DNSC: Patru din zece incidente cibernetice, raportate în primul semestru, reprezinta fraude prin telefon

Mai mult de patru din zece incidente (42%), raportate în prima jumatate a anului 2026, sunt înselatorii telefonice (vishing), arata o statistica a Directoratului National de Securitate Cibernetica (DNSC), prezentata recent în cadrul unui eveniment de specialitate.

Datele dezvaluite în cadrul ING Safe Talks releva faptul ca, în primele sase luni din acest an, fraudele de tip vishing sunt urmate de cele phishing (14%) si de cele prin SMS (smishing), cu 13% din total.

Potrivit unui comunicat de presa al DNSC, transmis miercuri AGERPRES, în intervalul analizat, la nivelul tuturor structurilor de investigatii criminale din cadrul Politiei Române (care au în competenta investigarea infractiunilor informatice si împotriva sistemelor informatice) au fost înregistrate aproximativ 15.000 de dosare penale.

La finalul lunii iunie, la nivel national, ramasesera în curs de solutionare aproximativ 72.000 de dosare, dupa ce, la 1 ianuarie 2026, existau înregistrate 67.000 de dosare, conform reprezentantilor Directiei de Investigatii Criminale, Politia Româna.

"Metodele folosite de atacatori nu sunt neaparat noi, însa tehnologia pe care o folosesc a evoluat semnificativ, inclusiv prin utilizarea instrumentelor de inteligenta artificiala. În acelasi timp, acestia stapânesc din ce în ce mai bine tehnici de inginerie sociala, prin care conving oamenii sa le ofere date, sa le trimita bani sau sa instaleze aplicatii malitioase. În continuare, noi ca utilizatori trebuie sa fim atenti la trei elemente pe care le putem identifica în fiecare tentativa de frauda - emotia, urgenta, urmata de solicitarea de date. Initiative precum cea de astazi, în care, DNSC, ING, Politia Româna, societatea civila si presa din România discuta împreuna despre cele mai recente scenarii si povesti folosite în tentativele de frauda, sunt esentiale - preventia ramâne la fel de importanta ca reactia în fata atacurilor cibernetice", a declarat Mihai Rotariu, manager Directia Comunicare, Marketing si Media, din cadrul DNSC.

În cadrul evenimentului de specialitate a fost lansat si primul studiu national privind fraudele financiare online în rândul persoanelor de peste 50 de ani, din care a reiesit faptul ca sase din zece persoane din aceasta categorie spun ca au experimentat cel putin un tip de frauda cibernetica, în timp ce doar 37% declara ca nu s-au confruntat niciodata cu o astfel de situatie.

Totodata, persoanele în vârsta cunosc, în medie, sapte dintre cele 13 tipuri de fraude analizate în studiu: 66% dintre respondenti spun ca au auzit de mesajele sau apelurile false care par sa provina de la banca sau alte institutii (spoofing si metode de impersonare), acestea fiind cea mai cunoscuta metoda de frauda.

De asemenea, phising-ul, adica trimiterea linkurilor frauduloase catre site-uri false care imita platforme oficiale, ocupa pozitia a doua (63%), iar la mica distanta se afla ofertele pentru produse sau servicii la preturi nerealist de mici si mesajele sau e-mailurile care solicita parole, date personale ori actualizarea contului (61%).

În acelasi timp, peste jumatate dintre respondenti spun ca au auzit de cererile de bani primite prin WhatsApp, Facebook sau TikTok (57%), precum si de investitiile false si promisiunile financiare nerealiste (56%).

Conform cercetarii, majoritatea persoanelor de peste 50 de ani aleg sa reactioneze atunci când se confrunta cu o tentativa de frauda. Astfel, sapte din zece respondenti (69%) au apelat la Politie sau alte autoritati, 47% au blocat contactul de la care au primit mesajul, 36% au verificat informatiile înainte de a reactiona, iar unul din cinci (19%) a ales sa ignore mesajul. Doar 11% dintre respondenti recunosc ca au accesat linkul primit, iar un procent similar a

contactat banca pentru verificari.

În acest context, specialistii DNSC recomanda utilizatorilor sa nu acceseze niciodata linkuri sau atasamente provenite din surse necunoscute, sa nu instaleze aplicatii la solicitarea unor presupusi agenti de investitii, prin care sa le oferiti control la dispozitivul utilizat, la telefonul mobil sau computer, sa contacteze banca în cazul în care este nevoie de ajutor în efectuarea unei operatiuni, sa se asigure ca nu se afla pe un site-clona, care arata similar cu cel oficial.

În plus, nu este indicata autentificarea în aplicatia de internet banking folosind un link primit pe SMS sau e-mail, dar nici accesarea de linkuri promovate.

DNSC precizeaza ca pentru a recunoaste tentativele de frauda online si a nu le cadea victima, utilizatorii pot accesa surse de încredere precum site-ul DNSC, sectiunea de securitate de pe site-ul ING Bank si site-ul sigurantaonline.ro.