DNSC: Continua frauda prin SMS, în care hackerii informeaza utilizatorii ca au de platit taxe sau amenzi restante

Directoratul National de Securitate Cibernetica (DNSC) avertizeaza asupra continuarii campaniei frauduloase, cu mesaje SMS, prin care infractorii încearca sa convinga utilizatorii ca au de achitat amenzi sau taxe restante.

"Atacatorii transmit SMS-uri care informeaza despre o presupusa amenda sau o plata restanta si încearca sa determine destinatarii sa acceseze un link pentru "achitare" sau "verificarea detaliilor". Mesajele folosesc un ton urgent si invoca penalitati, taxe suplimentare sau alte consecinte pentru a crea presiune", a transmis institutia, într-o postare publicata marti pe pagina sa de Facebook.

Potrivit expertilor, utilizatorii trebuie sa tina cont de anumite semne de alarma, atunci când primesc SMS-uri: solicitarea de a accesa un link primit prin SMS pentru efectuarea platii; domenii web care imita platforme oficiale, dar cu adrese diferite; mesaje care creeaza panica prin termene-limita foarte scurte sau consecinte severe.

În acest context, recomandarile specialistilor DNSC fac referire la neaccesarea linkurilor primite prin SMS sau prin aplicatii de mesagerie, verificarea eventualelor obligatii de plata exclusiv prin platformele si canalele oficiale, accesate prin introducerea manuala a adresei în browser, analizarea cu atentie a adresei site-ului înainte de a introduce date personale sau bancare.

"Daca ati furnizat deja date de card, contactati imediat banca pentru blocarea instrumentului de plata. Ati primit un mesaj asemanator? Raportati catre DNSC pe pnrisc.dnsc.ro si povestiti-ne scenariul prin platforma Siguranta Online - Uniti împotriva escrocheriilor: https://sigurantaonline.ro/uniti-impotriva-escrocheriilor/", noteaza Directoratul.

În acelasi timp, un domeniu de Internet poate fi verificat prin DNSC Blacklist Protection, o extensie gratuita.