Bitdefender a descoperit cea mai mare campanie de înselatorie online din 2026, ce are loc în România

Peste un milion de români au primit, prin SMS, mesaje frauduloase de livrare ce par sa provina de la compania de curierat Fan Courier, avertizeaza specialistii Bitdefender, într-un comunicat de presa .

"Atacatorii trimit SMS-uri care par sa vina de la Fan Courier, liderul pietei locale de curierat, si îi directioneaza pe destinatari catre un site fals prin care hackerii preiau controlul contului de WhatsApp si solicita mai apoi bani cunoscutilor victimei. (...) Peste un milion de oameni au primit aceste mesaje. Campania nu presupune instalarea unei amenintari informatice pe telefon, ci se bazeaza pe manipulare psihologica si pe furtul datelor de acces. Victima primeste un SMS care o informeaza ca un colet este asociat numarului sau de telefon si ca trebuie sa aleaga un locker pentru ridicare. Mesajul arata ca o notificare legitima de livrare, ceea ce face ca multi oameni sa acceseze link-ul fara suspiciuni. Link-ul duce catre un site care copiaza identitatea vizuala FAN Courier, dar care este gazduit pe un domeniu controlat de atacatori. În paralel, hackerii initiaza reînregistrarea numarului de telefon al victimei pe un alt dispozitiv. WhatsApp trimite un cod de verificare real pe telefonul victimei, iar pagina falsa îi solicita sa introduca acel cod, sub pretextul confirmarii livrarii", se mentioneaza în comunicat.

Expertii în securitate cibernetica explica faptul ca dupa preluarea contului victimei, atacatorii contacteaza persoanele din lista victimei si le trimit cereri urgente de bani.

"Mesajele mentioneaza de obicei o urgenta si promit returnarea sumei a doua zi. În unele cazuri, atacatorii cer ca banii sa fie trimisi într-un cont bancar diferit. Exista indicii ca aceste conturi, uneori deschise la banci românesti, apartin unor persoane care au pierdut la rândul lor accesul la conturile bancare în urma altor tipuri de atacuri informatice. Deoarece cererile de bani vin de la un contact de încredere, destinatarii au tendinta sa raspunda fara sa verifice situatia. Aceasta a doua faza a atacului este cea care genereaza câstigul financiar pentru atacatori. Exista mai multe semnale de alarma: domenii suspecte care nu corespund site-ului oficial FAN Courier, mesaje trimise de la numere de telefon aleatorii si, cel mai important, cererea de a introduce un cod de confirmare WhatsApp. Niciun serviciu de curierat legitim nu va solicita vreodata un astfel cod de verificare", noteaza compania.

În context, specialistii recomanda sa nu accesati link-uri de curierat primite prin SMS-uri neasteptate, sa introduceti manual adresa oficiala a curierului în browser, sa nu introduceti niciodata coduri de verificare WhatsApp în afara aplicatiei WhatsApp, sa activati verificarea în doi pasi în WhatsApp, sa verificati telefonic cu persoana care solicita banii orice cerere urgenta primita pe platforma de mesagerie si sa folositi aplicatia oficiala a companiei de curierat pentru a verifica statusul livrarii coletelor si a întreprinde alte operatiuni.