

Obsežen kibernetiski napad z lažnimi SMS sporočili

V zadnjih dneh je večje število imetnikov mobilnih telefonskih števil prejel lažna kratka SMS in iMessage sporočila, s katerimi poskušajo prevaranti od prejemnikov izvabiti podatke o plačilnih karticah.

Kako prepoznati to prevaro?

Pošiljatelj trdi, da je prejemnik sporočila storil prometni prekršek, in zahteva takojšnje plačilo izrečene globe preko priložene spletne povezave.

Ker mnogi prejemniki sporočil pomislijo, da se obvestilo nanaša na prekršek glede vožnje po avtocesti ali hitri cesti brez veljavne e-vinjete/povezan z uporabo naprave DarsGo, poudarjamo, da **uradne državne institucije od občanov nikoli ne zahtevajo plačila glob preko SMS povezav. Tudi Dars d.d. od cestninskih zavezancev nikoli ne zahteva vnosa podatkov o plačilnih karticah, gesel ali osebnih podatkov preko SMS ali iMessage sporočil.**

Napadalci izkoriščajo preizkušeno taktiko ustrahovanja in lažnega občutka nujnosti. Prevaro lahko prepoznate tudi po tem, da je bilo sporočilo poslano z neznane tuje telefonske številke s tujo klicno kodo.

Kaj se zgodi, če kliknete na povezavo?

Cilj napadalcev je pridobiti podatke o vaši plačilni kartici, ki jih napadalci nato takoj uporabijo za izvajanje spletnih nakupov v višjih zneskih.

Celotna prevara poteka v več korakih:

1. **Lažna spletna stran:** povezava vas usmeri na zlonamerno spletno stran, ki vizualno posnema uradne grafične podobe državnih organov.
2. **Navidezno preverjanje podatkov:** spletna stran najprej zahteva vnos registrske označbe vozila. Ker gre za avtomatizirano prevaro, sistem sprejme kakršnokoli kombinacijo znakov.
3. **Zahteva za vpis podatkov o kartici:** v naslednjem koraku sistem prikaže znesek domnevne kazni (npr. 39 €) in zahteva vnos vseh podatkov z vaše plačilne kartice za izvedbo plačila.
4. **Zloraba računa:** takoj ko podatke vnesete, jih napadalci prestrežejo in zlorabijo za izvajanje nakupov v višjih zneskih na različnih spletnih straneh.

Kako pravilno ukrepati?

Za preprečitev zlorab dosledno upoštevajte naslednja varnostna priporočila:

- **ne odpirajte povezav:** če prejmete sumljivo sporočilo, ne odpirajte povezav in ne sledite navodilom.
- **Ne vpisujte svojih podatkov:** nikoli ne vnašajte osebnih podatkov ali podatkov o plačilnih karticah na spletna mesta, do katerih ste dostopali preko SMS sporočil.
- **Izbrišite zlonamerno sporočilo:** prejeto sporočilo takoj izbrišite ali ga v telefonu označite kot neželeno pošto (spam).
- **Če ste podatke o bančni kartici že vnesli, nemudoma ukrepajte.** Takoj kontaktirajte svojo banko (številka je na hrbtni strani bančne kartice) in sledite njihovim navodilom.

Potrebuje pomoč ali ste v dvomu?

Če ste v imenu Darsa prejeli sumljivo sporočilo in niste prepričani o njegovi verodostojnosti, se nemudoma obrnite na naš klicni center za cestninjenje na telefonsko številko 01 518 8 350 ali nam pišite na evinjeta@dars.si.