



**INSPECTORATUL DE POLIȚIE JUDEȚEAN
B R A Ș O V
BIROUL DE ANALIZĂ ȘI PREVENIRE A CRIMINALITĂȚII**

ÎNȘELĂCIUNI ÎN MEDIUL ONLINE MODURI DE OPERARE

1. Cumpărarea online a diverselor produse

Acest mod de operare presupune achiziționarea de pe diverse site-uri de profil de bunuri care la livrare nu corespund descrierilor inițiale sau chiar se constată la momentul verificării coletului că sunt înlocuite cu alte produse.

Astfel, pentru livrarea produsului, se solicită depunerea sumei solicitate într-un cont, după care bunul fie nu mai este livrat și presupusul vânzător nu mai poate fi contactat, fie este foarte deteriorat și se refuză înlocuirea acestuia, vânzătorul susținând că este vina cumpărătorului că nu a verificat coletul la livrare, existând posibilitatea ca distrugerea bunului să fie din vina firmei de curierat.

2. Achiziționarea online de pachete turistice în străinătate

Se practică clonarea unor site-uri cu profil turistic, care propun pachete atractive, la prețuri promoționale, cu plata online a unui avans procentual din pachetul turistic achiziționat într-un anumit cont.

După depunerea sumei de bani în contul indicat, operatorul economic nu mai poate fi contactat, contractele nu se mai perfectează, iar recuperarea sumelor de bani depuse cu titlu de avans devine imposibilă.

3. Recrutarea online de personal cu promisiuni de găsire a unui loc de muncă în străinătate și oferirea unui salariu tentant

Anumite site-uri de recrutare online promit găsirea unui job atractiv în străinătate în schimbul unui comision dat unei firme de recrutare de personal. Se furnizează un cont bancar unde se solicită depunerea unei sume de bani, iar ulterior reprezentanții firmei fictive nu mai pot fi contactați.

De obicei, firma nu este înregistrată la Oficiul Registrului Comerțului și nu se întocmesc niciun fel de contracte de intermediere cu clauze de restituire a comisionului plătit (în cazul nerespectării promisiunii găsirii unui loc de muncă), iar banii nu mai pot fi recuperați.

4. Achiziționarea unor autoturisme la un preț avantajos de pe site-uri de comercializare bunuri

Prin acest mod de înșelăciune, presupusul vânzător se prezintă în general drept femeie, ca fiind proprietară a unui autoturism cu vechime de câțiva ani, în stare impecabilă de funcționare, susținând că este plecată la muncă în străinătate, că nu are semnal la telefonul mobil în zona în care se află, și că negocierea se va face exclusiv pe internet.

Presupusul proprietar solicită pe mail depunerea unei sume de bani într-un cont bancar, după care scanarea biletului la ordin și trimiterea acestuia ca dovadă pe o adresă de mail. După ce dovada plății este făcută, urmează să fie predată mașina despre care vânzătorul susține că se află în grija unei cunoștințe în țară, fără a da însă alte detalii.

După depunerea sumei de bani în contul presupusului vânzător, acesta nu mai răspunde mesajelor de pe mail în vederea predării autoturismului și nici suma de bani depusă nu mai poate fi recuperată.

5. Întâlnirile online

Pe unele site-uri cu profil de întâlniri online, anumite persoane care presupun că își caută parteneri ajung să câștige încrederea persoanei vizate (victimă) iar în timp îi expun acesteia faptul că se află într-o situație personală dificilă și solicită diverse sume de bani în numele relației de afecțiune.

Presupusa relație continuă atât timp cât victima depune sumele solicitate în conturile furnizate, iar la primul refuz se întrerupe orice legătură, posibilitatea de recuperare a banilor devine imposibilă.

6. Solicitarea unor sume de bani în numele unor vedete care promovează cazuri sociale

Se clonează profiluri ale unor vedete pe rețele sociale (tip Facebook) care promovează cazuri sociale (familii nevoiașe cu mulți copii, tineri care suferă de boli incurabile și trebuie să strângă o anumită sumă de bani pentru intervenții chirurgicale costisitoare în străinătate) și se solicită depunerea unor sume de bani într-un anumit cont bancar pentru a ajuta persoanele în cauză.

De obicei se recomandă evitarea depunerii oricărei sume de bani cu tilu de donație pentru cazuri sociale care pot fi fictive, în spatele profilului de Facebook putându-se afla altă persoană decât cea presupusă, care își însușește sumele de bani.

7. Frauda infobuisness

Metoda de fraudare presupune achiziționarea de pachete de cursuri, lecții, care stau la baza creării unor afaceri care promit câștiguri rapide online.

Furnizorul acestor pachete de cursuri propune vinderea unor „secrete” prin care, lucrând câteva ore pe zi, câștigi foarte mulți bani.

După depunerea sumelor de bani reprezentând contravaloarea acestor cursuri, materialele sunt trimise , dar nu conțin informațiile deosebite promise, punerea în practică a afacerilor presupune investirea unor mari sume de bani, despre care nu se menționează inițial, iar recuperarea banilor devine imposibilă.

8. Site-uri de tip PTC (paid to click)

Prin acest tip de înșelăciune online, site-ul accesat îți propune o metodă simplă de a face bani, aceea de a vizualiza cât mai multe reclame pentru care ești plătit, sumele crescând dacă faci publice reclamele respective pe conturile proprii de socializare (Facebook, Twitter, Instagram). La final, după ce instrucțiunile sunt respectate, sumele câștigate sunt modice, iar aceste site-uri dispar înainte ca plata să fie efectuată.

9. False proiecte de investiții

Ideea principală a acestui tip de înșelăciune constă în propunerea de a face un depozit bănesc de tip „caritas” (joc piramidal, care a și atras în România în perioada 1992-1994 milioane de deponenți din toată țara care au investit echivalentul a milioane de dolari), cu promisiunea că peste o perioadă de timp câștigul este dublu.

Pentru fidelizarea inverstitorilor, în prima etapă plățile sunt efectuate, dar peste o perioadă de timp plățile sunt sistate iar sumele depuse nu mai pot fi recuperate.

10.Promisiunea unui câștig garantat din asamblarea diverselor obiecte handmade

Pentru munca de asamblare a unor obiecte handmade, unele site-uri de profil promit câștiguri consistente de bani, sub forma unui parteneriat de muncă de tip angajator-prestator. Inițial sunt trimise spre asamblare diverse obiecte persoanelor interesate, apoi obiectele, odată asamblate, sunt primite de presupusul angajator fără niciun cost solicitat, pentru fidelizare.

Pentru continuarea activității și efectuarea plăților promise inițial pe munca de asamblare, se solicită depunerea unei sume de bani într-un cont reprezentând un gaj, în ideea în care există riscul distrugerii obiectelor trimise.

Odată suma de bani depusă, orice colaborare în acest sens sistează, iar sumele rămân nerecuperat. Localizarea firmelor-fantomă se face destul de dificil, neexistând numere de telefon de contact și niciun fel de contract de prestare servicii între părțile implicate

RECOMANDĂRI PREVENTIVE

Pentru a evita ca orice persoană utilizatoare a internetului să fie victima vreunui tip de înșelăciune în mediul online, se recomandă următoarele:

-Nu plătiți în avans bunurile comandate prin internet, mai ales dacă sunt de la persoane necunoscute anterior cumpărării

-Dacă faceți cumpărături online de produse, folosiți un serviciu de curierat cu plata ramburs ce permite deschiderea și verificarea coletului la primire, pentru a putea refuza efectuarea plății în cazul în care bunul nu corespunde descrierilor inițiale

-Plătiți produsul achiziționat pe internet doar după ce v-ați asigurat că ați primit ce ați comandat și nu un alt produs

-Verificați politica de returnare a produsului de la diverși operatori economici și condițiile exacte în care este posibil acest lucru pentru eventualitatea în care nu sunteți mulțumit (perioada de returnare să fie în general de 30 de zile iar procedura să nu impună condiții restrictive, să existe comunicare și disponibilitate în acest sens)

-Încercați să luați informații de la persoane avizate care au mai comandat de pe internet sau au mai beneficiat de servicii cu plata online a cardului bancar, pentru a evita divulgarea datelor personale și însușirea unor sume de bani pe nedrept, respectiv imposibilitatea de recuperare ulterioară a sumelor depuse în diverse conturi bancare

-Manifestați deosebită atenție în cazul în care oferta de cumpărare a unui produs este foarte tentantă, deoarece există posibilitatea ca produsul să nu posedă toate calitățile prezentate sau să fie foarte deteriorat

- În cazul achiziționării unor bunuri costisitoare de tip second hand de pe site-uri de profil, încercați să contactați vânzătorul și să încheiați cu acesta un act care atestă posibilitatea returnării sumei de bani dacă bunul nu corespunde descrierilor

-La plata bunurilor sau ofertelor online (pachete turistice, oferte de investiții de tip caritas, planuri de afaceri, etc) evitați să oferiți detaliile cardului de credit sau debit

-Verificați dacă preluarea datelor se face prin protocol securizat, de exemplu:

- **https:// - protocol securizat**
- **http:// - protocol nesecurizat**

-Evitați persoanele fizice sau operatorii economici care nu afișează date de contact complete (adresă, numere de telefon, CUI) și se rezumă la o simplă adresă de mail, întrucât localizarea ulterioară și recuperarea pagubei este dificilă

- Nu vă încredeți în testimoniale “uimitoare” referitoare la eficiența unui produs sau a unei afaceri promovate online: verificați din alte surse probe solide cu privire la eficiența unui produs sau eficiența unei companii

-Pe internet, accesați direct site-ul de care sunteți interesat, evitați să utilizați link-urile trimise prin email

-Navigați în siguranță pe internet, folosiți antivirus, care protejează calculatorul personal și datele împotriva problemelor cauzate de viruși, malware, spyware

-Actualizați periodic sistemul de operare utilizat de calculator, laptop sau smartphone prin care accesați internetul și serviciul de internet banking (prin actualizări, producătorul de sisteme de operare remediază continuu vulnerabilitățile care apar)

-Nu instalați aplicații din surse nesigure, care te pot expune unor riscuri cum ar fi: crearea de breșe de securitate, copierea datelor personale, căutarea informațiilor confidențiale (parole, numere de carduri, conturi bancare).