

Intensificarea numărului și a metodelor de fraude cibernetice în perioade de incertitudine. Care sunt pașii de urmat în cazul în care ați fost victima noilor atacuri de tip smishing



Departamentul de White Collar Crime al casei de avocatura Mușat & Asociații, cu o vasta expertiza în domeniul cybersecurity, respectiv în oferirea de asistență și reprezentare juridică în cauze complexe privind fraudele cibernetice, informează clienții săi și publicul interesat despre o nouă modalitate de smishing (phishing prin intermediul mesageriei telefoanelor mobile) apărută recent în spațiul virtual, prin care faptuitorii vizează compromiterea unor conturi pe platforme de mesagerie și telefonie (de ex. Whatsapp) pentru a clona aceste conturi și a savârși prin intermediul lor diferite infracțiuni.

Prin urmare, aducem în atenția publicului anumite aspecte privind noile metode de atacuri cibernetice apărute recent.

În prezent, se derulează o nouă campanie de smishing (o formă de phishing care utilizează drept platforma de atac telefoanele mobile), care presupune transmiterea către utilizatori a unui mesaj pe Whatsapp prin care se solicită votarea unei anumite persoane în scopul de a câștiga un anumit premiu. Un exemplu de mesaj este: „Te rog să o susții pe Ana, verișoara mea, la concursul școlii ei! Poate câștiga un an de școlarizare gratuită, iar un vot din partea ta ar conta enorm. Mulțumesc mult! (link)”.

În realitate, ca urmare a accesării link-ului respectiv și a finalizării „votului”, utilizatorul oferă acces la contul său de Whatsapp faptuitorilor, care îl folosesc ulterior pentru a compromite alte conturi sau pentru a solicita sume de bani.

Acesta este doar un exemplu recent al campaniilor de smishing folosite în practică, existând și alte metode care sunt în continuare actuale, precum metoda accidentului, fraudă de tip 1800 și schema plată pentru click (sau plată pentru like-uri pe anumite platforme).

Aceste metode de fraudă, indiferent de tipul lor, se intensifică, de regulă, în perioade de incertitudine economică, politică și socială, în prezent aceste atacuri fiind îndreptate atât împotriva marilor corporații, cât și împotriva persoanelor vulnerabile, respectiv persoane în vârstă, din medii defavorizate sau care nu dețin cunoștințe tehnice.

Casa de avocatura *Mușat & Asociații* are o vastă experiență în asistarea clienților, societăți și persoane fizice în diverse tipuri de fraude, spre exemplu: (i) cea mai mare fraudă de tip „CEO Fraud” din România; (ii) atacuri cibernetice privind perturbarea unor platforme online de streaming video; (iii) fraude împotriva persoanelor fizice prin furt de cryptomonede din portofelele electronice; (iv) compromiterea datelor conturilor și a cardurilor bancare; (v) plata unor taxe inexistente în vederea ridicării unor premii substanțiale, precum și altele asemenea.

În cazul unor astfel de atacuri cibernetice, ar trebui urmați o serie de pași în vederea înlăturării sau diminuării efectelor negative generate de atacatori.

Daca fraudatorii reușesc să intre în posesia datelor conturilor bancare sau a datelor de card, primul pas ar fi contactarea unității bancare pentru blocarea conturilor și a cardurilor compromise, precum și luarea tuturor măsurilor de conservare a sumelor de bani aflate în conturi și anularea potențialelor tranzacții efectuate ca urmare a fraudei informatice.

În cazul fraudei de tip smishing menționate mai sus, dacă utilizatorul mai are acces la contul de Whatsapp, recomandarea este să acceseze secțiunea Settings (Setari/Configurari), să selecteze 'Linked devices' (Dispozitive asociate) și să elimine din lista dispozitivele necunoscute, apoi să activeze autentificarea în doi pași (2FA), dacă nu a făcut-o deja.

În cazul în care utilizatorul nu mai are acces la cont, va fi necesară contactarea Centrului de Ajutor al Whatsapp pentru a parcurge pașii necesari recuperării contului.

Imediat ce accesul la cont a fost recuperat/securizat, este recomandată trimiterea unui mesaj persoanelor care au primit mesaje nesolicitate din partea atacatorilor din contul utilizatorului, pentru a evita ca aceștia să ajungă și ei victime ale respectivei fraude.

În cazul în care sunt înregistrate pagube financiare, este indicată raportarea cât mai rapidă a incidentului atât către organele de urmărire penală, respectiv parchet sau poliție, cât și către DNSC (Directoratul Național de Securitate Cibernetică).

Totodată, considerăm oportună consultarea unor avocați specializați în acest domeniu pentru asistența și îndrumare în vederea înlăturării sau diminuării consecințelor atacurilor cibernetice descrise anterior.

Astfel, Casa de avocatură Mușat & Asociații, prin [Ștefan Diaconescu](#) – Partner și [Florian Negurici](#) – Associate, avocați din cadrul *Departamentului de White Collar-Crime*, specializați în domeniul infracțiunilor informatice, vă sta la dispoziție pentru orice solicitare privind aceste tipuri de atacuri cibernetice.