

VAROVÁNÍ: Podvodné SMS a weby se vydávají za ČSSZ

7.3.2025 - | Česká správa sociálního zabezpečení

Smishing je forma útoku, kdy je na telefonní číslo zaslána SMS zpráva obsahující odkaz na podvodnou webovou stránku, která se tváří jako oficiální web.

Snaží se občany přimět, aby zde zadali a vyplnili své citlivé osobní údaje (přihlašovací ID, heslo, mobilní klíč apod.) včetně údajů o bankovních kartách (celé číslo karty, datum platnosti, kód CVC, kód 3D Secure atd.). Ve skutečnosti se nejedná o oficiální web ČSSZ, ale o podvod.

ČSSZ TENTO TYP SMS ZPRÁV NEROZESÍLÁ.

ČSSZ VÁS NIKDY NEVYZVE V SMS KE SDÍLENÍ PŘIHLAŠOVACÍCH ANI PLATEBNÍCH ÚDAJŮ PRO VÁŠ ÚČET A KARTU.

NA TAKOVÉ SMS ZPRÁVY NIKDY NEREAGUJTE.

TAKOVÉ WEBOVÉ ODKAZY NIKDY NEOTVÍREJTE.

Součástí podvodné SMS může být také jméno majitele telefonu. V případě, že jste již zadali své bankovní údaje, kontaktujte neprodleně svou banku. Podezřelé domény jsou postupně blokovány, přesto stále vznikají jejich nové formy. Proto ČSSZ varuje a důrazně vyzývá občany, aby veškeré stránky ověřovali a nevyplňovali své údaje, pokud si nejsou stoprocentně jisti původem stránky.

Jediné oficiální stránky ČSSZ jsou www.cssz.cz a eportal.cssz.cz, jejichž bezpečnost garantuje digitální pečeť společnosti DigiCert umístěná na webové stránce vpravo dole. Po kliknutí na pečeť se zobrazí identifikační údaje ČSSZ a návštěvník stránek snadno zjistí všechny informace o majiteli webu.

SMS nejsou realizovány na základě uniklých údajů ČSSZ. Podvodníci oslovují občany na jejich telefonní číslo bez ohledu na to, zda majitel telefonního čísla pobírá, nebo nepobírá dávky sociálního zabezpečení.

Nedávno jsme varovali také před podvodnými telefonáty.

https://www.cssz.cz/web/cz/uvod/-/asset_publisher/GQ48v1KeNe0J/content/id/2915174