ING Bank & DNSC: La nivel global, doar 7% dintre victimele fraudelor reușesc sa își recupereze banii. Tentativele de frauda se intensifica în perioada sarbatorilor, iar tehnologia deep fake este tot mai folosita

La nivel internațional, doar 7% dintre victimele fraudelor din mediul online reușesc sa își recupereze banii pierduți, potrivit unui raport realizat de Global Anti Scam Alliance. Aproximativ 60% dintre respondenții acestui raport au declarat ca aceste atacuri le-au provocat un impact emoțional foarte puternic.

Tentativele de frauda cresc exponențial, de pâna la doua sau trei ori, în preajma sarbatorilor de iarna, când utilizatorii fac mai multe cumparaturi online. În acelaşi timp, atacatorii cibernetici au început sa foloseasca tot mai mult tehnologia deep fake, pentru a induce în eroare potențialele victime şi pentru a oferi un grad sporit de încredere informației prezentate.

În acest context, ING Bank România şi Directoratul National pentru Securitate Cibernetica (DNSC) lanseaza un avertisment pentru toți utilizatorii de carduri pentru a fi vigilenți atunci când fac cumparaturi online, vad oferte promoționale pe rețelele sociale sau rezerva o vacanța.

„Frecvent, atacatorii mizeaza pe manipularea victimelor pentru a-şi introduce datele personale şi financiare pe diferite pagini de phishing, nu pe dezvoltarea de soluții software sofisticate care sa le fure datele. Tentativele de frauda apar în toate industriile, așa ca vedem de la oferte promoționale sau vouchere cadou de sarbatori, la scheme false de investiții şi mesaje ce impersoneaza diferite companii sau platforme de rezervare calatorii. În ING, investim permanent în sisteme de monitorizare în timp real pentru a identifica şi preveni cazurile de frauda, precum şi în campanii de conştientizare şi informare a tuturor utilizatorilor de carduri cu privire la noile tipologii de frauda. Mai mult, punem accent pe sprijinirea autorităților în lupta cu criminalitatea prin furnizarea de informații rapide în format digital. ING este prima banca care a intrat în proiectul de schimb de date cu DIICOT şi urmeaza, mai departe, şi DNA şi IGPR.” – **Alin Becheanu, Head of Fraud Monitoring and Prevention, ING Bank România**.

De la falşi ambasadori la deep fake. Ce sunt şi cum pot fi identificate deep fake-urile?

Tehnologia deep fake este utilizata de atacatori pentru manipularea înregistrarilor video, pentru a promova oferte „incredibile” şi oportunitați de investiții sau îmbogațire rapida. De regula, aceştia se folosesc de imaginea unor persoane faimoase, oameni politici, oameni de afaceri şi chiar jurnalişti, pentru a oferi un plus de încredere potențialelor victime. În unele cazuri, materialul pare un reportaj din cadrul ştirilor de televiziune.

„În ultima perioada, pe rețelele sociale, sunt propagate tot mai multe campanii frauduloase în care vedem anunțuri sponsorizate cu un videoclip de tip deep fake. Conturile de social media pot fi nou create și folosite exclusiv în acest scop sau sunt conturi compromise, care au aparținut în trecut altor utilizatori.
Analizați întotdeauna cu atenție conținutul video! Pentru identificarea deep fake-urilor, indicii pot fi: calitatea imaginii este precara, mișcarea gurii nu este naturala atunci când personajul din imagine vorbește, sunetul nu este sincronizat perfect cu mișcarea buzelor, iar cuvintele pot fi pronunțate greșit în limba româna, semn ca atacatorii s-au folosit la varianta audio de o soluție de tip text-to-speech.
Mai mult, daca informațiile prezentate sunt șocante sau deosebit de importante, verificați existența acestora. Daca nicio sursa de încredere nu vorbește despre asta, ar putea însemna ca videoclipul este, de fapt, un deep fake.” – **Mihai Rotariu, coordonator al Direcției Comunicare, Marketing și Media din cadrul DNSC**.

Dark web, un marketplace cu scheme de frauda. Un card de credit poate costa 20 dolari, un profil de social media un dolar.

Dark web-ul, o parte ascunsa a internetului, este un loc unde informațiile furate de la diferite persoane sau organizații sunt comercializate de catre atacatorii cibernetici.

„Pe computer sunt stocate parole și date personale, iar toate aceste informații sunt salvate în browser. Atacatorii reușesc sa captureze aceste informații din browser și le pun la vânzare pe dark web. Prețurile pot varia, în funcție de anumite criterii. Astfel, un card de credit poate costa 25 de dolari, un profil de social media un dolar, în timp ce datele bancare pot costa 1.000 de dolari, iar un pașaport 1.500 de dolari. Oricine are acces la acel dark market poate avea accces la aceste date. Info stealer-ul este cel mai popular tip de malware, este foarte simplu de folosit și captureaza credențialele salvate din browser, inclusiv datele cardurilor.
În ceea ce privește companiile mici și mijlocii, atacatorii le vizeaza pentru atacurile de tip ransomware.
Dark web monitoring este o practica vitala pentru detectarea și prevenirea amenințarilor cibernetice. Prin urmarirea activităților de pe dark web, organizațiile pot lua masuri proactive pentru a preveni furtul de identitate, fraudele financiare și alte riscuri de securitate.” - **George Dragușin, Presales manager, Provision.**

Tranzacțiile bancare sunt automate și nu pot fi anulate. Utilizați cardurile virtuale, pentru un plus de siguranța

Din momentul în care un utilizator confirma o tranzacție, aceasta nu mai poate fi anulata. Potrivit Directivei Europene Privind Serviciile de Plați - PSD2, nu sunt considerate tranzacții frauduloase în cazul în care sunt furnizate datele cardului și plățile sunt aprobate prin autentificare cu doi factori (în aplicația bancara sau prin cod primit pe SMS). În consecința, șansele ca bancile sa recupereze sumele pentru clienții lor sunt aproape nule în astfel de cazuri.

„Pentru un plus de siguranța atunci când efectueaza cumparaturi online sau la POS, utilizatorii își pot deschide un cont secundar, caruia sa îi atașeze un card, preferabil virtual. În Home’Bank, aceștia pot emite un card virtual oricând, de oriunde, fara costuri. Astfel, sunt în control deplin, pentru ca pot decide câți bani vor cheltui, pe care îi transfera din contul principal. Indiferent ce s-ar întâmpla, un fraudator nu va putea niciodata sa cheltuiasca mai mult decât exista pe acel card virtual.” – **Cristian Lia, Cards Tribe Lead, ING Bank România**.

Sfaturi de la ING, DNSC & ProVision pentru securitatea în mediul online, înainte de sarbatori:

1. **Utilizați o parola unica pentru fiecare cont și schimbați parolele în mod regulat.** Folosiți parole puternice, care cuprind litere majuscule și minuscule, numere și simboluri. Reutilizarea aceleiași parole pe mai multe platforme nu este recomandata. Daca un cont este compromis, pot urma și altele. Pentru a gestiona acest lucru, luați în considerare utilizarea unui manager de parole. Aceste instrumente nu doar ca stocheaza parolele în siguranța, dar ajuta și la generarea unor parole puternice, aleatorii, greu de ghicit. În plus, schimbarea regulata a parolelor poate reduce și mai mult riscul accesului neautorizat.

Opțiuni: KeePass (gratuit); 1Password (platit).

2. Utilizați autentificarea cu doi factori (2FA), întrucât adauga un nivel suplimentar de securitate. Implica primirea unui cod pe telefon/ email sau utilizarea unei aplicații de autentificare și introducererea unui cod suplimentar împreuna cu parola. Prin activarea autentificarii cu doi factori, daca un atacator obține parola utilizatorului, ar avea nevoie de aceasta a doua informație pentru a accesa contul acestuia, ceea ce reduce semnificativ riscul accesului neautorizat.

3. Fiți prudenți cu informațiile personale online, în special pe platformele publice. Date personale precum adresa, numarul de telefon sau data nașterii pot fi folosite de catre atacatori pentru furt de identitate sau alte activitați rau intenționate.

4. Nu furnizați detalii bancare pentru oferte care par prea bune pentru a fi adevarate. Abordați întotdeauna astfel de oferte cu scepticism și nu divulgați informații financiare pentru super oferte.

5. Nu permiteți accesul la distanța la telefonul mobil sau computer (prin aplicații de tip AnyDesk, LogMeIn etc), pentru „ajutor" sau „suport" tehnic, întrucât poate expune dispozitivul la malware sau permite accesul neautorizat la datele personale sau bancare.

6. De ce sunt EU cel care primeste acest PONT și nu altcineva? „Experții" nu va vor suna sau contacta pe whatsapp sau rețelele de social media sa împartașeasca secretele unor investiții de mare succes, fara riscuri. Așadar, ignorați mesajele care ofera câștiguri ușoare.

Alaturi de DNSC și ProVision, ING Bank România a organizat o întâlnire informala în care am discutat despre noile tendințe în fraude online și cum ne putem feri de acestea. Au participat: Alin Becheanu - Head of Fraud Monitoring & Prevention și Cristian Lia – Cards Tribe Lead în cadrul ING, Mihai Rotariu - coordonator al Direcției Comunicare, Marketing și Media în cadrul DNSC și - George Dragușin, Presales manager, Provision.