

Pozor na podvodné SMS od ZSE Drive.

Falošná faktúra vás môže pripraviť o peniaze

Datum 23.9.2026
Subjekt Zajtra studio spol. s r.o.
Autor Lenka Ivančíková
Region Slowakei
Kategorie IT und Kommunikation

Spoločnosť ZSE Drive upozorňuje svojich zákazníkov na podvodné SMS správy, ktoré sa vydávajú za výzvu na zaplatenie faktúry. Podvodníci sa snažia príjemcov presvedčiť, aby klikli na priložený odkaz a uhradili údajný nedoplatok.

Namiesto oficiálnej stránky služby sa však môžu dostať na **podvodný web**, ktorý **napodobňuje vzhľad ZSE Drive**. Cieľom takéhoto podvodu je získať citlivé údaje zákazníkov vrátane prihlasovacích informácií či údajov o platobnej karte.

Ako rozpoznať podvodnú SMS?

Falošná správa má niekoľko charakteristických znakov. Nemusí obsahovať identifikáciu odosielateľa a príjemcu vyzýva na zaplatenie faktúry prostredníctvom priloženého odkazu. Ten smeruje na podozrivú internetovú stránku, ktorá sa môže na prvý pohľad podobať oficiálnemu webu ZSE Drive.

Zdroj: email

Po otvorení stránky môže byť používateľ vyzvaný na zadanie osobných údajov, prihlasovacích informácií alebo údajov o platobnej karte. Práve v tomto momente hrozí, že sa citlivé informácie dostanú do rúk podvodníkov.

ZSE Drive preto odporúča na odkazy v podozrivých SMS správach vôbec neklikať. Ak si chcete overiť, či máte neuhradenú faktúru, využite výhradne oficiálne komunikačné kanály služby.

Čo robiť, ak ste už na odkaz klikli?

Samotné otvorenie odkazu ešte nemusí znamenať, že ste prišli o peniaze. Ak ste však na podvodnej stránke zadali prihlasovacie alebo platobné údaje, je potrebné konať čo najrýchlejšie.

Bezodkladne kontaktujte svoju banku a postupujte podľa jej pokynov. V prípade zadania údajov o platobnej karte môže byť potrebné kartu zablokovať. Ak ste prezradili aj prihlasovacie údaje, zmeňte si heslo k príslušnému účtu.

Mohlo by vás zaujímať:

- Xiaomi vydalo septembrovú bezpečnostnú aktualizáciu. Opravuje až 180 chýb
- OpenAI predstavilo nové AI modely GPT-6 Sol a Luna. Sú presnejšie a lacnejšie
- Používate lacné smart okuliare? Dajú ovládnuť cez Bluetooth a útočník sa dostane k fotkám

Podozrivú SMS následne vymažte a na prípadné ďalšie správy nereagujte. Podvodníci často zneužívajú názvy známych spoločností, aby ich správy pôsobili dôveryhodne. Podobné výzvy na zaplatenie faktúr preto vždy overujte priamo u poskytovateľa služby, nie prostredníctvom odkazu doručeného v SMS.

<https://www.mojandroid.sk/pozor-na-podvodne-sms-od-zse-drive>