšmejdy upozorňuje opakovaně. I na začátku letošního roku to byly e-maily slibující fiktivní přeplatek. V únoru se pak jednalo o profesionální náboráře, kteří se vydávali za pracovníky VZP. Dříve podvodné e-maily o údajném dluhu na pojistném či zapojení do falešného průzkumu, kdy měla být odměnou lékárnička v hodnotě 4000 Kč. Více informací k jednotlivým incidentům i formám podvodů najdete v sekci Podvodné zprávy.

Co dělat, když dostanete podobný e-mail:

- Neotevírejte přílohy ani neklikejte na odkazy
- Nezadávejte žádné osobní ani bankovní údaje; v případě, že jste tak již učinili, neprodleně kontaktujte svou banku a policii!!!
- V případě podezření kontaktujte info@vzp.cz
- Vždy si ověřujte, že jste na **oficiální stránce VZP ČR:** www.vzp.cz
- Upozorněte na tento podvod své okolí, zejména seniory, kteří mohou být častým cílem

Jak se klient dozví, jestli dluží na pojistném nebo má přeplatek:

- Přes aplikaci **Moje VZP**
- **Osobně** na pobočce VZP

Viktorie Plívová
tisková mluvčí

https://www.vzp.cz/o-nas/aktuality/zdarily-pokus-o-podvod-kybersmejdi-zneuzivaji-autenticke-formulare-pojistovny